



UNIVERSIDAD  
NACIONAL  
DE LOJA

CIS-UNL



*Facultad de Energía, las Industrias y los Recursos Naturales No Renovables*

---

CARRERA DE INGENIERÍA EN SISTEMAS

# “Análisis de la seguridad de datos en la arquitectura de Software como Servicio (SaaS)”

TESIS PREVIA LA OBTENCIÓN DEL TÍTULO  
DE INGENIERO EN SISTEMAS.

**Autora:**

- Esther Elizabeth Jaramillo Malla

**Director:**

Ing. Roberto Carlos Pineda López, Mg. Sc.

LOJA-ECUADOR

2017

# **CERTIFICACIÓN**

Ing. Roberto Carlos Pineda López, Mg. Sc.

**DOCENTE DE LA CARRERA DE INGENIERÍA EN SISTEMAS, DE LA FACULTAD DE  
ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES  
DE LA UNIVERSIDAD NACIONAL DE LOJA.**

**CERTIFICA:**

Que la Srta. Esther Elizabeth Jaramillo Malla, egresada de la carrera de Ingeniería en Sistemas y cuyo tema versa sobre “**ANÁLISIS DE LA SEGURIDAD DE DATOS EN LA ARQUITECTURA DE SOFTWARE COMO SERVICIO (SaaS)**”, ha sido monitoreado, revisado y orientado bajo mi asesoramiento, con pertinencia y con la rigurosidad científica que el trabajo de investigación debe cumplir, por lo cual autorizo su presentación y sustentación.

Loja, 12 de Mayo de 2017



---

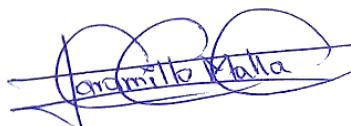
Ing. Roberto Carlos Pineda López, Mg. Sc.  
**Director del Trabajo de Titulación**

## **AUTORÍA**

Yo, **ESTHER ELIZABETH JARAMILLO MALLA**, declaro ser la autora del presente trabajo de titulación y eximo expresamente a la Universidad Nacional de Loja y sus representantes jurídicos de posibles reclamos o acciones legales, por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi trabajo de titulación en el Repositorio Institucional – Biblioteca Virtual.

**Firma:** \_\_\_\_\_

A handwritten signature in blue ink, appearing to read "Jaramillo Malla". It is written over a horizontal line and has a stylized, flowing appearance.

**Cédula:** 1105167199

**Fecha:** 06 de junio de 2017

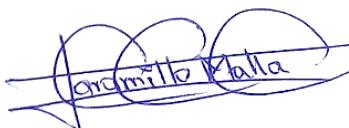
# **CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DE LA AUTORA, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO**

Yo, **ESTHER ELIZABETH JARAMILLO MALLA**, declaro ser autora del trabajo de titulación titulado: “**ANÁLISIS DE LA SEGURIDAD DE DATOS EN LA ARQUITECTURA DE SOFTWARE COMO SERVICIO**”, como requisito para optar al título de: **INGENIERO EN SISTEMAS**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional (RDI):

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con los cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para constancia de esta autorización, en la Ciudad de Loja, a los seis días del mes de junio de dos mil diecisiete.



Firma: \_\_\_\_\_

**Autor:** Esther Elizabeth Jaramillo Malla

**Cédula:** 1105167199

**Dirección:** Loja (Francisco Valdivieso y Bolívar Bailón)

**Correo Electrónico:** eejaramillom@unl.edu.ec

**Teléfono:** 2713076 **Celular:** 0981632988

## **DATOS COMPLEMENTARIOS:**

**Director de Tesis:** Ing. Roberto Carlos Pineda López, Mg. Sc.

**Tribunal de Grado:** Ing. Carlos Miguel Jaramillo Castro, Mg. Sc.

Ing. Jorge Tilio Carrión González, Mg. Sc.

Ing. Marlon Santiago Viñan Ludeña, Mg. Sc.

## **DEDICATORIA**

El presente trabajo de titulación lo dedico principalmente a Dios por brindarme la vida, permitirme que cumpla una de las metas trazadas y por darme fortaleza en los momentos difíciles. De forma muy especial y con todo mi amor a mis padres, quienes me han apoyado incondicionalmente y me han enseñado con su ejemplo a rebasar todas las barreras que la vida nos presenta, a ser mejor cada día, a entender que no hay nada imposible y que sólo hay que esmerarse y sacrificarse, para lograr las metas que se plantea. A mi pequeña hija quien es la personita quien me motiva a seguir adelante y alcanzar todo lo que me he propuesto en la vida, finalmente pero no menos importante a mi hermana quien me ha apoyado en los momentos más difíciles, con la que he podido contar a cada instante.

## **LA AUTORA**

## **AGRADECIMIENTO**

Agradezco primeramente a Dios por haberme acompañado y guiado a lo largo de mi vida y carrera profesional, por ser mi fortaleza en los momentos de debilidad. A mis padres por apoyarme moral y económicamente a lo largo mi vida estudiantil y proporcionarme las herramientas necesarias para cumplir con la meta propuesta, también quiero agradecer de una manera muy especial a mí querida hermana por estar conmigo, apoyarme y alentarme para que no me rinda ante las circunstancias de la vida. A mi director de tesis por haberme guiado y apoyado con sus conocimientos para hacer efectivo el trabajo de titulación.

**LA AUTORA**

# Índice de Contenidos

<b>PORTEADA .....</b>	I
<b>CERTIFICACIÓN .....</b>	II
<b>AUTORÍA .....</b>	III
<b>CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DE LA AUTORA, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.....</b>	IV
<b>DEDICATORIA.....</b>	V
<b>AGRADECIMIENTO .....</b>	VI
<b>1. TÍTULO .....</b>	1
<b>2. RESUMEN .....</b>	2
<b>2.1. SUMMARY.....</b>	3
<b>3. INTRODUCCIÓN.....</b>	4
<b>4. REVISIÓN DE LITERATURA.....</b>	6
<b>4.1. CAPÍTULO I: CONOCIMIENTOS GENERALES SaaS.....</b>	6
4.1.1. Escenarios habituales de SaaS.....	6
4.1.2. Aspectos que ayudaran a saber si su empresa está preparada para SaaS.	7
4.1.2.1. Adaptación al cambio.....	7
4.1.2.2. Seguridad .....	7
4.1.2.3. Control .....	7
4.1.2.4. Arquitectura de la organización .....	8
4.1.2.5. Organización.....	8
4.1.2.6. Confianza.....	8
4.1.3. Pasos para contratar SaaS .....	8
4.1.3.1. Establecer las necesidades a solventar .....	8
4.1.3.2. Buscar un proveedor.....	9
4.1.3.3. Solicitar el servicio .....	9
4.1.4. Ranking proveedores SaaS .....	9
4.1.4.1. Accenture.....	9
4.1.4.2. SalesForce.....	10
4.1.4.3. Workday.....	10

4.1.4.4.	Oracle .....	11
4.1.4.5.	Microsoft .....	11
4.1.4.6.	NetSuite .....	12
4.1.4.7.	Eloqua.....	12
4.1.4.8.	Veeva .....	12
4.1.4.9.	Google Apps .....	13
4.1.5.	Comparativa entre los principales proveedores de SaaS .....	13
4.1.6.	Requisitos técnicos de las aplicaciones SaaS.....	15
4.1.6.1.	Aplicación multi-tenant .....	16
4.1.6.2.	Aplicación escalable y mecanismos de balanceo de carga.....	16
4.1.6.3.	Aplicación personalizable y configurable.....	16
4.1.6.4.	La aplicación debe proveer mecanismos de suscripción, monitoreo, monetización y facturación .....	17
4.1.6.5.	La aplicación debe dar soporte para el aprovisionamiento de recursos .....	17
<b>4.2.</b>	<b>CAPÍTULO II: IMPLEMENTACIÓN DE LA GUÍA MULTIMEDIA .....</b>	<b>18</b>
4.2.1.	Definiciones Generales .....	18
4.2.1.1.	Guía Multimedia.....	18
4.2.1.2.	Redes Bayesianas .....	18
4.2.2.	Herramientas tecnológicas.....	19
4.2.2.1.	Openmarkov .....	19
4.2.2.2.	NetBeans IDE .....	19
4.2.2.3.	Java .....	20
4.2.2.4.	Html5 .....	20
4.2.2.5.	Bootstrap .....	20
4.2.2.6.	Xampp .....	20
4.2.2.7.	Sublime text .....	20
<b>4.3.</b>	<b>CAPÍTULO III: CASOS DE ESTUDIO .....</b>	<b>21</b>
4.3.1.	Aplicación SaaS “Shop-List”.....	21
4.3.1.1.	Capa de aplicación .....	23
4.3.1.2.	Capa de plataforma.....	23
4.3.1.3.	Capa de infraestructura.....	26
4.3.2.	Universidad Nacional de Loja hace uso del DRIVE .....	33
4.3.2.1.	Instalaciones y transferencia de datos .....	33

4.3.2.2.	Retención de datos .....	33
4.3.2.3.	Administración de los Servicios.....	34
4.3.2.4.	Ley de Privacidad y Derechos Educativos de la Familia .....	35
4.3.3.	Universidad Técnica Particular de Loja hace uso de office 365.....	37
4.3.3.1.	Principios clave de privacidad de Microsoft.....	37
4.3.3.2.	¿Qué tipos de datos recopila Microsoft? .....	37
4.3.3.3.	Mecanismos de seguridad de Microsoft para proteger sus datos .....	38
<b>5.</b>	<b>MATERIALES Y MÉTODOS .....</b>	<b>42</b>
5.1.	Materiales .....	42
5.1.1.	Talento Humano .....	42
5.1.2.	Bienes.....	42
5.1.3.	Servicios .....	43
5.1.4.	Financiamiento.....	43
5.2.	Métodos .....	43
5.2.1.	Método deductivo.....	43
5.2.2.	Método Inductivo.....	44
5.2.3.	Método Investigativo .....	44
5.3.	Técnicas .....	44
5.3.1.	Técnica de observación .....	44
5.3.2.	Técnica de entrevista .....	44
5.3.3.	Técnica de procesamiento y análisis de información.....	44
5.4.	Metodología de desarrollo.....	44
5.4.1.	Estado del Arte .....	45
5.4.2.	Guía multimedia .....	45
<b>6.</b>	<b>RESULTADOS .....</b>	<b>46</b>
6.1.	<b>Primer objetivo específico: “Estudiar la arquitectura de servicio SaaS, como modelo tecnológico en la nube” .....</b>	<b>46</b>
6.1.1.	Historia de SaaS .....	46
6.1.2.	Preeminencias de SaaS sobre ASP .....	47
6.1.3.	Definición del modelo SaaS .....	48
6.1.4.	Características de SaaS.....	50
6.1.5.	Estructura de capas SaaS.....	51
a.	Capa de aplicación.....	53
b.	Capa de plataforma.....	54

c. Capa de infraestructura.....	55
6.1.6. Riesgos más destacados .....	56
6.1.7. Oportunidades más destacadas.....	57
6.1.8. Ventajas de SaaS .....	58
6.1.9. Desventajas de SaaS.....	60
6.1.10. Aspectos compartidos entre el Software tradicional y SaaS.....	61
6.1.11. Estimaciones de costos entre el Software tradicional y SaaS .....	62
6.1.12. Factores de SaaS .....	65
6.1.13. Dos vistas de SaaS.....	66
6.1.14. Ciclo de vida de SaaS.....	67
<b>6.2. Segundo objetivo específico: “Investigar acerca de la seguridad de datos en la nube, basándose específicamente en el modelo SaaS”.....</b>	<b>69</b>
6.2.1. Seguridad de datos .....	69
6.2.2. Acuerdo de Nivel de Servicios SLA.....	71
6.2.3. Factores de riesgo en la seguridad de datos en SaaS .....	73
6.2.3.1. Almacenamiento de datos.....	74
6.2.3.2. Control de acceso a los datos .....	76
6.2.3.3. Copia de seguridad y recuperación de datos .....	77
6.2.3.4. Integridad de los datos.....	78
6.2.3.5. Transferencia de datos .....	80
6.2.4. Vulnerabilidades en la seguridad de datos y recomendaciones para mitigar estas vulnerabilidades .....	81
6.2.4.1. Esquema de Base de Datos.....	81
6.2.4.2. Servidor no autorizado .....	83
6.2.4.3. Ataque de fuerza bruta.....	84
6.2.4.4. Manipulación de los datos.....	84
6.2.4.5. Pérdida de identidad de usuario y contraseña.....	85
6.2.4.6. Algoritmo de cifrado de contraseñas débil.....	87
6.2.4.7. Protocolo de seguridad de datos en la red .....	88
6.2.4.8. Aseguramiento por parte del proveedor de SaaS.....	89
6.2.4.9. Técnicas de cifrado .....	90
6.2.4.10. Sistema de almacenamiento .....	91
6.2.5. Cláusulas imprescindibles en un contrato SaaS.....	91
6.2.5.1. Confidencialidad .....	92

6.2.5.2.	Disponibilidad.....	92
6.2.5.3.	Rendimiento.....	92
6.2.5.4.	Seguridad .....	92
6.2.5.5.	Plan de Continuidad de Negocio y Recuperación ante desastres .....	93
6.2.5.6.	Pagos .....	93
6.2.5.7.	Suspensión del servicio .....	93
6.2.5.8.	Servicios de soporte.....	93
6.2.5.9.	Terminación o modificación.....	93
6.2.5.10.	Privacidad y cumplimiento normativo .....	93
<b>6.3.</b>	<b>Tercer objetivo específico: “Producir una guía de análisis acerca de la seguridad en esta arquitectura” .....</b>	<b>94</b>
6.3.1.	Al hacer click en el botón INICIO se presenta un carrusel de imágenes y el siguiente panel de navegación:.....	94
6.3.2.	Al hacer click en el botón DEFINICIÓN se muestra la siguiente información:.....	106
6.3.4.	Al hacer click en el botón RIESGOS se presenta la siguiente información: .....	107
6.3.5.	Al hacer click en el botón VULNERABILIDADES se presenta la siguiente información: .....	109
6.3.6.	Al hacer click en el botón SOLUCIONES se presenta la siguiente información: .....	109
<b>7.</b>	<b>DISCUSIÓN DE RESULTADOS .....</b>	<b>117</b>
7.1.	Desarrollo de la propuesta alternativa .....	117
7.1.1.	Actividades del primer y segundo objetivo específico.....	117
7.1.2.	Resultado del primer objetivo específico .....	118
7.1.3.	Resultado del segundo objetivo específico.....	118
7.1.4.	Actividades del tercer objetivo específico.....	118
7.1.5.	Resultado del tercer objetivo específico .....	119
7.2.	Valoración social, técnica, económica, ambiental.....	124
<b>8.</b>	<b>CONCLUSIONES .....</b>	<b>125</b>
<b>9.</b>	<b>RECOMENDACIONES .....</b>	<b>127</b>
<b>10.</b>	<b>BIBLIOGRAFÍA .....</b>	<b>129</b>
<b>11.</b>	<b>ANEXOS .....</b>	<b>140</b>

Anexo 1: Captura de pantalla de la entrega del Estado del Arte a las Jornadas de Ingeniería de Sistemas Informáticos y de Computación (JISIC)..... 140

Anexo 2: Estado del Arte derivado del entregable del segundo objetivo, documento enviado a las JISIC.....	140
Anexo 3: Solicitud enviada a la Unidad de Telecomunicaciones e Información (UTI). 146	
Anexo 4: Correo proporcionando información solicitada a la UTI.....	147
Anexo 5: Información proporcionada por la UTI.....	148
Anexo 6: Guía para construir Estados del Arte .....	166
Anexo 7: Contratación SaaS con el proveedor Google Apps .....	202

## **Índice de Figuras**

<i>Figura 1 Pirámide de esquematización del trabajo de titulación .....</i>	4
<i>Figura 2 Logo del proveedor SaaS "Accenture".....</i>	9
<i>Figura 3 Logo del proveedor SaaS "SalesForce" .....</i>	10
<i>Figura 4 Logo del proveedor SaaS "Workday" .....</i>	10
<i>Figura 5 Logo del proveedor SaaS "Oracle".....</i>	11
<i>Figura 6 Logo del proveedor SaaS "Microsoft" .....</i>	11
<i>Figura 7 Logo del proveedor SaaS "NetSuite" .....</i>	12
<i>Figura 8 Logo del proveedor SaaS "Eloqua".....</i>	12
<i>Figura 9 Logo del proveedor SaaS "Veeva".....</i>	12
<i>Figura 10 Logo del proveedor SaaS "Google Apps" .....</i>	13
<i>Figura 11 Estructura de capas SaaS para la aplicación Shop-List.....</i>	22
<i>Figura 12 SaaS, PaaS, IaaS .....</i>	49
<i>Figura 13 Definición de SaaS.....</i>	49
<i>Figura 14 Estructura de capas SaaS.....</i>	52
<i>Figura 15 Modelo de costos locales.....</i>	62
<i>Figura 16 Modelo de costos SaaS .....</i>	63
<i>Figura 17 Ciclo de vida de SaaS .....</i>	68
<i>Figura 18 Factor de riesgo "Almacenamiento de datos".....</i>	75
<i>Figura 19 Factor de riesgo "Control de acceso a los datos" .....</i>	77
<i>Figura 20 Factor de riesgo "Control de seguridad y recuperación de datos" .....</i>	78
<i>Figura 21 Factor de riesgo "Integridad de los datos" .....</i>	79
<i>Figura 22 Factor de riesgo "Transferencia de datos" .....</i>	81
<i>Figura 23 Esquemas de base de datos IDII.....</i>	82
<i>Figura 24 Esquemas de base de datos ITSI.....</i>	82
<i>Figura 25 Esquemas de base de datos STSI.....</i>	82
<i>Figura 26 Vulnerabilidad "Servidor no autorizado" .....</i>	83
<i>Figura 27 Vulnerabilidad "Ataque de fuerza bruta" .....</i>	84
<i>Figura 28 Vulnerabilidad "Manipulación de los datos" .....</i>	84
<i>Figura 29 Vulnerabilidad "Pérdida de identidad de usuario y contraseña" .....</i>	85
<i>Figura 30 Vulnerabilidad "Algoritmo de cifrado de contraseñas débil" .....</i>	87
<i>Figura 31 Vulnerabilidad "Protocolo de seguridad de datos en la red" .....</i>	88

<i>Figura 32 Menú principal de navegación.....</i>	94
<i>Figura 33 Imagen inicial de la guía .....</i>	94
<i>Figura 34 Panel de navegación de la pestaña INICIO.....</i>	95
<i>Figura 35 Primer ícono del panel de navegación de la pestaña INICIO .....</i>	96
<i>Figura 36 Primera pantalla del simulador.....</i>	97
<i>Figura 37 Mensaje presentado al usuario al elegir la opción NO.....</i>	97
<i>Figura 38 Segunda pantalla del simulador.....</i>	98
<i>Figura 39 Tercera pantalla del simulador.....</i>	101
<i>Figura 40 Pantalla en la que se muestra el resultado.....</i>	104
<i>Figura 41 Segundo ícono del panel de navegación de la pestaña INICIO .....</i>	104
<i>Figura 42 Tercer ícono del panel de navegación de la pestaña INICIO .....</i>	105
<i>Figura 43 Cuarto ícono del panel de navegación de la pestaña INICIO .....</i>	105
<i>Figura 44 Definición de SaaS.....</i>	106
<i>Figura 45 Imagen Acuerdo de Nivel de Servicio.....</i>	106
<i>Figura 46 Información Acuerdo de Nivel de Servicio .....</i>	107
<i>Figura 47 Factores de riesgo en SaaS.....</i>	108
<i>Figura 48 Imagen de las vulnerabilidades en SaaS.....</i>	109
<i>Figura 49 Información de vulnerabilidades en SaaS.....</i>	109
<i>Figura 50 Soluciones planteadas para mitigar las vulnerabilidades .....</i>	114
<i>Figura 51 Tipo de contrato.....</i>	115
<i>Figura 52 Cláusulas imprescindibles en un contrato.....</i>	116
<i>Figura 53 Red Bayesiana utilizada para el simulador.....</i>	122
<i>Figura 54 Peso de cada variable establecido de acuerdo a la probabilidad de ocurrencia .....</i>	123

## Índice de Tablas

<i>Tabla 1 Comparativa de las medidas de seguridad proveedores SaaS .....</i>	14
<i>Tabla 2 Riesgos de seguridad de la aplicación Shop-List.....</i>	27
<i>Tabla 3 Costo del talento humano empleado en el trabajo de titulación .....</i>	42
<i>Tabla 4 Costo de los bienes físicos empleados en el trabajo de titulación.....</i>	42
<i>Tabla 5 Costo de los servicios empleados en el trabajo de titulación .....</i>	43
<i>Tabla 6 Costo totales empleados en el trabajo de titulación.....</i>	43
<i>Tabla 7 Aspectos compartidos entre el Software tradicional y SaaS .....</i>	61
<i>Tabla 8. Estimaciones de costos iniciales.....</i>	63
<i>Tabla 9. Estimaciones de costos anuales.....</i>	64
<i>Tabla 10 Requisitos no funcionales de SaaS.....</i>	66
<i>Tabla 11 Riesgos en la seguridad de datos SaaS.....</i>	70
<i>Tabla 12 Riesgos de seguridad establecidos en SLA.....</i>	72
<i>Tabla 13 Cláusulas imprescindibles en el contrato SaaS.....</i>	92
<i>Tabla 14 Botones comunes en el simulador.....</i>	96
<i>Tabla 15 Actividades del primer y segundo objetivo específicos .....</i>	117
<i>Tabla 16 Actividades del tercer objetivo específico.....</i>	119

## **1. TÍTULO**

**“ANÁLISIS DE LA SEGURIDAD DE DATOS EN LA ARQUITECTURA DE  
SOFTWARE COMO SERVICIO (SAAS)”**

## **2. RESUMEN**

El presente trabajo de titulación se basa en el análisis de la seguridad de datos de la arquitectura SaaS de cloud computing, se realiza con la finalidad de que las organizaciones tengan una base para realizar un análisis previo al proveedor de servicios que deseen contratar, se ha evidenciado la necesidad de contar con una guía de análisis de la seguridad de datos que nos ofrece este modelo, ya que las instituciones hacen uso de este servicios estrictamente por una necesidad dejando rezagado el tema de seguridad, el mismo es un factor sumamente importante para cualquier empresa ya que los datos son un activo transcendental para la perpetuidad y continuidad de las funciones de una organización.

El espionaje corporativo ha tomado fuerza los últimos años con la inmersión de la tecnología, este problema se agudiza con la utilización de los servicios en la nube debido a que los datos transitan por diferentes localidades del mundo, desconociendo las políticas de seguridad de datos que son aplicables en cada país quedando así nuestros datos a disposición de los dueños de los centros donde se almacenan, este tipo de vulnerabilidades en la arquitectura SaaS son explotadas por los intrusos para obtener información que pueda llevar a la competencia a la quiebra, aun así las instituciones que hacen uso de este modelo no toman en cuenta los contratos y políticas que deberían ser entregados por los proveedores para llegar a un acuerdo consensual con el cliente; los clientes deben velar por la seguridad de la información ya que este es el activo más importante de toda entidad, y es susceptible a robo, pérdida, modificaciones, constituyéndose como un activo demasiado vulnerable, por tal razón se debería realizar un previo análisis a los términos de seguridad de los datos que les ofrece el proveedor para que sean difundidos en la nube.

## **2.1. SUMMARY**

The present work of titration is based on the data security analysis of the SaaS architecture of cloud computing, is done in order that organizations with a basis to perform a prior analysis to the service provider who wish to contract, has been Evidenced the need to have a guide to data security analysis that do not offer this model, since institutions make use of this service strictly by a necessity leaving behind the security issue, it is a highly important factor for any Company as the data is a transcendental asset for the perpetuity and continuity of the functions of an organization.

Corporate espionage has become stronger in recent years with the immersion of technology. This problem is exacerbated by the use of cloud services because data travels around the world, ignoring the security policies of the data that The son Applicable in each country thus leaving our data a disposition of the owners of the centers where it is stored, this type of vulnerabilities in the SaaS architecture are exploited by intruders to obtain information that can lead to competition to bankruptcy, as well To the institutions that make use of this model and do not take into account the contracts and the policies that must be delivered by the suppliers to arrive at a consensual agreement with the client; Customers must have information security and that is the most important asset of the whole entity, and is susceptible to theft, loss, modifications, constituting itself as an asset too vulnerable, for that reason The security terms of the data that they offer The provider to be broadcast in the cloud.

### **3. INTRODUCCIÓN**

Software como Servicio proporcionan agilidad y eficacia para adquirir nuevos servicios de forma instantánea, sin embargo la utilización de SaaS conlleva un conjunto de problemas de seguridad tales como: datos mezclados en entornos compartidos, abuso de usuario con privilegios, eliminación y filtración de datos, localizaciones geográficas, respaldo de los datos, en fin múltiples riesgos a los que está expuesta la información.

Afortunadamente, los expertos concuerdan que el cifrado es el control de unificación de seguridad en SaaS, lo que le permite proteger, controlar y cumplir con los servicios.

En la siguiente figura se presenta como está esquematizado el trabajo de titulación:



*Figura 1 Pirámide de esquematización del trabajo de titulación*

Siendo la base para el desarrollo la revisión literaria ya que estos son los fundamentos teóricos del trabajo realizado.

Posteriormente se hace constar los materiales y métodos utilizados para efectuar la investigación, dentro de los materiales se presenta el talento humano, bienes, servicios

y financiamiento; en lo concerniente a los métodos se hace constar el método deductivo, inductivo e investigativo; referente a las técnicas utilizadas se muestra la técnica de observación, entrevista, procesamiento y análisis de información; seguidamente se hace constar la metodología de desarrollo utilizada, la cual está compuesta por: estado del arte y guía multimedia; para la construcción del estado del arte se realizó las consultas en bases de datos científicas y revistas indexadas, consiguiendo así que la información presentada sea de calidad y verificable.

Consecutivamente se presentan los resultados alcanzados en cada objetivo. Primer objetivo específico: “Estudiar la arquitectura de servicio SaaS, como modelo tecnológico en la nube”, del cual se obtuvo como resultado un estado del arte de información estructurada para conocer la arquitectura. Segundo objetivo específico: “Investigar acerca de la seguridad de datos en la nube, basándose específicamente en el modelo SaaS”, de este se obtuvo como entregable un estado del arte de información sobre la seguridad de datos en SaaS. Tercer objetivo específico: “Producir una guía de análisis acerca de la seguridad en esta arquitectura”, se obtuvo como resultado una guía multimedia en la que se presenta información sobre SaaS y la seguridad de datos en esta arquitectura, además se ofrece un simulador para calcular la confiabilidad del proveedor de estos servicios, para calcular la confiabilidad se hizo uso de redes bayesianas.

Seguidamente se muestra la discusión de resultados, en este apartado se presenta las actividades sistemáticas que se siguió para obtener resultados en cada objetivo; tanto el primer como segundo objetivo se han efectuado bajo la mismas actividades debido a que se ha seguido los pasos para realizar una investigación.

A continuación de este apartado se presenta las conclusiones y recomendaciones a las que se llegó en base a los hallazgos encontrados en la investigación.

## **4. REVISIÓN DE LITERATURA**

### **4.1. CAPÍTULO I: CONOCIMIENTOS GENERALES SaaS**

#### **4.1.1. Escenarios habituales de SaaS**

Software como Servicio (SaaS), es un modelo de distribución de software en el que tanto el software como los datos manejados son centralizados y alojados en un servidor externo a la empresa. Esto implica que el software utilizado por la empresa no se encuentra en la misma, sino que un proveedor se ocupa del hosting de dicho software en la nube, así como del mantenimiento y el soporte.

La empresa contratante accede al software y todos sus datos a través de un navegador web desde cualquier ordenador. Eso quiere decir que toda la información, procesos, resultados, etc. almacenados en este software son de fácil acceso desde cualquier lugar. Tanto el software como los datos están centralizados y hospedados en el servidor del almacenamiento del proveedor [1] [2].

Si se ha utilizado un servicio de correo electrónico basado en web, como Outlook, Hotmail o Yahoo! Mail, entonces ya ha usado una forma de SaaS. Con estos servicios, usted inicia sesión en su cuenta a través de Internet, a menudo desde un explorador web.

El software de correo electrónico se encuentra en la red del proveedor de servicios, donde también se almacenan los mensajes. Puede obtener acceso a su correo electrónico y a los mensajes almacenados desde un explorador web en cualquier equipo o dispositivo conectado a Internet, estos son ejemplos de servicios gratuitos para uso personal.

Para el uso en una organización, puede alquilar aplicaciones de productividad, como correo electrónico, colaboración y calendario y aplicaciones empresariales sofisticadas, como: CRM (Gestión de relaciones con los clientes) es un término de la industria de la información que se aplica a metodologías, software y, en general, a las capacidades de Internet que ayudan a una empresa a gestionar las relaciones con sus clientes de una manera organizada [3]; ERP (Planificación de Recursos Empresariales) es un conjunto

de sistemas de información que permite la integración de ciertas operaciones de una empresa, especialmente las que tienen que ver con la producción, la logística, el inventario, los envíos y la contabilidad [4]; y administración de documentos. Usted paga por el uso que hace de estas aplicaciones a través de una suscripción o conforme al nivel de uso [5].

#### **4.1.2. Aspectos que ayudaran a saber si su empresa está preparada para SaaS**

Actualmente el mundo de los sistemas informáticos empresariales está experimentando una verdadera revolución, es por ello que se debe evaluar si nuestra empresa está apta para adoptar nuevos cambios.

##### **4.1.2.1. Adaptación al cambio**

Si su empresa tiene una escasa capacidad de adaptación al cambio, llevar sus procesos empresariales a la nube puede considerarse ir de 0 a 100 en poco tiempo.

No todas las compañías o empleados están preparados para afrontar un cambio en su forma de entender el día a día de los procesos de la empresa. En ese caso, pueden plantearse cambios pequeños, estableciendo aplicaciones en la nube que no supongan una integración drástica.

##### **4.1.2.2. Seguridad**

Este aspecto es uno de los temas más controvertidos. Certificar la seguridad de algo intangible supone todo un reto, pero una vez conseguido, el problema se traslada hasta convencer al mercado de que dicha seguridad es real.

Aspectos como la viabilidad de proveedor o la pérdida de control físico sobre los datos y aplicaciones son clave para asimilar la integración de la nube en cualquier empresa. Si su compañía no termina de fiarse de este nuevo servicio, nunca explotará al máximo las posibilidades que ofrece y experimentará un desembolso económico que tardará más tiempo en recuperar.

##### **4.1.2.3. Control**

En el momento en el que los procesos empresariales pasan a formar parte de la nube, la compañía pierde el control sobre los cambios, el mantenimiento y las actualizaciones. Cada organización debe tener muy claro que no tiene poder de decisión en lo que a las

actualizaciones se refiere. Con un SaaS el proveedor ofrece el servicio total, incluyendo mantenimiento y mejoras en el sistema.

#### **4.1.2.4. Arquitectura de la organización**

Las funcionalidades en la nube no requieren mucha inversión en hardware, sin embargo, para poder explotar el potencial que la nube puede aportar a su empresa, una buena conectividad a internet es básica. Antes de plantearse este tipo de soluciones debe realizarse un análisis de la compañía con el propósito de estudiar la viabilidad del sistema que se busca implantar.

#### **4.1.2.5. Organización**

Las compañías muy centradas en características on-premise, este término se refiere a las soluciones locales, es decir aquellas que se despliegan de la manera tradicional; los servidores son adquiridos, los sistemas operativos están instalados dentro de su centro de datos [6], con grandes departamentos de TIC y acostumbradas a llevar el mantenimiento y problemas de los servidores de la empresa, experimentarán un cambio drástico que en algunos casos incluirá incluso la reestructuración del departamento. Si la elección de la empresa es contratar un SaaS, el departamento de sistemas deberá centrarse principalmente en la formación del personal, ya que el resto corre a cargo del proveedor.

#### **4.1.2.6. Confianza**

Cualquier proveedor de SaaS ofrece hoy en día un 99% de eficiencia, en lo que a posibilidad de acceso se refiere. Sin embargo, se pueden encontrar momentos en los que el sistema se “caiga” y el departamento de sistemas no pueda hacer nada por solucionarlo, esto ocasiona que la empresa pierda dinero, pero esperar es lo único efectivo en este tipo de escenarios [7] .

### **4.1.3. Pasos para contratar SaaS**

Se requiere de unos pocos pasos para hacer uso de SaaS, a continuación se detalla cada uno de ellos:

#### **4.1.3.1. Establecer las necesidades a solventar**

Al instituir las necesidades que va a solventar la empresa haciendo uso de SaaS, se debe tomar en cuenta el tipo de datos que se va a procesar.

#### **4.1.3.2. Buscar un proveedor**

Se debe buscar un proveedor que se adapte a las necesidades de la empresa y que tenga experiencia en la implantación de Software como Servicio.

#### **4.1.3.3. Solicitar el servicio**

Se debe completar una serie de formularios, en los que solicitan información de la empresa contratante. En el Anexo 7 se muestra un ejemplo de la contratación SaaS con el proveedor Google Apps, cabe mencionar que los formularios que se llenaron son correspondientes a una prueba free.

### **4.1.4. Ranking proveedores SaaS**

Un proveedor SaaS es una empresa que proporciona un modelo de distribución de software en el que tanto el software como los datos manejados son centralizados y alojados en un único servidor externo a la empresa cliente, para que ésta pueda explotarlos en su actividad económica [8] [9].

A continuación se cita a los principales proveedores SaaS:

#### **4.1.4.1. Accenture**



*Figura 2 Logo del proveedor SaaS "Accenture"*

Durante los últimos cinco años, Accenture ha llevado a cabo implementaciones de SaaS complejas a gran escala, basándose en una experiencia en integración de sistemas y gestión de datos que supera los treinta años.

La suite Accenture SaaS Business Solutions es un enfoque interactivo de desarrollo de tecnologías SaaS y en la nube, proporciona a los clientes los métodos y las herramientas necesarias para facilitar soluciones SaaS a terceros.

Accenture cuenta con amplia experiencia en la implementación de soluciones SaaS y en la integración de sistemas de gestión de relaciones con los clientes [10].

#### **4.1.4.2. SalesForce**



*Figura 3 Logo del proveedor SaaS "SalesForce"*

Este es un gigante de SaaS, debido a su historial de éxitos en la nube. Con su base de clientes que asciende a más de 200.000 clientes, y su tienda de aplicaciones incluye más de 1.400 soluciones.

Ayuda a los clientes en la utilización de las tecnologías y servicios SaaS y de cloud computing con el fin de transformar la empresa y así lograr una implementación de aplicaciones más rápida, mayor flexibilidad y una disminución del coste total [11] [12] [13] [14] [10].

#### **4.1.4.3. Workday**



*Figura 4 Logo del proveedor SaaS "Workday"*

Ofrece en la actualidad servicios de gestión de capital humano en la nube que pueden analizar los gastos de la mano de obra y gestionar el proceso de pago de personal.

Ayuda a las organizaciones a mejorar el rendimiento de sus inversiones y el rendimiento general del negocio por medio de soluciones punteras de gestión financiera y de recursos humanos. Sus innovadoras soluciones basadas en SaaS pueden ayudar a los clientes a obtener valor con mayor rapidez [13] [14] [10].

#### **4.1.4.4. Oracle**



*Figura 5 Logo del proveedor SaaS "Oracle"*

Oracle ofrece soluciones de CRM escalables bajo demanda y a través de suscripción que permiten a los clientes aprovechar y personalizar diferentes servicios con una tarifa mensual por usuario, y al mismo tiempo gestionar y proteger de manera eficiente la información de la empresa. El software bajo pedido gestiona toda la plataforma de Oracle, la cual incluye base de datos, middleware y aplicaciones, con un total de más de 360 soluciones. También bajo demanda, con la ventaja de que la responsabilidad corresponde a un solo proveedor, ofrece opciones de implementación SaaS flexibles en servidores compartidos con otras empresas, en servidores para una única empresa o “en el cliente”, lo cual permite personalizar los servicios basándose en las necesidades de cada compañía [10] [15].

#### **4.1.4.5. Microsoft**



*Figura 6 Logo del proveedor SaaS "Microsoft"*

Está comprometido con el desarrollo de soluciones de cloud computing mediante la Plataforma Windows Azure en busca de la mejora del rendimiento y de la reducción de costes. Microsoft ofrece a sus clientes la exclusiva combinación de visión y tecnologías SaaS, es una nube líder en el mercado.

Además ofrece una Dinámica de Gestión de Relaciones con los Clientes (CRM) como una solución SaaS corporativa mediante los Servicios on-line de Avanade, un negocio nuevo que centrado en ayudar a las organizaciones [12] [10].

#### **4.1.4.6. NetSuite**



*Figura 7 Logo del proveedor SaaS "NetSuite"*

Es un líder indiscutible en los segmentos de contabilidad y ERP del mercado de SaaS. Siguió el modelo de Salesforce.com en la construcción de su mercado de aplicaciones SuiteApp.com en torno a su oferta principal. Pero la compañía también ha establecido varias asociaciones clave dentro de su programa SuiteCloud, incluyendo a Google Apps, Salesforce.com, SAP y Oracle, para proporcionar una integración completa entre el on-premise y las aplicaciones en la nube [13] [14].

#### **4.1.4.7. Eloqua**



*Figura 8 Logo del proveedor SaaS "Eloqua"*

Colabora con los clientes para proporcionar valor más rápido, al facilitar soluciones basadas en SaaS para la gestión de las relaciones con los clientes, la generación de demanda, la automatización del marketing y la gestión de oportunidades. El software bajo pedido de Eloqua permite a los directivos rastrear el éxito de las campañas, la calidad y el flujo de oportunidades, y hacer el seguimiento de las necesidades futuras de sus ventas [10].

#### **4.1.4.8. Veeva**



*Figura 9 Logo del proveedor SaaS "Veeva"*

Desarrolla soluciones de gestión de las relaciones con los clientes basadas en SaaS y utilizadas en Force.com para el sector internacional de las ciencias biológicas. Estas soluciones ofrecen aplicaciones de gestión de relaciones con los clientes completamente funcionales que resultan flexibles, fáciles de implementar, operativamente económicas y que proporcionan una experiencia del usuario superior [10].

#### **4.1.4.9. Google Apps**



*Figura 10 Logo del proveedor SaaS "Google Apps"*

Todo lo que necesita para optimizar su trabajo, en un solo paquete que funciona a la perfección desde su computadora, teléfono o tablet [11] [12].

#### **4.1.5. Comparativa entre los principales proveedores de SaaS**

Se realizará un cuadro comparativo de las medidas de seguridad adoptadas por los proveedores de Software como Servicio, cabe mencionar que se realizará la comparación entre los proveedores que tengan disponibles al público sus contratos.

En la parte inferior de la tabla comparativa se muestra la descripción de los códigos que se utilizan para denominar a cada medida de seguridad.

*Tabla 1 Comparativa de las medidas de seguridad proveedores SaaS*

Proveedor	Medida de Seguridad																			
	EXPERIENCIA (años)				TIPO DE CONTRATO		CLAUSULAS										SLA			
	0-2	3-5	6-10	Más	Adhesión	Negociado	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	B1	B2	B3	B4
Accenture				X	X		X	X	X	X	X	X	X	X	X					
SalesForce					X			X	X	X	X	X	X	X	X	X	X	X		
Workday					X				X		X			X						
Oracle				X	X			X	X	X	X	X	X			X			X	X
Microsoft				X	X				X	X			X	X	X	X	X	X		X
Eloqua					X			X	X	X	X	X	X	X		X			X	X
Google Apps				X	X			X	X				X		X	X	X			

Proveedor	Medida de Seguridad																			
	CUESTIONAMIENTOS ADICIONALES									BASE DE DATOS			PROTOCOLO DE TRANSFERENCIA DE DATOS							
	C1	C2	C3	C4	C5	C6	C7	C8	C9	STSI	ITSI	IDII	HTTP	HTTPS	TLS	SSH				
Accenture	X	X	X	X	X		X		X							X	X	X		X
SalesForce	X	X	X		X		X									X	X	X		X
Workday	X	X					X									X	X	X		
Oracle	X	X		X	X		X									X	X	X		X
Microsoft	X	X	X		X		X									X	X	X		X
Eloqua	X	X					X									X	X	X		X
Google Apps	X	X	X	X	X		X		X							X	X	X		X

## **CLAUSULAS IMPRESCINDIBLES EN UN CONTRATO SaaS**

Plan de Continuidad	=>	A1
Confidencialidad	=>	A2
Rendimiento	=>	A3
Servicio de Soporte	=>	A4
Privacidad y cumplimiento normativo	=>	A5
Terminación o modificación	=>	A6
Disponibilidad	=>	A7
Suspensión del servicio	=>	A8
Seguridad	=>	A9
Pagos	=>	A10

## **FATORES A TRATAR EN EL ACUERDO DE NIVEL DE SERVICIO (SLA)**

Recuperación de los datos	=>	B1
Viabilidad a largo plazo	=>	B2
Acceso de usuarios privilegiados	=>	B3
Ubicación de los datos	=>	B4

## **CUESTIONAMIENTOS ADICIONALES DE SEGURIDAD**

Requerimiento de contraseña	=>	C1
Certificado SSL	=>	C2
MAC (código de autenticación de mensajes)	=>	C3
Lista Blanca de URL	=>	C4
SSO (inicio de sesión único)	=>	C5
Restringir el número de intentos	=>	C6
Datos Cifrados	=>	C7
Pregunta de Seguridad	=>	C8
OTP (contraseña de un solo uso)	=>	C9

### **4.1.6. Requisitos técnicos de las aplicaciones SaaS**

Para que el proveedor construya una solución SaaS, implica considerar ciertos requisitos técnicos, que ayudarán a cumplir las características principales de una solución SaaS.

A continuación se enumeran dichos requisitos.

#### **4.1.6.1. Aplicación multi-tenant**

El concepto de multi-tenant o multi-cliente refiere a un principio de arquitectura de software en donde una única instancia de un producto de software corre en un servidor, atendiendo a múltiples organizaciones o clientes. Cada cliente u organización dentro de la misma instancia de la aplicación tiene su propio ambiente o partición, es decir, puede personalizar la aplicación definiendo sus propios usuarios, mecanismos de seguridad, parámetros y configuraciones visuales sin interferir a las otras organizaciones y de forma totalmente transparente. El objetivo primario de la arquitectura multi-tenant es maximizar recursos de hardware y de software.

La arquitectura multi-tenant se opone de alguna forma a la arquitectura multi instancia, en donde para cada cliente u organización se necesita instalar una nueva instancia de la aplicación con sus respectivos recursos de hardware y software dedicados para cada organización.

El middleware de una plataforma como servicio es esencialmente multi-tenant, ya que un desarrollador, o una organización con muchos desarrolladores, utiliza el middleware de la plataforma de forma aislada y transparente de otras organizaciones o desarrolladores.

#### **4.1.6.2. Aplicación escalable y mecanismos de balanceo de carga**

Las aplicaciones SaaS deben estar preparadas para soportar una gran cantidad de clientes. En aplicaciones single-tenant la escalabilidad se logra instalando un nuevo servidor web con la misma aplicación y balanceando la carga. Eso para soluciones multitenant es una solución de grano grueso, por lo que es necesario definir mecanismos de escalabilidad que contemplen el uso de recursos por tenant y la posibilidad de asignar recursos de grano fino.

#### **4.1.6.3. Aplicación personalizable y configurable**

Cada cliente que se suscribe al servicio, utiliza la aplicación como si fuera el único cliente de la misma, por lo que la aplicación necesita diseñarse de tal forma que permita a cada cliente personalizarla según sus necesidades sin interferir a los otros clientes.

#### **4.1.6.4. La aplicación debe proveer mecanismos de suscripción, monitoreo, monetización y facturación**

El modelo de pago por uso implica que en la aplicación se tenga que diseñar específicamente los mecanismos de suscripción, monetización y facturación, por lo que se necesita monitorear constantemente el uso que cada tenant le da a la misma.

Es prioritario ofrecer al cliente una buena variedad de precios, y que el cliente sepa exactamente qué se le está cobrando.

#### **4.1.6.5. La aplicación debe dar soporte para el aprovisionamiento de recursos**

Debido al modelo de suscripción dinámico de las aplicaciones SaaS deben estar preparadas para reservar y dedicar recursos a cada nuevo suscriptor. Además cuando la cantidad de suscriptores es muy grande se hace inviable que las tareas de aprovisionamiento se realicen de forma manual, y es necesario tener un proceso automático [12].

## **4.2. CAPÍTULO II: IMPLEMENTACIÓN DE LA GUÍA MULTIMEDIA**

### **4.2.1. Definiciones Generales**

A continuación se define cada uno de los elementos utilizados para implementar la guía multimedia.

#### **4.2.1.1. Guía Multimedia**

La guía multimedia es un dispositivo que mejora las prestaciones de las tradicionales guías, transmitiendo la información sobre la exposición en diversos formatos texto, imagen, vídeo y audio [13].

#### **4.2.1.2. Redes Bayesianas**

##### **Definición**

Las redes bayesianas son una representación gráfica de dependencias para razonamiento probabilístico, en la cual los nodos representan variables aleatorias y los arcos representan relaciones de dependencia directa entre las variables [14].

##### **Elementos de una Red Bayesiana**

Una red bayesiana es un grafo dirigido acíclico que consta de:

- Un conjunto de nodos, uno por cada variable aleatoria del “mundo”.
- Un conjunto de arcos dirigidos que conectan los nodos; si hay un arco de X a Y decimos que X es un parente de Y ( $\text{padres}(X)$  denota el conjunto de variables que son padres de X).
- Cada nodo  $X_i$  contiene la distribución de probabilidad condicional  $P(X_i | \text{padres}(X_i))$  [15].

##### **Teorema de Bayes**

La interpretación más aceptada del teorema de Bayes, es que su estructura permite el cálculo de probabilidades después de haber sido realizado un experimento, basándose en el conocimiento de la ocurrencia de ciertos eventos que dependan del evento estudiado, o sea, se parte de probabilidades conocidas antes de efectuar el experimento, las cuales son afectadas por las probabilidades propias del experimento [16]. La probabilidad condicional de  $A_i$  dado  $B$ , para cualquier  $i$ , es:

$$P(A_i | B) = \frac{P(A_i) P(B | A_i)}{\sum_{i=1}^n P(A_i) P(B | A_i)}$$

*Ecuación 1. Fórmula del Teorema de Bayes*

### Inferencia en Redes Bayesianas

Se pretende hallar la distribución de probabilidad de determinadas variables de interés dados los valores de otras variables que se observan [17].

#### 4.2.2. Herramientas tecnológicas

A continuación se define cada uno de las herramientas utilizadas para implementar la guía multimedia.

##### 4.2.2.1. Openmarkov

OpenMarkov es una herramienta de software de código abierto para modelos gráficos probabilistas (MGPs), desarrollada en el Centro de Investigación sobre Sistemas Inteligentes de Apoyo a la Decisión (CISIAD) de la Universidad Nacional de Educación a Distancia (UNED), en Madrid [18].

Está diseñada para:

- Editar y evaluar varios tipos de MGPs, tales como redes bayesianas, diagramas de influencia, modelos de Markov factorizados, etc.
- Aprender redes bayesianas a partir de bases de datos de forma interactiva.
- Análisis de coste-efectividad [19].

##### 4.2.2.2. NetBeans IDE

NetBeans IDE le permite desarrollar rápida y fácilmente aplicaciones de escritorio, móviles y web Java, así como aplicaciones HTML5 con HTML, JavaScript y CSS. El IDE también proporciona un gran conjunto de herramientas para desarrolladores de PHP y C / C ++. Es gratuito y de código abierto y tiene una gran comunidad de usuarios y desarrolladores de todo el mundo [20].

#### **4.2.2.3. Java**

Java es un lenguaje de programación orientado a objetos que se popularizó a partir del lanzamiento de su primera versión comercial de amplia difusión, la JDK 1.0 en 1996. Actualmente es uno de los lenguajes más usados para la programación en todo el mundo [21].

#### **4.2.2.4. Html5**

HTML5 (Hyper Text Markup Language) es un lenguaje markup usado para estructurar y presentar el contenido para la web.

Como su nombre lo indica es la quinta revisión del estándar HTML y permite soportar lo último en multimedia, agrega elementos como video, audio y canvas, como así también integración para gráficos vectoriales (SVG) y MathML para fórmulas matemáticas [22][23].

#### **4.2.2.5. Bootstrap**

Bootstrap es un framework de css, en otras palabras es un conjunto de archivos CSS que se incluye en una página y se empieza a maquetar el sitio web en minutos, sin tocar una sola línea de CSS [24].

#### **4.2.2.6. Xampp**

XAMPP es el entorno más popular de desarrollo con PHP, es una distribución de Apache completamente gratuita y fácil de instalar que contiene MariaDB, PHP y Perl. El paquete de instalación de XAMPP ha sido diseñado para ser increíblemente fácil de instalar y usar [25].

#### **4.2.2.7. Sublime text**

Sublime Text es un sofisticado editor de texto para código, marcado y prosa.

Le encantará la interfaz de usuario elegante, características extraordinarias y un rendimiento increíble [26].

## **4.3. CAPÍTULO III: CASOS DE ESTUDIO**

### **4.3.1. Aplicación SaaS “Shop-List”**

El presente caso de estudio es el producto del trabajo de titulación para obtener el título de ingeniero en sistemas, desarrollado en la Universidad Nacional de Loja, esta aplicación se basa en el análisis y desarrollo de una aplicación móvil para la localización de productos y el control de compras en los supermercados, con la finalidad de brindar a sus clientes una nueva experiencia al momento de adquirirlos, de una manera más ordenada y eficiente, con información actualizada de los mismos, acorde a las actuales tendencias tecnológicas y aprovechando las ventajas que brinda las tecnologías móviles en la actualidad, tales como portabilidad y facilidad de acceso a la información en cualquier lugar y momento [27].

En la figura que se presenta a continuación, se especifica el flujo de trabajo de Shop-List, la cual hace uso de las tres capas que componen SaaS, en la capa de aplicación se podría hacer referencia a la interfaz que facilita la interacción del usuario con la aplicación, en la capa de plataforma, Shop-List hace uso de OpenShift para la asignación de recursos y la programación en sí, y finalmente OpenShift hace uso de los servidores de Amazon para dar respuesta a las peticiones de los usuarios.

A breves rasgos se ha mencionado cómo se realiza la interacción para acceder a los servicios de la aplicación en estudio, más adelante se proporcionará información detallada de cómo se realiza el trabajo en cada capa.

Como es de conocimiento el flujo de trabajo de SaaS empieza con la petición del usuario, para que se proporcione una respuesta, este proceso consiste en una serie de pasos los cuales están alojados en capas, después de la figura se muestra cómo interactúan para brindar servicios en Shop-List.

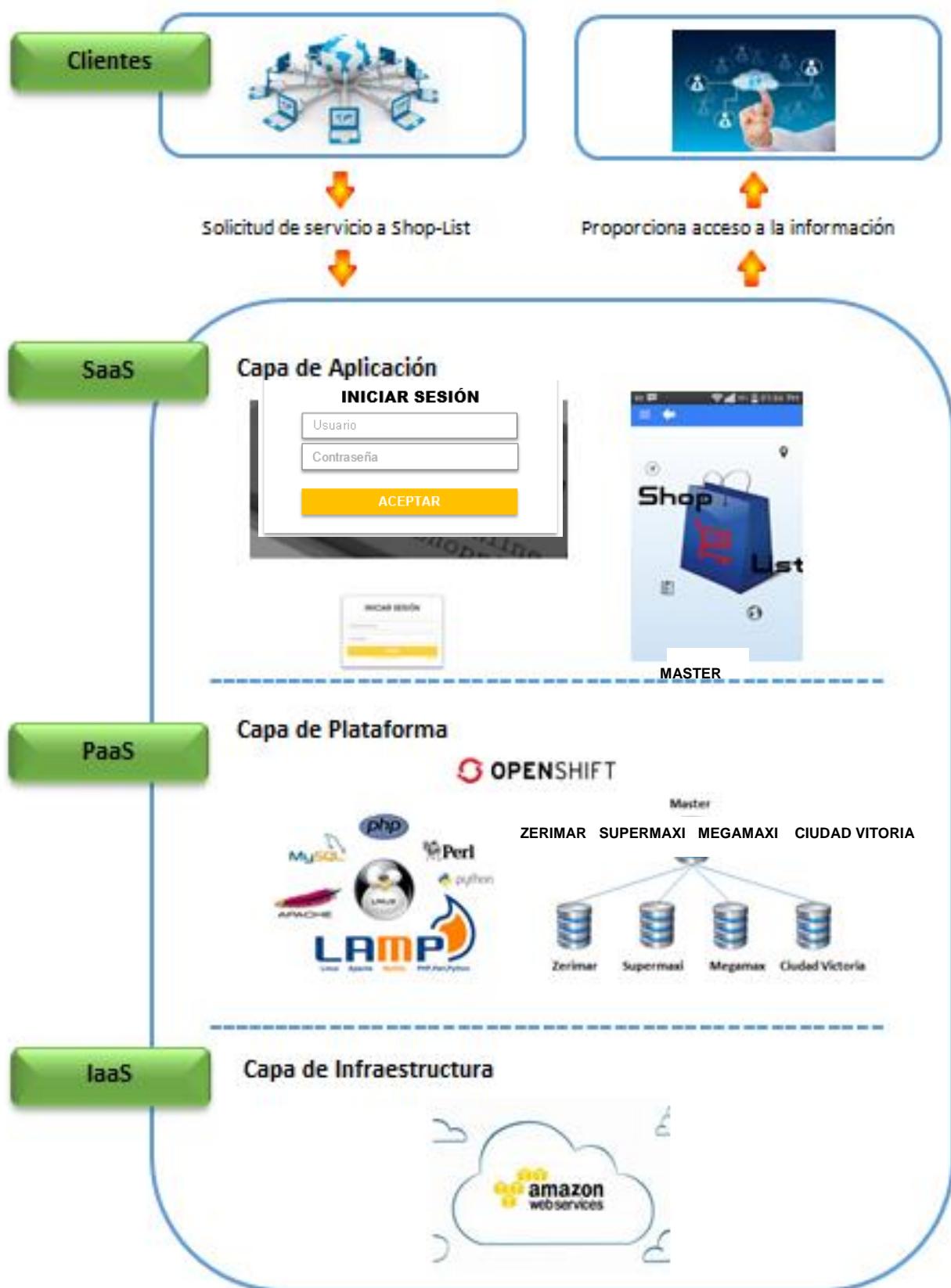


Figura 11 Estructura de capas SaaS para la aplicación Shop-List

#### **4.3.1.1. Capa de aplicación**

La aplicación Shop-List, propiamente dicha la aplicación como tal es SaaS, en esta capa ofrece la personalización de tres partes lógicamente divididas, servicio, proceso e interfaz de usuario.

A continuación se especifica cómo se brinda a los administradores de los supermercados el servicio de personalización, en cada uno de los elementos lógicos de esta.

**Módulo de Servicio:** consta de un módulo lógico general, el cual es responsable de la ejecución de la lógica de negocio por defecto para todos los inquilinos, mientras que el módulo lógico extendido está a cargo de la implementación de la lógica de negocio personalizado, esta es la que permite a los administradores de los supermercados adecuar la aplicación de acuerdo a los servicios que estén ofertando, se puede agregar o quitar servicios, los cuales se ven reflejados en la aplicación móvil de los consumidores.

**Módulo de proceso:** haciendo referencia a lo mencionado anteriormente se puede evidenciar que en el software desarrollado utiliza la orquestación de servicios Web, ya que lleva a cabo la disposición y la personalización de los procesos, es decir solo se ejecuta los servicios invocados por el usuario.

**Módulo de interfaz de usuario:** esta parte proporciona una interfaz de procesos en la cual permite realizar la personalización para transformar el formulario por defecto a un formulario que describe la lógica de negocio del supermercado, es el módulo que permite que los servicios invocados se vean reflejados en opciones de la aplicación para el usuario consumidor.

#### **4.3.1.2. Capa de plataforma**

En la capa de aplicación Shop-List hace uso de OpenShift de Red Hat este permite desarrollar, presentar y ajustar Aplicaciones en la Nube, ofreciendo una variedad de lenguajes de programación, frameworks, bases de datos y herramientas de desarrollo que permiten hacer el trabajo, utilizando los lenguajes y herramientas que ya conoce y confía [28].

Además permite a los desarrolladores crear rápida y fácilmente una aplicación. Utilizando la consola web, herramientas de línea de comandos o IDE basado en Eclipse, un desarrollador simplemente solicita una instancia de la aplicación de OpenShift.

Crea una instancia de la aplicación en la nube de soporte y proporciona acceso a la información necesaria para el desarrollador, para que pueda empezar a codificar inmediatamente. El desarrollador empuja las actualizaciones de código hacia la aplicación basada en la nube a través del sistema de control de código fuente de Git y el protocolo Git asegurado con SSH [29].

Haciendo referencia [115] en el cual menciona que, Secure Shell (SSH) ofrece un protocolo abierto para asegurar las comunicaciones de red, asegurar soluciones cliente/servidor, Shell proporciona shell de comandos, transferencia de archivos y servicios de túnel de datos para las aplicaciones TCP/IP. SSH utiliza la autenticación de claves pública/privada RSA para comprobar la identidad de la comunicación de las máquinas de pares, el cifrado de todos los datos intercambiados.

Secure Shell SSH es un protocolo que proporciona autenticación, cifrado e integridad de datos para asegurar las comunicaciones de la red.

El protocolo Secure Shell ofrece cuatro beneficios básicos de seguridad:

### **Autenticación de usuario**

Autenticación, también conocida como la identidad del usuario, es el medio por el cual un sistema verifica que el acceso sólo se da a los usuarios previstos y se niega a los demás. La mayoría de las implementaciones de Secure Shell incluyen contraseña y métodos de autenticación de clave pública y privada.

### **Autenticación de host**

Una clave de host es utilizado por un servidor para probar su identidad a un cliente y por un cliente para verificar que se está conectando a un servidor anfitrión conocido.

Las claves de host se describen como persistentes (que se cambian con poca frecuencia) y son asimétricos. Si una máquina está funcionando en un sólo servidor SSH, una única clave de host sirve para identificar la máquina y el servidor. Si una

máquina se está ejecutando en múltiples servidores SSH, puede tener múltiples claves de host o utilizar una sola llave para múltiples servidores.

### **Cifrado de datos**

Un sistema de cifrado de bloques es la forma más común de los algoritmos de clave simétrica, estas operan en un bloque de tamaño fijo de datos, utiliza una clave única, secreta, compartida, los datos son encriptados y no se pueden invertir sin la clave compartida. Cuando un cliente establece una conexión con un servidor Secure Shell, que deben acordar el algoritmo que van a utilizar para cifrar y descifrar datos.

El servidor generalmente presenta una lista de los sistemas de cifrado con los que trabaja, y el cliente selecciona el primer sistema de cifrado en su lista que coincide con uno en la lista del servidor.

Las claves de sesión son las claves compartidas, se generan aleatoriamente por el cliente y el servidor, durante el establecimiento de una conexión. Tanto el cliente y el host utilizan la misma clave de sesión para cifrar y descifrar datos, aunque una clave diferente se utiliza para el envío y recepción de canales.

Las claves de sesión se generan después de que la autenticación del host se realiza con éxito, pero antes de la autenticación de usuario para que los nombres de usuario y contraseñas pueden ser enviados cifrados.

### **Integridad de los datos**

La integridad de datos garantiza que los datos enviados desde un extremo de una transacción llegan inalterados al otro extremo. Incluso con el cifrado de Secure Shell, los datos que se envían a través de la red podrían ser vulnerables a alguna inserción de datos no deseada. Secure Shell utiliza el código de autenticación de mensajes (MAC).

Por otra parte OpenShift ofrece los denominados gears estos son contenedores seguros para el código, para cada gear se asigna la CPU, memoria, disco y ancho de banda. Puede utilizar un solo gear para crear una aplicación completa, con una instancia de base de datos privada.

Con lo mencionado se puede evidenciar que en la capa de aplicación se realiza la programación lógica y la asignación de recursos para dar respuesta a la petición del usuario [30].

#### **4.3.1.3. Capa de infraestructura**

OpenShift se basa en la infraestructura hardware de Amazon Web Services (AWS), este ofrece máquinas virtuales que se ejecutan en la infraestructura de Amazon, proporcionando máquinas de arranque virtuales, redes, almacenamiento de bloques, el almacenamiento de objetos, etc.

Los servicios y centros de datos disponen de múltiples capas de seguridad operativa y física para asegurar la integridad y seguridad de los datos.

A continuación se menciona las capacidades y servicios de seguridad para mejorar la privacidad y controlar el acceso de redes que proporciona AWS.

- Los firewalls de red integrados en Amazon VPC y las capacidades de firewall para aplicaciones web existentes en AWS WAF permiten crear redes privadas y controlar el acceso a las instancias y aplicaciones, proporcionando, cifrado en tránsito con TLS en todos los servicio, opciones de conectividad que permiten conexiones privadas o dedicadas desde la oficina o entorno on-premise.
- AWS ofrece la capacidad de agregar una capa adicional de seguridad a los datos en la nube que incluye características de cifrado eficientes y escalables, incluyendo capacidades de cifrado de datos disponibles en los servicios de base de datos y almacenamiento de AWS, opciones flexibles de administración de claves, como AWS Key Management Service, que permiten elegir si desea que AWS administre las claves de cifrado o si el usuario desea mantener el control total sobre las claves, almacenamiento de claves criptográficas dedicado y basado en hardware que utiliza AWS CloudHSM permite satisfacer los requisitos de conformidad.
- AWS proporciona diversas API para que pueda integrar el cifrado y la protección de los datos con cualquiera de los servicios que desarrolle o implemente en un entorno de AWS

- AWS le ofrece capacidades para definir, hacer cumplir y gestionar las políticas de acceso de los usuarios en los servicios de AWS, incorporando gestión de identidades y acceso (Identity and Access Management) IAM permite definir cuentas de usuarios individuales con permisos en los recursos de AWS, autenticación de múltiples factores (Multi-Factor Authentication) es utilizado para identificar cuentas con privilegios e incluye opciones para autenticadores basados en hardware, servicio de directorio (Directory Service) permite integrarse y federarse con directorios corporativos para reducir la sobrecarga administrativa y mejorar la experiencia del usuario final.

Una vez analizado el flujo de trabajo de la aplicación, se examinará los riesgos de seguridad a los que están expuestos los clientes que hacen uso de la aplicación Shop-List, estos serán contrastados con las vulnerabilidades que se ha investigado en el entregable del segundo objetivo.

*Tabla 2 Riesgos de seguridad de la aplicación Shop-List*

Qué tipo de cifrado fue utilizado para la integridad de las credenciales
Red Hat en su programa de instalación configura el sistema para usar Secure Hash Algorithm 512 (SHA512) y contraseñas ocultas.
Recomienda no alterar esta configuración, ya que si las contraseñas ocultas se desactivan durante la instalación, todas las contraseñas se almacenan como un hash de una vía, lo que hace al sistema vulnerable a ataques de piratas de contraseñas. Si el intruso obtiene acceso a la máquina como un usuario normal, puede copiar este archivo en su propia máquina y ejecutar cualquier cantidad de programas para descifrar las contraseñas. Si hay una contraseña insegura en el archivo, es sólo cuestión de tiempo antes de que el pirata la descubra.
Las contraseñas ocultas previenen este tipo de ataque al almacenar hash de contraseñas en un archivo especial, el cual únicamente puede ser leído por el usuario root.
Esto obliga al intruso que intente descubrir la contraseña de forma remota a ingresar a los servicios de red SSH. Este tipo de ataque de fuerza bruta es mucho más lento y deja un rastro evidente, pues los intentos fallidos de conexión son registrados en los archivos del sistema.

Con lo mencionado anteriormente y tomando en cuenta lo mentado por el desarrollador de la aplicación, el cual confirmó que las contraseñas ocultas no fueron desactivadas al momento de la desinstalación, se puede concluir que las integridad de las credenciales es garantizada por la aplicación.

### **Arquitectura utilizada para la aplicación**

Para la implementación de Shop-List se utilizó la arquitectura multi-tenant, en el que se emplea la estrategia de gestión de base de datos independientes, para su implementación, lo que hace de la seguridad de los datos esté bien resguardada, debido al total aislamiento de los datos de otros clientes.

El esquema de base de datos separado, es el método más sencillo para el aislamiento de datos. Los recursos informáticos y código de la aplicación general se comparten entre todos los tenants de un servidor, pero cada tenant tiene su propio conjunto de datos que permanecen aislados, de datos que pertenece a todos los otros tenants. Cada base de datos de metadatos asociados con el tenant correcto, y la seguridad de base de datos evita que cualquier tenant de forma accidental o maliciosamente tenga acceso a los datos de otros clientes.

Por lo que se puede inferir que con la utilización de este esquema para la BD, se está avalando la seguridad de los datos ya que están totalmente apartados de los datos de los demás clientes, evitando filtraciones por cualquier razón.

### **Mecanismos de seguridad empleados para el control de acceso**

Para el ingreso a la aplicación web y móvil, utilizaron validaciones de, nombre de usuario y contraseña, como ya se mencionó Red Hat utiliza el algoritmo SHA512 y contraseñas ocultas, este algoritmo es aplicado durante el ingreso a la aplicación.

En el caso de que el usuario haya olvidado su contraseña para el ingreso a la aplicación web, y solicite recuperarla, el sistema requerirá que conteste una serie de preguntas, las mismas que serán respondidas por el usuario la primera vez que ingresa al sistema.

En cuanto a la recuperación de la contraseña en la aplicación móvil, el sistema enviará al correo registrado un código, este correo será proporcionado por el usuario al momento de crear una cuenta, el código enviado deberá ser ingresado en la aplicación móvil, el sistema verificará ese código y si es correcto le permitirá cambiar la contraseña.

Haciendo alusión a lo especificado en los párrafos precedentes en referencia al tema de control de acceso se ha mencionado que en Shop-List simplemente se hace uso de un nombre de usuario y contraseña para acceder a la aplicación, es una gran desventaja en seguridad ya que lo recomendado es utilizar un mecanismo mucho más eficiente denominado inicio de sesión único SSO, este permite la adopción de varias medidas para mejorar la seguridad en cuanto al inicio de sesión.

#### **Técnica para verificar que las credenciales son ingresadas por el cliente**

Según lo manifestado por el autor de la aplicación, no se aplica ninguna técnica, cualquier persona que tenga conocimiento del usuario y contraseña puede acceder, siendo una gran vulnerabilidad para Shop-List ya que no tiene la certeza de que las credenciales hayan sido ingresadas por el usuario original, para dar solución a esto, como una medida de seguridad se puede realizar una pregunta al usuario cuya respuesta sólo la sabe el usuario autorizado, ya que esta será respondida al momento de registrarse, otra medida de seguridad es implementar el código de un solo uso para el ingreso a la cuenta, este será enviado al celular o correo electrónico del usuario, sin contar con este código aunque tenga las credenciales no podrá acceder a la información.

#### **Cuál es el requerimiento de contraseña mínimo para el usuario**

Controlan que la contraseña tenga una longitud no menor a siete caracteres, esta es una puerta abierta para la violación a la seguridad ya que los usuarios establecen contraseñas con la longitud exigida, pero mediante el mecanismo de ataque de fuerza bruta pueden ser burladas y por ende son vulnerables porque no emplean caracteres alfanúmeros para que al momento de que intenten descifrar su contraseña tengan menos probabilidades de obtenerla.

### **Algoritmo criptográfico utilizado para garantizar la integridad de los datos almacenados**

AWS inicia las instancias en dos grupos de seguridad de Amazon EC2, uno para el maestro y otro para los esclavos. El grupo de seguridad principal tiene un puerto abierto para comunicarse con el servicio. También tiene abierto el puerto SSH para que pueda utilizar SSH en las instancias por medio de la clave especificada al iniciar sesión en vez de utilizar sockets TCP / IP entre el cliente y el servidor.

Los esclavos se inician en otro grupo de seguridad aparte, que solamente permite la interacción con la instancia principal.

De forma predeterminada, ninguno de estos dos grupos de seguridad está configurado para permitir el acceso de fuentes externas, ni siquiera de las instancias de Amazon EC2 pertenecientes a otros clientes, sin embargo estas configuraciones de seguridad están incluidas en su cuenta, permitiendo cambiar la configuración [109].

Como ya se mencionó anteriormente el SSH ofrece la integridad de datos garantizando que los datos enviados desde un extremo de una comunicación llegan inalterados al otro extremo. Secure Shell utiliza el código de autenticación de mensajes (MAC), el cual permite el reconocimiento de cualquier modificación o manipulación del mensaje durante la transmisión y la autenticación de origen de los datos, en secciones anteriores se ha mencionado este algoritmo como uno de los más confiables para garantizar la integridad de los datos.

Poniendo a consideración lo citado y lo que se expone en las soluciones dadas a las posibles vulnerabilidades que se presentan en SaaS, se puede concluir que el almacenamiento de los datos se realiza en forma íntegra velando por la fidelidad de los datos, lo que conlleva a deducir qué Shop-List es una aplicación confiable en cuanto a la integridad de los datos.

### **Algoritmo criptográfico utilizado para garantizar la integridad de los datos de la copia de seguridad**

AWS cuenta con Amazon Glacier este se encarga del cifrado automático de los datos en reposo mediante las claves simétricas del estándar de cifrado avanzado (AES) de

256 bits, es una técnica de cifrado considerado como el más potente en la criptografía, es un cifrado de bloques de clave simétrica que cifra y descifra el bloque de datos, puede ser implementado tanto en software como hardware teniendo mayor rendimiento y mayor seguridad, Amazon Glacier también soporta la transferencia segura de los datos a través de la capa de conexión segura SSL [110].

Basándose en lo expuesto anteriormente se puede concluir que, con la utilización de esta técnica de cifrado, los datos en reposo refiriéndose a los datos almacenados en backup están respaldados de forma segura.

### Cómo realiza la recuperación de desastres

AWS permite realizar una recuperación de desastres más rápida de los sistemas de TI fundamentales sin incurrir en gastos adicionales de infraestructuras de un segundo sitio físico. La nube de AWS soporta muchas arquitecturas de recuperación de desastres conocidas de entornos de “luz piloto” que están listos para escalar en un momento a entornos de “espera activa” que permiten una rápida comutación por error. Gracias a los centros de datos con los que cuenta en 12 regiones de todo el mundo, AWS ofrece una serie de servicios de recuperación de desastres basados en la nube que permiten una rápida recuperación de los datos y de la infraestructura de TI.

Esta es una gran ventaja para la aplicación Shop-List ya que hace uso de AWS, esto le permite garantizar que, en caso que suceda un desastre natural se puede realizar la recuperación en tiempos prodigiosos.

### Cuál es el mecanismo empleado para realizar la copia de seguridad

La copia de seguridad es realizada a nivel de cada base de datos de los supermercado contando con la gestión de base de datos (BD) a nivel gráfico, que es controlada por el superusuario el mismo que puede realizar la copia de seguridad (backup) exportando los datos en formato correspondiente al tipo de BD utilizada, este es un procedimiento relativamente simple ya que la aplicación implementa un enfoque de BD, en el cual cada cliente tiene una base de datos dedicada para cada uno.

### **En caso de pérdida cuál es la técnica utilizada para la recuperación de información**

Una vez realizada la copia de seguridad de la BD, simplemente se ingresa a la sección de administración de datos para importar los datos correspondientes.

Para exportar la copia de seguridad a AWS se utiliza la opción de Import/Export estándar que acelera la transferencia de grandes volúmenes de datos hacia AWS utilizando dispositivos de almacenamiento portátiles. AWS extrae datos de dispositivos de almacenamiento y transfiere datos a estos utilizando la red interna de alta velocidad de Amazon, sin tener que pasar por Internet, esta transferencia la realiza gracias a que AWS tiene a su disposición Direct Connect facilitando el establecimiento de una conexión de red dedicada con gran ancho de banda desde las instalaciones del cliente a AWS. Con AWS Direct Connect, puede transferir los datos críticos de su empresa directamente desde el centro de datos a AWS pasando por alto a su proveedor de Internet y evitando la congestión de la red.

Por esta razón la transferencia de un conjunto de datos significativos, utilizando AWS Import/Export suele ser más rápido que realizar transferencias a través de Internet.

### **Protocolo de seguridad de datos en la red**

El autor manifiesta que una aplicación web, es una aplicación cliente/servidor, donde tanto el cliente (el navegador web, explorador o visualizador) como el servidor (el servidor web) y el protocolo mediante el que se comunican (HTTP) están estandarizados y no han de ser creados por el programador de aplicaciones.

Este protocolo para transmitir datos a través de la red, no es considerado como seguro, por lo que se deja a responsabilidad del usuario limitar el tipo de datos que se transmite, a través de la aplicación.

### **Mecanismo que determina el nivel de privilegios de un usuario**

La aplicación cuenta con tres tipos de usuarios, cada uno de ellos tiene asignado roles y de esta manera se controla los privilegios que posee cada uno, se realiza una consulta al server para verificar que tipo de rol tiene el usuario que está accediendo al sistema y de esta manera otorgarle los privilegios correspondientes.

#### **4.3.2. Universidad Nacional de Loja hace uso del DRIVE**

En el siguiente apartado se dará a conocer el acuerdo que tiene la Universidad Nacional de Loja con Google Apps, este acuerdo fue proporcionado por el Ing. Milton Labanda, Director General de la Unidad de Telecomunicaciones e Información (Véase [Anexo 5](#)), el mismo que rige a todas las entidades educativas que hagan uso de los servicios de este proveedor SaaS, cabe indicar que únicamente se analizará los términos relevantes en cuanto a la seguridad de los datos.

##### **4.3.2.1. Instalaciones y transferencia de datos**

Este tema es considerado como uno de los más críticos, porque no se tiene conocimiento a que partes del mundo serán transferidos los datos, en el acuerdo manifiesta que todas las instalaciones que se utilizan para almacenar y procesar datos del cliente deberán cumplir con las normas de seguridad razonables, protección no inferior a las normas de seguridad de las instalaciones de Google, que almacenan y procesan información de un tipo similar. Google ha puesto en práctica sistemas y procedimientos estándar de la industria, al menos, para garantizar la seguridad y confidencialidad de los datos de los clientes, la protección contra las amenazas o riesgos previstos para la seguridad o integridad de dicha información, y proteger contra el acceso no autorizado o la utilización de datos de clientes.

En lo referente al marco de la prestación de los servicios, Google podrá realizar las siguientes operaciones en cuanto al tema de los datos, transmitir, almacenar y procesar los datos de los clientes en los Estados Unidos o cualquier otro país en el que Google o sus representantes tengan instalaciones. Esto se realiza con el consentimiento del usuario ya que al momento de utilizar los servicios, el cliente consiente a esta transferencia, procesamiento y almacenamiento de datos.

##### **4.3.2.2. Retención de datos**

Google declara que no está obligado a conservar los datos archivados de clientes más allá del período de retención especificado por el cliente, al menos que sea necesario por motivos legales, si el cliente no renueva Google Apps Vault, Google no tendrá ninguna obligación de conservar los datos archivados de los clientes, pero no especifica si los datos son eliminados de todos los centros de datos ubicados alrededor del mundo.

#### **4.3.2.3. Administración de los Servicios**

La confidencialidad de los datos de los usuarios finales está en manos de los administradores informáticos de la UNL, la institución educativa puede especificar uno o más administradores a través de la consola de administración, el mismo tendrá los derechos de acceso a la cuenta de administrador y de administrar las cuentas de usuario final.

La institución educativa es responsable de:

- Mantener la confidencialidad de la contraseña y el administrador de la cuenta.
- Designar a las personas que están autorizadas a acceder a la cuenta de administración.
- Asegurar que todas las actividades que se producen en relación con el Administrador de cuentas cumplen con el Acuerdo. El cliente acepta que las responsabilidades de Google no se extienden a la gestión interna o la administración de los servicios de atención al cliente y que Google no es más que un procesador de datos.

Por lo mencionado se considera que los datos que conserve en la cuenta el usuario final podrán ser vistos, accedidos, supervisados, utilizados o divulgados o se podrá realizar cualquier otra operación sobre ellos, se deberá confiar en la ética profesional del administrador para que los datos estén seguros y permanezcan íntegros, por otra parte el cliente es responsable de mantener la confidencialidad de la contraseña y también por parte del administrador de las cuentas, este será responsable de todo aquello que se refiere a la gestión interna de las cuentas, deslindando a Google de todo gravamen puesto que el cliente acepta que este solo es utilizado para la acumulación y manipulación de elementos de datos para producir información significativa.

Además, tanto el administrador de las cuentas como el proveedor SaaS, tendrán la obligación de proteger la información confidencial de la otra parte con el mismo nivel de atención que utiliza para proteger su propia información confidencial; y no revelarla, excepto a los afiliados, empleados y agentes que necesiten conocerla y que hayan acordado por escrito a mantener la confidencialidad. Cada parte y todos los que tengan

conocimiento de la información confidencial, pueden utilizar la información únicamente para ejercer los derechos y cumplir con sus obligaciones en virtud al acuerdo otorgado.

Las partes podrán revelar la información confidencial de la otra parte cuando sea requerido por la ley, pero sólo después de que la ley permita utilizar esfuerzos comercialmente razonables para notificar a la otra parte y la otra parte da la oportunidad de impugnar la divulgación.

#### **4.3.2.4. Ley de Privacidad y Derechos Educativos de la Familia**

Las partes reconocen que los datos del cliente pueden incluir información de identificación personal de los registros de educación que están sujetos a esta ley y Google es considerado como un "Oficial de la Escuela" y deberá cumplir con la misma.

Lo mencionado en los párrafos preliminares es todo cuanto conoce la entidad educativa citada al inicio de este análisis, acerca de la seguridad, confidencialidad, privacidad de los datos, como se puede observar el acuerdo y los términos a los que está sujeta la organización que utiliza los servicios de Google Apps, es bastante incompleta, por lo que no se conoce a profundidad cuales son los mecanismos de seguridad que se utiliza para garantizar la seguridad de los datos.

El acuerdo no menciona nada referente al esquema de base de datos utilizada, este es un factor trascendental para la seguridad de los datos ya que los datos dependen directamente del esquema utilizado para que se garantice que los clientes no violen la seguridad de otros.

Acerca de los mecanismos de seguridad empleados para el control de acceso, se sabe que las validaciones son de usuario y contraseña, pero no se conoce el algoritmo de encriptación del cual hacen uso para garantizar la integridad de las credenciales, por otra parte el uso del mecanismo de credenciales para el ingreso es visto como una gran desventaja ya que la contraseña puede ser obtenida de alguna de las formas citadas en el estado del arte correspondiente al segundo objetivo, lo recomendado es utilizar un mecanismo mucho más eficiente denominado inicio de sesión único SSO, este permite la adopción de varias medidas para mejorar la seguridad en cuanto al inicio de sesión.

Tampoco se conoce cómo se asegura que un servidor no autorizado de respuesta a las peticiones de los clientes, por otro lado no se tiene la certeza dónde están ubicados los datos ya que el proveedor no especifica en qué centros de datos de todo el mundo está alojada la información, en fin en el acuerdo no se especifica las acciones que son tomadas para mitigar las vulnerabilidades que son inherentes a SaaS.

#### **4.3.3. Universidad Técnica Particular de Loja hace uso de office 365**

En el siguiente apartado se dará a conocer el acuerdo que tiene la Universidad Técnica Particular de Loja con Microsoft, relacionado con la privacidad.

##### **4.3.3.1. Principios clave de privacidad de Microsoft**

- **Control:** Le pondremos al control de su privacidad, con herramientas fáciles de usar y opciones claras.
- **Transparencia:** Seremos transparentes sobre la recopilación de datos y su uso, para que pueda tomar decisiones informadas.
- **Seguridad:** Protegeremos los datos que nos confíe, mediante seguridad y cifrado eficaces.
- **Sólida protección legal:** Respetaremos las leyes de privacidad local y defenderemos la protección legal de su privacidad como un derecho humano fundamental.
- **Sin identificación basada en contenidos:** No usaremos su correo electrónico, chat, archivos ni ningún otro contenido personal para dirigirle anuncios.
- **Beneficios que obtendrá:** Cuando recopilemos datos, los usaremos para beneficiarle y mejorar sus experiencias.

Estos principios forman la base del enfoque de Microsoft en cuanto a la privacidad y continuarán forjando el modo en que creamos nuestros productos y servicios [31].

##### **4.3.3.2. ¿Qué tipos de datos recopila Microsoft?**

Microsoft recopila datos para ayudarte a hacer más cosas. Para ello, usamos los datos que recopilamos para operar y mejorar nuestro software, servicios y dispositivos, proporcionarte experiencias personalizadas y ayudarte a mantenerte seguro. Estas son algunas de las categorías de datos más comunes que recopilamos.

- Exploración web y búsquedas en línea
- Lugares a los que va

- Datos que nos ayudan a atenderle de forma personalizada
- Salud y forma física
- Datos que usamos para mostrar anuncios más interesantes
- Inicio de sesión y datos de pago
- Información de los sensores de dispositivo [31]

#### **4.3.3.3. Mecanismos de seguridad de Microsoft para proteger sus datos**

- **Auditoría y registro**

Auditoría y registro de eventos relacionados con la seguridad y alertas relacionadas, son componentes importantes de una estrategia eficaz de protección de datos. Los registros de seguridad e informes le proporcionan un registro electrónico de actividades sospechosas y le ayudan a detectar patrones que pueden indicar la penetración externa en la red, así como los ataques internos. Puede utilizar la auditoría para supervisar la actividad del usuario, documentar el cumplimiento normativo, realizar el análisis forense, y mucho más. Las alertas proporcionan notificación inmediata cuando se producen eventos de seguridad.

Servicios y productos comerciales de Microsoft le proporcionan opciones de auditoría de seguridad y de registro configurables para ayudar a identificar las lagunas en sus políticas y mecanismos de seguridad, y hacer frente a esos vacíos para ayudar a prevenir las infracciones. Servicios de Microsoft ofrecen algunos (y, en algunos casos, todas) de las siguientes opciones: monitorización centralizada, registro y sistemas de análisis para proporcionar una visibilidad continua; alertas oportunas; y los informes que le ayudan a manejar la gran cantidad de información generada por los dispositivos y servicios [32].

- **Delitos informáticos**

La ciberdelincuencia es un desafío constante y cada vez mayor para todas las organizaciones. La combinación de la expansión del acceso a Internet, el aumento explosivo de los dispositivos conectados, y la rápida expansión de los servicios innovadores basados en la nube está creando gran oportunidad económica y social para los consumidores, los gobiernos y las empresas. Por desgracia, también ha abierto nuevas vías de ataque para los cibercriminales y otros agentes maliciosos.

Al igual que todos los avances técnicos, el almacenamiento de datos y aplicaciones en la nube ha atraído a todo un ecosistema penal, de los hackers individuales a grupos altamente organizados que tienen como objetivo acabar con las redes enteras. Los criminales cibernéticos, motivados por todo, desde fines de lucro para obtener beneficios políticos, utilizan Internet para interrumpir las actividades comerciales y de acceso sensibles datos personales y financieros. Debido a que la mayoría de las empresas dependen de un tercero para administrar sus servicios en la nube, es fundamental que las empresas que prestan servicios en la nube, como Microsoft, se han comprometido a, y capaz de, la ciberdelincuencia luchando.

Por desgracia, la delincuencia informática no es puramente un problema técnico-ni nunca “desaparecerá.” Proveedores de servicios de nube debe luchar continuamente los delitos informáticos en múltiples niveles usando equipos de especialistas, de expertos en seguridad a defensores de la política. Se necesita un esfuerzo concertado, así como profunda inversión financiera y operativa para comprender verdaderamente la ciberdelincuencia y efectivamente luchar contra ella.

Microsoft sabe que la seguridad y la privacidad están conectados, lo intrínsecamente datos que confía a los servicios de nube de Microsoft debe mantenerse privada.

Trabajamos diligentemente para ayudar a proteger sus datos contra el acceso no autorizado, tanto interna como externamente. Microsoft ha realizado importantes inversiones en la seguridad de su plataforma, que, cuando se combina con altos niveles de seguridad y de inteligencia y las asociaciones estratégicas, ayuda a mantener nuestros productos y servicios basados en la nube más segura [33].

- **Diseño y seguridad operacional**

Servicios en la nube de Microsoft y el software están construidos sobre la misma base de tecnología confiable que se aplica a todos los productos y servicios. Microsoft diseña sus servicios y software pensando en la seguridad para ayudar a asegurar que su infraestructura en la nube es resistente y defendió de los ataques.

El principio rector de la estrategia de seguridad de Microsoft es “asumir incumplimiento.” Por lo tanto, nuestro equipo global de respuesta a incidentes trabaja continuamente para mitigar los efectos de los ataques contra los servicios de nube de Microsoft. Estas

prácticas están respaldados por “centros de excelencia” de seguridad que combaten el crimen digital, software malicioso combate y responder a los incidentes de seguridad y vulnerabilidades en nuestro software [34].

- **Encriptación**

Los datos son el activo más valioso e irremplazable de una organización, y el cifrado sirve como el último y más fuerte línea de defensa en una estrategia de seguridad de datos de varias capas. Microsoft servicios de negocios nube y productos utilizan el cifrado para proteger los datos de los clientes y ayudan a mantener el control sobre ella. Encriptar su información hace que resulte ilegible para personas no autorizadas, incluso si se rompen a través de los servidores de seguridad, se infiltran en la red, obtener acceso físico a los dispositivos, o pasar por alto los permisos en el equipo local. Cifrado transforma los datos de modo que sólo una persona con la clave de descifrado se puede acceder a él.

Nuestros productos también utilizan protocolos de transporte seguros estándar de la industria para datos a medida que se mueve a través de una red, ya sea entre los dispositivos de usuario y centros de datos de Microsoft o dentro de los propios centros de datos. Para ayudar a proteger los datos en reposo, Microsoft ofrece una gama de funciones de cifrado incorporados [35].

- **Gestión de acceso e identificación**

Los sistemas de sujeción, las aplicaciones y los datos contienen con los controles de acceso basados en la identidad. Las características de gestión de identidades y acceso que están incorporadas en productos y servicios comerciales de Microsoft ayudan a proteger su información personal y organizacional del acceso no autorizado, mientras que ponerla a disposición de los usuarios legítimos cuando y donde lo necesiten.

Estas características le permiten administrar las identidades de usuario, credenciales y permisos de acceso desde la creación hasta la jubilación, y ayudar a automatizar y centralizar los procesos del ciclo de vida de identidad. Microsoft va más allá del modelo de nombre de usuario y la contraseña para la autenticación fuerte, al tiempo que la seguridad más conveniente para los usuarios con procesos simplificados y de sesión único (SSO). Herramientas robustas hacen que sea más fácil para los administradores

gestionar la identidad, y los desarrolladores construir la gestión de identidades basada en políticas en sus aplicaciones [36].

- **Seguridad de la red**

La protección de la seguridad y confidencialidad de tráfico de la red, ya sea en la nube o en las instalaciones, es una parte fundamental de cualquier estrategia de protección de datos. Fijación de la infraestructura de la red ayuda a prevenir ataques, bloquear el malware y proteger sus datos del acceso no autorizado, el acceso interrumpido, o pérdida.

En la nube pública, el aislamiento de la infraestructura del cliente es fundamental para mantener la seguridad. Microsoft Azure, sobre el que se construyen la mayoría de los servicios de negocios de Microsoft en la nube, logra esto principalmente a través de un cortafuegos virtual distribuido, redes de área local (LAN) con particiones, y la separación física de los servidores de back-end.

Los clientes pueden desplegar múltiples redes privadas aisladas lógicamente, y cada red virtual está aislada de las otras redes virtuales. Para los clientes de correo locales, Windows Server 2016 incluye cortafuegos, análisis de amenazas, y numerosas características de seguridad de red [37].

- **Gestión de amenazas**

La gestión de amenazas incluye la protección tanto de software malicioso y los ataques contra los sistemas y redes. Productos y servicios de Microsoft han incorporado en las características de protección para ayudar a defender sus datos contra el malware y otros tipos de amenazas.

Servicios en la nube de Microsoft que ayudan a proteger contra las amenazas de malware en múltiples formas. Microsoft Antimalware se construye para la nube, y las protecciones antimalware adicionales se proporcionan en los servicios específicos. De denegación de servicio (DoS) puede denegar el acceso a los recursos importantes y dar lugar a la pérdida de productividad, por lo que Microsoft construye sus servicios a defenderse contra este tipo de ataques. Servidor de Windows y sistemas operativos de cliente incluyen múltiples tecnologías de protección contra estas amenazas en el ámbito local [38].

## **5. MATERIALES Y MÉTODOS**

El tipo de proyecto que se desarrolló es basado en la investigación, en el cuál se revisó información relevante acerca de la arquitectura SaaS y la seguridad que ofrecen los proveedores de este servicio.

Tomando en consideración lo expuesto, a continuación se menciona los métodos y técnicas de los que se hizo uso para el desarrollo del trabajo de titulación.

### **5.1. Materiales**

En el presente Trabajo de Trabajo de Titulación se hizo uso de los siguientes materiales:

#### **5.1.1. Talento Humano**

El trabajo de titulación fue realizado por el estudiante y la asesoría del director de tesis, con un total de 480 horas. Considerando estas variables se tiene la siguiente tabla:

*Tabla 3 Costo del talento humano empleado en el trabajo de titulación*

Talento Humano	Número de horas	Valor por hora (\$)	Valor Total (\$)
Director	80	30.00	2 400.00
Estudiante	400	10.00	4 000.00
Subtotal			<b>6 400.00</b>

El rubro de \$2 400.00 por concepto de asesoramiento del director del trabajo de titulación fue financiado por la Universidad Nacional de Loja, por lo tanto el costo de talento humano es \$ 4 000.00 valor que pertenece a las horas de trabajo del estudiante.

#### **5.1.2. Bienes**

Los costos acordados en la siguiente tabla son calculados mediante fórmulas para determinar el valor de depreciación de los bienes.

*Tabla 4 Costo de los bienes físicos empleados en el trabajo de titulación*

Bien	Cantidad	Costo de Depreciación(\$)
Computador Portátil HP CORE i5-450M	1	200.00
Impresora multifunción EPSON	1	83.33
Pendrive de 16 GB	1	4.00
Subtotal		<b>287.33</b>

### **5.1.3. Servicios**

Los servicios utilizados para la ejecución del proyecto se detallan a continuación:

*Tabla 5 Costo de los servicios empleados en el trabajo de titulación*

Servicio	Cantidad	Valor Unitario (\$)	Valor Total (\$)
Impresiones	600	0,10	60.00
Copias	50	0,02	10.00
Empastado	1	15.00	15.00
Anillados	4	1.50	6.00
Internet	12 meses	20.00	240.00
Trasporte	24 semanas	20.00	480.00
Subtotal			<b>811.00</b>

### **5.1.4. Financiamiento**

Los gastos totales empleados en el trabajo de titulación, se describen en la siguiente tabla:

*Tabla 6 Costo totales empleados en el trabajo de titulación*

Materiales	Valor Total (\$)
Talento Humano	4 000.00
Bienes	287.33
Servicios	811.00
Total	<b>5 098.33</b>

Los gastos en los que se incurre para hacer efectivo el proyecto de titulación son de **\$ 5 098.33** el cual fue asumido por el estudiante.

## **5.2. Métodos**

Para el desarrollo del trabajo de titulación fue necesario utilizar diferentes métodos, los mismos se describen a continuación:

### **5.2.1. Método deductivo**

Fue útil para la realización del primer objetivo ya que mediante este se conoció la arquitectura SaaS y a partir de ello, llegar a conclusiones específicas [45].

### **5.2.2. Método Inductivo**

Se lo utilizó para recolectar información específica de cada vulnerabilidad a la que está expuesta la seguridad de los datos, luego de haber obtenido esta información se determinó la seguridad que deberían ofrecer los proveedores de SaaS [45].

### **5.2.3. Método Investigativo**

Este método fue utilizado con mayor inclinación debido al tipo de proyecto el cual es investigativo, gracias a este se pudo sistematizar los criterios de búsqueda y encontrar información de fuentes confiables, para la consumación del proyecto [46].

## **5.3. Técnicas**

Para la ejecución del trabajo de titulación fue necesario utilizar diferentes técnicas, las mismas se describen a continuación:

### **5.3.1. Técnica de observación**

Fue útil para evidenciar la utilización de servicios SaaS por parte de las organizaciones, afianzando el problema encontrado [40].

### **5.3.2. Técnica de entrevista**

Se realizó una entrevista al Ing. Milton Labanda e Ing. Raúl Gómez, personas involucradas en los casos de estudio, presentados en el tercer capítulo de este documento, con la finalidad de conocer como garantiza la seguridad, en un caso como proveedor, y en el otro caso como cliente [41].

### **5.3.3. Técnica de procesamiento y análisis de información**

Esta técnica contribuyó en la clasificación, registro y análisis de la información recolectada con la finalidad de discernir información verificable [42].

## **5.4. Metodología de desarrollo**

Para efectuar el trabajo de titulación se utilizó dos metodologías de desarrollo, las mismas se describen a continuación:

#### **5.4.1. Estado del Arte**

Para los entregables correspondientes al primer y segundo objetivo se utilizó esta metodología de desarrollo, para realizar un análisis narrativo y crítico frente a la arquitectura y seguridad de SaaS [43].

#### **5.4.2. Guía multimedia**

Para llevar a cabo el tercer objetivo se hizo uso de una guía multimedia en la cual se presenta información acerca de la arquitectura SaaS, con la finalidad que el usuario conozca las vulnerabilidades de SaaS, las cláusulas imprescindibles en un contrato, y las observaciones que deberían tomar en cuenta las instituciones que deseen hacer uso de SaaS [44].

## **6. RESULTADOS**

En este apartado se da a conocer los resultados obtenidos en cada uno de los objetivos planteados para llevar a efecto el trabajo de titulación.

### **6.1. Primer objetivo específico: “Estudiar la arquitectura de servicio SaaS, como modelo tecnológico en la nube”**

Del cual se obtuvo como resultado un estado del arte de información estructurada para conocer la arquitectura; en el primer punto se dará a conocer cómo surgió este modelo; luego se mostrará las supremacías que tiene en relación al modelo de Provisión de Servicios de Aplicaciones (ASP) el cual sirvió como base para el desarrollo de la arquitectura anteriormente citada; seguidamente se presenta la definición y características de SaaS; posteriormente se pone a disposición la estructura de capas con el que está conformado el modelo; consecutivamente se contempla los riesgos, oportunidades, ventajas y desventajas de SaaS; continuadamente se muestra los aspectos compartidos y las estimaciones de costos entre el software tradicional y SaaS; finalmente se expondrá dos puntos de vista de la arquitectura SaaS y el ciclo de vida en el cual se desarrolla.

A continuación se presenta el estado del arte que se realizó como entregable para dar cumplimiento al primer objetivo.

#### **Estado del Arte “Estudio de la arquitectura de Software como Servicio (SaaS)”**

Esther Elizabeth Jaramillo Malla

Área de Energía, las Industrias y los Recursos Naturales No Renovables

Universidad Nacional de Loja

Loja, Ecuador

[eejaramillom@unl.edu.ec](mailto:eejaramillom@unl.edu.ec)

30 de Mayo de 2016

#### **6.1.1. Historia de SaaS**

Según los autores de los artículos [45] [46], el modelo SaaS ha evolucionado a partir del modelo de provisión de servicios de aplicaciones (ASP), que surgió a finales de 1990 como una opción de entrega de software bajo demanda para el desarrollo de

aplicaciones off-the-shelf comercial, refiriéndose a las aplicaciones de software estándar es decir no personalizadas.

El modelo ASP es un proveedor de alojamiento, que realiza la gestión y el despliegue de capacidades de aplicación de forma remota desde un centro de datos accesible a través de Internet. Los problemas técnicos de ASP durante la última década del año en el que surgió incluyen los problemas iniciales de diseño (es decir, algunas aplicaciones de software fueron diseñados para ser accesibles remotamente en ese momento), la disponibilidad de ancho de banda limitado, y velocidades lentas de conexión a Internet. Estos inconvenientes en esa época hicieron de ASP una solución muy cara y poco práctica durante ese tiempo.

Por las contrariedades expuestas coexistió la resistencia de los proveedores de software para impulsar completamente este nuevo modelo de entrega de software, principalmente la desventaja económica obstaculizó el progreso de ASP en gran medida, dado que el modelo ASP inicial se basaba en una arquitectura de un solo inquilino, los proveedores de software no podían compartir la infraestructura de tecnología de información (TI), y el código de la aplicación eficiente a través de sus clientes, lo que creó bajas economías de escala, por lo que se puede definir como software a medida.

Tomando como referencia y en respuesta a las limitaciones técnicas del modelo ASP y las carencias económicas por las que padecía, surgió SaaS como una forma avanzada para proporcionar servicios de software y dar solución a las restricciones del modelo tomado como base [45] [46] [47] [48] [49] [50] [51].

### **6.1.2. Preeminencias de SaaS sobre ASP**

En la nueva arquitectura SaaS, de múltiples usuarios, sólo hay una única instancia de los datos y de código, es decir una determinada aplicación en el servidor del proveedor. Este código no se puede personalizar, las configuraciones específicas del cliente sólo se pueden hacer en la capa de metadatos en la parte superior del código común mediante el uso de las interfaces de que el proveedor de SaaS ofrece. Esta arquitectura tiene implicaciones importantes para la percepción de los clientes en cuanto a las oportunidades y riesgos.

Según [51] la similitud principal y la más importante entre ASP y SaaS es: asumir la responsabilidad de la gestión del servicio, incluida la seguridad, el rendimiento, la disponibilidad, fiabilidad y escalabilidad.

Las distinciones de acuerdo a [45], entre los dos modelos son las que se muestran a continuación, con esto se puede evidenciar que el modelo que ha surgido a partir del otro lo ha superado completamente:

- A diferencia del modelo clásico ASP en el que las aplicaciones de software e infraestructura de TI están dedicados a cada cliente, las aplicaciones y la infraestructura se comparten entre los clientes en el modelo SaaS.
- El modelo SaaS limita las opciones de personalización de los clientes de las principales estructuras de datos y funcionalidad del software.
- Proporciona el proveedor más control sobre el desarrollo futuro:

Con ASP los clientes tienen que adquirir futuras actualizaciones de software, ya que las interfaces por lo general no son compatibles con versiones anteriores. Por lo tanto, este modelo ya no requiere que el proveedor realice inversiones específicas para el cliente.

Además, ayuda a los proveedores a crear importantes economías de escala, ya que no necesitan aumentar constantemente el tamaño de sus centros de datos.

Esto, a su vez, puede tener implicaciones para el proveedor con respecto al rendimiento y disponibilidad del sistema, seguridad de datos y privacidad, y la eficiencia de costes, sino también para el cliente con respecto a la oportunidad y evaluación de riesgos. [45] [51]

#### **6.1.3. Definición del modelo SaaS**

En la arquitectura SaaS las aplicaciones ya no son un producto sino un servicio [52], es un modelo de negocio para la distribución de software [53], que proporciona acceso al mismo y a sus funciones a través de Internet siendo una de las principales amenazas contra los datos[54], el modelo se refiere a la utilización de los servicios de software (SaaS), plataformas (PaaS) e infraestructura (IaaS) basados en web [46] [55].



Figura 12 SaaS, PaaS, IaaS

Permite que varios clientes (inquilinos) puedan compartir la misma instancia de un software y acceder a los datos [56] que se alojan en los servidores de la compañía de tecnologías de información y comunicación través de internet, múltiples clientes pueden utilizar las mismas instalaciones y con ello aumentar las tasas de utilización de hardware y redes [57], las organizaciones pueden tener a la disposición estos servicios a cambio de una tarifa [58] [59], un inquilino es la unidad organizativa que paga por el uso de una aplicación SaaS de forma regular de acuerdo a un determinado contrato de suscripción [60] [61], además los proveedores de SaaS son subsidiarios de toda la infraestructura de red, software, hardware, plataforma operativa, y es responsable del mantenimiento y otros servicios.

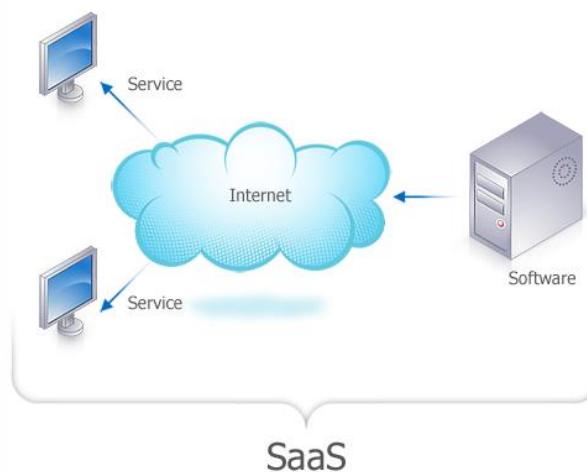


Figura 13 Definición de SaaS

Hacer uso de este servicio implica estar expuesto a grandes riesgos de seguridad de los datos [62], siendo la confiabilidad el mayor desafío en la amplia aceptación de SaaS [63], los datos se encuentran alojados fuera de las organizaciones, pudiendo ser víctima de robo, modificación, pérdida entre otras vulnerabilidades, quedando expuesto el activo más importante hoy en día de toda entidad.

#### **6.1.4. Características de SaaS**

Entre las principales características de las que puede ostentar SaaS son las siguientes, en las cuales se destaca las cualidades que definen e identifican a esta arquitectura.

- Desaparece el concepto de licencia, se pasa a hablar de pago por uso, según las necesidades de la organización que contrata los servicios.
- Software comercial para el acceso y administración de las operaciones de la organización a través de la red, el software comercial es aquel en el que existen sectores de la economía que lo sostiene a través de su producción, su distribución o soporte.
- Gestión centralizada, actividades gestionadas desde ubicaciones centrales, desde la sede de cada cliente, permitiendo a los clientes el acceso remoto a las aplicaciones mediante la web.
- Este modelo de software ofrece una relación "uno a muchos", es decir una instancia, múltiples usuarios aprovechando los servicios de esta instancia.
- Actualizaciones centralizadas, los usuarios no necesitan manejar las actualizaciones y parches de software.
- Cuenta con una API que permite la integración entre las diferentes piezas de software.
- Multi-servicio individual, los servicios ofrecidos son particularmente para el uso de cada usuario.

- Datos de aislamiento entre los diferentes clientes para la seguridad y la privacidad de cada dato, esto permite que las transacciones que se ejecutan simultáneamente no interfieran con otras, ya que si los datos no tuvieran esta propiedad se podría modificar los datos que otra transacción está leyendo creando una inconsistencia cuando se crean los datos.
- El software de la aplicación puede ser accedido a cualquier distancia y en todo momento a través de internet.
- SaaS proporciona la funcionalidad del software y la característica que son comunes entre sí y por lo tanto potencialmente reutilizados por un número de consumidores de servicios.
- SaaS proporciona la funcionalidad de un determinado software en la forma de servicio. Esto está en contraste con un servicio de mash-up que proporciona sólo una parte de toda la funcionalidad del software.
- Modelo de cliente liviano, los servicios SaaS se ejecutan en el lado de los proveedores, mientras que los consumidores de los servicios utilizan navegadores para acceder a los resultados calculados, cuando se habla de cliente liviano se trata de un software de cliente en una arquitectura de red cliente-servidor que depende del servidor central para las tareas de procesamiento, y se enfoca principalmente en transportar la entrada y la salida entre el usuario y el servidor remoto.
- Los conjuntos de datos de consumo específico que se producen por SaaS, se ejecutan, se almacenan y se mantienen en el lado de los proveedores. [53] [64] [65]

#### **6.1.5. Estructura de capas SaaS**

SaaS se ejecuta en la parte superior de PaaS, aprovechando la API de almacén de datos de esta arquitectura, que cuenta con un acceso de datos eficiente y se almacena en la memoria caché de datos, en [66] se refiere a que el enfoque basado en PaaS depende de las PaaS subyacentes para apoyar a SaaS, incluyendo su programación, los mecanismos de tolerancia a fallos y escalabilidad.

En [67] explica que PaaS a su vez se ejecuta en la parte superior de IaaS la cual proporciona hardware virtualizado dicho en otras palabras, infraestructura de procesamiento, abarcando aspectos como el espacio en servidores virtuales, conexiones de red, ancho de banda, direcciones IP y balanceadores de carga.

SaaS tiene no sólo su modelo de negocio, sino también sus procesos de desarrollo y de infraestructura de cómputo únicos. A nivel del sistema, a diferencia del software tradicional que funciona en sistemas operativos, SaaS se suele implementar en un sistema de PaaS o de la infraestructura SaaS especializada.

En la siguiente figura se muestra la estructura de capas y el flujo de trabajo que SaaS realiza para brindar servicios a los clientes en la nube, un cliente envía solicitudes para la utilización de servicios de software de la empresa, ofrecidos por un proveedor de SaaS, haciendo uso de tres capas, la capa de aplicación, capa de plataforma y capa de infraestructura, todas estas interactuando para satisfacer la petición del cliente, lo mencionado anteriormente concuerda con la referencia [68].

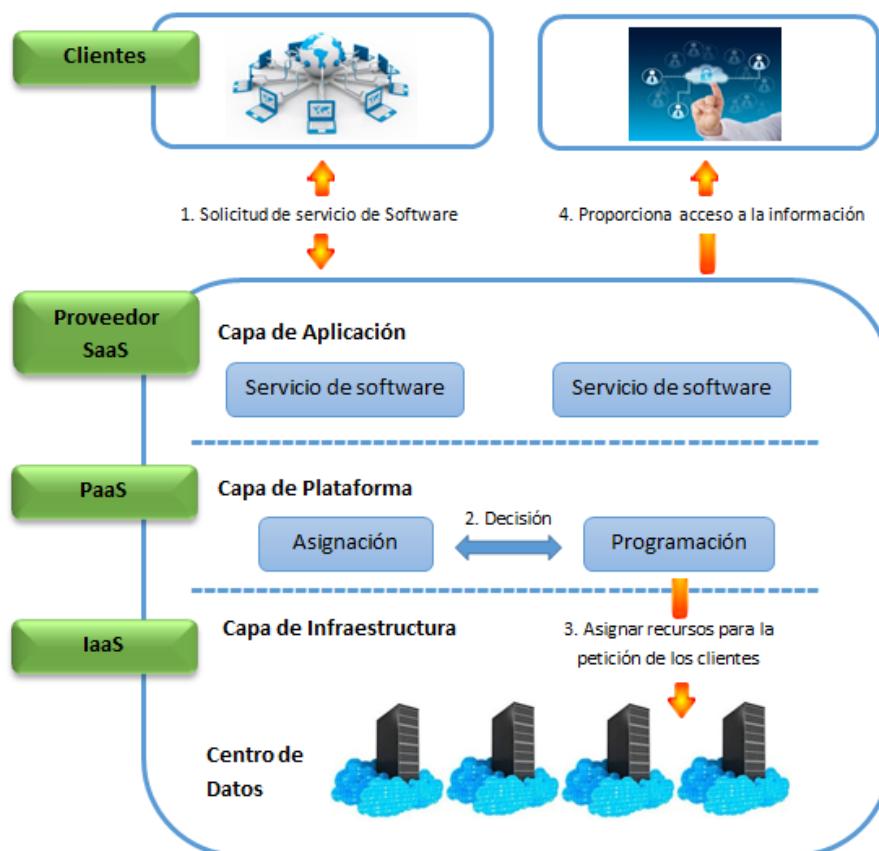


Figura 14 Estructura de capas SaaS

Como podemos observar en la Figura 14, con la petición por parte del cliente comienza el flujo de trabajo de SaaS con el objetivo de atender a las solicitudes de los inquilinos.

En [69] se describe como se realiza el proceso de solicitud al proveedor de SaaS, los inquilinos utilizan los servicios SaaS a través de un navegador web, cuando el navegador envía la solicitud, el servidor de aplicaciones proporciona la aplicación web desarrollada y responde a la solicitud de la aplicación web.

#### a. Capa de aplicación

Una vez recibida la solicitud del usuario la capa de aplicación se encarga de gestionar todos los servicios de aplicaciones que se ofrecen a los clientes por parte del proveedor de SaaS, como se menciona en [23] la capa de aplicación es proporcionada para múltiples usuarios, los sistemas SaaS proporcionan un cierto grado de personalización según las exigencias de los clientes.

La personalización de la capa de aplicación de los sistemas de SaaS es más compleja que la de los sistemas de información tradicionales, especialmente en su aplicación técnica específica para equilibrar la personalización de la lógica de negocio y el intercambio entre los sistemas.

El modelo de personalización de la capa de aplicación SaaS se divide lógicamente en tres partes: servicio, proceso e interfaz de usuario.

A continuación se definirá los tres módulos de la capa de aplicación de la arquitectura SaaS.

1) **Módulo de Servicio:** la ejecución de la lógica de negocio específico que se logra mediante la tecnología de desarrollo de servicios Web es apropiado, ya que durante el desarrollo, patrones de diseño pueden ser usados para construir programas de servicio relevantes y las demandas personalizadas se pueden satisfacer mediante el uso de clases de interfaz. En relación a esto, el módulo lógico universal es responsable de la ejecución de la lógica de negocio por defecto para todos los inquilinos, mientras que el módulo lógico extendido está a cargo de la implementación de la lógica de negocio personalizado.

**2) Módulo de proceso:** el uso de la tecnología asociada con BPEL según [71] este se ha establecido como el estándar para el modelado de procesos de negocio mediante la orquestación de servicios Web, se utiliza este estándar para llevar a cabo la disposición y la personalización de los procesos. El servidor de BPEL es responsable del funcionamiento de las instancias de proceso y llamar a los servicios correspondientes.

**3) Módulo de interfaz de usuario:** esta parte proporciona una interfaz de procesos relativamente sencilla para transformar el formulario de la descripción del negocio de usuarios en la descripción del proceso BPEL estándar.

Con el modelo de personalización de la capa de aplicación SaaS, los procesos de negocio universal pueden ser definidos por el usuario y transformados en procesos BPEL ejecutables, y las funciones específicas se pueden realizar mediante la ejecución de instancias BPEL que se implementan en el servidor de aplicaciones para llamar a los Servicios Web relevantes.

#### **b. Capa de plataforma**

Esta capa incluye las políticas de asignación y programación para la traducción de Calidad de Servicio (QoS) de los requisitos del cliente, a los parámetros a nivel de infraestructura, y la asignación de máquinas virtuales (VM) para servir a sus peticiones.

En la Figura 14 se muestra la capa de plataforma en la que están contenidas las políticas de asignación y programación.

En [72] define a un algoritmo de asignación de recursos como una política que desea minimizar el coste de la infraestructura y violaciones SLA, las políticas a las que recurre la capa de aplicación para el mapeo y la programación se las utiliza con el fin de lograr la maximización del beneficio para el proveedor de SaaS a través del uso de varios proveedores de IaaS.

El algoritmo de programación se ejecuta en el proveedor de SaaS y determina qué proveedor de IaaS y el tipo de máquina virtual (VM) tiene que ser alquilado para ejecutar el flujo de trabajo con el fin de garantizar la calidad de servicio a clientes de SaaS.

Como segundo punto del flujo de trabajo en esta capa se toma la decisión, sobre que recursos se requiere para atender a la petición y cuál va a ser su asignación, se podría decir que aquí se desarrolla la lógica para el flujo de trabajo.

De acuerdo a la referencia [73] PaaS es uno de los patrones más importantes de servicio en la nube, proporciona una plataforma completa de desarrollo, despliegue y ejecución para aplicaciones SaaS.

#### **c. Capa de infraestructura**

Según [72] el proveedor de SaaS puede arrendar instancias de VM proporcionados por los proveedores de IaaS a través de dos tipos de contratos de SLA, el primer tipo es pedido, el cual tiene el mecanismo de operación de que el proveedor de SaaS alquilará máquinas virtuales sin compromisos a largo plazo y pagará sólo por la potencia de cálculo por unidad de tiempo. El segundo tipo es reservado, el proveedor de SaaS alquilará máquinas virtuales con un compromiso a largo plazo y pagará una cuota por adelantado para reservar cada máquina virtual. A su vez, el proveedor de SaaS recibe un descuento significativo en el cargo por uso en una unidad de tiempo para cada instancia reservada.

Como tercer paso del flujo de trabajo y de acuerdo a la decisión que se tomó en la capa mencionada anteriormente, esta nueva capa que interviene provee de los recursos ya asignados, es decir es el hardware necesario para atender la petición.

Esta capa controla la iniciación real y la eliminación de las máquinas virtuales. Las máquinas virtuales pueden ser arrendadas a proveedores de IaaS como Amazon EC2 o agrupaciones privadas virtuales, propiedad del proveedor de SaaS. En ambos casos, la reducción al mínimo del número de máquinas virtuales proporcionará ahorros.

La arquitectura típica del centro de datos de IaaS, se especifica en [74], en la cual los inquilinos compiten por los recursos informáticos compartidos en el centro de datos, tales como los recursos de red y almacenamiento. Además, la migración en vivo de máquinas virtuales afecta gravemente a los arrendatarios y al rendimiento de las aplicaciones que se ejecutan en máquinas virtuales.

Actualmente, los proveedores de SaaS como Compiere ERP proporcionan una máquina virtual individual para cada cliente para mantener los requisitos de nivel de servicio en términos de tiempo de respuesta y la capacidad.

Sin embargo, esto provoca el desperdicio de recursos de hardware que se traduce en altos costos de infraestructura ya que los clientes no pueden utilizar la capacidad completa de VM que está reservado para servir a sus peticiones. Un enfoque multi-alquiler puede reducir la infraestructura necesaria, pero se debe tener cuidado en proporcionar acceso a los recursos para que los acuerdos de nivel de servicio (SLA) no se violen.

Para terminar con este proceso, SaaS proporciona el acceso a la información, dando respuesta a la petición del usuario [67] [61] [65] [66] [75].

#### **6.1.6. Riesgos más destacados**

De lo expuesto por los autores Alexander Benlian y Thomas Hess [45], se ha recuperado de su trabajo investigativo los siguientes riesgos, la inseguridad de datos se contrasta con la referencia [76] como el principal riesgo a lo que están expuestas las organizaciones.

- Riesgos económicos, un cliente SaaS puede tener que pagar más para alcanzar el nivel esperado de servicio de lo inicialmente previsto, a estos rubros se los denomina costos ocultos, los clientes deben pagar más si desean acceder a nuevos servicios.
- Riesgos estratégicos, una empresa pierde el control de los recursos y capacidades críticos cuando se gestiona a través de aplicaciones SaaS, la disminución de la capacidad se debe a que el proveedor SaaS tiene el control total sobre el desarrollo de la aplicación y el mantenimiento.
- Riesgos de datos, cuando un cliente utiliza SaaS, algunos, o incluso la totalidad, de los datos de ese cliente se almacenarán en el centro de datos del proveedor de SaaS, los clientes SaaS dan un control directo a sus proveedor, sin saber exactamente cómo este proveedor asegura los datos y qué copia de seguridad y recuperación de desastres implementa. Los acuerdos de nivel de servicio se pueden utilizar para indicar los niveles de seguridad de datos exactos que deben mantenerse.

Sin embargo, los avances tecnológicos avanzan con tanta rapidez, que los clientes en su mayoría desconocen los riesgos de seguridad potenciales que surgen de flexibilidad contractual cuando firman contratos de servicios. Ambigüedades y vacíos en el contrato pueden provocar un comportamiento oportunista por parte del proveedor

- La externalización también puede afectar a los asuntos personales de los directivos responsables de la contratación externa de la aplicación, los riesgos de gestión denominados riesgos psicosociales, son la posibilidad de que la reputación profesional del gestor responsable de la aplicación se vea perjudicada ya que existen algunas inseguridades, falta de confianza y de costumbre por parte de la sociedad en cuanto al software que ofrece el proveedor de servicios externo. [45] [76]

#### **6.1.7. Oportunidades más destacadas**

Se ha recopilado información acerca de las circunstancia en la cual existe la posibilidad de lograr algún tipo de mejora de índole económica y competencia laboral para las empresas que hagan uso de SaaS, a continuación se exhibe algunas oportunidades que son las más relevantes y las que redundan en los artículos citados.

- La adopción de SaaS ofrece un alto grado de flexibilidad en cuanto a la utilización de los recursos de TI fácilmente escalables. Esta flexibilidad hace que sea más fácil para las empresas responder a la volatilidad a nivel de negocio, debido a que el proveedor de SaaS se encarga de las fluctuaciones en las cargas de trabajo. En este sentido, una empresa cliente puede aprovechar la capacidad de un proveedor de SaaS para adaptarse al cambio.
- La externalización permite a las empresas centrarse en su negocio principal, ya que pueden liberar recursos, que puede ser utilizado de manera más productiva en las zonas que crean valor, también facilita la reorientación de las empresas en sus competencias básicas, esta reorientación es posible desplazando por completo la responsabilidad de desarrollar, pruebas y mantenimiento de una aplicación software y la infraestructura subyacente. Este cambio no sólo aliviará a los gerentes la tarea de coordinar un gran departamento de ingeniería de software, sino que también eliminará los miembros del personal de apoyo a las actividades de rutina. El personal, entonces puede dedicar su tiempo a actividades más estratégicas, determinar cómo la empresa puede agregar valor al negocio.

- El acceso a los recursos de TI de última generación se ha demostrado que es uno de los principales indicadores del éxito, es un motor importante de las decisiones de externalización. Dado que el modelo de negocio SaaS se basa en una arquitectura de plataforma multiusuario, el proveedor se beneficia de las economías de escala mediante la consolidación y virtualización de sus centros de datos, los clientes de SaaS se benefician de las economías de habilidades mediante el aprovechamiento de los recursos y capacidades que ofrece el proveedor de servicios.
- Mejoras de calidad, es decir existe un aumento en la eficiencia y eficacia de los procesos de apoyo, mejores prácticas de la industria y los procedimientos de gestión total de la calidad [45] [46] [77] [78].

#### **6.1.8. Ventajas de SaaS**

Según [55] [59] las principales ventajas de SaaS son: reducción de los costes iniciales, el tiempo más rápido para la implementación de aplicaciones, eliminación de mantenimiento de software, servicio y soporte, aplicaciones alojadas de forma remota, capacidad de configuración de cliente, actualizaciones instantáneas, atractivo retorno de la inversión, no hay necesidad de personal adicional y la fijación de precios basada en el uso.

A continuación se presenta una lista de las ventajas que ofrece SaaS, lo cual hace de este modelo una alternativa útil para las organizaciones.

- Almacena datos en formatos de código abierto por lo que si una empresa cierra por cualquier razón, se mantienen los datos, la meta fundamental de los formatos abiertos es garantizar el acceso a largo plazo a los datos almacenados sin necesidad de preocuparse por la incertidumbre respecto a los derechos legales.
- Contratos con proveedores de SaaS que cubre los datos, copia de seguridad, emergencias imprevistas, derechos de licencia, mejoras y los costos de mantenimiento bien planificado con el fin de controlar el coste total de propiedad y minimizar los excesos de costes.

- La seguridad ofrecida por los proveedores de servicios de renombre es de mayor confianza en relación a las medidas de seguridad de la propia empresa.
- Las empresas que utilizan SaaS están en una ventaja significativa frente a sus competidores, ya que cambian sus estructuras internas de TI haciendo que sea menos costoso y los recursos humanos son utilizados para apoyar sus competencias básicas.
- No hay una tarifa de licencia adicional para nuevas versiones y la complejidad de la transición a las nuevas versiones es manejado por los proveedores de SaaS.
- Promete ayudar a reducir los costos más predecibles, el consumidor tiene la oportunidad de desplazar la carga de parches, la modernización, la adición de nuevos servicios, y garantizar la disponibilidad de un proveedor de servicios fuera de las instalaciones. Anualizando costos a través de un contrato de servicios, gerentes de negocios pueden centrar su atención en el crecimiento y desarrollo de la propia actividad principal.
- Mediante el uso de SaaS, los proveedores pueden amortizar el costo del hardware, software y experiencia empresarial, así como otros recursos, a través de múltiples consumidores de servicios. En particular, el modelo de alojamiento multi-alquiler hace posible la creación de la eficiencia del negocio al compartir los recursos entre múltiples servicios a los consumidores.
- Tanto los consumidores como los proveedores tienen interés mutuo en asegurar que los servicios SaaS pueden cumplir con los requisitos de escalabilidad, disponibilidad y rendimiento.
- Las aplicaciones SaaS son fáciles de usar no requieren más que un navegador web.
- SaaS hace que sea asequible para las pequeñas empresas ya que cuenta con pagos según un modelo de precios.
- Para satisfacer la demanda de los consumidores, la aplicación SaaS se puede escalar fácilmente hacia arriba o hacia abajo, los consumidores no tienen que preocuparse por la infraestructura de cálculo adicional.

- Las aplicaciones SaaS son menos torpe, en comparación con las aplicaciones tradicionales. No requieren de los usuarios para instalar/desinstalar código binario en sus máquinas.
- Las aplicaciones SaaS son capaces de funcionar en una amplia variedad de dispositivos, debido a la naturaleza de entrega de SaaS a través de internet.
- Mejor colaboración entre equipos ya que los datos se almacenan en una ubicación central.
- Evita los cambios de software frecuente y bajo demanda.
- Se le permite al cliente completa flexibilidad en el uso de los sistemas operativos de su preferencia, o al cual pueda tener acceso [55] [59] [53] [78] [79] [65] [80] [81].

#### **6.1.9. Desventajas de SaaS**

Las desventajas en las que se ve involucrada esta arquitectura, se da más por deficiencias en las herramientas colaborativas para el funcionamiento de SaaS, consiguientemente se muestran las desventajas de este modelo:

- Debido a las limitaciones del navegador, SaaS puede no ser tan robusta como aplicaciones de software tradicionales.
- Requiere de una conexión a Internet ya que SaaS (como una aplicación en línea) tendrá que cargar todo en el navegador. La función esperada ni siquiera podría avanzar sin conectividad a Internet.
- Tener todos los datos de un usuario en la nube plantea problemas de seguridad y privacidad, los proveedores de SaaS suelen ser el blanco de explotación de hackers.
- Una amplia gama de clientes dependientes podría verse afectada, en el raro caso de que a un proveedor SaaS se le dé la baja.

- Depende de la modalidad del contrato de servicios que tenga con la compañía para que el usuario tenga acceso al programa, y puede realizar modificaciones.
- Si el servicio de Internet no está disponible por parte del ISP, el usuario no tendrá acceso al programa, por lo que sus operaciones se verán afectadas hasta que el servicio se restablezca [51] [53] [80] [81].

#### **6.1.10. Aspectos compartidos entre el Software tradicional y SaaS**

De acuerdo a [59] [79] las características que definen, una aplicación dentro de las instalaciones y una aplicación SaaS están graduadas en tres dimensiones diferentes: cómo obtiene su licencia de software, donde se encuentra, y cómo se gestiona, con el software tradicional en las instalaciones en un extremo y SaaS en el otro. Sin embargo hay opciones adicionales que combinan aspectos de ambos.

*Tabla 7 Aspectos compartidos entre el Software tradicional y SaaS*

Aspectos compartidos entre el Software tradicional y SaaS		
Licencias	Instalación	Gestión
Las aplicaciones On-premise (aplicaciones locales) normalmente tienen licencia a perpetuidad, con un solo costo inicial para cada usuario o sitio, o (en el caso de aplicaciones personalizadas) propiedad pura y simple. Las aplicaciones SaaS a menudo tienen	Las aplicaciones SaaS están instaladas en las disposiciones del proveedor de alojamiento SaaS, mientras que las aplicaciones en las instalaciones son instaladas dentro de su propio entorno de TI.	Tradicionalmente, el departamento de TI es responsable de proporcionar servicios a los usuarios, lo que significa estar familiarizado con la red, servidores y plataformas de aplicaciones; la prestación de apoyo y resolución de problemas; y resolver los problemas de TI de seguridad, fiabilidad, rendimiento y disponibilidad. Este es un gran trabajo, y algunos departamentos de TI subcontratar algunas de estas responsabilidades de gestión a los proveedores de servicios de terceros que se especializan en la gestión de TI. En el otro extremo del espectro, las aplicaciones SaaS están

licencia con un modelo de transacción basada en el uso, en el que el cliente sólo se factura por el número de transacciones de servicios utilizados.		completamente manejados por el vendedor o proveedor de alojamiento SaaS; de hecho, la ejecución de las tareas y responsabilidades de gestión es opaca para el consumidor. Acuerdos de nivel de servicio (SLA) regulan los compromisos de calidad, disponibilidad y apoyo que el prestador ofrece.
--	--	---

#### 6.1.11. Estimaciones de costos entre el Software tradicional y SaaS

Poniendo como referencias la investigación realizada por los autores de la referencia [82], se presenta las estimaciones de costos realizando un contraste con el software tradicional y SaaS.

En la Figura 15 se muestra el modelo de costos en los que se incurre al utilizar el software tradicional y en la Figura 16 se presenta el modelo de costos en los que se incide al recurrir a SaaS.

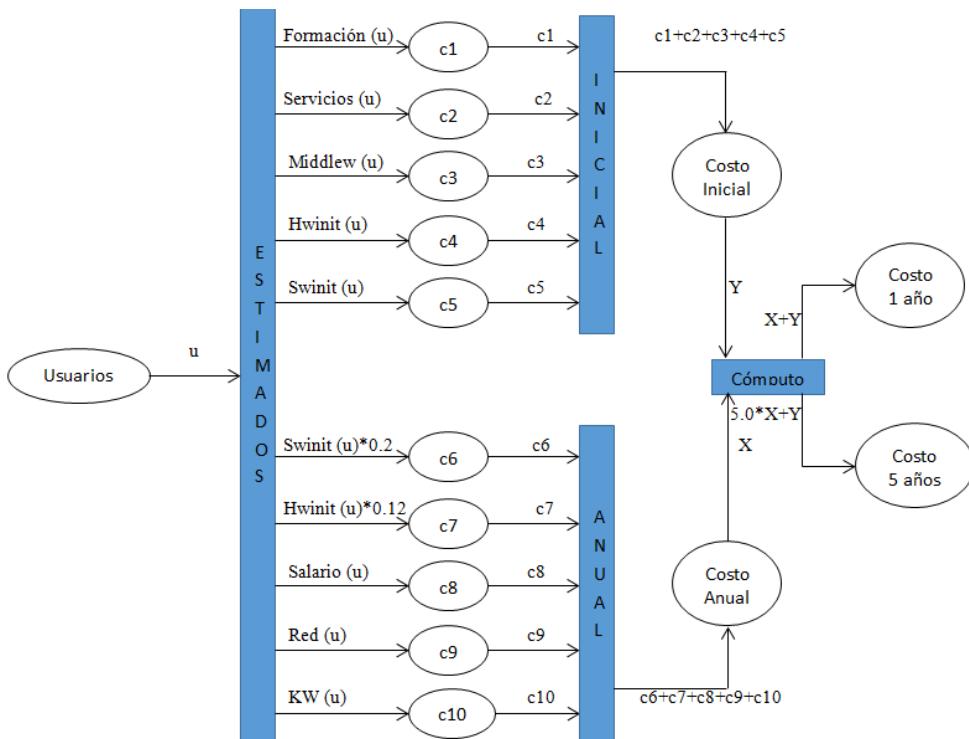
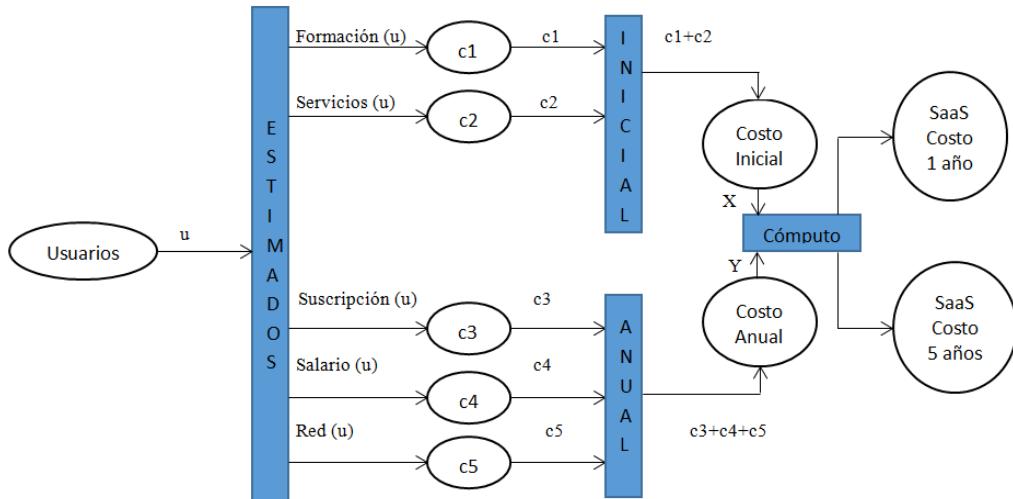


Figura 15 Modelo de costos locales

Las estimaciones de costos para SaaS pueden variar mucho, dependiendo de la aplicación, el tamaño de la empresa, así como la complejidad de los procesos de negocio.



*Figura 16 Modelo de costos SaaS*

Los usuarios representan el número de usuarios del software, es la información básica para alguien con el tamaño del hardware necesario y para adquirir las licencias de software necesarias, además de ser capaz de estimar los gastos de servicios públicos anuales, como la energía y el acceso a Internet.

La transición estimaciones valorará los costos, utilizando funciones escalonadas en función del número de usuarios, y almacenar valores en lugares como se describe en la Tabla 8, aquí se especificará los costos iniciales, y en la Tabla 9 se detallará los costos en lo que se incurre anualmente.

*Tabla 8. Estimaciones de costos iniciales*

Costo	Descripción de costo	Código de costo
<b>Formación</b>	Los costos para la formación inicial y los esfuerzos necesarios para los usuarios de aplicaciones y el personal de TI.	c1
<b>Servicios</b>	Los costos para la personalización e integración.	c2

<b>Middlew</b>	Costo de licencias para el middleware necesario para ejecutar la aplicación, el sistema operativo y los servidores de base.	c3
<b>Hwinit</b>	Los gastos iniciales para la adquisición de hardware.	c4
<b>Swinit</b>	Los costos de licencias de software de aplicación	c5

*Tabla 9. Estimaciones de costos anuales*

Función	Descripción	Código de costo
<b>Swinit * 0.2</b>	Porcentaje de los gastos de adquisición de software por adelantado estima para el mantenimiento anual.	c6
<b>Hwinit * 0.12</b>	Porcentaje de los costos de licencias de hardware calcula para el mantenimiento anual.	c7
<b>Salario</b>	Los costos anuales de salarios del personal de TI necesarios para ejecutar la aplicación y su correspondiente infraestructura.	c8
<b>Red</b>	Los costos anuales de conectividad de red necesarios para ejecutar la aplicación.	c9
<b>KW</b>	Los costos anuales de energía para la infraestructura necesaria para ejecutar la aplicación.	c10

La transición inicial es directamente proporcional a la suma de todos los gastos iniciales almacenados en los códigos de costos C1, C2, C3, C4 y C5, con el fin de calcular el costo inicial en cuanto a las instalaciones y almacenará el valor calculado en la variable costo inicial.

Del mismo modo, en la transición anual, se agruparán todos los costos anuales almacenados en los códigos de costos C6, C7, C8, C9 y C10 y guardará el valor calculado en la variable costo anual.

Tenga en cuenta que los costes C6 y C7 son un porcentaje de los costos iniciales para la adquisición de hardware y software.

Por último, la transición calcular añadirá costos acumulados en las variables, costo inicial y costo anual, para el primer año y durante 5 años, y almacenará los valores calculados en los lugares, costo 1 año y costo 5 años, respectivamente.

El modelo de costos de SaaS es diferente, como se puede observar en la Figura 16, las transiciones son conservadas; usuarios representa el número de usuarios del software, estimaciones, inicial, anual y calcular igualmente son transiciones para computarizar costos. Sin embargo, estos utilizan diferentes funciones escalonadas, ya que los valores pueden ser diferentes.

No existen funciones de hardware inicial, software y adquisición de middleware. En su lugar, hay una función de suscripción que calcula la cuota anual que se cobra por el servicio en la nube SaaS, que proporciona acceso al software de la aplicación a través de Internet, el valor calculado se almacena en c3.

La transición inicial añade los costes iniciales almacenados en C1 y C2 para calcular los costes iniciales de SaaS, y guarda el valor calculado en la variable costo inicial.

La transición anual, amplía todos los costos anuales almacenados en C3, C4 y C5 para calcular el costo anual de SaaS, y almacena el valor calculado en costo anual.

La transición calcular, añade costes iniciales almacenados en las variables costo inicial y costo anual para el primer año y durante 5 años, almacenados respectivamente en las variables SaaS costo 1 año y SaaS costo 5 años.

#### **6.1.12. Factores de SaaS**

No hay duda que SaaS facilita la entrega de software y los precios en la nube se están convirtiendo en nuevas plataformas para el cómputo empresarial y personal, los factores que se detallan a continuación son los requisitos no funcionales con los que todo software debería cumplir para que sea considerado como un producto de calidad y confiable, estos son cumplidos por el modelo en estudio.

*Tabla 10 Requisitos no funcionales de SaaS*

Requisitos no funcionales SaaS	
<b>Integración</b>	Incluye la capacidad de un producto para la integrarse con otras aplicaciones, es muy relevante para los productos SaaS, ya que están alojados fuera y por lo tanto pueden ser percibidas como difíciles de integrar con los sistemas heredados en las instalaciones [83] [84] [85].
<b>Escalabilidad</b>	Se refiere a la capacidad del producto SaaS para mantener el tiempo de respuesta razonable para los usuarios, incluso durante la carga pico [83] [84] [85].
<b>Fiabilidad</b>	Se refiere a la capacidad del producto SaaS de permanecer disponible para todos los usuarios en tiempo dado. Se requiere personal para implementar el monitoreo y herramientas de diagnóstico [83] [84] [85].
<b>Seguridad</b>	Se considera que es la principal preocupación de los productos SaaS. Es un proveedor que tiene certificaciones como la ISO 27000 que ayuda a garantizar la seguridad adoptada para la manipulación de los datos del cliente [83] [84] [85].

#### **6.1.13. Dos vistas de SaaS**

Seguidamente se da a conocer dos puntos de vista del modelo SaaS, el primera es acerca del modelo de negocio de esta arquitectura, como ya se ha mencionado presta servicios según se establezca en el contrato entre el proveedor y el cliente, pagando únicamente por los servicios y el tiempo que consume, el segundo trata sobre las funcionalidades que presta el producto ofrecido por el proveedor.

#### **Vista de negocios de SaaS**

SaaS adoptó una arquitectura multi-servicios, es decir, un conjunto de equipos de hardware estándar y el sistema de software que podría proporcionar servicios para muchos clientes diferentes al mismo tiempo, los proveedores de software proporcionan las aplicaciones de Internet y las operaciones fuera de la línea de venta de software y almacenamiento de datos local, los clientes arriendan cierto tipo de servicios de software para la gestión de sus actividades comerciales sin necesidad de inversión para el hardware, software a medida, excepto computadora personal y hardware de conexión a Internet.

El modelo SaaS pone el acento en los servicios y presta mucha atención a la personalización de la aplicación de software.

Las aplicaciones SaaS se pagan de acuerdo al número de funciones de software alquilado o la longitud de tiempo utilizada por los clientes, que eligen estas funciones o el tiempo utilizado para satisfacer sus necesidades reales.

SaaS sigue con interés en grandes cantidades a pequeñas y medianas empresas; el modelo SaaS puede reducir la compra y mantener los costes de infraestructura y aplicaciones.

#### **Vista Técnica de SaaS**

La capa de la tecnología de servicios incluye la descripción del servicio, el descubrimiento de servicios, la negociación del servicio, la prestación de servicios, la composición de servicios, que manejan la personalización del usuario, la escalabilidad y la eficiencia multi-usuario y la conexión de aplicaciones SaaS proporcionados por los proveedores.

Los proveedores SaaS utilizan multi-servicio para reducir los costos de mantenimiento y actualización. Los clientes pueden utilizar cierta tecnología para definir el flujo de trabajo y el flujo de aprobación y ampliar la aplicación sin conocimientos de programación, de acuerdo con la lógica de negocio de la compañía. [1] [64] [86]

#### **6.1.14. Ciclo de vida de SaaS**

SaaS tiene un ciclo de vida diferente en comparación con un producto de software tradicional. Contrastando con [87] los escenarios como el análisis de requerimientos, desarrollo y pruebas siguen siendo muy fundamentales; sin embargo, se requieren nuevas actividades.

Seguidamente se muestra el ciclo de vida de SaaS, haciendo referencia a [88] encontramos la Figura 17 en la que se muestra el ciclo de vida.

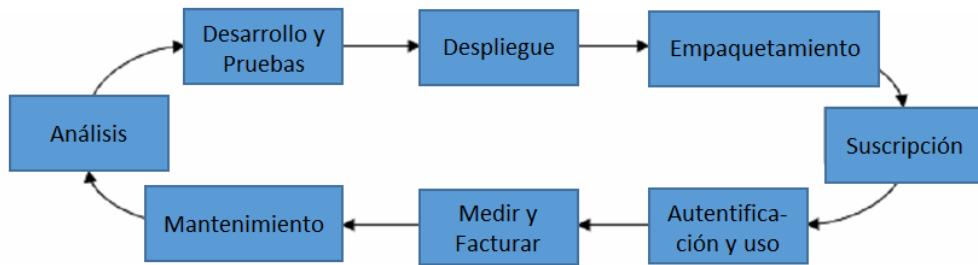


Figura 17 Ciclo de vida de SaaS

Después de que una aplicación de software ha sido desarrollada y desplegada, tiene que ser introducida en términos de negocio, aplicación de políticas de facturación, hasta que esté lista para la suscripción de un cliente, después de que un cliente ha contratado este servicio únicamente tiene que autenticarse y hacer uso del software, en caso de que el cliente requiera nuevas funcionalidades, será medido de acuerdo al modelo de suscripción y tendrá que facturar el nuevo valor. Finalmente en una de las etapas del ciclo de vida de SaaS, se proporciona el mantenimiento del software [51] [85] [87] [88].

## **6.2. Segundo objetivo específico: “Investigar acerca de la seguridad de datos en la nube, basándose específicamente en el modelo SaaS”.**

Se obtuvo como resultado producto de la investigación, un estado del arte del cual se derivó una nueva versión con la finalidad de enviarlo a las Jornadas de Ingeniería de Sistemas Informáticos y de Computación (JISIC), de la Escuela Politécnica Nacional (Véase Anexo 1).

El estado del arte que se realizó como entregable para dar cumplimiento a este objetivo es presentado a continuación, la versión corta enviada a las JISIC puede verse en el Anexo 2.

### **Estado del Arte “Vulnerabilidades de los datos en la arquitectura de Software como Servicio (SaaS)”**

Esther Elizabeth Jaramillo Malla

Área de Energía, las Industrias y los Recursos Naturales No Renovables

Universidad Nacional de Loja

Loja, Ecuador

[eejaramillom@unl.edu.ec](mailto:eejaramillom@unl.edu.ec)

30 de Julio de 2016

#### **6.2.1. Seguridad de datos**

En la actualidad los datos se han convertido en uno de los activos más importantes de las organizaciones de tal manera que estos se ven involucrados en diferentes amenazas como pérdida, robo, modificación entre otras vulnerabilidades por lo que deben mantenerse de forma segura.

Conforme a lo expuesto en [89], los autores realizaron una encuesta con el fin de obtener una imagen clara de los principales desafíos que rodean a SaaS recogieron y analizaron las aportaciones de los usuarios finales y expertos de la industria, la principal preocupación es la seguridad y privacidad de los datos, la cual en la tabulación obtuvo el porcentaje mayoritario.

A continuación se muestra los principales riesgos en la seguridad de datos a los que están expuestas las organizaciones que hacen uso de las aplicaciones SaaS.

**Tabla 11 Riesgos en la seguridad de datos SaaS**

<b>Violación de datos</b>	• Los datos sensibles o valiosos de una organización pueden estar bajo el control de los atacantes maliciosos o de los competidores [46] [47].
<b>Pérdida de datos</b>	• Existe la posibilidad de que los datos de una empresa desaparezcan sin dejar rastro [46] [47].
<b>Secuestro de credenciales</b>	• Un atacante con malas intenciones puede obtener acceso a las credenciales [46] [47].
<b>Interfaces y API inseguras</b>	• Los atacantes pueden descubrir vulnerabilidades dentro de las interfaces o en las interfaces gerente de API [46] [47].
<b>Negación de servicio</b>	• Ataques DOS (denegación de servicio) pueden hacer que los programas de la nube no estén disponibles, lo que podría ocasionar que un negocio llegue a un punto muerto [46] [47].
<b>Tecnología compartida</b>	• Una vulnerabilidad o mala configuración podría comprometer todos los datos alojados en la infraestructura compartida [46] [47].

Según [90], en el modelo SaaS, los datos residen en la base de datos que se encuentra fuera de los límites de la empresa y depende de las medidas de seguridad que utilice el proveedor para proteger los datos de una forma adecuada.

Por otro lado las organizaciones que hacen uso de SaaS no tienen idea de qué tan fuerte es el sistema de control de acceso para evitar el ingreso no autorizado. El canal de transmisión entre proveedores y usuarios de SaaS no siempre se considera seguro.

Según lo planteado en [91] afirma que los proveedores utilizan SSL (Secure Socket Layer) según [92], [93], es un estándar de facto para proporcionar transacciones de comercio electrónico seguras a través de la Web, es popular por permitir el cifrado del tráfico HTTP entre los sitios web y los navegadores, pero también ampliamente utilizado para otras aplicaciones, tales como las transferencias de mensajería instantánea y correo electrónico, estos proveedores utilizan este estándar durante la primera sesión de inicio, dejando sin protección los datos en las siguientes sesiones.

Además la copia de seguridad y recuperación de datos deben ser tomados en consideración por el proveedor de SaaS para minimizar el impacto de los accidentes.

Las propiedades básicas de seguridad de la información son CIAAN (confidencialidad, integridad, disponibilidad, autenticidad y no rechazo). Teniendo en cuenta que SaaS se ocupa de las aplicaciones, los datos y la información, un nivel similar de seguridad tiene que ser proporcionada por SaaS.

El concepto de seguridad de los datos en el entorno SaaS atraviesa varias áreas, que incluye confidencialidad de los datos, la disponibilidad de datos, integridad de los datos, los datos de autorización, copia de seguridad y recuperación de datos, transferencia de datos, etc.

En algunos casos los proveedores utilizan el testigo homomorphic, según [94] este es considerado como uno de los métodos prometedores para ser empleados en la red inteligente para proporcionar privacidad de los datos, la técnica de contadores homomorphic es altamente eficiente y resistente al fracaso bizantino, el ataque de modificación de datos maliciosos e incluso conspiración de servidores. [95]

El tema relacionado con la seguridad de los datos dentro de SaaS puede ser clasificado en cinco grupos, almacenamiento de datos, control de acceso, backup y recuperación de datos, integridad de datos y seguridad de transferencia de los mismos.

### **6.2.2. Acuerdo de Nivel de Servicios SLA**

La tecnología de la computación en nube se enfrenta a retos como, proporcionar seguridad e integridad de los datos sensibles que se está transmitiendo [96], es por ello que existen los denominados SLA, este es un acuerdo o un vínculo jurídico entre el proveedor y las instituciones en el contexto de la prestación de un servicio en particular [97] [98] [99], cabe señalar que se generaliza como computación en la nube ya que SLA es un acuerdo que captura las garantías acordadas entre un proveedor de servicios y su cliente, en lo que respecta a proveedor de servicios, este acuerdo es válido para las arquitecturas SaaS, PaaS e IaaS de la nube.

Los SLA se han convertido en una parte importante del modelo de prestación de servicios de la nube [100], los clientes y los proveedores de SaaS deben establecer un

SLA para definir la calidad de servicio (QoS) [101], es un enfoque para especificar y administrar la seguridad, esta es rara vez considerada ya que es diferente de otros atributos como la calidad de servicio, rendimiento y fiabilidad [102], sin embargo SLA abarca aspectos relacionados con la seguridad de los datos.

De acuerdo al artículo de los autores Kandukuri, Balachandra, Ramakrishna, Rakshit, Atanu [103] mencionan que, SLA tiene que discutir cómo se manejan los siguientes riesgos de seguridad:

*Tabla 12 Riesgos de seguridad establecidos en SLA*

#### **6.2.2.1. Acceso de usuarios privilegiados**

Procesar los datos sensibles fuera de la empresa trae consigo un nivel de riesgo inherente, ya que los servicios externalizados evitan los controles físicos, lógicos y de personal de tecnología de información (TI) del cliente, se podría decir que el cliente no tiene el control de los datos porque están en manos de un proveedor de servicios, se debería obtener la mayor información posible acerca de las personas que manejan nuestros datos y no hacer uso de estos servicios por una necesidad y dejar de lado los riesgos a los que se están exponiendo, en el contrato se debe especificar los términos y condiciones no solo del proveedor sino incluir los del cliente también.

Pedir a los proveedores suministrar información específica sobre la contratación y supervisión de los administradores privilegiados, y sobre los controles de acceso realizados [104] [105].

#### **6.2.2.2. Cumplimiento de la normativa**

Los clientes son en última instancia, responsables de la seguridad e integridad de sus propios datos, incluso cuando está en manos de un proveedor de servicios. Los proveedores de servicios tradicionales son sometidos a auditorías y certificaciones de seguridad externas pero algunos de estos proveedores se niegan a someterse a este escrutinio, se debería observar detenidamente ya que están dando señales de que sólo pueden ser utilizados para las funciones más triviales o de poca significancia real, ya que si no permiten que se les realice una auditoría está claramente definido que no son confiables, es por ello que antes de contratar este servicio se debe realizar un análisis previo a los términos y condiciones que los proveedores nos proporcionan, además es fundamental conocer acerca de la reputación de los mismos.

#### **6.2.2.3. Ubicación de los datos**

Los usuarios finales al utilizar los servicios proporcionados por los proveedores de la nube, no conocen la ubicación de los recursos de almacenamiento de datos [106], el consumidor no sabe exactamente dónde se encuentran alojados los datos [90]. De hecho, ni siquiera se sabe en qué país se almacenará. Los proveedores deberían comprometerse con el almacenamiento y procesamiento de datos en jurisdicciones específicas, y realizar un compromiso contractual para obedecer los requisitos de privacidad locales en nombre de sus clientes [104] [105].

#### **6.2.2.4. Recuperación de los datos**

Incluso si no se sabe dónde están incrustados los datos, el proveedor debe manifestar lo que ocurrirá con los datos y el servicio de recuperación de datos en caso de un desastre. Cualquier oferta que no se replica en la infraestructura de datos y aplicaciones a través de múltiples sitios es vulnerable a un fracaso total. El cliente tendrá que asegurarse, si el proveedor tiene la capacidad de hacer una restauración completa, y cuánto tiempo tomará en realizar dicha actividad [104] [105].

#### **6.2.2.5. Viabilidad a largo plazo**

Idealmente, el proveedor nunca irá a la quiebra o será adquirida por otra gran empresa. Pero se deberá considerar esta posibilidad y asegurar que los datos estarán disponibles incluso después de tal evento. Pedir a los proveedores que nos hagan conocer cómo se recuperan los datos; si estos son entregados a la nueva empresa propietaria o son entregados en primera instancia al cliente, además se debe tener en cuenta que los datos recuperados sean entregados en un formato en el que permita importar a una aplicación de reemplazo [104] [105].

### **6.2.3. Factores de riesgo en la seguridad de datos en SaaS**

A continuación se pone a consideración lo que podría ocurrir si la seguridad de los datos no está completamente garantizada por el proveedor de SaaS, se debería pedir al proveedor de este servicio que por lo menos nos ponga al tanto de cómo se realiza la gestión para subsanar los riesgos expuestos posteriormente, para saber a qué atenerse en caso de que suceda.

#### **6.2.3.1. Almacenamiento de datos**

El requisito fundamental es que el proveedor de SaaS mantenga múltiples usuarios sin que unos vean los datos de otros, debido a esto existe un alto riesgo que los datos alojados en otra instancia pero en el mismo servidor se vean comprometidos también.

Con la finalidad de asegurar que los datos tengan una alta disponibilidad, redundancia y copia de seguridad, el proveedor de servicios se ve en la necesidad de duplicar los datos y almacenarlos en otros países. Tiene un alto grado de riesgo que la información sensible sea filtrada a partes inesperadas, los datos en otra ubicación pueden viajar a través de fronteras. Sin embargo, en algunos países, la ley establece que cierto tipo de datos sensibles no se les permite cruzar la frontera, y en tiempos de emergencia el gobierno tiene el derecho de invocar el sistema de registro para comprobar la entrada y salida de tráfico, esto es considerado como una gran amenaza a la confidencialidad de los datos de los usuarios.

Del mismo modo, cuando los usuarios toman la decisión de ya no emplear SaaS, se supone que los datos de los usuarios deben ser completamente destruidos y que no puedan ser recuperados por ningún medio. No obstante, el medio ambiente SaaS complica este panorama porque como se mencionó anteriormente, los datos de los usuarios podrían ser replicados en varias partes del mundo, afirmando que se hace esto para mantener la disponibilidad, redundancia o la copia de seguridad. No hay garantía de que todos los archivos sean eliminados, se puede encontrar múltiples copias de datos por el almacenamiento en múltiples ubicaciones.

Puede suceder que algunos discos de copia de seguridad o de otros medios de comunicación se dejan olvidados en algún lugar que no están conectados con el medio ambiente de SaaS, por lo que se podría deducir que los métodos tradicionales tales como la destrucción física resulta ser obsoleta en la plataforma SaaS.

Para protegerse contra la pérdida ocasional de datos, el proveedor de SaaS adopta cifrado de datos siendo considerada como una buena solución a este problema [62], según [107] este método se refiere a los cálculos matemáticos y algoritmo que convierte el texto sin formato a texto cifrado, que no pueda ser leída por usuarios no autorizados, este es utilizado con el fin de mejorar la confidencialidad de los datos alojados en la base de datos. Sin embargo, las técnicas de cifrado tienen su propio conjunto de

desafíos, incluyendo la gestión de claves, el uso correcto de los algoritmos de criptografía y las bibliotecas.

La siguiente Figura muestra de forma resumida el factor de riesgo analizado:



Figura 18 Factor de riesgo "Almacenamiento de datos"

#### **6.2.3.2. Control de acceso a los datos**

La violación de la seguridad o la privacidad puede venir del socio de confianza en el interior, donde por negligencia o por alguna otra razón, causan la pérdida o fuga de datos, también puede originarse a partir de los atacantes maliciosos externos que tengan la intención de explotar la debilidad del sistema y beneficios de la misma.

En este caso, el proveedor debe garantizar que el acceso a los datos sólo se limitará a personal con autorización de acceso mediante el control de quién puede acceder a qué tipo de información en la base de datos.

Por lo general, el control de acceso de base de datos está establecido por los administradores autorizados a través de la consola del sistema de gestión de base de datos segura o interfaz.

Algunas veces la empresa cliente para que sus datos estén seguros solicita que el proveedor permita a la empresa adherir a la aplicación SaaS sus propias políticas de acceso, por lo tanto, los proveedores de SaaS deben ser capaces de incorporar estas políticas específicas en sus propios ajustes de control de acceso, en caso que el cliente logre que los datos estén protegidos con sus políticas particulares de acceso, el proveedor se verá libre de toda responsabilidad, ya que el cliente tendrá esta competencia a su cargo, sin embargo debe ser considerado que los usuarios no tienen las instalaciones al nivel de seguridad de SaaS.

La siguiente Figura muestra de forma resumida el factor de riesgo analizado:

## CONTROL DE ACCESO A LOS DATOS

**La violación de la seguridad o la privacidad puede originarse a partir de los atacantes maliciosos que tienen la intención de explotar la debilidad del sistema y beneficios de la misma.**



El proveedor debe garantizar que el acceso a los datos sólo se limitará a personal con autorización de acceso, mediante el control de quién puede acceder a qué tipo de información en la base de datos.



Por lo general, el control de acceso de base de datos está establecido por los administradores a través de la consola del sistema de gestión de base de datos segura o interfaz.



**¡IMPORTANTE!**

Para que la empresa cliente sienta que sus datos están seguros el proveedor de estos servicios debería dejar que las empresas adhieran a la aplicación SaaS sus propias políticas de acceso, por lo tanto, los proveedores de SaaS deben ser capaces de incorporar estas políticas específicas en sus propios ajustes de control de acceso, en caso que el cliente logre que los datos estén protegidos con sus políticas particulares de acceso, el proveedor se verá libre de toda responsabilidad, ya que el cliente tendrá esta competencia a su cargo, sin embargo debe ser considerado que los usuarios no tienen las instalaciones al nivel de seguridad de SaaS.

*Figura 19 Factor de riesgo "Control de acceso a los datos"*

### 6.2.3.3. Copia de seguridad y recuperación de datos

La corrupción de datos, fallos de hardware y fallas en los datos es posible en una base de datos, los clientes de SaaS son totalmente dependientes de los proveedores de este modelo para realizar la copia de seguridad y recuperación de datos, será devastador para los clientes sufrir una pérdida de datos ya que esto se ve reflejado en la pérdida de ingresos de retorno, la responsabilidad de asegurarse que cuando se produce un accidente estén disponibles algunas contramedidas para llevar la base de datos al estado anterior y minimizar el impacto del accidente, recae sobre los proveedores de SaaS.

La siguiente Figura muestra de forma resumida el factor de riesgo analizado:



Figura 20 Factor de riesgo "Control de seguridad y recuperación de datos"

#### 6.2.3.4. Integridad de los datos

Según [90] la integridad de los datos es uno de los elementos más críticos en cualquier sistema, significa proteger los datos contra accesos no autorizados, eliminación y modificación por parte de un intruso y da la seguridad para garantizar la transmisión de datos desde el origen al destino, refiriéndose a mantener y garantizar la exactitud y consistencia de datos a través de todo su ciclo de vida. La integridad de los datos puede verse comprometida por errores humanos cuando son introducidos en la base de datos o cuando los datos se migran de forma inapropiada de un servidor a otro. Los errores de software, hardware, virus y los desastres naturales pueden afectar el compromiso de mantener la integridad de los datos.

El proveedor de servicios debe asegurar que los datos se transmiten en un sistema seguro y que los datos son reales, el sistema de transacción de datos debe seguir ACID (atomicidad, coherencia, aislamiento y durabilidad) son propiedades para asegurar la integridad de los datos. La mayor parte de la base de datos utiliza las propiedades ACID para asegurar la transacción de datos y mantener la integridad de los mismos.

La siguiente Figura muestra de forma

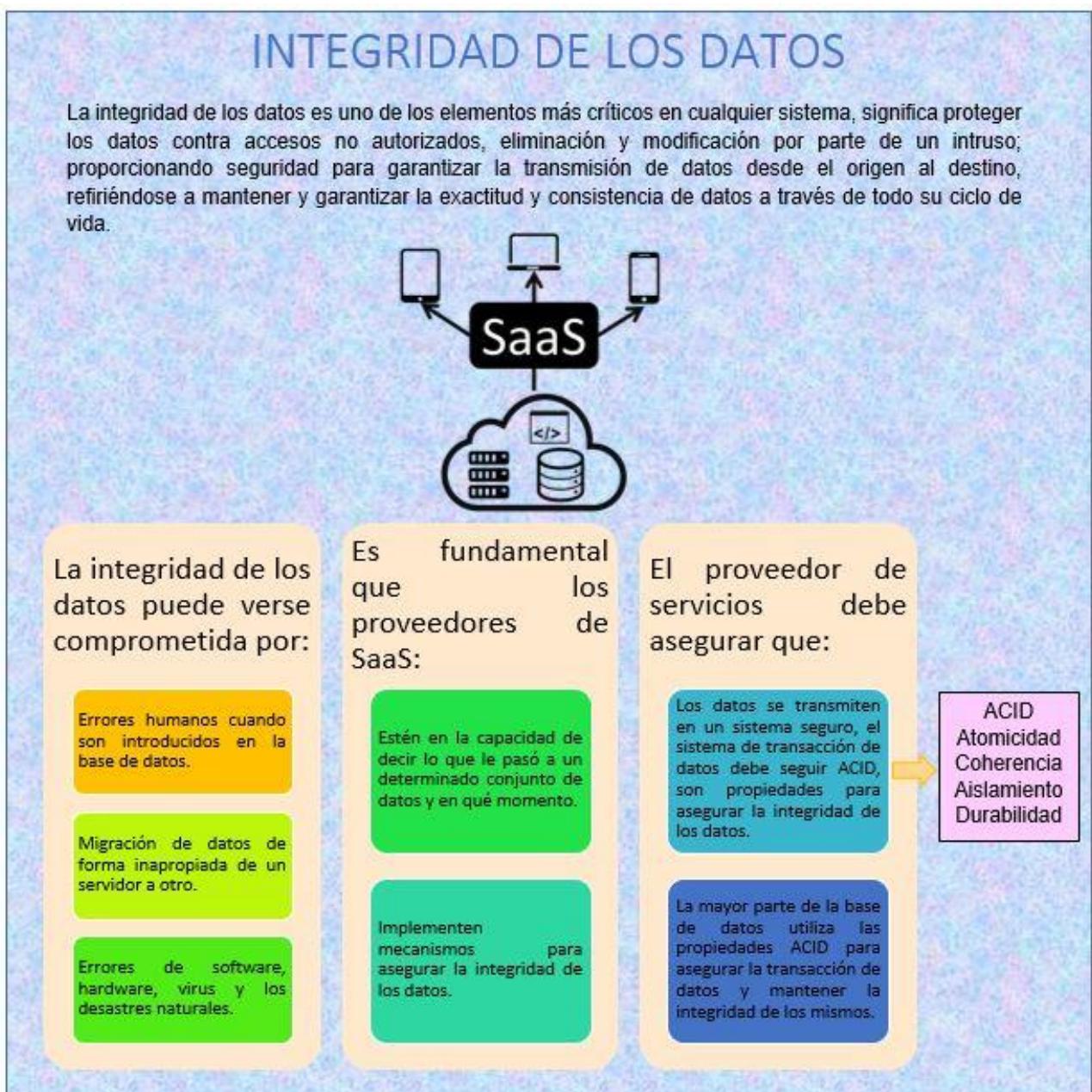


Figura 21 Factor de riesgo "Integridad de los datos"

#### **6.2.3.5. Transferencia de datos**

El canal de transmisión que se establece entre los proveedores de SaaS y los usuarios no siempre se considera seguro en el entorno SaaS.

Los datos se transmiten en un gran número de paquetes y fluyen a través de numerosos dispositivos de otras infraestructuras antes de llegar al destino.

Por lo tanto el proceso de transmisión del flujo de datos puede estar sujeto a las amenazas de la red, tales como ataque DNS, ataque MITM (man-in-the-middle), suplantación de IP, escaneo de puertos y ataques sniffer.

El proceso de transmisión de datos, incluye la parte remitente y la parte de recepción, por lo que la identidad de verificación entre ellos se convierte en esencial y deben asegurar que los datos transferidos no han sido modificados por un tercero.

Los riesgos de seguridad para los datos en tránsito han aumentado debido al espionaje, se lleva a cabo con sigilo esta tarea y es difícil de detectar que la red ha sido víctima de espionaje por los piratas informáticos.

Los atacantes pueden hacer uso de espionaje para interceptar la sesión TCP, luego los atacantes pueden buscar el número de secuencia de las comunicaciones en curso y forjar un segmento falso con una carga maliciosa o hacerse pasar como la dirección IP del remitente para hacer el acto aún más malicioso [108] [109].

La siguiente Figura muestra de forma resumida el factor de riesgo analizado:

## TRANSFERENCIA DE DATOS

Los datos se transmiten en un gran número de paquetes y fluyen a través de numerosos dispositivos de otras infraestructuras antes de llegar al destino. Por lo tanto el proceso de transmisión del flujo de datos puede estar sujeto a las amenazas de la red.



El canal de transmisión que se establece entre el proveedor de SaaS y los usuarios no siempre se considera seguro en el entorno SaaS.

Durante el procedimiento de transmisión, los datos de comunicación de las partes siempre incluye la parte remitente y la parte de recepción, por lo que la identidad de verificación entre ellos se convierte en esencial y deben asegurar que los datos transferidos no han sido modificados por un tercero.

Los riesgos de seguridad para los datos en tránsito han aumentado debido al espionaje, se lleva a cabo con sigilo esta tarea y es difícil de detectar que la red ha sido víctima de espionaje por los piratas informáticos.

Los atacantes pueden hacer uso de espionaje para interceptar la sesión TCP, luego los atacantes pueden buscar el número de secuencia de las comunicaciones en curso y forjar un segmento falso con una carga maliciosa o hacerse pasar como la dirección IP del remitente para hacer el acto aún más malicioso.

Figura 22 Factor de riesgo "Transferencia de datos"

### 6.2.4. Vulnerabilidades en la seguridad de datos y recomendaciones para mitigar estas vulnerabilidades

Los datos son susceptibles a amenazas como: la fuga de datos, modificación, privacidad de los usuarios, confidencialidad, entre otros. A continuación se manifiesta los principales problemas y la manera eficiente para hacer frente a estas vulnerabilidades de seguridad.

#### 6.2.4.1. Esquema de Base de Datos

Existen tres esquemas de base de datos para la gestión de datos Multi-Tenant, los mismos son:

Base de datos independientes e instancias de base de datos independientes (IDII)

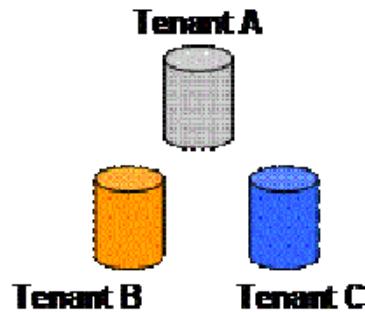


Figura 23 Esquemas de base de datos IDII

Tablas independientes e instancias de base de datos compartidos (ITSI)

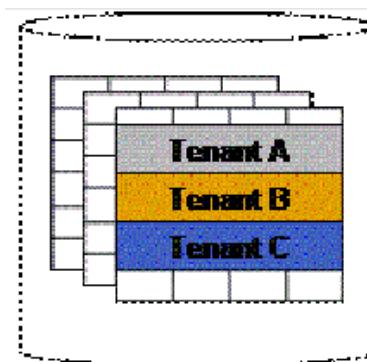


Figura 24 Esquemas de base de datos ITSI

Tablas compartidas e instancias de base de datos compartidos (STSI) [110].

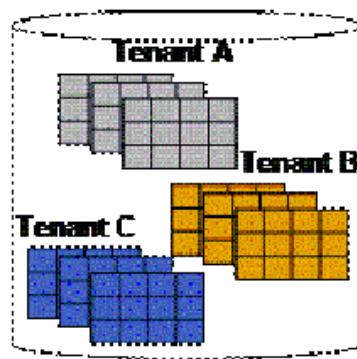


Figura 25 Esquemas de base de datos STSI

El esquema que es catalogado como el más seguro pero el más costoso, es IDII [110] [111], en este esquema existe para el almacenamiento una base de datos (BD) para cada inquilino, este es el método más sencillo para proporcionar un buen aislamiento y seguridad de datos [112], sería ideal que un proveedor de servicios ofrezca este esquema de BD.

#### 6.2.4.2. Servidor no autorizado

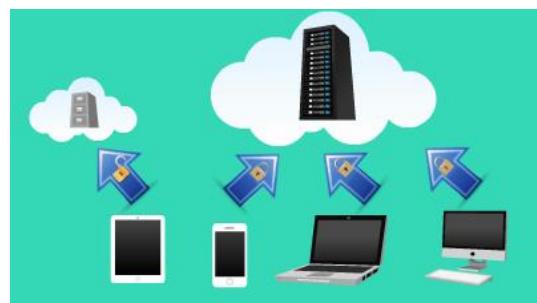


Figura 26 Vulnerabilidad "Servidor no autorizado"

Como es de conocimiento los datos deben ser transmitidos a través de una red a la nube, hay numerosos medios a través de los cuales un atacante puede conseguir actuar como un servidor titular de la nube, conllevando a la pérdida de datos.

Para evitar la pérdida de datos en esta situación, se usa el certificado SSL, las Autoridades de Certificación (CA) emiten este certificado, que es una credencial para el mundo en línea. Consiste en que el servidor de la nube envía la información de identificación al propietario cuando se conecta, a continuación envía al propietario una copia de su certificado SSL. El propietario verifica el certificado y luego envía un mensaje al servidor y el servidor devuelve un acuse de recibo firmado digitalmente para iniciar una sesión SSL cifrada, que permite la transferencia de datos cifrados entre el navegador y el servidor. Con la utilización de este certificado se tiene la certeza de que el servidor que está proporcionando la respuesta es el servidor anfitrión, y que se puede realizar la transmisión de forma segura, sabiendo que el servidor ha sido identificado previamente.

#### 6.2.4.3. Ataque de fuerza bruta

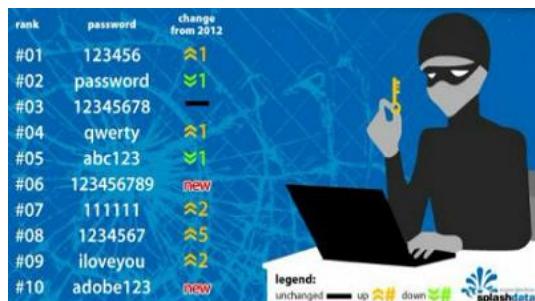


Figura 27 Vulnerabilidad "Ataque de fuerza bruta"

No es una tarea difícil descifrar las contraseñas, se puede realizar grandes números de combinaciones de forma rápida con el fin de determinar la clave, a esto se le denomina ataque de fuerza bruta, es la forma de conocer una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso. La mejor forma de defendernos de este tipo de ataques es restringir el número de intentos de autentificación, y tener una compleja combinación de usuario/contraseña.

#### 6.2.4.4. Manipulación de los datos



Figura 28 Vulnerabilidad "Manipulación de los datos"

Los datos están bajo la amenaza de ser manipulados por cualquier interceptor no autorizado. Las medidas de precaución, como el cifrado de datos, palabras clave y cifrado SSL son mencionados como medidas para no dejar que nadie manipule nuestros datos, pero aun así los datos necesitan ser comprobados después de la transmisión.

Para esto, MAC (código de autenticación de mensaje) según [113] son algoritmos criptográficos simétricos, que proporcionan integridad de los datos permitiendo el

reconocimiento de cualquier modificación o manipulación del mensaje durante la transmisión y la autenticación de origen de los datos, suministrando la confirmación de que el mensaje se originó por el remitente, que comparte la clave secreta utilizada por el receptor.

MAC de datos cifrados se genera por el propietario antes de enviarlo y MAC se transmite junto con los datos cifrados. Por otro lado, cuando el receptor recibe los datos, puede generar el MAC y compararlo con el MAC que generó el propietario y que fue recibido junto con los datos, si los códigos MAC son iguales, entonces se asegura el usuario de la integridad de los datos, es decir, los datos no han sido manipulados.

#### 6.2.4.5. Pérdida de identidad de usuario y contraseña



Figura 29 Vulnerabilidad "Pérdida de identidad de usuario y contraseña"

Según [103] un desafío clave de la implementación de aplicaciones centradas en el entorno multiusuario es asegurar que todo el procesamiento de consulta y el intercambio de datos se lleven a cabo de forma segura, es decir que las partes implicadas sean autenticadas y autorizadas de una forma estricta.

A continuación se pone a consideración dos formas en la que los usuarios podrían dejar que sus datos sean vulnerables a cualquier ataque, la primera trata sobre, el usuario evidencia sus credenciales revelándolas a una persona extraña, para la detección de la pérdida de información por este insignificante motivo los proveedores de SaaS deben implementar una técnica que impida el acceso del intruso al sistema, la segunda trata acerca de que los usuarios establecen contraseñas demasiado vulnerables por la

sencilla razón que si utilizan una contraseña segura que involucra caracteres alfanúmeros y los usuarios no recuerdan esta combinación.

Ahora se realizará un análisis a las dos maneras referidas anteriormente.

En caso de que el usuario revele su identidad de usuario y contraseña a cualquier persona no autorizada, los datos pueden estar en peligro. Para proteger los datos se deberá realizar una pregunta de seguridad a los usuarios cuya respuesta sólo la sabe el usuario autorizado, por lo que el usuario no autorizado no podrá acceder a los datos incluso después de tener las credenciales de ingreso correctas, otra medida de seguridad y la más eficiente es implementar el código de un solo uso para el ingreso a la cuenta, este mecanismo de autenticación es designado con el nombre de contraseña de un solo uso (OTP) conforme a [114] [115] estos se generan de forma dinámica sólo con fines de uso único y tienen una vida útil limitada utilizable. Tras el uso, la contraseña será invalidada por el cliente y el servidor del sistema de autenticación.

Por lo que se puede concluir que el uso de OTP es capaz de solucionar algunos de los problemas en los que se incurre al utilizar el mecanismo de contraseña fija tradicional.

Debido a la naturaleza de la OTP, los usuarios no van a tener la misma contraseña para los diferentes inicios de sesión.

Haciendo referencia a [116] [80] en los cuales plantean un medio de seguridad mucho más eficiente al cual se lo denota con el nombre de inicio de sesión único (SSO), este tiene muchas ventajas sobre los mecanismos simples de nombre de usuario y contraseña, en este caso el usuario tiene que recordar varias combinaciones diferentes, y la seguridad se basa únicamente en la fuerza de la contraseña proporcionada por el usuario, pero SSO permite la adopción de varias medidas técnicas para mejorar aún más la seguridad del procedimiento de inicio de sesión.

De forma general, el uso de la autenticación SSO se lleva a cabo utilizando un tercero de confianza denominado proveedor de identidad (IdP). Cuando un usuario utiliza su agente de usuario (UA), a través un navegador web, para solicitar un inicio de sesión al proveedor de servicio, en vez de pedir nombre de usuario y contraseña, el servicio emite una solicitud de emergencia y redirecciona al cliente IdP. Después de la

autenticación correcta, el IdP emite un token de autenticación firmado y redirige al cliente de SaaS, donde se validará el token y el usuario conectado [117] [118].

Otro medio de seguridad del que se puede hacer uso para reducir los ataques de suplantación de identidad es, que el proveedor de servicios de la nube (CSP) decida restringir el acceso al sistema solo para el conjunto de lista blanca de direcciones URL. Esta forma de proteger la identidad del usuario es eficiente ya que incluso si un cliente posee las credenciales legítimas no podrá ingresar al sistema debido a que la URL no se encuentra almacenada en los registros del CSP, razón por la cual el acceso se desactivará [80].

#### 6.2.4.6. Algoritmo de cifrado de contraseñas débil



Figura 30 Vulnerabilidad "Algoritmo de cifrado de contraseñas débil"

En el caso de que el proveedor SaaS no tenga implementado ningún otro mecanismo de seguridad para el ingreso a las cuentas, más que el de usuario y contraseña, se debería exigir al proveedor que por lo menos cuente con un algoritmo de cifrado seguro y que en añadidura a esto utilice el medio de contraseñas ocultas, ya que si no se hace uso de este mecanismo todas las contraseñas se almacenan como un archivo de una vía, lo que hace al sistema vulnerable a ataques de piratas de contraseñas. Un intruso puede acceder al sistema y copiar este archivo y ejecutar cualquier cantidad de programas para descifrar las contraseñas. Si hay una contraseña insegura en el archivo, es sólo cuestión de tiempo antes de que el pirata la descubra.

Las contraseñas ocultas previenen este tipo de ataque al almacenar este archivo de contraseñas en un archivo especial, el cual únicamente puede ser leído por el usuario root.

Esto obliga al intruso a ingresar a los servicios de red SSH, este proporciona claves criptográficamente fuertes para acceder a los datos [119]. El ataque de fuerza bruta es mucho más lento y deja un rastro evidente, pues los intentos fallidos de conexión son registrados en los archivos del sistema.

#### 6.2.4.7. Protocolo de seguridad de datos en la red

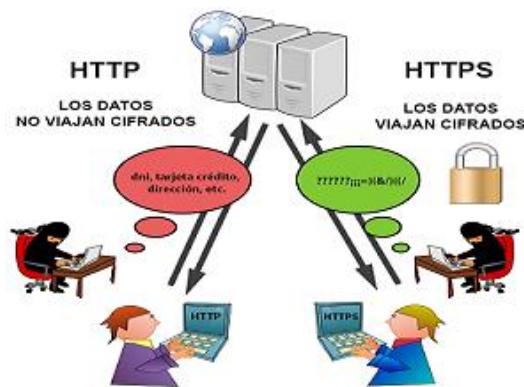


Figura 31 Vulnerabilidad "Protocolo de seguridad de datos en la red"

SaaS como tal es un sistema cliente/servidor, donde tanto el cliente (el navegador web, explorador o visualizador) como el servidor (el servidor web) y el protocolo mediante el que se comunican, son partes invariables para llevar a cabo el flujo de trabajo de SaaS, el proveedor SaaS debería establecer la comunicación por medio de los protocolos de seguridad existentes, tales como TLS, SSH o HTTPS, para asegurar que la información es transmitida por un canal seguro [120], este último proporciona tres garantías de seguridad, la autenticación del servidor, integridad de mensajes y confidencialidad de los mensajes [121], los cuales son factores importantes e influyentes para asegurar la seguridad de los datos, sin embargo en [54] afirma que TLS y SSH son los protocolos criptográficos anfitriones.

Algunos proveedores utilizan simplemente el protocolo HTTP porque es barato de usar pero no proporciona garantías de seguridad [121] para transmitir datos a través de la red, no es considerado como seguro ya que la protección depende de cada usuario final [122], por lo que dejan a responsabilidad del usuario limitar el tipo de información que se transmite.

#### **6.2.4.8. Aseguramiento por parte del proveedor de SaaS**

El proveedor de SaaS debe garantizar la seguridad y la copia de seguridad periódica de los datos sensibles con la facilidad de recuperación rápida en caso de cualquier tipo de desastre.

El proveedor también debe utilizar un fuerte mecanismo de seguridad como encriptación para proteger los datos almacenados en la copia de seguridad, para evitar el fraude ilícito y robo de información sensible.

Otro aspecto, según [90] que los proveedores SaaS deben asegurar es la localidad de datos, siendo este el problema más común para la organización, los clientes quieren saber los detalles donde su base de datos se almacena realmente y qué mecanismo de seguridad y qué método de certificación está utilizando para proteger los datos y donde se trasladan. Una vez que la información cruza las fronteras nacionales a partir de ahí es difícil proteger los datos, porque las normas y reglamentos de protección de datos cambian de acuerdo a la regla local del país donde se localizan los datos.

El entorno multi-usuario da la oportunidad para que un intruso secuestre los datos durante el acceso a las aplicaciones o acceder al código del cliente del sistema SaaS, el proveedor debe garantizar la segregación independiente del nivel físico de datos y el nivel de aplicación, debe ser lo suficientemente adecuado para aislar los datos de diferentes usuarios; la segregación de datos se refiere a que los datos de varios usuarios se van a localizar en la misma ubicación del servidor pudiéndose provocar interferencias de entre los clientes.

Además los proveedores de servicios deben asegurar que los datos estarán disponible 24\*7, sin ninguna interrupción. Esta arquitectura de la nube necesita adoptar mecanismos de equilibrio de carga efectiva durante el tratamiento de los datos. Se requieren cambios arquitectónicos y de infraestructura para lograr escalabilidad y accesibilidad de los datos con un tiempo de respuesta efectivo.

Por otro lado el proveedor de servicios debe tener recursos seguros para comprobar la autorización del usuario y validar mediante un mecanismo seguro los privilegios de cada usuario; la autorización es el mecanismo que determina el nivel de privilegios de un usuario en particular.

El control de acceso debe gestionarse de acuerdo a la función de los usuarios. La autorización para acceder a los datos seguros se realiza en base a diferentes niveles de clientes de acuerdo a la política de acceso y jerarquía. En general, el modelo de privilegio mínimo que se debe utilizar para los usuarios es CSP (Políticas de Seguridad de Contenido), sólo los administradores poseen los derechos suficientes para cumplir con sus tareas.

El proveedor de servicios SaaS debe implementar una reglamentación estricta para la protección de datos, de cualquier tipo de manipulación, robo y acceso ilícito de los datos.

La criptografía es la técnica más adecuada para la seguridad informática, pero debe ser certificada por los proveedores de servicios de seguridad, según [123] esta técnica es más especializada si se utiliza la criptografía de clave pública ya que es el método más común para la autenticación de un emisor y receptor. En la criptografía tradicional, una clave secreta se utiliza para el cifrado y el descifrado en ambos extremos; si la clave secreta o privada es descubierta por alguna razón los datos pueden ser fácilmente descifrados. Por este argumento, la criptografía de clave pública es el enfoque más adecuado en el Internet. Este sistema de clave pública es conocido como la criptografía asimétrica, las claves privadas y públicas se generan simultáneamente usando el mismo algoritmo por la autoridad de certificación de confianza. Este sistema, proporciona la clave privada al cliente de la nube que la solicite, cada cliente tiene una clave privada única, que es confidencial, la clave pública está disponible públicamente a todo el mundo.

#### **6.2.4.9. Técnicas de cifrado**

Secure Sockets Layer (SSL) es un protocolo diseñado para permitir que las aplicaciones transmitan información de ida y hacia atrás de manera segura. Las aplicaciones que utilizan el protocolo SSL saben cómo dar y recibir claves de cifrado con otras aplicaciones, así como la manera de cifrar y descifrar los datos enviados entre los dos.

Este enfoque no sólo preserva que los datos no sean víctima de los intrusos, sino que también ayuda a asegurar que los datos están seguros mientras están en tránsito. Es un protocolo de estado, orientado a la conexión cliente-servidor, se podría afirmar que este protocolo de seguridad de las comunicaciones es el de mayor despliegue en

Internet, que proporciona confidencialidad, integridad de datos y autenticación de la identidad para comunicaciones a través de Internet de dos partes.

En [91] señala en concordancia a lo antes dicho que el uso de técnicas de cifrado fuerte como Secure Socket Layer (SSL) o Transport Layer Security (TLS) [119] puede reducir la vulnerabilidad de los datos, en gran medida, según menciona [124] estos protocolos son los mismos con diferentes denominaciones, es un protocolo de estado, orientado a la conexión cliente-servidor. Podría decirse que es el protocolo de seguridad de las comunicaciones de mayor despliegue en Internet, que proporciona confidencialidad, integridad de datos y autenticación de la identidad para comunicaciones a través de Internet de dos partes [125].

La técnica de acceso y seguridad de datos por la red TLS (Transport Layer Security) según [126] este protocolo protege los datos en tránsito entre dos puntos finales, con la autenticación de por lo menos un punto final, en Internet se utiliza TLS para validar la identidad de los servidores que alojan sitios web, realizando la autenticación mutua, permitiendo a los servidores verificar las identidades de los clientes y a los clientes verificar las identidades de los servidores.

Haciendo referencia a [103] en este artículo se menciona que las técnicas a utilizar deberían proporcionar la verificación de extremo a extremo de los resultados de una consulta a un servidor, uno de los métodos que cumple esto es TLS.

#### **6.2.4.10. Sistema de almacenamiento**

El sistema de almacenamiento en la nube debe ser incorporado con SSL y servicio TCCP (Trusted Platform Cloud Computing) tomando como referencia [127], este es un esquema basado en un servidor seguro, está diseñado para garantizar la integridad y confidencialidad de los datos de los usuarios alojados en la nube, y determina los derechos de acceso absoluto para los usuarios [90] [109] [128].

#### **6.2.5. Cláusulas imprescindibles en un contrato SaaS**

El contrato entre la organización como cliente y el proveedor de SaaS puede ser, un acuerdo contractual negociado o de adhesión.

- **Contrato Negociado**

Este tipo de contrato permite flexibilidad, ofreciéndole al cliente la capacidad para fijar las condiciones de contratación en función del tipo de datos que se van a procesar, las medidas de seguridad exigibles, el esquema de subcontratación, la localización de los datos y la portabilidad de los mismos [129].

- **Contrato de Adhesión**

Este contrato está constituido por cláusulas contractuales cerradas, sin que el usuario tenga ninguna opción para negociar sus términos, simplemente hay que adaptarse [129].

Las cláusulas que se mencionan a continuación son imprescindibles en el contrato proporcionado por el proveedor.

*Tabla 13 Cláusulas imprescindibles en el contrato SaaS*

<b>6.2.5.1. Confidencialidad</b>
Fundamentalmente en las operaciones de traslado de datos y almacenamiento en servidores [129] [130] [131].
<b>6.2.5.2. Disponibilidad</b>
Esta cláusula especifica el nivel de disponibilidad que el proveedor de servicios se compromete a mantener [129] [130] [131].
<b>6.2.5.3. Rendimiento</b>
Este apartado asegura que se alcanzan los niveles de potencia de cálculo, almacenamiento y ancho de banda contratados con el proveedor de servicios [129] [130] [131].
<b>6.2.5.4. Seguridad</b>
El proveedor de servicios se compromete a mantener un nivel de seguridad suficiente en sus instalaciones para albergar sus datos y procesos, por lo que debe dar al cliente una lista de las medidas de seguridad que está aplicando en sus sistemas [129] [130] [131].

#### **6.2.5.5. Plan de Continuidad de Negocio y Recuperación ante desastres**

Es conveniente que el proveedor cuente con este documento que este operativo y actualizado [129] [130] [131].

#### **6.2.5.6. Pagos**

Esta sección contiene los detalles de los pagos que debe realizar el cliente para usar los servicios contratados. Debe incluir claramente la cantidad y la periodicidad de dichos pago [129] [130] [131].

#### **6.2.5.7. Suspensión del servicio**

Esta cláusula indica al cliente que es posible que se suspenda momentáneamente el servicio debido a actualizaciones en su infraestructura informática [129] [130] [131].

#### **6.2.5.8. Servicios de soporte**

Esta sección contendrá los compromisos del proveedor de servicios en cuanto al soporte prestado al cliente. Es importante que el contrato especifique el tiempo que el proveedor requiere para recuperar el sistema cuando se ha producido un error [129] [130] [131].

#### **6.2.5.9. Terminación o modificación**

Las características de SaaS permiten una gran flexibilidad a la hora de modificar los servicios que el cliente necesita. El acuerdo legal debe contener claramente las opciones de modificación del contrato o terminación del mismo, sobre todo en lo relativo a recuperación y borrado de la información [129] [130] [131].

#### **6.2.5.10. Privacidad y cumplimiento normativo**

Esta cláusula define el nivel de compromiso del proveedor de servicios con el cumplimiento de las leyes en especial las relativas a la privacidad y protección de datos [129] [130] [131].

### **6.3. Tercer objetivo específico: “Producir una guía de análisis acerca de la seguridad en esta arquitectura”**

Se tomó como base principalmente el entregable del segundo objetivo ya que en este constan las vulnerabilidades encontradas en la investigación realizada a la seguridad de SaaS.

Para efectuar este objetivo se realizó una guía multimedia en la cual se presenta información, mediante: texto, videos e imágenes, además se puede realizar la comprobación de la confiabilidad del proveedor, para ello se hizo uso de redes bayesianas, el sitio web está disponible en:

<http://174.37.68.55:8080/SaaS/faces/index.html>

A continuación se presenta el uso e interacción que el usuario puede tener con la guía multimedia.

En el encabezado principal cuenta con el siguiente menú de desplazamiento para navegar por el contenido de la guía.

INICIO    DEFINICIÓN    SLA    RIESGOS    VULNERABILIDADES    SOLUCIONES    CONTRATO

*Figura 32 Menú principal de navegación*

**6.3.1. Al hacer click en el botón INICIO se presenta un carrusel de imágenes y el siguiente panel de navegación:**



*Figura 33 Imagen inicial de la guía*



### SIMULADOR PARA CALCULAR LA CONFIABILIDAD DEL PROVEEDOR

Le permite verificar la confiabilidad del proveedor, para ello debe poseer conocimientos previos, los mismos serán adquiridos al interactuar con la presente guía.



### DESCARGAR PDF

Obtenga toda la información acerca de SaaS, contenida en esta guía



### BIBLIOGRAFÍA

La información recolectada es el producto de la investigación efectuada, para ello se ha recurrido a fuentes primarias confiables.

Puede acceder a la bibliografía en el siguiente enlace.



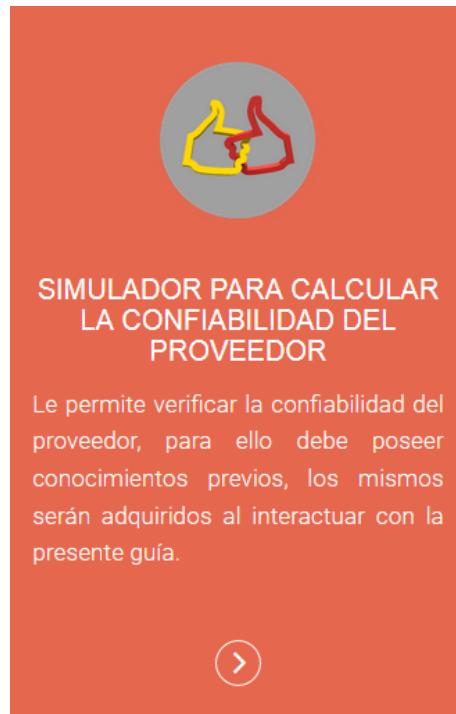
### VIDEO RESUMEN

En el video se simula la contratación de SaaS, exemplificando dos escenarios, en el primero se contrata SaaS haciendo caso a las recomendaciones para asegurar los datos y en el segundo haciendo caso omiso a dichas recomendaciones



*Figura 34 Panel de navegación de la pestaña INICIO*

Cada uno de los íconos tiene una funcionalidad específica, la misma se los detalla a continuación:



*Figura 35 Primer ícono del panel de navegación de la pestaña INICIO*

Antes de comenzar con la descripción del simulador, se muestra los botones comunes durante el recorrido.

*Tabla 14 Botones comunes en el simulador*

BOTONES COMUNES	DESCRIPCIÓN
	Cada una de las opciones cuenta con un enlace de información, en el cual se puede visualizar la información referente al tema tratado.
	Botón para acceder a la siguiente pantalla del simulador.
	Botón para volver a la pantalla anterior del simulador.
	Botón para regresar a la página inicial de la guía.

La primera pantalla que se presenta sirve para recolectar información a cerca del proveedor.

## VERIFICAR CONFIABILIDAD DEL PROVEEDOR

Proveedor Contrato Cuestionamientos Adicionales

INFORMACIÓN

Cuenta con un proveedor:

Si  
 No

Los campos son requeridos

EXPERIENCIA DEL PROVEEDOR

Seleccione la experiencia del proveedor:

0-2 años  
 3-5 años  
 5-10 años  
 Más de 10 años

i

Los campos son requeridos

Siguiente

Inicio

Figura 36 Primera pantalla del simulador

En la primera sección se inicia el flujo del simulador, siempre y cuando el usuario elija la opción **SI**, en el caso contrario no podrá hacer uso del simulador y se presenta el siguiente mensaje

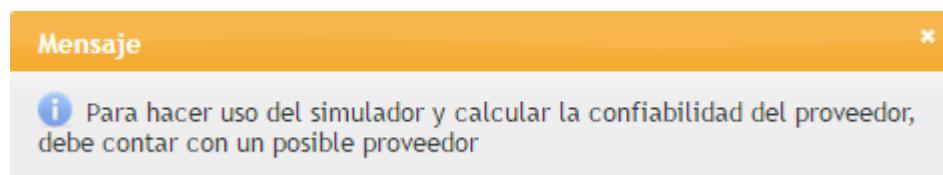


Figura 37 Mensaje presentado al usuario al elegir la opción NO

En la segunda sección de la figura, se requiere información acerca de la experiencia del proveedor, se ha tomado como referencia los rangos de acuerdo a los años de experiencia de los proveedores mas y menos utilizados.

Al dar click en **SIGUIENTE** se muestra la pantalla especificada a continuación, en la cual el ususario deberá proporcionar información relacionada con el contrato.

## VERIFICAR CONFIABILIDAD DEL PROVEEDOR

Proveedor Contrato Cuestionamientos Adicionales

**TIPO DE CONTRATO**

Seleccione una opción:

Adhesión  
 Negociado

*i*

Si no cuenta con un contrato, no elija ninguna opción

**CLAUSULAS EN EL CONTRATO**

Seleccione una o varias opciones:

El plan de continuidad de negocios  Terminación o Modificación  
 Confidencialidad  Disponibilidad  
 Rendimiento  Suspensión del Servicio  
 Servicio de Soporte  Seguridad  
 Privacidad y Cumplimiento Normativo  Pagos

*i*

Si no conoce las cláusulas del contrato, no elija ninguna opción

**ACUERDO DE NIVEL DE SERVICIO (SLA)**

Seleccione una o varias opciones:

Recuperación de los datos  
 Viabilidad a largo plazo  
 Acceso de usuarios privilegiados  
 Ubicación de los datos

*i*

Si no cuenta con un SLA, no elija ninguna opción

[Atrás](#) [Siguiente](#)

Figura 38 Segunda pantalla del simulador

En la sección **TIPO DE CONTRATO**, se pide ingresar el tipo de contrato ya sea de **ADHESIÓN** o **NEGOCIADO**, lo cual se refiere a que si, el proveedor ofrece un acuerdo contractual de adhesión el cliente estrictamente se rige a las políticas del proveedor; en cambio si el proveedor ofrece un acuerdo contractual negociado el cliente tiene la potestad de añadir, modificar o cambiar cláusulas en el contrato

En la sección **CLAUSULAS EN EL CONTRATO** se debe señalar las cláusulas establecidas en el acuerdo contractual las misma son:

- **Plan de Continuidad**

El plan de continuidad de negocio y recuperación ante desastres, es un documento clave para la asegurar la persistencia de la empresa cliente.

- **Confidencialidad**

La cláusula de confidencialidad debe estar garantizada en lo que respecta a las operaciones de traslado de datos y almacenamiento en servidores.

- **Rendimiento**

Este asegura la utilidad de los servicios prestados por el proveedor en relación con la tarifa pagada.

- **Servicio de Soporte**

Es la asistencia que brindan los proveedores a sus clientes para que puedan hacer uso de sus servicios.

- **Privacidad y cumplimiento normativo**

Se refiere al cumplimiento de las leyes en especial las relativas a la privacidad y protección de datos por parte de los proveedores.

- **Terminación o modificación**

El acuerdo debe contener las opciones sobre la modificación del contrato o terminación del mismo.

- **Disponibilidad**

Especifica la disponibilidad que el proveedor se compromete a mantener con respecto a los servicios.

- **Suspensión del servicio**

Esta cláusula advierte al cliente que puede suspenderse momentáneamente el servicio, estableciendo el lapso de tiempo aproximado y las posibles razones.

- **Seguridad**

El proveedor de servicios debe proporcionar al cliente una lista de las medidas de seguridad que está aplicando en sus sistemas.

- **Pagos**

Se establece la cantidad y periodicidad de los pagos que debe realizar el cliente para usar los servicios contratados.

En la sección **ACUERDO DE NIVEL DE SERVICIO** se hace referencia a los riesgos de seguridad que se discuten en un SLA, los mismos se mencionan a continuación:

- **Recuperación de los datos**

El cliente debe asegurarse que el proveedor tiene la capacidad de hacer una restauración completa de los datos y cuánto tiempo tomará en realizar dicha actividad en caso de un desastre.

- **Viabilidad a largo plazo**

Se debe pedir a los proveedores que nos hagan conocer cómo se recuperan los datos y el formato en el que son entregados en caso de que el proveedor vaya a la quiebra.

- **Acceso de usuarios privilegiados**

Pedir a los proveedores suministrar información específica sobre la contratación y supervisión de los administradores privilegiados, y sobre los controles de acceso realizados.

- **Ubicación de los datos**

Los proveedores deben hacer conocer al cliente las jurisdicciones territoriales donde se almacenan y procesan los datos.

Al seguir el flujo normal de la interacción se presenta la siguiente pantalla:

## VERIFICAR CONFIABILIDAD DEL PROVEEDOR

**Proveedor** **Contrato** **Cuestionamientos Adicionales**

**MEDIDAS DE SEGURIDAD EXIGIBLES**

Seleccione una o varias opciones:

Requerimiento de contraseña  Restringir el número de intentos  
 Certificado SSL  Datos Cifrados  
 MAC  Pregunta de Seguridad  
 Lista Blanca de URL  OTP  
 SSO

**i**

*Si no tiene conocimiento, no elija ninguna opción*

**ESQUEMA DE BASE DE DATOS**

Seleccione una opción:

STSI  
 ITSI  
 IDII

**i**

*Si no conoce el esquema de base de datos, no elija ninguna opción*

**PROTOCOLO DE TRANSFERENCIA**

Seleccione una opción:

HTTP  
 HTTPS  
 TLS  
 SSH

**i**

*Si no conoce el protocolo de transferencia, no elija ninguna opción*

**Resultado**

**Atrás**

**Inicio**

Figura 39 Tercera pantalla del simulador

En la sección **MEDIDAS DE SEGURIDAD EXIGIBLES** se presenta los elementos que un SaaS debe cumplir para asegurar los datos, los mismos se detallan a continuación:

- **Requerimiento de contraseña**

Para crear las cuentas debe existir un requerimiento exigente de la contraseña.

- **Certificado SSL**

Las Autoridades de Certificación (CA) emiten el certificado SSL, este es una credencial para el mundo en línea.

- **MAC**

El código de autenticación de mensajes, permite el reconocimiento de cualquier modificación o manipulación del mensaje durante la transmisión y la autenticación de origen de los datos.

- **Lista Blanca de URL**

Restringir el acceso al sistema solo para el conjunto de lista blanca de direcciones URL del proveedor.

- **SSO**

El medio de seguridad, inicio de sesión único permite la adopción de varias medidas para mejorar aún más la seguridad del procedimiento de inicio de sesión con usuario/contraseña.

- **Restringir el número de intentos**

Para el ingreso a la cuenta se debe restringir el número de intentos para evitar un ataque de fuerza bruta.

- **Datos Cifrados**

Es el proceso por el que la información legible se transforma mediante un algoritmo en información ilegible o criptograma.

- **Pregunta de Seguridad**

Para ingresar a la cuenta se deberá realizar una pregunta de seguridad a los usuarios cuya respuesta sólo la sabe el usuario autorizado, por lo que el usuario no autorizado

no podrá acceder a los datos incluso después de tener las credenciales de ingreso correctas.

- **OTP**

El mecanismo de autenticación, contraseña de un solo uso es una solución eficiente para el ingreso a la cuenta, estos se generan de forma dinámica sólo con fines de uso único y tienen una vida útil limitada.

En la sección **ESQUEMA DE BASE DE DATOS** se pide elegir entre los tipos de BD de SaaS, los mismos son:

- **STSI**

Tablas compartidas e instancias de base de datos compartidos

- **ITSI**

Tablas independientes e instancias de base de datos compartidos

- **IDII**

Base de datos independientes e instancias de base de datos independientes

En la sección **PROTOCOLO DE TRANSFERENCIA** se debe elegir el canal por donde se transmite la información, los mismos son los siguientes:

- **HTTP**

Es barato de usar pero no proporciona garantías de seguridad para transmitir datos a través de la red.

- **HTTPS**

Proporciona tres garantías de seguridad, la autenticación del servidor, integridad de mensajes y confidencialidad de los mensajes.

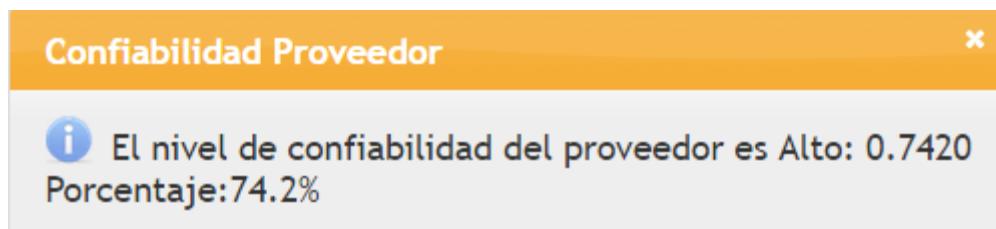
- **TLS**

Es un protocolo criptográfico que proporciona comunicaciones seguras por Internet.

- **SSH**

Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor, encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

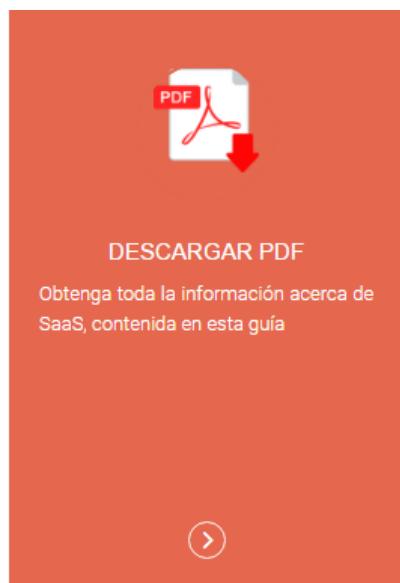
Al dar click en el botón **RESULTADO** se realiza el cálculo de la confiabilidad del proveedor en base a las variables ingresadas por el usuario.



*Figura 40 Pantalla en la que se muestra el resultado*

Además muestra el nivel de confianza de su posible proveedor, para ello se ha tomado los siguientes rangos de porcentaje:

- **1% - 20% => nivel de confiabilidad del proveedor muy bajo.**
- **21% - 45% => nivel de confiabilidad del proveedor bajo.**
- **46% - 60% => nivel de confiabilidad del proveedor medio.**
- **61% - 100% => nivel de confiabilidad del proveedor alto.**



El segundo ícono nos sirve para descargar la información contenida en la guía en formato PDF.

*Figura 41 Segundo ícono del panel de navegación de la pestaña INICIO*



### BIBLIOGRAFÍA

La información recolectada es el producto de la investigación efectuada, para ello se ha recurrido a fuentes primarias confiables.

Puede acceder a la bibliografía en el siguiente enlace.



El tercer ícono muestra la bibliografía de la información investigada, la misma que se presenta en formato xml, la cual ha sido exportada del gestor bibliográfico Mendeley.

*Figura 42 Tercer ícono del panel de navegación de la pestaña INICIO*



### VIDEO RESUMEN

En el video se simula la contratación de SaaS, ejemplificando dos escenarios, en el primero se contrata SaaS haciendo caso a las recomendaciones para asegurar los datos y en el segundo haciendo caso omiso a dichas recomendaciones



El cuarto ícono conduce a un video en el que se supone la contratación de SaaS, ejemplificando dos escenarios, en el primero se contrata SaaS haciendo caso a las recomendaciones para asegurar los datos y en el segundo haciendo caso omiso a dichas recomendaciones

*Figura 43 Cuarto ícono del panel de navegación de la pestaña INICIO*

### 6.3.2. Al hacer click en el botón DEFINICIÓN se muestra la siguiente información:

#### QUÉ ES SaaS?

En la arquitectura SaaS las aplicaciones no son un producto sino un servicio, es un modelo de negocio para la distribución de software, que proporciona acceso al mismo y a sus funciones a través de Internet, refiriéndose a la utilización de los servicios de software, plataformas e infraestructura basados en la nube.

#### SaaS

Permite que varios clientes (inquilinos) puedan compartir la misma instancia de un software y acceder a los datos que se alojan en los servidores de la compañía de tecnologías de información y comunicación través de internet, múltiples clientes pueden utilizar las mismas instalaciones y con ello aumentar las tasas de utilización de hardware y redes.

#### CLIENTES O INQUILINOS

Las organizaciones pueden tener a la disposición estos servicios a cambio de una tarifa, un inquilino es la unidad organizativa que paga por el uso de una aplicación SaaS de forma regular de acuerdo a un determinado contrato de suscripción.



#### SUBSIDIARIOS

Los proveedores de SaaS son subsidiarios de toda la infraestructura de red, software, hardware, plataforma operativa, y es responsable del mantenimiento y otros servicios.

#### DESAFÍO SaaS

Hacer uso de este servicio implica estar expuesto a grandes riesgos de seguridad de los datos, siendo la confiabilidad el mayor desafío en la amplia aceptación de SaaS, los datos se encuentran alojados fuera de las organizaciones, pudiendo ser víctima de robo, modificación, pérdida entre otras vulnerabilidades, quedando expuesto el activo más importante hoy en día de toda entidad.

Figura 44 Definición de SaaS

### 6.3.3. Al hacer click en el botón SLA se presenta la siguiente información:

Primeramente se presenta la imagen mostrada a continuación, haciendo click en el botón **VIDEO** se reproduce un video a cerca del Acuerdo de Nivel de Servicio.

#### ACUERDO DE NIVEL DE SERVICIO (SLA)



Figura 45 Imagen Acuerdo de Nivel de Servicio

Seguidamente se muestra la siguiente información.

#### QUÉ ES SLA?



#### RIESGOS DE SEGURIDAD

SLA discute cómo se manejan los siguientes riesgos de seguridad:

- 1 Acceso de usuarios privilegiados
- 2 Cumplimiento de la normativa
- 3 Ubicación de los datos
- 4 Recuperación de los datos
- 5 Viabilidad a largo plazo

#### DESCRIPCIÓN DEL RIESGO



SLA es un acuerdo o un vínculo jurídico entre el proveedor y las instituciones en el contexto de la prestación de un servicio en particular, los SLA se han convertido en una parte importante del modelo de prestación de servicios de la nube, los clientes y los proveedores de SaaS deben establecer un SLA para definir la calidad de servicio (QoS), este es un enfoque para especificar y administrar la seguridad, esta es rara vez considerada ya que es diferente de otros atributos como la calidad de servicio, rendimiento y fiabilidad, sin embargo SLA abarca aspectos relacionados con la seguridad de los datos.

*Figura 46 Información Acuerdo de Nivel de Servicio*

Para acceder a los riesgos de seguridad tratados en el SLA se tiene q hacer click en cada uno de ellos y se presenta la información detallada.

#### 6.3.4. Al hacer click en el botón RIESGOS se presenta la siguiente información:

## | FACTORES DE RIESGO |

A continuación se pone a consideración lo que podría suceder si la seguridad de los datos no está completamente garantizada por el proveedor SaaS.



Almacenamiento de datos	Control de acceso a los datos	Copia de seguridad y recuperación de datos
		
<a href="#">INFOGRAFÍA</a>	<a href="#">INFOGRAFÍA</a>	<a href="#">INFOGRAFÍA</a>

Integridad de los datos

Transferencia de datos

Integridad de los datos	Transferencia de datos
	
<a href="#">INFOGRAFÍA</a>	<a href="#">INFOGRAFÍA</a>

*Figura 47 Factores de riesgo en SaaS*

En cada uno de los factores de riesgo hay un botón **INFOGRAFÍA** haciendo click en este se presenta la información completa del riesgo.

### 6.3.5. Al hacer click en el botón VULNERABILIDADES se presenta la siguiente información:

Primeramente se presenta la imagen mostrada a continuación, haciendo click en el botón **VIDEO** se reproduce un video acerca de las vulnerabilidades en SaaS.



Figura 48 Imagen de las vulnerabilidades en SaaS

Seguidamente se muestra la información de las vulnerabilidades, en cada uno de los links se puede hacer click y obtener mas información.

Los datos son muy vulnerables a amenazas como la fuga de datos, modificación, privacidad de los usuarios y confidencialidad entre otros. A continuación se manifiesta los principales problemas y una manera eficiente para hacer frente a todos estas vulnerabilidades de seguridad.

ESQUEMA DE BASE DE DATOS INSEGURO

SERVIDOR NO AUTORIZADO

ATAQUE DE FUERZA BRUTA

MANIPULACIÓN DE LOS DATOS

PÉRDIDA DE IDENTIDAD DE USUARIO Y CONTRASEÑA

ALGORITMO DE CIFRADO DE CONTRASEÑAS DÉBIL

PROTOCOLO DE SEGURIDAD DE DATOS EN LA RED

Figura 49 Información de vulnerabilidades en SaaS

### 6.3.6. Al hacer click en el botón SOLUCIONES se presenta la siguiente información:

## | SOLUCIONES PLANTEADAS |

Para mitigar los problemas de seguridad se propone las siguientes soluciones:



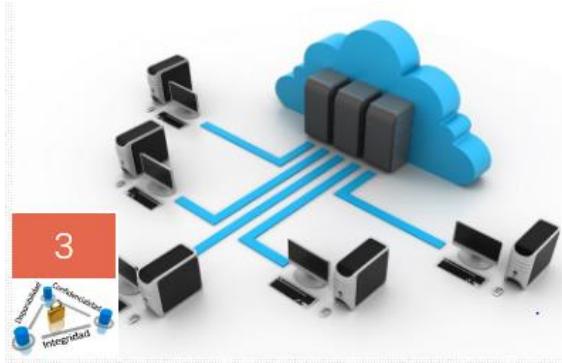
SECURE SOCKETS LAYER (SSL)  
CAPA DE PUERTOS SEGUROS



TRANSPORT LAYER SECURITY (TLS)  
SEGURIDAD DE LA CAPA DE TRANSPORTE

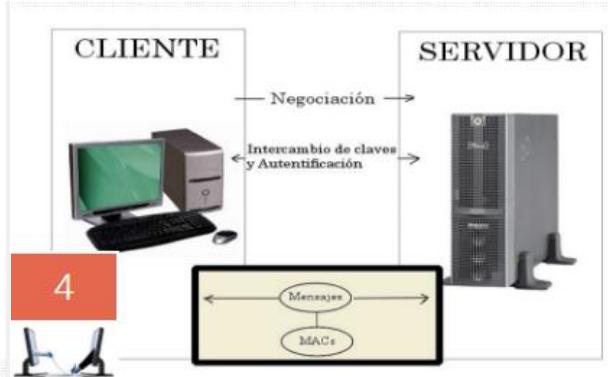
Es un protocolo diseñado para permitir que las aplicaciones transmitan información de ida y hacia atrás de manera segura. Las aplicaciones que utilizan el protocolo SSL saben cómo dar y recibir claves de cifrado con otras aplicaciones, así como la manera de cifrar y descifrar los datos enviados entre los dos. Este enfoque no sólo preserva que los datos no sean víctima de los intrusos, sino que también ayuda a asegurar que los datos están seguros mientras están en tránsito. Es un protocolo de estado, orientado a la conexión cliente-servidor; se podría afirmar que este protocolo de seguridad de las comunicaciones es el de mayor despliegue en Internet, que proporciona confidencialidad, integridad de datos y autenticación de la identidad para comunicaciones a través de Internet de dos partes.

Una versión actualizada y más segura de SSL es el protocolo de acceso y seguridad de datos por la red TLS, protege los datos en tránsito entre dos puntos finales, con la autenticación de por lo menos un punto, se utiliza TLS para validar la identidad de los servidores que alojan sitios web, realizando la autenticación mutua, permitiendo a los servidores verificar la identidad de los clientes y a los clientes verificar la identidad de los servidores. Esta técnica proporciona la verificación de extremo a extremo de los resultados de una consulta a un servidor.



TRUSTED PLATFORM CLOUD COMPUTING (TCCP)  
PLATAFORMA DE CONFIANZA CLOUD COMPUTING

El sistema de almacenamiento en la nube debe ser incorporado con TCCP este es un esquema basado en un servidor seguro, está diseñado para garantizar la integridad y confidencialidad de los datos de los usuarios alojados en la nube, y determina los derechos de acceso absoluto de los usuarios.

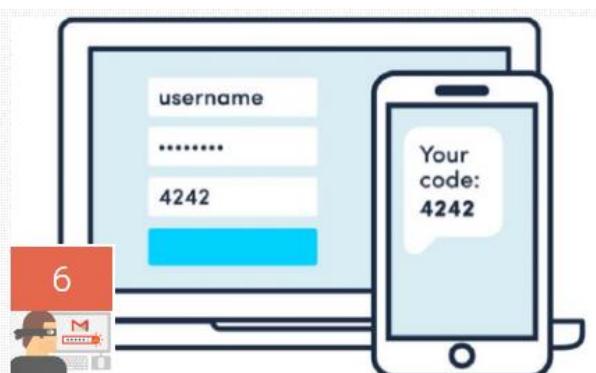


CÓDIGO DE AUTENTICACIÓN DE MENSAJES (MAC)

Los datos necesitan ser comprobados después de la transmisión, para esto se hace uso de MAC, proporcionando integridad a los datos ya que permite el reconocimiento de cualquier modificación o manipulación del mensaje durante la transmisión y asegura el no repudio.

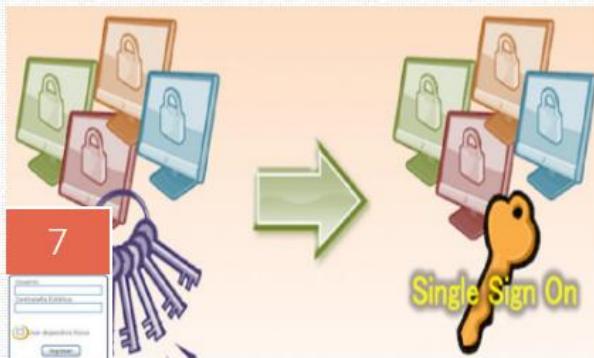
ROBO DE IDENTIDAD

Restringir el número de intentos de autentificación.  
Tener una compleja combinación de usuario/contraseña.  
Pregunta de seguridad para el inicio de sesión.



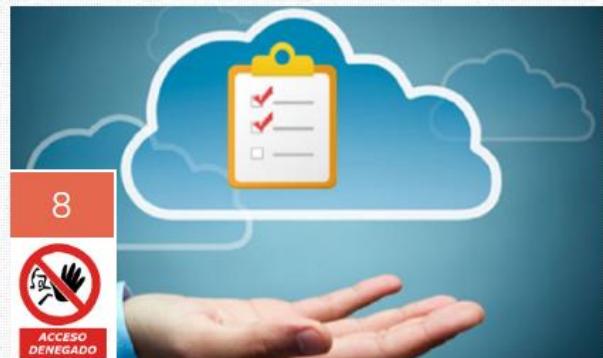
CONTRASEÑA DE UN SOLO USO (OTP)

Implementar OTP se generan de forma dinámica sólo con fines de uso único y tienen una vida útil limitada utilizable.



INICIO DE SESIÓN ÚNICO (SSO)

Medio de seguridad SSO el servicio emite una solicitud de emergencia y redirecciona al cliente IdP (proveedor de identidad), después de la autenticación correcta, el IdP emite un token de autenticación firmado y redirige al cliente de SaaS, donde se validará el token y el usuario conectado.



LISTA BLANCA DE DIRECCIONES URL

El proveedor de servicios de la nube (CSP) debe establecer la lista blanca de direcciones URL, es una forma eficiente de proteger la identidad del usuario debido a que si la URL no se encuentra almacenada en los registros del CSP, el acceso a la cuenta se desactivará.

CONTRASEÑAS OCULTAS

Se debe exigir al proveedor que utilice el medio de contraseñas ocultas, ya que este es un archivo de contraseñas especial, el cual únicamente puede ser leído por el usuario root.



PROTOCOLOS DE SEGURIDAD

Se debería establecer la comunicación por medio de un canal seguro, estos protocolos de seguridad podrían ser: TLS, SSH o HTTPS, para asegurar que la información es transmitida de forma segura.



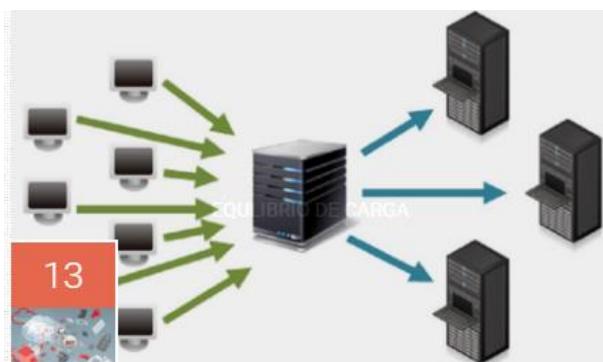
COPIA DE SEGURIDAD

La copia de seguridad es sumamente importante, ya que no se está exento de algún desastre.



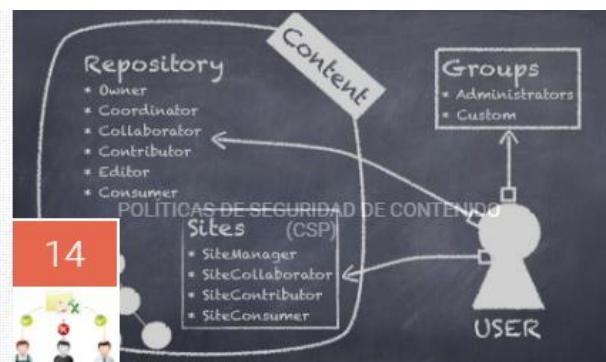
ALOJAMIENTO DE LOS DATOS

Estar al tanto de los lugares donde van a ser almacenados los datos, debido a que el ordenamiento jurídico cambia en cada país.



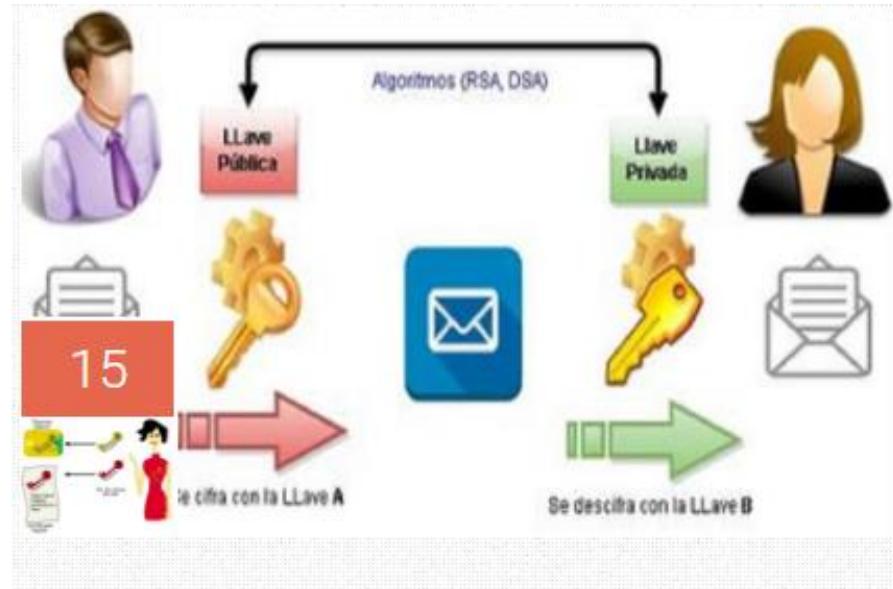
EQUILIBRIO DE CARGA

Los datos deben estar disponibles 24\*7, sin ninguna interrupción, para ello se necesita adoptar mecanismos de equilibrio de carga efectiva durante el tratamiento de los datos.



POLÍTICAS DE SEGURIDAD DE CONTENIDO (CSP)

El modelo de privilegio mínimo que se debe utilizar el proveedor para dar acceso a los usuarios es CSP, este mecanismo determina el nivel de privilegios de un usuario en particular.



## CRIPTOGRAFÍA ASIMÉTRICA

---

Criptografía asimétrica, proporciona una clave privada al cliente para encriptar la información, cada cliente tiene una clave privada única, y una clave pública la misma que está disponible públicamente para las personas que deseen enviar información.

*Figura 50 Soluciones planteadas para mitigar las vulnerabilidades*

### 6.3.7. Al hacer click en el botón CONTRATO se presenta la siguiente información:

CONTRATO	
El contrato entre la organización como cliente y el proveedor de SaaS puede ser, un acuerdo contractual negociado o de adhesión.	
<b>CONTRATO DE ADHESIÓN</b>  Está constituidos por cláusulas contractuales cerradas, sin que el usuario tenga ninguna opción para negociar sus términos	<b>CONTRATO NEGOCIADO</b>  Permite flexibilidad, ofreciéndole al cliente la capacidad para fijar las condiciones de contratación en función del tipo de datos que se van a procesar, las medidas de seguridad exigibles, el esquema de subcontratación, la localización de los datos y la portabilidad de los mismos.

Figura 51 Tipo de contrato

Seguidamente se muestra las cláusulas imprescindibles en un contrato:



1  
**CONFIDENCIALIDAD**

Fundamentalmente en las operaciones de traslado de datos y almacenamiento en servidores.



2  
**DISPONIBILIDAD**

Esta cláusula especifica el nivel de disponibilidad que el proveedor de servicios se compromete a mantener.



3  
**RENDIMIENTO**

Este apartado asegura que se alcanzan los niveles de potencia de cálculo, almacenamiento y ancho de banda contratados con el proveedor de servicios.



4  
**SEGURIDAD**

El proveedor de servicios se compromete a mantener un nivel de seguridad suficiente en sus instalaciones para albergar sus datos y procesos, por lo que debe dar al cliente una lista de las medidas de seguridad que está aplicando en sus sistemas.



5  
**PLAN DE CONTINUIDAD DE NEGOCIO Y RECUPERACIÓN ANTE DESASTRES**

Es conveniente que el proveedor cuente con este documento que este operativo y actualizado.



6  
**PAGOS**

Esta sección contiene los detalles de los pagos que debe realizar el cliente para usar los servicios contratados. Debe incluir claramente la cantidad y la periodicidad de dichos pago.



7  
**SUSPENSIÓN DEL SERVICIO**

Esta cláusula indica al cliente que es posible que se suspenda momentáneamente el servicio debido a actualizaciones en su infraestructura informática.



8  
**SERVICIOS DE SOPORTE**

Esta sección contendrá los compromisos del proveedor de servicios en cuanto al soporte prestado al cliente. Es importante que el contrato especifique el tiempo que el proveedor requiere para recuperar el sistema cuando se ha producido un error.



9  
**TERMINACIÓN O MODIFICACIÓN**

Las características de SaaS permiten una gran flexibilidad a la hora de modificar los servicios que el cliente necesita. El acuerdo legal debe contener claramente las opciones de modificación del contrato o terminación del mismo, sobre todo en lo relativo a recuperación y borrado de la información.



10  
**PRIVACIDAD Y CUMPLIMIENTO NORMATIVO**

Esta cláusula define el nivel de compromiso del proveedor de servicios con el cumplimiento de las leyes en especial las relativas a la privacidad y protección de datos.

*Figura 52 Cláusulas imprescindibles en un contrato*

## 7. DISCUSIÓN DE RESULTADOS

En este apartado se da a conocer las actividades sistemáticas que se siguió para ejecutar los objetivos específicos y los resultados obtenidos en cada uno de ellos.

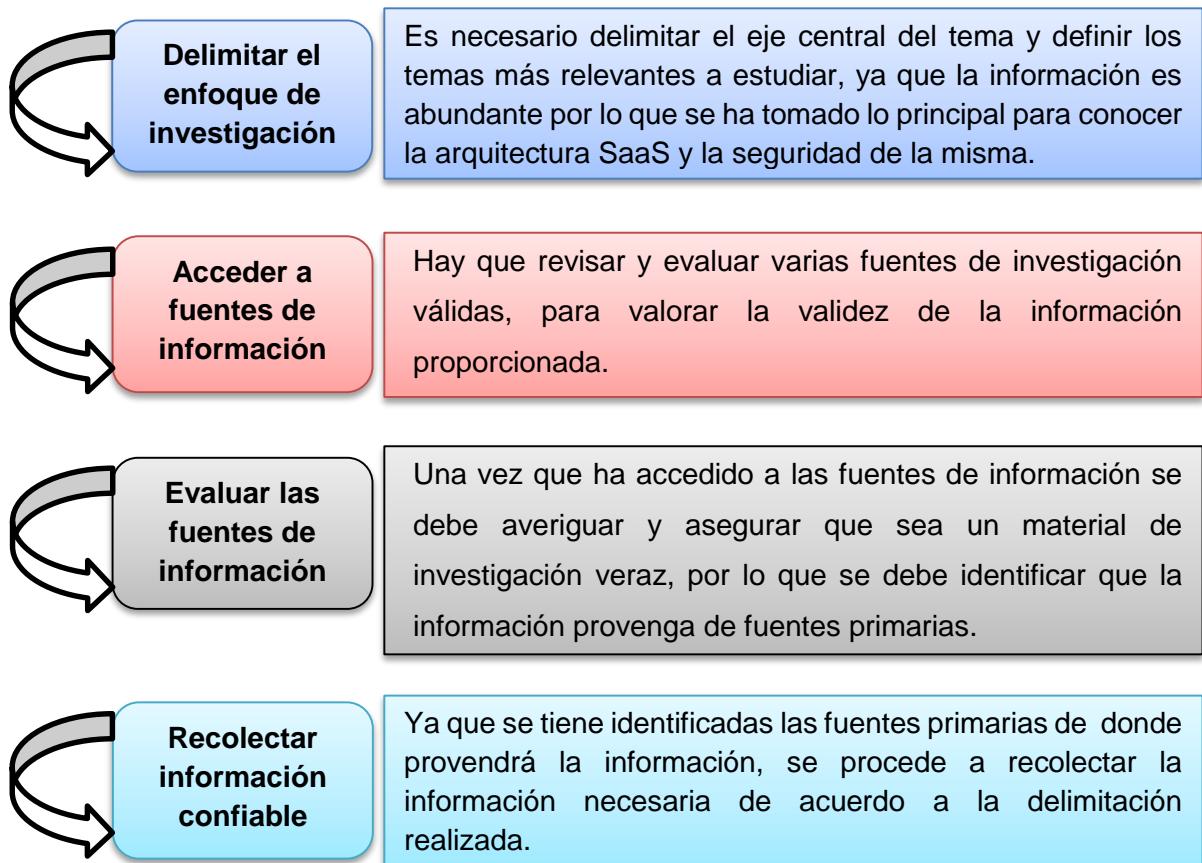
### 7.1. Desarrollo de la propuesta alternativa

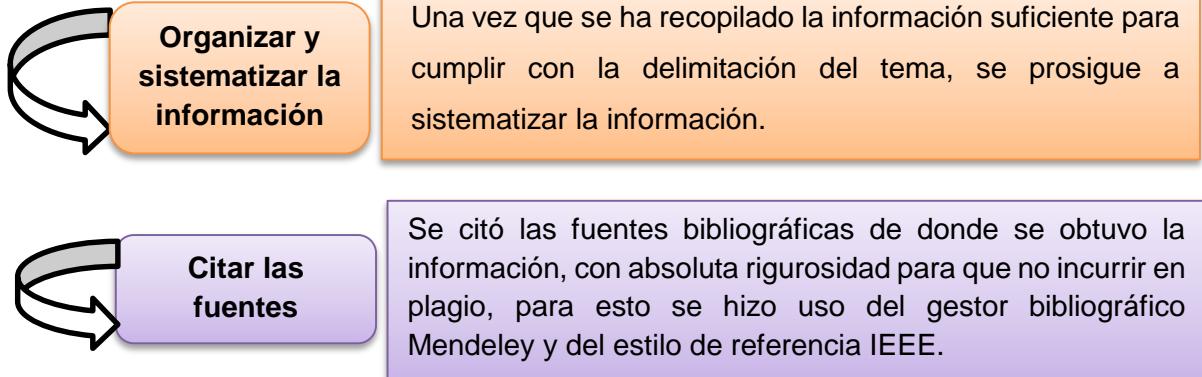
Para dar cumplimiento al presente trabajo de titulación se ha planteado tres objetivos específicos, para llevar a cabo cada uno de ellos se ha realizado una serie de actividades y se ha obtenido los siguientes resultados.

#### 7.1.1. Actividades del primer y segundo objetivo específico

Los objetivos “**Estudiar la arquitectura de servicio SaaS, como modelo tecnológico en la nube**” e “**Investigar acerca de la seguridad de datos en la nube, basándose específicamente en el modelo SaaS**”, se han efectuado bajo las mismas actividades, debido a que se ha seguido los pasos para realizar investigación.

*Tabla 15 Actividades del primer y segundo objetivo específicos*





### 7.1.2. Resultado del primer objetivo específico

Como resultado del primer objetivo se obtuvo un estado del arte, para la realización del mismo se basó en la GUÍA PARA CONSTRUIR ESTADOS DEL ARTE (Véase **Anexo 6**), producto de ello y de la investigación se consiguió información estructurada para conocer la arquitectura; en el cual se hace referencia a la historia de SaaS, definición, estructura de capas de la arquitectura, riesgos, oportunidades, ventajas y desventajas de SaaS, aspectos compartidos entre el software tradicional y SaaS, las estimaciones de costo entre estas dos modalidades, dos perspectivas de SaaS, finalmente el ciclo de vida por el que transita para ser desarrollado como un modelo de servicios.

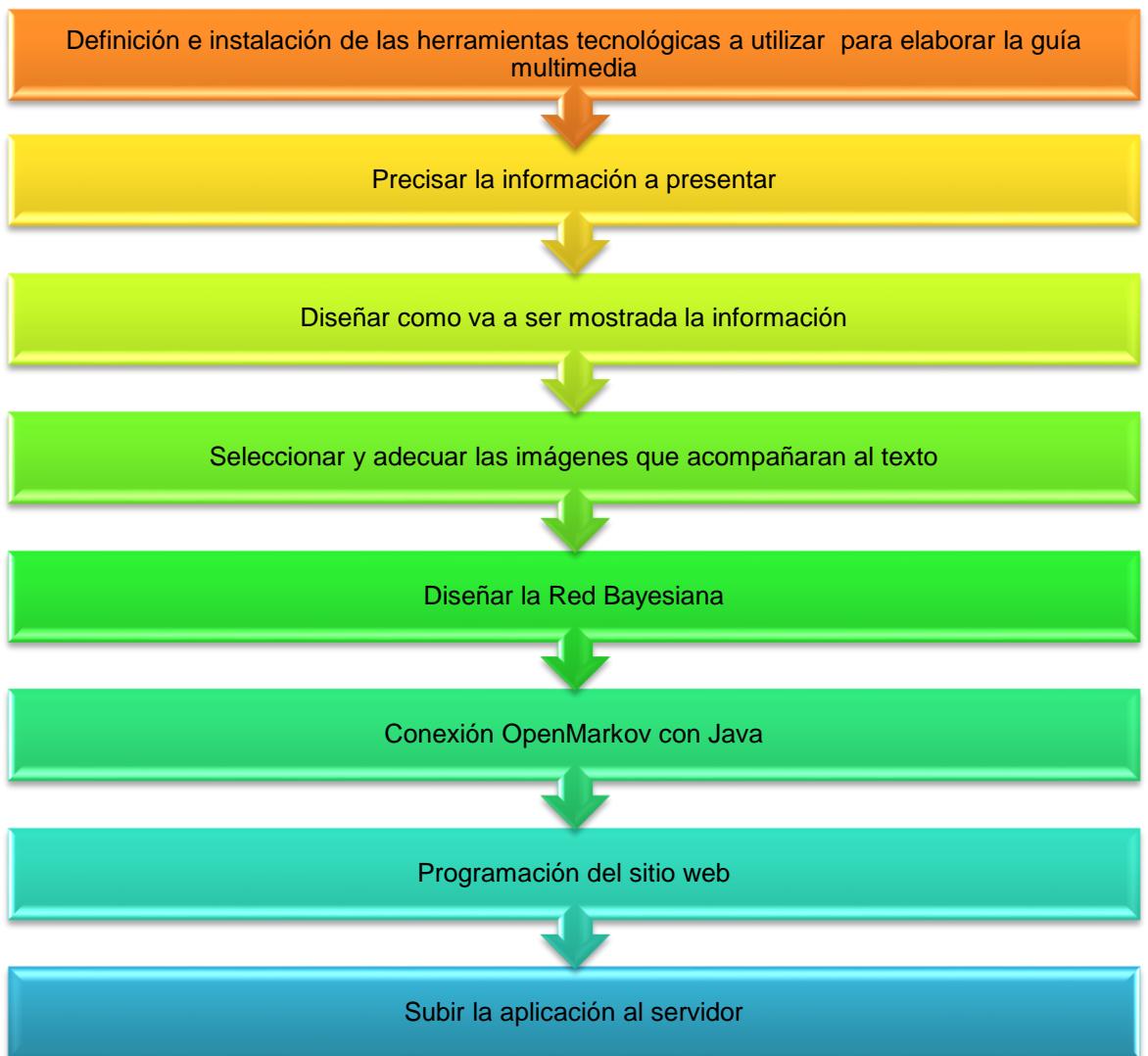
### 7.1.3. Resultado del segundo objetivo específico

Del segundo objetivo planteado se obtuvo como resultado producto de la investigación, un estado del arte general del cual se derivó una nueva versión, con la finalidad de enviarlo a las Jornadas de Ingeniería de Sistemas Informáticos y de Computación (JISIC), de la Escuela Politécnica Nacional.

### 7.1.4. Actividades del tercer objetivo específico

El último objetivo “**Producir una guía de análisis acerca de la seguridad en esta arquitectura**”, para dar cumplimiento al mismo se siguió las actividades especificadas a continuación:

**Tabla 16 Actividades del tercer objetivo específico**



#### **7.1.5. Resultado del tercer objetivo específico**

Como resultado del tercer objetivo se obtiene una guía multimedia, en la cual se da a conocer información acerca de la arquitectura SaaS, tal como: definición, Acuerdo de Nivel de Servicio (SLA), riesgos, vulnerabilidades y las soluciones para mitigar estos problemas de seguridad, además se presenta los tipos de contrato y las cláusulas que deben constar en los mismos.

También se cuenta con un simulador que permite verificar la confiabilidad del proveedor, para ello debe poseer conocimientos previos, los mismos serán adquiridos al interactuar con la guía; para el desarrollo del mismo se hizo uso de Redes Bayesianas.

Además se puede obtener toda la información plasmada en la guía, haciendo click en **DESCARGAR PDF**.

Asimismo se puede acceder a la bibliografía de la información recolectada producto de la investigación efectuada, haciendo click en **BIBLIOGRAFÍA**.

Finalmente en la guía se presenta un video resumen en el que se realiza la contratación de SaaS, exemplificando dos escenarios, en el primero se contrata SaaS haciendo caso a las recomendaciones para asegurar los datos y en el segundo haciendo caso omiso a dichas recomendaciones.

En la figura 53 se muestra la Red Bayesiana diseñada para el simulador, a continuación se desglosa la herencia de variables que tiene cada una.

La primera variable se refiere a la probabilidad de ocurrencia de la variable **EXPERIENCIA DEL PROVEEDOR**, para lo que ha designado variables hijas del nodo:

- **0 – 2 años**
- **3 – 5 años**
- **6 – 10 años**
- **Más de 10 años**

La segunda variable se refiere a la probabilidad de ocurrencia de la variable **TIPO DE CONTRATO**, la cual se desglosa en contrato de:

- **Adhesión**
- **Negociado**

La tercera variable se refiere a la probabilidad de ocurrencia de la variable **CLAUSULAS DEL CONTRATO**, las variables heredadas son:

- **Plan de Continuidad**
- **Confidencialidad**
- **Rendimiento**
- **Servicio de Soporte**
- **Privacidad y cumplimiento normativo**
- **Terminación o modificación**

- **Disponibilidad**
- **Suspensión del servicio**
- **Seguridad**
- **Pagos**

La cuarta variable se refiere a la probabilidad de ocurrencia de la variable **ACUERDO DE NIVEL DE SERVICIO**, siendo padre de los riesgos de seguridad que se discuten en un SLA:

- **Recuperación de los datos**
- **Viabilidad a largo plazo**
- **Acceso de usuarios privilegiados**
- **Ubicación de los datos**

La quinta variable se refiere a la probabilidad de ocurrencia de la variable **CUESTIONAMIENTOS ADICIONALES**, las variables hijas son:

- **Requerimiento de contraseña**
- **Certificado SSL**
- **MAC** (código de autenticación de mensajes)
- **Lista Blanca de URL**
- **SSO** (inicio de sesión único)
- **Restringir el número de intentos**
- **Datos Cifrados**
- **Pregunta de Seguridad**
- **OTP** (contraseña de un solo uso)
- **Esquema de base de datos**, esta variable hija tiene subvariables las mismas son:  
**STSI** (Tablas compartidas e instancias de base de datos compartidos)  
**ITSI** (Tablas independientes e instancias de base de datos compartidos)  
**IDII** (Base de datos independientes e instancias de base de datos independientes)
- **Protocolo de transferencia**, esta variable hija tiene subvariables las mismas son:  
**HTTP**  
**HTTPS**  
**TLS**  
**SSH**

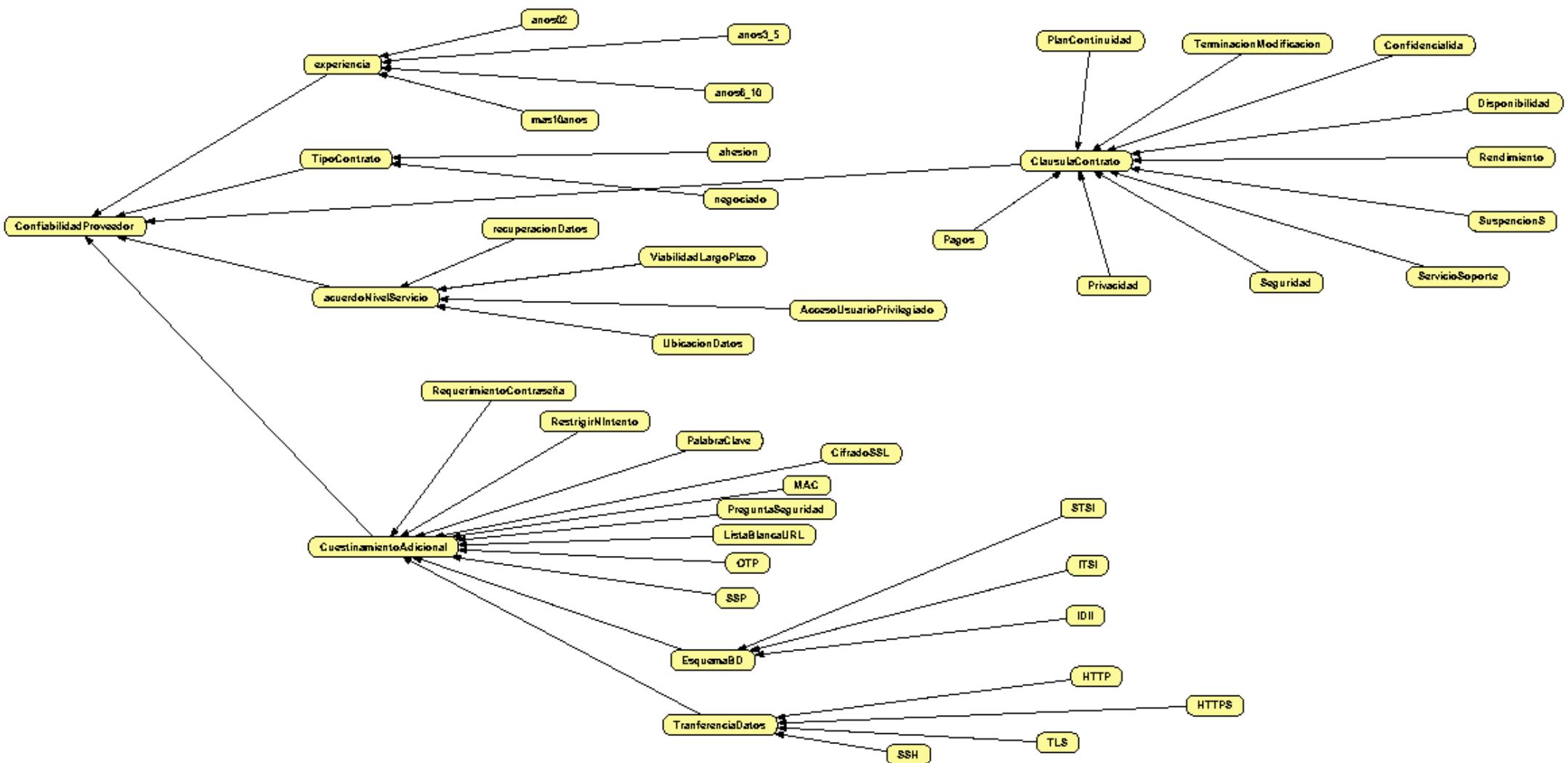


Figura 53 Red Bayesiana utilizada para el simulador

Para determinar la confiabilidad se definió el peso de cada variable y de acuerdo a la probabilidad de ocurrencia se establece la confiabilidad del proveedor.

Potencial del Nodo: ConfiabilidadProveedor							
		Tipo de relación:		Table		Reordenar variables	
TipoContrato	no	no	no	no	no	no	no
experiencia	no	no	no	no	no	no	no
ClausulaContrato	no	no	no	no	yes	yes	yes
acuerdoNivelServicio	no	no	yes	yes	no	no	yes
CuestionamientoAdicional	no	yes	no	yes	no	yes	no
yes	0	0.3	0.3	0.6	0.3	0.6	0.6
no	1	0.7	0.7	0.4	0.7	0.4	0.4

Potencial del Nodo: ConfiabilidadProveedor								
		Tipo de relación:		Table		Reordenar variables		
no	no	no	no	no	no	no	no	no
no	yes	yes	yes	yes	yes	yes	yes	yes
yes	no	no	no	no	yes	yes	yes	yes
yes	no	no	yes	yes	no	no	yes	yes
yes	no	yes	no	yes	no	yes	no	yes
0.9	0.05	0.35	0.35	0.65	0.35	0.65	0.65	0.95
0.1	0.95	0.65	0.65	0.35	0.65	0.35	0.35	0.05

Potencial del Nodo: ConfiabilidadProveedor								
		Tipo de relación:		Table		Reordenar variables		
yes	yes	yes	yes	yes	yes	yes	yes	yes
no	no	no	no	no	no	no	no	yes
no	no	no	no	yes	yes	yes	yes	no
no	no	yes	yes	no	no	yes	yes	no
no	yes	no	yes	no	yes	no	yes	no
0.05	0.35	0.35	0.65	0.35	0.65	0.65	0.95	0.1
0.95	0.65	0.65	0.35	0.65	0.35	0.35	0.05	0.9

Potencial del Nodo: ConfiabilidadProveedor								
		Tipo de relación:		Table		Reordenar variables		
yes	yes	yes	yes	yes	yes	yes	yes	yes
no	yes	yes	yes	yes	yes	yes	yes	yes
yes	no	no	no	no	yes	yes	yes	yes
yes	no	no	yes	yes	no	no	yes	yes
yes	no	yes	no	yes	no	yes	no	yes
0.95	0.1	0.4	0.4	0.7	0.4	0.7	0.7	1
0.05	0.9	0.6	0.6	0.3	0.6	0.3	0.3	0

Figura 54 Peso de cada variable establecido de acuerdo a la probabilidad de ocurrencia

## **7.2. Valoración social, técnica, económica, ambiental**

En lo que respecta a la valoración social y considerando que la Universidad Nacional de Loja, ha implementado un modelo pedagógico en el que es importante la investigación; por lo tanto con la presente se pretende contribuir con las organizaciones que deseen cambiar de alternativa de servicio de almacenamiento de información, para que conozcan los riesgos acerca de la seguridad, a los que están expuestos si utilizan los servicios del modelo SaaS, de esta forma se cumple con el deber que como estudiantes en formación tenemos con la sociedad.

Concerniente a la valoración técnica, la investigación que se ha efectuado ha sido posible, porque se ha contado con la información necesaria, equipos informáticos, y con la guía del director del trabajo de titulación que ha ofrecido las suficientes bases técnicas para desarrollar el presente trabajo.

En cuanto a la valoración económica, debido a la relevancia e importancia que constituye para el estudiante, el presupuesto fue asumido por el autor del trabajo de titulación ya que la investigación es de tipo formativa y en el reglamento general de la Universidad Nacional de Loja estipula esta cláusula.

Finalmente la valoración ambiental, hoy por hoy estamos inmersos en los avances tecnológicos por ende las instituciones buscan nuevas alternativas de servicio como el modelo SaaS, siendo este muy beneficioso porque no causa ningún impacto ambiental, por el contrario mediante la utilización de estos servicios, el software es reutilizado por múltiples usuarios y además aumenta la tasa de utilización de un solo equipo hardware para el abastecimiento de varios usuarios, contribuyendo así con menos equipos deteriorados.

## **8. CONCLUSIONES**

Después de lo investigado y analizado se ha llegado a las siguientes conclusiones.

- La arquitectura SaaS tiene una falencia muy grande en cuanto a la seguridad de los datos, por lo que las organizaciones no hacen uso pleno de este modelo.
- Los datos viajan por diferentes nodos hasta llegar a la región geográfica en la que se encuentra físicamente ubicado el entorno de servicios y el centro de datos de respaldo, pudiendo ser intersectados en este tránsito.
- La seguridad depende de los mecanismos que implemente el proveedor para mitigar las vulnerabilidades inherentes a este tipo de sistemas, además es proporcionalmente dependiente de los hábitos de los usuarios.
- La mayoría de proveedores ofrecen contratos de adhesión, sin que los usuarios tengan la potestad de modificar las cláusulas contractuales del contrato.
- Con la elaboración de la tabla comparativa, se llegó a la conclusión que los proveedores que conforman la alianza de Accenture, brindan seguridad de datos a sus clientes, siendo confiables para depositar nuestros datos a estos proveedores.
- Se utilizó la herramienta de modelos gráficos probabilísticos, Openmarkov, esta fue la mejor opción para diseñar la red bayesiana, ya que la herramienta arroja las posibles combinaciones de la diferentes variables, se establece un peso para cada una de las variables y se procede a calcular la confiabilidad del proveedor.
- Se hizo uso del lenguaje de programación java para la implementación del simulador, mediante este lenguaje se realizó la conexión con openmarkov; para leer la red bayesiana se implementó el constructor; un método para recorrer cada uno de los nodos del archivo pgmx y guardar los valores en una lista creada para ello; finalmente el otro método sirve para obtener el valor calculado y presentarlo en la interfaz.



## **9. RECOMENDACIONES**

Después de lo investigado y analizado se cree conveniente hacer las siguientes recomendaciones.

- Se recomienda como una alternativa de trabajo futuro al proyecto de titulación, que se contraste cada una de las vulnerabilidades citadas mediante un trabajo práctico e implementar las soluciones planteadas, con la finalidad de comprobar que estas sean las más óptimas.
- El sitio web puede ser mejorado, implementando un sistema experto que realice preguntas a los usuarios y que el sistema vaya aprendiendo por sí solo; en base a esta información se plantee nuevas o mejores soluciones, para mantener actualizada la guía.
- Se recomienda a los usuarios que adquieran buenos hábitos en cuanto a la seguridad de las credenciales de acceso y no expongan los datos por insignificantes motivos.
- En cuanto a los contratos, es favorable para los clientes que este sea un contrato negociado, debido a que en él se pueden negociar las cláusulas estipuladas, en cambio en el contrato de adhesión el cliente acepta lo que el proveedor le impone.
- Para identificar rápidamente a los proveedores de SaaS se recomienda recurrir a la red de alianza de proveedores instituida por Accenture, ya que esta alianza está constituida por los mejores proveedores.
- Para el diseño de redes bayesianas se recomienda hacer uso de Openmarkov, ya que esta herramienta por si sola proyecta las posibles combinaciones de las variables, mientras que en otras herramientas el usuario tiene que realizar esta tediosa tarea.
- Se recomienda utilizar el lenguaje de programación java, ya que mediante este se facilita la conexión de la herramienta de modelos probabilísticos para ser utilizado como parte de aplicaciones desarrolladas en un lenguaje de programación.



## **10. BIBLIOGRAFÍA**

- [1] W. Huang, X. Wei, and Y. Zhao, “A Multi-tenant Software as a Service Model for Large Organization,” *Cloud Serv.* ..., pp. 112–119, 2013.
- [2] M. Azure, “¿Qué es SaaS? Software como servicio.” [Online]. Available: <https://azure.microsoft.com/es-es/overview/what-is-saas/>.
- [3] European Knowledge Center for Information Technology, “Guía de Cloud Computing.” Europa, p. 37, 2017.
- [4] Economía Simple, “Definición de proveedor,” 2016. [Online]. Available: <http://www.economiasimple.net/glosario/proveedores>. [Accessed: 04-Apr-2017].
- [5] Marco Goicolea, “¿Qué es SaaS? Definición y ventajas de Software as a Service,” 2014. [Online]. Available: <http://comunidad.iebschool.com/iebs/software-de-gestion/que-es-saas-definicion-ventajas/>. [Accessed: 04-Apr-2017].
- [6] Accenture, “Software como servicio (SaaS): Información general en España,” 2017. [Online]. Available: <https://www.accenture.com/es-es/service-software-service-overview-summary#>. [Accessed: 01-Apr-2017].
- [7] Tonny Rodríguez, “Entendiendo la nube: el significado de SaaS, PaaS y IaaS,” 2012. [Online]. Available: <https://www.genbetadev.com/programacion-en-la-nube/entendiendo-la-nube-el-significado-de-saas-paas-y-iaas>. [Accessed: 31-Mar-2017].
- [8] Jorge Sanchez, “Algunos proveedores IaaS, Paas y/o SaaS,” 2011. [Online]. Available: <https://blogjordisanchez.wordpress.com/2011/11/23/algunos-proveedores-iaas-paas-yo-saas/>. [Accessed: 31-Mar-2017].
- [9] Computerworld, “Diez proveedores SaaS a tener en cuenta,” 2012. [Online]. Available: <http://www.computerworld.es/cloud/diez-proveedores-saas-a-tener-en-cuenta>. [Accessed: 31-Mar-2017].
- [10] Christine Burns, “Diez empresas SaaS a tener en cuenta,” 2016. [Online]. Available: <http://cioperu.pe/fotoreportaje/10269/diez-empresas-saas-a-tener-en-cuenta/?foto=6>. [Accessed: 31-Mar-2017].
- [11] Oracle, “Aplicaciones en la nube (SaaS) Oracle Cloud.” [Online]. Available: [https://cloud.oracle.com/es\\_ES/saas](https://cloud.oracle.com/es_ES/saas). [Accessed: 03-Apr-2017].
- [12] E. Nieto, “Diseño de aplicaciones SaaS sobre plataformas de Cloud Computing,”

2013.

- [13] M. A. Nacional, “Guía Multimedia.” [Online]. Available: <http://www.man.es/man/visita/guias-multimedia.html>.
- [14] L. Sucar, “Redes Bayesianas,” *Decis. Theory Model. Appl. Artif. Intell. Concepts Solut.*, pp. 9–32, 2012.
- [15] J. L. R. Reina, “Tema 8 : Introducción a las Redes Bayesianas,” *Dpto. Ciencias la Comput. e Intel. Artif. Univ. Sevilla*, pp. 1–46, 2006.
- [16] M. Serrano, “Teorema de Bayes.” [Online]. Available: [http://www.sites.upiicsa.ipn.mx/polilibros/portal/Polilibros/P\\_terminados/Probabilidad/doc/Unidad 1/1.3.5.htm](http://www.sites.upiicsa.ipn.mx/polilibros/portal/Polilibros/P_terminados/Probabilidad/doc/Unidad 1/1.3.5.htm).
- [17] F. P. Nava, “Redes Bayesianas : Introducción Redes Bayesianas : Inferencia , Decisión y Aprendizaje,” *Intel. Artif. e Ing. del Conoc. Cent. Super. Informática.*, vol. 70.
- [18] C. Uned, “Openmarkov tutorial,” 2016.
- [19] Org, “OpenMarkov.” [Online]. Available: <http://www.openmarkov.org/>.
- [20] Org, “NetBeans IDE.” [Online]. Available: <https://netbeans.org/features/index.html>.
- [21] O. Belmonte Fernández, “Introduccion al lenguaje de programacion Java,” p. 50, 2005.
- [22] Leandro Alegsa, “Definicion de HTML5.” [Online]. Available: <http://www.alegsa.com.ar/Dic/html5.php>.
- [23] Barbara Pérez, “Qué es HTML5,” 2013. [Online]. Available: <https://hipertextual.com/archivo/2013/05/entendiendo-html5-guia-para-principiantes/>.
- [24] Alan Chavez, “Bootstrap.” .
- [25] XAMPP homepage, “XAMPP.” [Online]. Available: <https://www.apachefriends.org/es/index.html>.
- [26] Sublime Text homepage, “Sublime Text.” [Online]. Available: <https://www.sublimetext.com/>.
- [27] Y. K. B. Sarango and R. A. G. Armijos, “ Aplicación Móvil que permite la localización de productos y control de compras a clientes en supermercados ’ . Director ;,” 2016.
- [28] OpenShift Enterprise, “Web Application Hosting Platform | Red Hat OpenShift.” [Online]. Available: <https://www.openshift.com/web->

- hosting/index.html?sc\_cid=701600000011p9xAAA&gclid=CNjzp4n7t80CFVUkgQodQtwE9Q.
- [29] OpenShift Enterprise, “OpenShift Enterprise: una PaaS privada y en sus instalaciones de Red Hat.”
  - [30] M. ATWOOD, “OpenShift Origin vs OpenStack.” [Online]. Available: <https://blog.openshift.com/openshift-origin-vs-openstack/>.
  - [31] Satya Nadella, “Privacidad de Microsoft.” [Online]. Available: <https://privacy.microsoft.com/es-es/privacy>. [Accessed: 09-May-2017].
  - [32] Satya Nadella, “Auditoría y registro.” [Online]. Available: <https://www.microsoft.com/en-us/trustcenter/security/auditingandlogging>. [Accessed: 09-May-2017].
  - [33] Satya Nadella, “Microsoft Centro de confianza | los delitos informáticos.” [Online]. Available: <https://www.microsoft.com/en-us/trustcenter/security/cybercrime>. [Accessed: 09-May-2017].
  - [34] Satya Nadella, “Microsoft Centro de confianza | El diseño y la seguridad operacional.” [Online]. Available: <https://www.microsoft.com/en-us/trustcenter/security//designopsecurity>. [Accessed: 09-May-2017].
  - [35] Satya Nadella, “Microsoft Centro de confianza | encriptación.” [Online]. Available: <https://www.microsoft.com/en-us/trustcenter/security/encryption>. [Accessed: 09-May-2017].
  - [36] Satya Nadella, “Microsoft Centro de confianza | Identificar y gestión de accesos.” [Online]. Available: <https://www.microsoft.com/en-us/trustcenter/security/identity>. [Accessed: 09-May-2017].
  - [37] Satya Nadella, “Microsoft Centro de confianza | Seguridad de la red.” [Online]. Available: <https://www.microsoft.com/en-us/trustcenter/security/networksecurity>. [Accessed: 09-May-2017].
  - [38] Satya Nadella, “Microsoft Centro de confianza | la gestión de amenazas.” [Online]. Available: <https://www.microsoft.com/en-us/trustcenter/security/threatmanagement>. [Accessed: 09-May-2017].
  - [39] J. C. Sánchez, *Los métodos de investigación*. 2012.
  - [40] M. De, “MÉTODO INVESTIGATIVO PROCEDIMIENTOS : 1 . Observación de hechos y fenómenos : Situarnos en la realidad local y global , de acuerdo a nuestra

ubicación en determinada Establecer de lo observado , específicamente que nos parece que está vacío o es un hecho .”

- [41] A. J. Maia, “Técnicas de entrevista,” *Work. Pap. - OBEGEF*, vol. 2013, p. 28, 2013.
- [42] R. S. Carvajal, “Tecnica De Análisis De Información.” pp. 1–6.
- [43] O. L. Londoño, L. F. Maldonado, and L. C. Calderón, “Guía para construir estados del arte,” *Int. Corp. Networks Knowl.*, pp. 1–39, 2014.
- [44] E. García Montoya, “Sistemas Multimedia : Introducción a los Sistemas Multimedia para Formación,” *Sist. Multimed.*, pp. 407–522, 2001.
- [45] A. Benlian and T. Hess, “Opportunities and risks of software-as-a-service: Findings from a survey of IT executives,” *Decis. Support Syst.*, vol. 52, no. 1, pp. 232–246, Dec. 2011.
- [46] D. Ma and A. Seidmann, “Analyzing software as a service with per-transaction charges,” *Inf. Syst. Res.*, vol. 26, no. 2, pp. 360–378, 2015.
- [47] M. Armbrust, A. Fox, R. Griffith, A. Joseph, and RH, “Above the clouds: A Berkeley view of cloud computing,” *Univ. California, Berkeley, Tech. Rep. UCB* , pp. 07–013, 2009.
- [48] J. J. Lyu, R. C. Hsu, and C. Y. Chen, “AN EMPIRICAL STUDY OF APPLICATION SERVICE PROVIDER (ASP) ADOPTION IN SMEs,” *Int. J. Electron. Bus.*, vol. 7, no. 1, pp. 1–11, 2009.
- [49] X. Tang, C. Y. Chiang, Z. Liu, and J. Lin, “Application Service Provider (ASP) in China: An empirical study of system and service satisfaction,” *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 1–10, 2011.
- [50] R. Vidhyalakshmi and V. Kumar, “Design comparison of traditional application and SaaS,” *2014 Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2014*, pp. 541–544, 2014.
- [51] G. Liu, H. Jiang, and R. Geng, “Software design on a SaaS platform,” *ICCET 2010 - 2010 Int. Conf. Comput. Eng. Technol. Proc.*, vol. 4, pp. 355–358, 2010.
- [52] A. Rico, M. Noguera, J. L. Garrido, K. Benghazi, and J. Barjis, “Extending multi-tenant architectures: a database model for a multi-target support in SaaS applications,” *Enterp. Inf. Syst.*, no. November 2014, pp. 1–22, 2014.
- [53] N. Narasimhaiah and R. P. Sam, “THEORY AND FEATURES OF SAAS (SOFTWARE AS A SERVICE) FOR CLOUD COMPUTING,” *Int. Res. J. Eng.*

- Technol.*, vol. 2, no. 3, p. 1625, 2015.
- [54] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. In??cio, “Security issues in cloud environments: A survey,” *Int. J. Inf. Secur.*, vol. 13, no. 2, pp. 113–170, 2014.
  - [55] M. Baldwin and J. Cromity, “SaaS and Cloud Computing, the Rise of Compartmentalizing Users Online Via Subscription,” *New Rev. Inf. Netw.*, vol. 17, no. February 2013, pp. 120–126, 2012.
  - [56] D. Ma and A. Seidmann, “Analyzing software as a service with per-transaction charges,” *Inf. Syst. Res.*, vol. 26, no. 2, pp. 360–378, 2015.
  - [57] C.-S. Hsu, S.-W. Chou, and H.-T. Min, “Understanding Software-as-a-Service (SaaS) Commitment from a Client-Provider Collaboration Approach,” *PACIS 2015 Proc.*, 2015.
  - [58] M. Cusumano, “Cloud Computing and SaaS as New Computing Platforms,” *Commun. ACM*, vol. 53, no. 4, p. 27, 2010.
  - [59] G. Carraro and F. Chong, “Software as a Service (SaaS): An Enterprise Perspective,” *October*, 2006. [Online]. Available: <https://msdn.microsoft.com/en-us/library/aa905332.aspx>. [Accessed: 05-May-2015].
  - [60] N. Baliyan and S. Kumar, “Towards software engineering paradigm for software as a service,” *2014 7th Int. Conf. Contemp. Comput. IC3 2014*, pp. 329–333, 2014.
  - [61] L. Ertaul, S. Singhal, and G. Saldamli, “Security Challenges in Cloud Computing,” *Secur. Manag.*, pp. 36–42, 2010.
  - [62] G. Z. Yang, F. Zhou, and Z. Zhu, “The application of Saas-based cloud computing in the university research and teaching platform,” in *Proceedings - 2011 International Conference on Intelligence Science and Information Engineering, ISIE 2011*, 2011, pp. 210–213.
  - [63] K. Zhang, Y. Shi, Q. Li, and J. Bian, “Data privacy preserving mechanism based on tenant customization for SaaS,” *1st Int. Conf. Multimed. Inf. Netw. Secur. MINES 2009*, vol. 1, pp. 599–603, 2009.
  - [64] H. Liao, “SaaS business model for software enterprise,” in *ICIME 2010 - 2010 2nd IEEE International Conference on Information Management and Engineering*, 2010, vol. 2, pp. 604–607.
  - [65] H. J. La and S. D. Kim, “A systematic process for developing high quality SaaS cloud

- services," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5931 LNCS, pp. 278–289, 2009.
- [66] W. T. Tsai, X. Y. Bai, and Y. Huang, "Software-as-a-service (SaaS): Perspectives and challenges," *Sci. China Inf. Sci.*, vol. 57, no. 5, pp. 1–15, 2014.
  - [67] L. Wu, S. K. Garg, and R. Buyya, "SLA-Based Resource Allocation for Software as a Service Provider (SaaS) in Cloud Computing Environments," in *2011 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, 2011, pp. 195–204.
  - [68] B. Simmons, H. Ghanbari, M. Litoiu, and G. Iszlai, "Managing a SaaS application in the cloud using PaaS policy sets and a strategy-tree," *Proc. 7th ...*, pp. 343–347, 2011.
  - [69] S. Kang, S. Kang, and S. Hur, "A design of the conceptual architecture for a multitenant SaaS application platform," *Proc. - 1st ACIS/JNU Int. Conf. Comput. Networks, Syst. Ind. Eng. CNSI 2011*, no. Level 1, pp. 462–467, 2011.
  - [70] "Hao-yu WEN, Zhao-jun YANG," no. 72104994, pp. 316–319.
  - [71] Z. Ma and F. Leymann, "BPEL fragments for modularized reuse in modeling BPEL processes," *Proc. 5th Int. Conf. Netw. Serv. ICNS 2009*, pp. 63–68, 2009.
  - [72] T. A. L. Genez, L. F. Bittencourt, and E. R. M. Madeira, "Workflow scheduling for SaaS / PaaS cloud providers considering two SLA levels," *Proc. 2012 IEEE Netw. Oper. Manag. Symp. NOMS 2012*, pp. 906–912, 2012.
  - [73] Z. Zhang, W. He, and Q. Li, "A component model based on semantic for e-commerce PaaS platform," *Proc. - 2013 10th Web Inf. Syst. Appl. Conf. WISA 2013*, pp. 465–470, 2013.
  - [74] F. Xu, F. Liu, H. Jin, and A. V. Vasilakos, "Managing performance overhead of virtual machines in cloud computing: A survey, state of the art, and future directions," *Proc. IEEE*, vol. 102, no. 1, pp. 11–31, 2014.
  - [75] W. T. Tsai, Y. Huang, X. Bai, and J. Gao, "Scalable architectures for SaaS," *Proc. - 2012 15th IEEE Int. Symp. Object/Component/Service-Oriented Real-Time Distrib. Comput. Work. ISORCW 2012*, pp. 112–117, 2012.
  - [76] T. Heart, "Who is Out There? Exploring the Effects of Trust and Perceived Risk on Saas Adoption Intentions," *Data Base Adv. Inf. Syst.*, vol. 41, no. 3, pp. 49–68, 2010.
  - [77] C. Computing, "SULTAN : A Composite Data Consistency Approach for SaaS Multi-Cloud Deployment," 2015.

- [78] A. Goel and N. Yang, "The adoption of software-as-a-service (SaaS): ranking the determinants," pp. 1–6, 2015.
- [79] N. Baliyan and S. Kumar, "Towards software engineering paradigm for software as a service," *2014 7th Int. Conf. Contemp. Comput. IC3 2014*, pp. 329–333, 2014.
- [80] R. Ganesan, S. Sarkar, and N. Tewari, "An independent verification of errors and vulnerabilities in SaaS cloud," *Proc. Int. Conf. Dependable Syst. Networks*, pp. 1–6, 2012.
- [81] V. Kukreja, J. Singh, and A. Sharma, "Contemporary study of cloud computing environment," *Proc. Int. Conf. Adv. Comput. Artif. Intell. - ACAI '11*, pp. 233–235, 2011.
- [82] M. Ribas, A. S. Lima, N. Souza, A. Moura, F. R. C. Sousa, and G. Fenner, "Assessing cloud computing SaaS adoption for enterprise applications using a Petri net MCDM framework," in *IEEE/IFIP NOMS 2014 - IEEE/IFIP Network Operations and Management Symposium: Management in a Software Defined World*, 2014.
- [83] M. Godse and S. Mulik, "An approach for selecting Software-as-a-Service (SaaS) product," in *CLOUD 2009 - 2009 IEEE International Conference on Cloud Computing*, 2009, pp. 155–158.
- [84] N. . Leavitt, "Is Cloud Computing Really Ready for Prime Time?," *Comput. IEEE Comput. Soc.*, vol. 42, no. 1, p. 6, 2009.
- [85] S. A. Cabrera, E. M. Abad, H. Danilo Jaramillo, G. A. Poma, and J. C. Verdum, "Incidencia de atributos de calidad de software en el diseño, construcción y despliegue de ambientes arquitectónicos Cloud," *2015 10th Iber. Conf. Inf. Syst. Technol. Cist. 2015*, 2015.
- [86] T. Hurkmans, "Zero downtime for multi tenant SaaS systems," *Proc. 2009 ESEC/FSE Work. Softw. Integr. Evol. @ runtime - SINTER '09*, p. 1, 2009.
- [87] Z. Jiang, W. Sun, K. Tang, J. L. Snowdon, and X. Zhang, "A Pattern-Based Design Approach for Subscription Management of Software as a Service," in *2009 Congress on Services - I*, 2009, no. PART 1, pp. 678–685.
- [88] A. B. Bondi and R. Bank, "Incorporating Software Performance Engineering Methods and Practices into the Software Development Life Cycle," pp. 327–330.
- [89] C. Tang and J. Liu, "Selecting a trusted cloud service provider for your SaaS program," *Comput. Secur.*, vol. 50, pp. 60–73, 2015.

- [90] A. Murray and G. Begna, "Cloud Service Security & application vulnerability," *SoutheastCon 2015*, pp. 1–8, 2015.
- [91] D. Freet, R. Agrawal, S. John, and J. J. Walker, "Cloud forensics challenges from a service model standpoint," *Proc. 7th Int. Conf. Manag. Comput. Collect. Intell. Digit. Ecosyst. - MEDES '15*, pp. 148–155, 2015.
- [92] L. S. Huang, A. Rice, E. Ellingsen, and C. Jackson, "Analyzing forged SSL certificates in the wild," *Proc. - IEEE Symp. Secur. Priv.*, pp. 83–97, 2014.
- [93] W. Chou, "Inside SSL: The secure sockets layer protocol," *IT Prof.*, vol. 4, no. 4, pp. 47–52, 2002.
- [94] N. Saputro and K. Akkaya, "Performance evaluation of smart grid data aggregation via homomorphic encryption," *Wirel. Commun. Netw. Conf. (WCNC), 2012 IEEE*, pp. 2945–2950, 2012.
- [95] P. K. Chouhan, F. Yao, S. Y. Yerima, and S. Sezer, "Software as a Service : Analyzing Security Issues," no. Bdab, 2014.
- [96] S. R. Lenkala, S. Shetty, and K. Xiong, "Security risk assessment of cloud carrier," *Proc. - 13th IEEE/ACM Int. Symp. Clust. Cloud, Grid Comput. CCGrid 2013*, pp. 442–449, 2013.
- [97] A. Maarouf, A. Marzouk, and A. Haqiq, "A Review of SLA Specification Languages in the Cloud Computing," *10th Int. Conf. Intell. Syst. Theor. Appl. (SITA)*, 2015, pp. 1–6, 2015.
- [98] K. Radha, "A Relative Study on Service Level Agreements in Cloud Computing," no. Gcct, 2015.
- [99] S.-H. Na and E.-N. Huh, "A methodology of assessing security risk of cloud computing in user perspective for security-service-level agreements," *Innov. Comput. Technol. (INTECH), 2014 Fourth Int. Conf.*, pp. 87–92, 2014.
- [100] K. Bernsmed, M. G. Jaatun, P. H. Meland, and A. Undheimy, "Security SLAs for federated Cloud services," *Proc. 2011 6th Int. Conf. Availability, Reliab. Secur. ARES 2011*, pp. 202–209, 2011.
- [101] L. Wu, S. Kumar Garg, S. Versteeg, and R. Buyya, "SLA-based Resource Provisioning for Hosted Software as a Service Applications in Cloud Computing Environments," *IEEE Trans. Serv. Comput.*, vol. 7, no. 3, pp. 1–1, 2014.
- [102] M. Almorsy, J. Grundy, and A. S. Ibrahim, "Collaboration-based cloud computing

- security management framework,” *Proc. - 2011 IEEE 4th Int. Conf. Cloud Comput. CLOUD 2011*, pp. 364–371, 2011.
- [103] W. Zhou *et al.*, “Towards a Data-centric View of Cloud Security,” *Challenges*, pp. 25–32, 2010.
- [104] L. Zhao, S. Sakr, and A. Liu, “Consumer-Centric SLA Manager for Cloud-Hosted Databases,” *Proc. 22nd ACM Int. Conf. Conf. Inf. Knowl. Manag. - CIKM ’13*, pp. 2453–2456, 2013.
- [105] B. R. Kandukuri, R. P. V., and A. Rakshit, “Cloud Security Issues,” *2009 IEEE Int. Conf. Serv. Comput.*, pp. 517–520, 2009.
- [106] C. Rong, S. T. Nguyen, and M. G. Jaatun, “Beyond lightning: A survey on security challenges in cloud computing,” *Comput. Electr. Eng.*, vol. 39, no. 1, pp. 47–54, 2013.
- [107] K. Nishikawa, K. Oki, and A. Matsuo, “SaaS application framework using information gateway enabling cloud service with data confidentiality,” *Proc. - Asia-Pacific Softw. Eng. Conf. APSEC*, vol. 1, pp. 334–337, 2012.
- [108] P. K. Chouhan, F. Yao, and S. Sezer, “Software as a service: Understanding security issues,” *Proc. 2015 Sci. Inf. Conf. SAI 2015*, pp. 162–170, 2015.
- [109] P. K. Tiwari, “A Review of Data Security and Privacy Issues over SaaS,” 2014.
- [110] J. Ni, G. Li, L. Wang, J. Feng, J. Zhang, and L. Li, “Adaptive Database Schema Design for Multi-Tenant Data Management,” *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 9, pp. 2079–2093, 2014.
- [111] “Multi-Tenant Arquitectura de Datos.” .
- [112] M. Hui, D. Jiang, G. Li, and Y. Zhou, “Supporting database applications as a service,” *Proc. - Int. Conf. Data Eng.*, pp. 832–843, 2009.
- [113] N. Zivic, “Reliability of soft verification of message authentication codes,” *Proc. - 5th Int. Conf. Comput. Intell. Commun. Syst. Networks, CICSYN 2013*, pp. 191–196, 2013.
- [114] A. Beikverdi and I. K. T. Tan, “Improved Look-Ahead Re-Synchronization Window for Hmac-Based One-Time Password.”
- [115] W.-B. Hsieh and J.-S. Leu, “Design of a time and location based One-Time Password authentication scheme,” *Wirel. Commun. Mob. Comput. Conf. IWCMC 2011 7th Int.*, pp. 201–206, 2011.
- [116] C. Mainka, “Your Software at my Service Security Analysis of SaaS Single Sign-On

- Solutions in the Cloud,” pp. 93–104, 2014.
- [117] S. K. Sood, “A combined approach to ensure data security in cloud computing,” *J. Netw. Comput. Appl.*, vol. 35, no. 6, pp. 1831–1838, 2012.
  - [118] M. Monshizadeh, Z. Yan, L. Hippelainen, and V. Khatri, “Cloudification and security implications of TaaS,” *Comput. Networks Inf. Secur. (WSCNIS), 2015 World Symp.*, pp. 1–8, 2015.
  - [119] K. Surya, M. Nivedithaa, S. Uma, and C. Valliyammai, “Security issues and challenges in cloud,” *2013 Int. Conf. Green Comput. Commun. Conserv. Energy*, pp. 889–893, 2013.
  - [120] E. Saleh, I. Takouna, and C. Meinel, “SignedQuery: Protecting users data in multi-tenant SaaS environments,” *Proc. 2013 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2013*, pp. 213–218, 2013.
  - [121] T. Choi and M. G. Gouda, “HTTPI: An HTTP with integrity,” *Proc. - Int. Conf. Comput. Commun. Networks, ICCCN*, 2011.
  - [122] T. Kiuchi, “C-HTTP -- The Development of a Secure, Closed HTTP-based Network,” pp. 64–75, 1996.
  - [123] K. Patel, N. Singh, K. Parikh, K. S. S. Kumar, and N. Jaisankar, “Data security and privacy using data partition and centric key management in cloud,” *Int. Conf. Inf. Commun. Embed. Syst.*, no. 978, pp. 1–5, 2014.
  - [124] S. Turner, “Transport layer security,” *IEEE Internet Comput.*, vol. 18, no. 6, pp. 60–63, 2014.
  - [125] Z. Huawei and L. Ruixia, “A scheme to improve security of SSL,” *Proc. 2009 Pacific-Asia Conf. Circuits, Commun. Syst. PACC 2009*, no. 6, pp. 401–404, 2009.
  - [126] M. Atighetchi, N. Soule, P. P. Pal, J. P. Loyall, A. Sinclair, and R. Grant, “Safe configuration of {TLS} connections,” *Cns*, pp. 415–422, 2013.
  - [127] F. Yang, L. Pan, M. Xiong, and S. Tang, “Establishment of security levels in trusted cloud computing platforms,” *Proc. - 2013 IEEE Int. Conf. Green Comput. Commun. IEEE Internet Things IEEE Cyber, Phys. Soc. Comput. GreenCom-iThings-CPSCom 2013*, pp. 2119–2122, 2013.
  - [128] H. Z. Wang and L. S. Huang, “An improved trusted cloud computing platform model based on DAA and Privacy CA scheme,” *ICCASM 2010 - 2010 Int. Conf. Comput. Appl. Syst. Model. Proc.*, vol. 13, no. Iccasm, pp. 33–39, 2010.

- [129] A. E. D. P. DE DATOS, “Guía para clientes que contraten servicios de Cloud Computing,” p. 23, 2013.
- [130] P. Pérez San-José, C. Gutiérrez Borge, C. de la Fuente Rodríguez, L. García Pérez, and E. Álvarez Alonso, “Guía para empresas: seguridad y privacidad del cloud computing,” *Inst. Nac. Tecnol. la Comun.*, pp. 1–56, 2011.
- [131] T. I. C. Portal, E. European, and I. Technology, “TIC Portal es una iniciativa de EKCIT European Knowledge Center for Information Technology,” 2016.

## 11. ANEXOS

**Anexo 1:** Captura de pantalla de la entrega del Estado del Arte a las Jornadas de Ingeniería de Sistemas Informáticos y de Computación (JISIC).

De: EasyChair <[noreply@easychair.org](mailto:noreply@easychair.org)>  
Asunto: JISIC 2016 submission  
Fecha: 16 de agosto de 2016, 11:17:21 ECT  
Para: "Pablo F. =?UTF-8?B?T3Jkb8OxZXotT3Jkb8OxZXo=?=" <[pfordonez@unl.edu.ec](mailto:pfordonez@unl.edu.ec)>

Dear Pablo F. Ordoñez-Ordoñez,

Pablo Ordoñez <[pfordonez@unl.edu.ec](mailto:pfordonez@unl.edu.ec)> submitted the following paper to JISIC 2016:

---

Vulnerabilidad de datos en la Arquitectura del Software como Servicio (SaaS): Estado del Arte

---

You are listed as one of the authors of this paper. To enter the JISIC 2016 Web pages you should visit

<https://easychair.org/conferences/?conf=jisic2016>

and enter your EasyChair user name and .  
password.

If you forgot your user name or password,  
please visit

<https://easychair.org/account/forgot.cgi>

and specify [pfordonez@unl.edu.ec](mailto:pfordonez@unl.edu.ec) as your email address.

Best regards,  
EasyChair Messenger.

*Anexo 1. Confirmación de recepción del Estado del Arte*

**Anexo 2:** Estado del Arte derivado del entregable del segundo objetivo, documento enviado a las JISIC.

# Vulnerabilidad de datos en la Arquitectura del Software como Servicio (SaaS): Estado del Arte.

**Resumen**—SaaS es un modelo de negocio exitoso en la nube, su curva de implantación es la preferencia para muchas instituciones, entre ellas las educativas. La Universidad Nacional de Loja en Ecuador implementa estos servicios, es por ello que el presente trabajo es el resultado de las investigaciones de estudios acumulados en el conocimiento de las inseguridades SaaS, correlacionadas a la pregunta de investigación del acuerdo de nivel de servicio y las vulnerabilidades de datos en SaaS, vistas como factores de riesgo en la seguridad. Finalmente, no establecer acuerdos de nivel de servicios (SLA) es la vulnerabilidad más relevante del caso.

**Keywords**—Software como Servicio (SaaS), Seguridad, Vulnerabilidad, Acuerdo de Nivel de Servicio (SLA).

## I. INTRODUCCIÓN

SaaS permite que las aplicaciones sean desplegadas de forma remota y alojadas en la nube, esta arquitectura es la categoría más avanzada de este paradigma [1], siendo la capa más alta de la estructura de computación en la nube, estos servicios son bastante utilizados por las empresas porque permite reducir los costos de inversión en cuanto a la compra de hardware y software. Las entidades universitarias requieren de un gran número de recursos tecnológicos modernos, para abastecer las necesidades que conllevan los procesos de enseñanza e investigación, por lo que en el presupuesto anual, un porcentaje considerable es asignado para la adquisición de hardware y software [2]. Por tal razón las Universidades han optado por hacer uso de la tecnología SaaS, la cual le ha permitido realizar la implementación de servicios de aplicaciones de software, servicios de la plataforma de desarrollo, el modelado de los servicios informáticos, integración de la información, la enseñanza y la utilización integral de aplicaciones virtuales a distancia de la plataforma de trabajo [3], por consecuencia SaaS está siendo altamente utilizado por la mayoría de universidades ecuatorianas como una alternativa para mejorar los servicios y agilizar los procesos.

En la arquitectura SaaS las aplicaciones ya no son un producto sino un servicio [4], es un modelo de negocio para la distribución de software [5], que proporciona acceso al mismo y a sus funciones a través de Internet, constituyéndose como una de las principales amenazas para la seguridad de los datos ya que son transmitidos por esta red de redes [6]. Además la utilización de los servicios de software, plataformas e infraestructura basados en web [7] [8], permite que varios clientes (inquilinos) puedan compartir la misma instancia de un software y acceder a los datos [9] que se alojan en los servidores de la compañía de tecnologías de información y comunicación través de internet, haciendo referencia a que múltiples clientes pueden utilizar las mismas instalaciones se puede decir que con ello se aumenta las tasas de utilización de hardware y redes [10]. Las organizaciones pueden tener a

su disposición estos servicios a cambio de una tarifa [11] [12], pagando por el uso de la aplicación SaaS de forma regular de acuerdo a un determinado contrato de suscripción [13] [14], además los proveedores de SaaS son subsidiarios de toda la infraestructura de red, software, hardware, plataforma operativa, y es responsable del mantenimiento y otros servicios. Como ya se mencionó que hacer uso de este servicio implica estar expuesto a grandes riesgos de seguridad de los datos [2], por ello la confiabilidad es el mayor desafío en la amplia aceptación de SaaS [15], teniendo en cuenta que los datos se encuentran alojados fuera de la instituciones educativas, pudiendo ser víctima de robo, modificación, pérdida entre otras vulnerabilidades, quedando expuesto el activo más importante hoy en día de toda entidad.

Los temas que se expondrán en el presente estado del arte estarán distribuidos de acuerdo a la pregunta de investigación y de la siguiente manera: en la sección II se hace referencia a los Acuerdos de Nivel de Servicio (SLA) el cual es un contrato escrito que captura las garantías acordadas entre un proveedor de servicios y su cliente, este discute acerca de cómo se manejan algunos riesgos de seguridad [16]. La sección III trata sobre los factores de riesgo en los que se ve involucrado el cliente en cuanto a la seguridad de datos en SaaS. La sección IV hace mención a las inseguridades a las que están expuestos los datos, utilizando los servicios de esta arquitectura, además se adjunta los mecanismos de seguridad de los que se puede hacer uso para brindar una solución en la mitigación de estas vulnerabilidades. Finalmente en la sección V se presenta las conclusiones de los temas abordados en el presente documento.

## II. ACUERDO DE NIVEL DE SERVICIO (SLA)

La tecnología de la computación en la nube se enfrenta a retos como, proporcionar seguridad e integridad de los datos que se está transmitiendo [17], razón por la cual existen los denominados SLA, este es un acuerdo o un vínculo jurídico entre el proveedor y las instituciones en el contexto de la prestación de un servicio en particular [18] [19] [20]. Los SLA se han convertido en una parte importante del modelo de prestación de servicios en la nube [21], los clientes y los proveedores de SaaS deben establecer un SLA para definir la calidad de servicio (QoS) [22], además se debe tomar en cuenta que este enfoque sirve para especificar y administrar la seguridad, la cual es rara vez considerada ya que es diferente a otros atributos como la calidad de servicio, rendimiento y fiabilidad [23], sin embargo SLA abarca aspectos relacionados con la seguridad de los datos [24]. Cabe destacar que algunas universidades desconocen la existencia de este acuerdo o por lo menos lo especificado en él, por experiencia propia se ha evidenciado que no cuentan con un SLA para realizar el convenio con su proveedor, este es de gran importancia ya que también se encuentra en su contenido factores relacionados con

la seguridad de los datos [25]. De acuerdo al artículo de los autores de [26] [27] los cuales mencionan que, SLA tiene que discutir cómo se manejan los siguientes riesgos de seguridad:

#### *II-A. Acceso de usuarios privilegiados*

Procesar los datos sensibles fuera de la empresa trae consigo un nivel de riesgo inherente, ya que los servicios extremalizados evitan los controles físicos, lógicos y de personal de tecnología de información (TI) del cliente, por lo que se podría deducir que el cliente no tiene el control de los datos ya que se encuentran en manos de un proveedor de servicios, por esta razón las instituciones educativas en el papel de clientes deberían obtener la mayor información posible acerca de las personas que manejan los datos y no simplemente hacer uso de estos servicios por una necesidad y dejar de lado los riesgos a los que se están exponiendo. En el contrato se debe especificar los términos y condiciones no solo del proveedor sino incluir los de la Universidad también, otro requisito fundamental que deberían solicitar es que los proveedores suministren información específica sobre la contratación y supervisión de los administradores privilegiados, y sobre los controles de acceso realizados.

#### *II-B. Cumplimiento de la normativa*

Los clientes son en última instancia, responsables de la seguridad e integridad de sus propios datos, incluso cuando está en manos de un proveedor de servicios, según [28] la integridad de los datos es uno de los elementos más críticos en cualquier sistema y aún más en SaaS. Los proveedores de este tipo de servicios son sometidos a auditorías y certificaciones de seguridad externas pero algunos de estos proveedores se niegan a someterse a este escrutinio, se debería observar detenidamente ya que están dando señales claras que solo se puede utilizar estos servicios para las funciones más triviales o de poca significancia real de la entidad educativa, ya que si no permiten que les efectúen una auditoría es evidente que no son confiables, es por ello que antes de contratar este servicio se debe realizar un análisis previo a los términos y condiciones que los proveedores nos proporcionan, además es fundamental conocer acerca de la reputación de los mismos.

#### *II-C. Ubicación de los datos*

Los usuarios finales al utilizar los servicios proporcionados por los proveedores de la nube, no conocen la ubicación de los recursos de almacenamiento de datos [29], el consumidor no sabe exactamente dónde se encuentran alojados los datos [28], de hecho, ni siquiera se sabe en qué país se almacenarán. Los proveedores deberían comprometerse con el almacenamiento y procesamiento de datos en jurisdicciones específicas, evitando así problemas posteriores al cliente, además deberían elaborar un compromiso contractual para obedecer los requisitos de privacidad locales en nombre de sus clientes.

#### *II-D. Recuperación de los datos*

Incluso si no se sabe dónde están incrustados los datos, el proveedor debe manifestar lo que ocurrirá con los datos y el servicio de recuperación de datos en caso de un desastre. Cualquier oferta que no se replica en la infraestructura de datos y aplicaciones a través de múltiples sitios es vulnerable a un

fracaso total. El cliente tendrá que asegurarse, si el proveedor tiene la capacidad de hacer una restauración completa, y cuánto tiempo tomará en realizar dicha actividad.

#### *II-E. Viabilidad a largo plazo*

Idealmente, el proveedor nunca irá a la quiebra o será adquirida por otra gran empresa. Pero se deberá considerar esta posibilidad y asegurar que los datos estarán disponibles incluso después de tal evento. Pedir a los proveedores que nos hagan conocer cómo se recuperan los datos, y si estos son entregados a la nueva empresa propietaria o son entregados en primera instancia al cliente, además se debe tener en cuenta que los datos recuperados estén en un formato en el que permita importar a una aplicación de reemplazo. [30] [16]

### **III. VULNERABILIDADES DE LOS DATOS Y RECOMENDACIONES PARA SU MITIGACIÓN**

Los datos son muy vulnerables a amenazas como la fuga de datos, modificación, privacidad de los usuarios y confidencialidad entre otros. A continuación se manifiesta los principales problemas y se describe una manera eficiente para hacer frente a cada una de estas vulnerabilidades de seguridad.

#### *III-A. Esquema de Base de Datos inseguro*

En el ambiente SaaS, existen tres tipos de esquemas de BD para la gestión de datos Multi-Tenant, los mismos son: base de datos independientes e instancias de base de datos independientes (IDII), tablas independientes e instancias de base de datos compartidos (ITSI), y, tablas compartidas e instancias de base de datos compartidos (STSII) [31]. El esquema que es catalogado como el más seguro pero el más costoso, es IDII [31] [32], en este esquema existe para el almacenamiento de datos una BD para cada inquilino, siendo el método más sencillo para proporcionar un adecuado aislamiento y seguridad de datos [33], sería ideal que un proveedor de servicios ofrezca este esquema de BD.

#### *III-B. Servidor no autorizado*

Como es de conocimiento los datos deben ser transmitidos a través de la red a la nube, hay numerosos medios a través de los cuales un atacante puede actuar como un servidor titular de la nube, haciendo uso de la red basada en Internet, esto evidentemente conlleva a la pérdida de datos. Para evitar la pérdida de datos en esta situación, se usa el certificado SSL, las Autoridades de Certificación (CA) emiten este certificado, que es una credencial para el mundo en línea. Consiste en que el primer servidor de la nube envía la información de identificación al propietario cuando se conecta, a continuación envía al propietario una copia de su certificado SSL. El propietario verifica el certificado y luego envía un mensaje al servidor y el servidor devuelve un acuse de recibo firmado digitalmente para iniciar una sesión SSL cifrada, que permite la transferencia de datos cifrados entre el navegador y el servidor. Por lo que se recomienda hacer uso de este certificado, ya que con su utilización se tiene la certeza de que el servidor que está proporcionando una respuesta es el servidor anfitrión, y que se puede realizar la transmisión de forma segura, sabiendo que el servidor ha sido identificado previamente.

### *III-C. Ataque de fuerza bruta*

No es una tarea difícil descifrar las contraseñas de las computadoras, se puede realizar grandes números de combinaciones de forma rápida con el fin de determinar todas las posibles claves, a esto se le denomina ataque de fuerza bruta. Existen múltiples técnicas de cifrado fuerte que ayudan a mitigar el riesgo de sufrir un ataque de fuerza bruta y reducir las vulnerabilidades a las que están expuestos los datos [34], entre ellos encontramos al protocolo Secure Socket Layer (SSL) o también denominado Transport Layer Security (TLS) según [35] [36]. SSL es el protocolo de seguridad de las comunicaciones de mayor despliegue en Internet que proporciona confidencialidad, integridad de datos y autenticación de la identidad para comunicaciones a través de Internet entre dos partes [37], ya que se lo considera como un protocolo de estado, orientado a la conexión cliente-servidor. Además SSL ofrece encriptación que evita que los interceptores lean los datos que transitan en la nube, el cifrado SSL de 128 bits ofrece más bits de longitud de clave, además este tipo de cifrado consiste en una clave pública (que codifica la información) y una clave privada (que descifra la información), por lo que implica que solo los poseedores de claves pueden leerlo, esta es una adecuada opción que se puede tomar en vez de usar un cifrado SSL de 40 bits y también se puede desplazar a 256 bits siempre que sea necesario. SSL de 128 bits es lo suficientemente complejo como para que se lleve a efecto un ataque de fuerza bruta, conjuntamente se puede utilizar cifrado doble, uno por medio del propietario y otra mediante SSL. Por lo que se podría decir que la potencia de procesamiento que se necesita para romper la seguridad es insuficiente, siendo uno de los factores más relevantes que lograría que la mayoría de los ataques sean ineficaces. Este enfoque no solo preserva que los datos no sean víctima de los intrusos, sino que también ayuda a asegurar a los clientes que los datos están seguros mientras están en tránsito.

### *III-D. Manipulación de los datos*

Los datos están siempre bajo la amenaza de ser manipulados por cualquier interceptor no autorizado, siendo un desafío para el proveedor de SaaS garantizar la seguridad de los mismos para ello utiliza medidas de precaución, como el cifrado de datos de acuerdo a [2] es considerada como una buena solución a este problema, según [38] el cifrado de datos se refiere a los cálculos matemáticos y algoritmos que convierte el texto sin formato a texto cifrado, para que la información no pueda ser leída por usuarios no autorizados; otro método es cifrado SSL el cual ya ha sido mencionado en párrafos anteriores, estas son medidas adoptadas para no dejar que nadie manipule los datos, pero aun así los datos necesitan ser comprobados después de la transmisión. Una opción para dicha comprobación sería el uso de MAC (código de autenticación de mensaje) según [39] son algoritmos criptográficos simétricos, que proporcionan integridad de los datos permitiendo el reconocimiento de cualquier modificación o manipulación del mensaje durante la transmisión y la autenticación de origen de los datos, suministrando la confirmación de que el mensaje se originó por el remitente, que comparte la clave secreta utilizada por el receptor. MAC de datos cifrados se genera por el propietario antes de enviarlo y MAC se transmite junto con los datos cifrados. Por otro lado, cuando el receptor recibe los datos, puede generar el MAC y compararlo con el MAC que

generó el propietario y que fue recibido junto con los datos, si los códigos MAC son iguales, entonces se asegura el usuario de la integridad de los datos, es decir, los datos no han sido manipulados.

### *III-E. Pérdida de identidad de usuario y contraseña*

Según [26] un desafío clave de la implementación de aplicaciones centradas en el entorno multiusuario es asegurar que todo el procesamiento de consulta y el intercambio de datos se lleven a cabo de forma segura, es decir que las partes implicadas sean autenticadas y autorizadas de una forma estricta.

A continuación se pone a consideración dos formas en la que los usuarios colaborarían a que sus datos sean vulnerables a cualquier ataque, la primera contempla que el mismo usuario evidencia sus credenciales revelándolas a una persona extraña, para la detección de la pérdida de información por este insignificante motivo los proveedores de SaaS deben implementar una técnica que impida el acceso del intruso al sistema, la segunda se refiere a que los usuarios establecen contraseñas demasiado vulnerables por la sencilla razón que si utilizan una contraseña segura que involucra caracteres alfanuméricos los usuarios no recuerda esta combinación.

Ahora se realizará un análisis a las dos maneras referidas anteriormente. En caso de que el usuario revele su identidad de usuario y contraseña a cualquier persona no autorizada, los datos pueden estar en peligro. Para proteger los datos se deberá realizar una pregunta de seguridad a los usuarios cuya respuesta solo la sabe el usuario autorizado, por lo que el usuario no autorizado no podrá acceder a los datos incluso después de tener las credenciales de ingreso correctas, otra medida de seguridad y la más eficiente es implementar el código de un solo uso para el ingreso a la cuenta, este mecanismo de autenticación es designado con el nombre de contraseña de un solo uso (OTP) conforme a [40] [41] estos se generan de forma dinámica solo con fines de uso único y tienen una vida útil limitada utilizable. Tras el uso, la contraseña será invalidada por el cliente y el servidor del sistema de autenticación.

Por lo que se puede concluir que el uso de OTP es capaz de solucionar algunos de los problemas en los que se incurre al utilizar el mecanismo de contraseña fija tradicional. Debido a la naturaleza de la OTP, los usuarios no va a tener la misma contraseña para los diferentes inicios de sesión.

Haciendo referencia a [42] [43] en los cuales plantean un medio de seguridad mucho más eficiente al cual se lo denota con el nombre de inicio de sesión único (SSO), este tiene muchas ventajas sobre los mecanismos simples de nombre de usuario y contraseña, en este caso el usuario tiene que recordar varias combinaciones diferentes, y la seguridad se basa únicamente en la fuerza de la contraseña proporcionada por el usuario, pero SSO permite la adopción de varias medidas técnicas para mejorar aún más la seguridad del procedimiento de inicio de sesión. De forma general, el uso de la autenticación SSO se lleva a cabo utilizando un tercero de confianza denominado proveedor de identidad (IdP). Cuando un usuario utiliza su agente de usuario (UA), para solicitar un inicio de sesión al proveedor de servicio a través de un navegador web, en vez de pedir nombre de usuario y contraseña, el servicio

emite una solicitud de emergencia y redirecciona al cliente IdP. Después de la autenticación correcta, el IdP emite un token de autenticación firmado y redirige al cliente de SaaS, donde se validará el token y el usuario conectado. [44] [45]

Otro medio de seguridad del que se puede hacer uso para reducir los ataques de suplantación de identidad es, que el proveedor de servicios de la nube (CSP) decida restringir el acceso al sistema solo para el conjunto de lista blanca de direcciones URL. Esta forma de proteger la identidad del usuario es eficiente ya que incluso si un cliente posee las credenciales legítimas no podrá ingresar al sistema debido a que la URL no se encuentra almacenada en los registros del CSP, razón por la cual el acceso se desactivará. [43]

### III-F. Algoritmo de cifrado de contraseñas débil

En el caso de que el proveedor SaaS no tenga implementado ningún otro mecanismo de seguridad para el ingreso a las cuentas, más que el de usuario y contraseña, se debería exigir al proveedor que por lo menos cuente con un algoritmo de cifrado seguro y que en añadura a esto utilice el medio de contraseñas ocultas, ya que si no se hace uso de este mecanismo todas las contraseñas se almacenan como un archivo de una vía, lo que hace al sistema vulnerable a ataques de piratas de contraseñas. Incluso un intruso podría acceder al sistema y copiar este archivo en su propia máquina y ejecutar cualquier cantidad de programas para descifrar las contraseñas. Si hay una contraseña insegura en el archivo, es solo cuestión de tiempo antes de que el pirata la descubra. Las contraseñas ocultas previenen este tipo de ataque al almacenar este archivo de contraseñas en un archivo especial, el cual únicamente puede ser leído por el usuario root. Esto obliga al intruso que intente descubrir la contraseña de forma remota a ingresar a los servicios de red SSH, este proporciona claves criptográficamente fuertes para acceder a los datos [36]. Un tipo de ataque común para lograr obtener acceso a los sistemas es el denominado fuerza bruta, es mucho más lento y deja un rastro evidente, pues los intentos fallidos de conexión son registrados en los archivos del sistema.

### III-G. Protocolo de seguridad de datos en la red

SaaS como tal es un sistema cliente/servidor, donde tanto el cliente (el navegador web, explorador o visualizador) como el servidor (el servidor web) y el protocolo mediante el que se comunican (HTTP) son partes invariables para llevar a cabo el flujo de trabajo de SaaS, el canal de transmisión que se establece no siempre se considera seguro ya que en este proceso los datos se transmiten en un gran número de paquetes y fluyen a través de numerosos dispositivos de otras infraestructuras antes de llegar al destino [46] [47]. Por lo tanto el proceso de transmisión del flujo de datos puede estar sujeto a las amenazas de la red, tales como ataque DNS, ataque MITM, suplantación de IP, escaneo de puertos y ataques sniffer.

el proveedor SaaS debería establecer la comunicación por medio de los protocolos de seguridad existentes, tales como TLS, SSH o HTTPS, para asegurar que la información es transmitida por un canal seguro [48], este último proporciona tres garantías de seguridad, la autenticación del servidor, integridad de mensajes y confidencialidad de los mensajes [49], los cuales son factores importantes e influyentes para asegurar

la seguridad de los datos, sin embargo en [6] afirma que TLS y SSH son los protocolos criptográficos anfitriones. Algunos proveedores utilizan simplemente el protocolo HTTP porque es barato de usar pero no proporciona garantías de seguridad [49] para transmitir datos a través de la red, no es considerado como seguro ya que la protección depende de cada usuario final [50], por lo que dejan a responsabilidad del usuario limitar el tipo de información que se transmite.

## IV. CONCLUSIONES

El uso de la arquitectura SaaS está en auge, especialmente en las instituciones educativas, debido a los múltiples beneficios que esta presta y en especial por el ahorro significativo de costos financieros que la utilización de esta conlleva, por esto la alternativa más utilizada es SaaS, ayudando a mejorar el nivel de enseñanza e investigación.

Hacer uso de SaaS, significa compartir la responsabilidad tanto el cliente como el proveedor de servicios SaaS, los cuales hacen posible que la información que está en juego sea almacenada de la forma más segura posible, para llegar a este convenio se debería establecer un SLA entre las dos partes involucradas, donde se haga constar por medio de este acuerdo los compromisos, obligaciones y responsabilidades del cliente y proveedor.

Las instituciones que optan por hacer uso de SaaS, deben realizar un análisis previo acerca de la situación actual de su posible proveedor, antes de involucrarse por medio de un contrato legal, si bien es cierto el uso de SaaS provee múltiples beneficios, pero también se debe considerar los riesgos a los que se expone una Institución al compartir su información a terceros, considerando que todos los proveedores de SaaS no manejan el mismo nivel de seguridad de los datos.

## REFERENCIAS

- [1] P. Nawrocki, "Michał Sobociński PUBLIC CLOUD COMPUTING FOR SOFTWARE," vol. 15, no. 1, 2014.
- [2] G. Z. Yang, F. Zhou, and Z. Zhu, "The application of SaaS-based cloud computing in the university research and teaching platform," in *Proceedings - 2011 International Conference on Intelligence Science and Information Engineering, ISIE 2011*, pp. 210–213, 2011.
- [3] X. Sheng, G. W. Ren, and Z. Wang, "The application of cloud computing SaaS delivery model in university talents training," *Proceedings of the 2011 2nd International Conference on Digital Manufacturing and Automation, ICDMA 2011*, pp. 1203–1205, 2011.
- [4] A. Rico, M. Noguera, J. L. Garrido, K. Benghazi, and J. Barjis, "Extending multi-tenant architectures: a database model for a multi-target support in SaaS applications," *Enterprise Information Systems*, no. November 2014, pp. 1–22, 2014.
- [5] N. Narasimhaiah and R. P. Sam, "THEORY AND FEATURES OF SAAS (SOFTWARE AS A SERVICE) FOR CLOUD COMPUTING," *International Research Journal of Engineering and Technology (IRJET)*, vol. 02, no. 03, p. 1625, 2015.
- [6] D. A. B. Fernandes, L. F. B. Soárez, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, "Security issues in cloud environments: A survey," *International Journal of Information Security*, vol. 13, no. 2, pp. 113–170, 2014.
- [7] M. Baldwin and J. Cromity, "SaaS and Cloud Computing, the Rise of Compartmentalizing Users Online Via Subscription," *New Rev. Inf. Netw.*, vol. 17, no. February 2013, pp. 120–126, 2012.
- [8] D. Ma and A. Seidmann, "Analyzing software as a service with per-transaction charges," *Information Systems Research*, vol. 26, no. 2, pp. 360–378, 2015.

- [9] C.-S. Hsu, S.-W. Chou, and H.-T. Min, "Understanding Software-as-a-Service (SaaS) Commitment from a Client-Provider Collaboration Approach," *PACIS 2015 Proceedings*, 2015.
- [10] M. Cusumano, "Cloud Computing and SaaS as New Computing Platforms," *Communications of the ACM*, vol. 53, no. 4, p. 27, 2010.
- [11] G. Carraro and F. Chong, "Software as a Service (SaaS): An Enterprise Perspective," 2006.
- [12] N. Balyan and S. Kumar, "Towards software engineering paradigm for software as a service," *2014 7th International Conference on Contemporary Computing, IC3 2014*, pp. 329–333, 2014.
- [13] W. Huang, X. Wei, and Y. Zhao, "A Multi-tenant Software as a Service Model for Large Organization," *Cloud and Service ...*, pp. 112–119, 2013.
- [14] L. Ertaul, S. Singhal, and G. Sakkamli, "Security Challenges in Cloud Computing," *Security and Management*, pp. 36–42, 2010.
- [15] K. Zhang, Y. Shi, Q. Li, and J. Bian, "Data privacy preserving mechanism based on tenant customization for SaaS," *1st International Conference on Multimedia Information Networking and Security, MINES 2009*, vol. 1, pp. 599–603, 2009.
- [16] L. Zhao, S. Sakr, and A. Liu, "Consumer-Centric SLA Manager for Cloud-Hosted Databases," *Proceedings of the 22nd ACM international conference on Conference on information & knowledge management - CIKM '13*, pp. 2453–2456, 2013.
- [17] S. R. Lenkala, S. Shetty, and K. Xiong, "Security risk assessment of cloud carrier," *Proceedings - 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing, CCGrid 2013*, pp. 442–449, 2013.
- [18] A. Maaroni, A. Marzouk, and A. Haqiq, "A Review of SLA Specification Languages in the Cloud Computing," *10th International Conference on Intelligent Systems: Theories and Applications (SITA), 2015*, pp. 1–6, 2015.
- [19] K. Radha, "A Relative Study on Service Level Agreements in Cloud Computing," no. Geet, 2015.
- [20] S.-H. Na and E.-N. Huh, "A methodology of assessing security risk of cloud computing in user perspective for security-service-level agreements," *Innovative Computing Technology (INTECH), 2014 Fourth International Conference on*, pp. 87–92, 2014.
- [21] K. Bernsmoed, M. G. Jaatum, P. H. Meland, and A. Undheimy, "Security SLAs for federated Cloud services," *Proceedings of the 2011 6th International Conference on Availability, Reliability and Security, ARES 2011*, pp. 202–209, 2011.
- [22] L. Wu, S. Kumar Gang, S. Versteeg, and R. Buyya, "SLA-based Resource Provisioning for Hosted Software as a Service Applications in Cloud Computing Environments," *IEEE Transactions on Services Computing*, vol. 7, no. 3, pp. 1–1, 2014.
- [23] M. Almorsy, J. Grundy, and A. S. Ibrahim, "Collaboration-based cloud computing security management framework," *Proceedings - 2011 IEEE 4th International Conference on Cloud Computing, CLOUD 2011*, pp. 364–371, 2011.
- [24] K. Stamou, V. Kantere, and J. H. Morin, "SLA data management criteria," *Proceedings - 2013 IEEE International Conference on Big Data, Big Data 2013*, pp. 34–42, 2013.
- [25] M. Alhamad, T. Dillon, and E. Chang, "Conceptual SLA framework for cloud computing," *4th IEEE International Conference on Digital Ecosystems and Technologies - Conference Proceedings of IEEE-DEST 2010, DEST 2010*, pp. 606–610, 2010.
- [26] W. Zhou, M. Sherr, W. R. Marczak, Z. Zhang, T. Tao, B. T. Loo, and I. Lee, "Towards a Data-centric View of Cloud Security," *Challenges*, pp. 25–32, 2010.
- [27] M. Antonio, T. Rojas, N. M. Gonzalez, F. Shampato, and F. Red, "Inclusion of Security Requirements in SLA Lifecycle Management for Cloud Computing," pp. 7–12, 2015.
- [28] A. Murray and G. Begna, "Cloud Service Security & application vulnerability," *SoutheastCon 2015*, pp. 1 – 8, 2015.
- [29] C. Rong, S. T. Nguyen, and M. G. Jaatum, "Beyond lightning: A survey on security challenges in cloud computing," *Computers and Electrical Engineering*, vol. 39, no. 1, pp. 47–54, 2013.
- [30] B. R. Kandukuri, R. P. V., and A. Rakshit, "Cloud Security Issues," 2009 *IEEE International Conference on Services Computing*, pp. 517–520, 2009.
- [31] J. Ni, G. Li, L. Wang, J. Feng, J. Zhang, and L. Li, "Adaptive Database Schema Design for Multi-Tenant Data Management," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 9, pp. 2079–2093, 2014.
- [32] y. R. W. Frederick Chong, Gianpaolo Carrao, "Multi-Tenant Arquitectura de DataS," 2006.
- [33] M. Hui, D. Jiang, G. Li, and Y. Zhou, "Supporting database applications as a service," *Proceedings - International Conference on Data Engineering*, pp. 832–843, 2009.
- [34] D. Freet, R. Agrawal, S. John, and J. J. Walker, "Cloud forensics challenges from a service model standpoint," *Proceedings of the 7th International Conference on Management of computational and collective intelligence in Digital EcoSystems - MEDES '15*, pp. 148–155, 2015.
- [35] S. Turner, "Transport layer security," *IEEE Internet Computing*, vol. 18, no. 6, pp. 60–63, 2014.
- [36] K. Surya, M. Nivedithaa, S. Uma, and C. Valliyammai, "Security issues and challenges in cloud," *2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE)*, pp. 889–893, 2013.
- [37] Z. Huawei and L. Ruixia, "A scheme to improve security of SSL," *Proceedings of the 2009 Pacific-Asia Conference on Circuits, Communications and System, PACCS 2009*, no. 06, pp. 401–404, 2009.
- [38] K. Nishikawa, K. Oki, and A. Matsuo, "SaaS application framework using information gateway enabling cloud service with data confidentiality," *Proceedings - Asia-Pacific Software Engineering Conference, APSEC*, vol. 1, pp. 334–337, 2012.
- [39] N. Zivic, "Reliability of soft verification of message authentication codes," *Proceedings - 5th International Conference on Computational Intelligence, Communication Systems, and Networks, CICSyN 2013*, pp. 191–196, 2013.
- [40] A. Beikverdi and I. K. T. Tan, "Improved Look-Ahead Re-Synchronization Window for Hmac-Based One-Time Password,"
- [41] W.-B. Hsieh and J.-S. Leu, "Design of a time and location based One-Time Password authentication scheme," *Wireless Communications and Mobile Computing Conference IWCMC 2011 7th International*, pp. 201–206, 2011.
- [42] C. Mainka, "Your Software at my Service Security Analysis of SaaS Single Sign-On Solutions in the Cloud," pp. 93–104, 2014.
- [43] R. Ganeshan, S. Sarkar, and N. Tewari, "An independent verification of errors and vulnerabilities in SaaS cloud," *Proceedings of the International Conference on Dependable Systems and Networks*, pp. 1–6, 2012.
- [44] S. K. Sood, "A combined approach to ensure data security in cloud computing," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1831–1838, 2012.
- [45] M. Momshizadeh, Z. Yan, L. Hippelainen, and V. Khatri, "Cloudification and security implications of TaaS," *Computer Networks and Information Security (WSCNIS), 2015 World Symposium on*, pp. 1–8, 2015.
- [46] P. K. Chouhan, F. Yao, and S. Sezer, "Software as a service: Understanding security issues," *Proceedings of the 2015 Science and Information Conference, SAI 2015*, pp. 162–170, 2015.
- [47] P. K. Tiwari, "A Review of Data Security and Privacy Issues over SaaS," 2014.
- [48] E. Saleh, I. Takouna, and C. Meinel, "SignedQuery: Protecting users data in multi-tenant SaaS environments," *Proceedings of the 2013 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2013*, pp. 213–218, 2013.
- [49] T. Choi and M. G. Gouda, "HTTP: An HTTP with integrity," *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, 2011.
- [50] T. Kiuchi, "C-HTTP – The Development of a Secure, Closed HTTP-based Network," pp. 64–75, 1996.

#### Anexo 2. Artículo enviado a las JISIC

**Anexo 3:** Solicitud enviada a la Unidad de Telecomunicaciones e Información (UTI).

**Anexo 4:** Correo proporcionando información solicitada a la UTI.

Petición de información de SaaS       Recibidos   

---

Esther Elizabeth Jaramillo Malla 16/6/16   
Buenos días ingeniero, el motivo del presente es para coordinar la reunión en...

---

Milton Labanda Uni <miltonlab@unl.edu.ec> 16/6/16   
para mí

Estimada Ester, sería el lunes lo q pasa es q estoy pidiendo permiso pues tengo q ausentarme.

---

Esther Elizabeth Jaramillo Malla <eejaramillom@unl.edu.ec> 16/6/16   
para Milton

Muchas gracias ingeniero, queda para el día lunes, por favor si me puede confirmar la hora.

---

Milton Labanda Uni <miltonlab@unl.edu.ec> 4/7/16   
para mí

Ester esto es lo que se puede considerar como términos de la relación de la UNL con Google, como le comenté no existe documentación impresa y luego de hacer la consulta a los administradores de Google esto es lo que me proporcionario.  
[http://www.google.com/apps/intl/en/terms/education\\_terms.html](http://www.google.com/apps/intl/en/terms/education_terms.html)

*Anexo 3 Correo proporcionando información UTI*

## **Anexo 5: Información proporcionada por la UTI**

### **Acuerdo de G Suite for Education (online)**

El presente Acuerdo de G Suite for Education (el "Acuerdo") se establece entre Google Inc. ("Google") y el cliente identificado en el Documento de pedido (el "Cliente"). El presente Acuerdo tendrá validez a partir de la fecha en la que el Cliente haga clic en el botón "Acepto" que se muestra más abajo o, si es aplicable, en la fecha en la que se firme el Acuerdo (la "Fecha de Entrada en Vigor"). Si aceptas el Acuerdo en representación del Cliente, manifiestas y garantizas que: i) cuentas con la autoridad legal suficiente para vincular a tu superior o a la correspondiente entidad a los presentes términos y condiciones, ii) has leído y comprendido el Acuerdo y iii) lo aceptas en nombre de la parte a la que representas. Si no cuentas con la autoridad legal para vincular al Cliente, no hagas clic en el botón "Acepto" que se muestra más abajo (o, si corresponde, no firmes este Acuerdo). Este Acuerdo rige el acceso por parte del Cliente a los Servicios y la utilización de los mismos, y estará en vigor a partir de la Fecha de Entrada en Vigor.

## **1. Servicios.**

**1.1 Instalaciones y Transferencia de Datos.** Todas las instalaciones utilizadas para almacenar y procesar los Datos del Cliente deberán cumplir con los estándares razonables de seguridad y en ningún caso podrán ser inferiores a los estándares de seguridad de las instalaciones donde Google almacena y procesa información similar propia. Google ha implementado sistemas y procedimientos que se ajustan, como mínimo, a los estándares del sector, con el fin de garantizar la seguridad y la confidencialidad de los Datos del Cliente, proteger dichos datos contra amenazas o riesgos previsibles para la seguridad o la integridad y evitar el acceso o el uso no autorizado de los mismos. Como parte del proceso de proporcionar los Servicios, Google puede transferir, almacenar y procesar los Datos del Cliente en los EE.UU. y en otros países donde Google o sus representantes tengan instalaciones. Al hacer uso de los Servicios, el Cliente da su consentimiento para la transferencia, el procesamiento y el almacenamiento de Datos del Cliente.

## **1.2 Modificaciones.**

a. En los Servicios. Google puede realizar cambios comercialmente razonables en los Servicios cuando lo considere oportuno. En caso de realizar un cambio sustancial en los Servicios, Google informará al Cliente, siempre y cuando el Cliente se haya suscrito en Google para que se le informe de dicho tipo de cambio.

b. En las Condiciones de las URL. Google puede realizar cambios comercialmente razonables en las Condiciones de las URL cuando lo estime oportuno. Si Google realiza un cambio sustancial en las Condiciones de las URL, entonces informará de ello al Cliente, ya sea mediante el envío de un mensaje a la Dirección de Correo Electrónico de Notificación o bien avisando al Cliente a través de la Consola de Administración. Si el cambio tiene un impacto negativo importante para el Cliente y este no lo acepta, el Cliente debe informar de ello a Google a través del Centro de Ayuda en un plazo máximo de treinta días tras la recepción del aviso del cambio. Si el Cliente informa a Google conforme a lo establecido, se seguirá rigiendo por las condiciones vigentes previas al cambio hasta que finalice el Período de Vigencia estipulado. Si se renuevan los Servicios, se renovarán según las Condiciones de las URL de Google en ese momento.

**1.3 Alias.** El Cliente es el único responsable de supervisar, responder y procesar de cualquier otro modo los mensajes de correo electrónico enviados a los alias "abuse" y "postmaster" para los Nombres de Dominio del Cliente. No obstante, Google también puede supervisar los correos electrónicos enviados a estos alias para los Nombres de Dominio del Cliente con el fin de que Google pueda detectar abusos relacionados con los Servicios.

**1.4 Anuncios.** Google no incluye Anuncios en los Servicios ni utiliza los Datos del Cliente con fines publicitarios.

**1.5 Cuentas de Usuario Final.** El Cliente puede solicitar Cuentas de Usuario Final de las siguientes formas: i) solicitándolas online a través de la Consola de administración, o bien ii) después de la Fecha de Comienzo de los Servicios, poniéndose en contacto con el personal de asistencia de Google. El Cliente puede suspender o eliminar Cuentas de Usuario Final en cualquier momento a través de la Consola de Administración.

**1.6 Google Vault.** Si el Cliente adquiere Google Vault, se aplicarán también las condiciones siguientes:

a. Retención. Google no tendrá ninguna obligación de retener ningún Dato del Cliente archivado después del periodo de retención especificado por el Cliente (a menos que sea necesaria su conservación en caso de litigio). Si el Cliente no renueva Google Vault, Google no estará obligado a conservar los Datos del Cliente archivados.

b. Compra inicial de Google Vault. En su compra inicial de Google Vault, el Cliente acepta adquirir Cuentas de Usuario Final de Google Vault para todos los miembros de su Plantilla que tengan Cuentas de Usuario Final de G Suite for Education. El Cliente puede utilizar Google Vault para Estudiantes y Antiguos Alumnos sin que se le aplique ninguna tarifa.

c. Cuentas de Usuario Final Adicionales para la Plantilla. Una vez que el Cliente haya realizado su compra inicial de Google Vault, si durante el Periodo de Vigencia de los Servicios añade al menos un 20% más de Cuentas de Usuario Final para empleados que

las que se adquirieron en un principio, el Cliente acepta adquirir Google Vault para dichas Cuentas de Usuario Final adicionales para el tiempo que reste del Periodo de Vigencia de los Servicios del Cliente. Además, en cada aniversario de la Fecha de Inicio de Facturación, el Cliente acepta adquirir Google Vault para las Cuentas de Usuario Final para empleados que haya adquirido además de las que ya adquirió en un principio para el tiempo que reste del Periodo de Vigencia de los Servicios de Google Vault.

**1.7 Aviso de Privacidad.** El Aviso de Privacidad de G Suite for Education regula cómo recoge y utiliza Google la información del Cliente o los Usuarios Finales.

#### **Obligaciones del Cliente.**

**2.1 Usuarios Permitidos.** Los Servicios solo los podrán utilizar a) instituciones educativas sin ánimo de lucro y b) otras entidades sin ánimo de lucro (tal y como se define en los estatutos de estado relevantes).

**2.2 Cumplimiento.** El Cliente utilizará los Servicios de conformidad con la Política de Uso Aceptable. Google puede ofrecer, según considere oportuno, aplicaciones, herramientas, características o funciones nuevas a través de los Servicios, cuyo uso puede depender de la aceptación por parte del Cliente de ciertas condiciones adicionales. Asimismo, Google pondrá a disposición del Cliente y de sus Usuarios Finales otros Productos No Pertenecientes a G Suite (además de los Servicios) en virtud de las Condiciones de los Productos No Pertenecientes a G Suite y de las Condiciones de servicio de Google específicas del producto aplicables. Si el Cliente no desea habilitar ninguno de los Productos No Pertenecientes a G Suite, el Cliente puede habilitarlos o inhabilitarlos en cualquier momento a través de la Consola de Administración.

**2.3 Administración de los Servicios por parte del Cliente.** A través de la Consola de Administración, el Cliente puede designar a uno o a más Administradores, los cuales tendrán derecho a acceder a las Cuentas de Administrador y a administrar las Cuentas de Usuario Final. El Cliente es responsable de: a) mantener la confidencialidad de la contraseña y de las Cuentas de Administrador, b) designar a las personas autorizadas a acceder a las Cuentas de Administrador y c) garantizar que todas las actividades que tengan lugar en relación con las Cuentas de Administrador cumplan con las condiciones del presente Acuerdo. El Cliente acepta que las responsabilidades de Google no incluyen la administración o gestión interna de los Servicios para el Cliente y que Google actúa únicamente como procesador de datos.

**2.4 Consentimiento del Usuario Final.** Los Administradores del Cliente pueden tener la capacidad para acceder, supervisar, utilizar o divulgar los datos disponibles para los Usuarios Finales dentro de las Cuentas de Usuario Final. El Cliente obtendrá y conservará todos los consentimientos necesarios de los Usuarios Finales para: i) permitir que el Cliente

acceda, supervise, utilice y divulgue dichos datos, y que Google le proporcione la capacidad para ello, y ii) permitir que Google proporcione los Servicios.

**2.5 Consentimiento de los padres.** De conformidad con la sección 10.1 del presente acuerdo, el Cliente es responsable de cumplir con la ley de protección de la privacidad infantil online (COPPA, Children's Online Privacy Protection Act) de 1998, incluida la obtención del consentimiento de los padres para recabar información personal en los Servicios o en los Productos No Pertenecientes a G Suite a los que el Cliente conceda acceso a los Usuarios Finales. El Cliente también deberá obtener el consentimiento previo de los padres para permitir que los Usuarios Finales menores de 18 años utilicen los Productos No Pertenecientes a G Suite.

**2.6 Uso no autorizado.** El Cliente realizará todos los esfuerzos razonables desde el punto de vista comercial para impedir un uso no autorizado de los Servicios y para poner fin a dicho uso. El Cliente informará rápidamente a Google de cualquier uso o acceso no autorizado a los Servicios del que tenga conocimiento.

**2.7 Restricciones de uso.** A no ser que Google lo acuerde específicamente por escrito, el Cliente no llevará a cabo ninguna de las acciones descritas a continuación y realizará todos los esfuerzos razonables desde un punto de vista comercial para evitar que terceras partes lleven a cabo las acciones siguientes: a) vender, revender, arrendar (o su equivalente funcional) los Servicios a terceros (a menos que dichas acciones se hayan autorizado expresamente en este Acuerdo), b) intentar realizar ingeniería inversa en los Servicios o en cualquier componente, c) intentar crear un servicio sustitutivo o similar a través del uso o del acceso a los Servicios, d) utilizar los Servicios para Actividades de Alto Riesgo o e) utilizar los Servicios para almacenar o transferir Datos del Cliente de cualquier tipo cuya exportación esté regulada por las Leyes de Control sobre Exportación aplicables. El Cliente es el único responsable del cumplimiento con la ley estadounidense de portabilidad y responsabilidad de seguros médicos (HIPAA), si fuera aplicable.

**2.8 Solicitudes de Terceros.** El Cliente es responsable de responder a las Solicitudes de Terceros. En la medida permitida por la ley o por las condiciones de las Solicitudes de Terceros, Google: a) informará de inmediato al Cliente de la recepción de una Solicitud de un Tercero, b) satisfará las solicitudes razonables del Cliente en relación con sus esfuerzos para oponerse a una Solicitud de un Tercero y c) proporcionará al Cliente la información o las herramientas necesarias para que este responda a una Solicitud de un Tercero. El Cliente intentará, en primer lugar, obtener por sí mismo la información necesaria para responder a una Solicitud de un Tercero. Se pondrá en contacto con Google solamente en caso de que no consiga obtener de una manera razonable dicha información.

**3. Pago.** Si alguno de los Servicios se ha adquirido por una Cuota, las condiciones de esta Sección 3 se aplicarán a dichos Servicios.

**3.1 Pago.** Todas las Cuotas se harán efectivas durante los 30 días siguientes a la fecha de emisión de la factura. Todos los pagos se efectuarán en dólares estadounidenses a menos que se indique lo contrario en el Formulario de Pedido. Los pagos realizados por transferencia bancaria deben incluir las siguientes instrucciones:

Nombre de la entidad bancaria: Número de ABA: Número de cuenta:

Wells Fargo Bank

Palo Alto, California EE. UU. 121000248

Google Inc. 4375669785

**3.2 Pagos Adeudados.** Puede que se aplique a los pagos adeudados un interés del 1,5% al mes (o el tipo más alto que permita la ley, si es inferior) desde la fecha de vencimiento del pago hasta que este se abone en su totalidad. El Cliente será responsable de asumir todos los gastos razonables (incluidos honorarios de abogados) en los que incurra Google para cobrar los importes atrasados, salvo si dichos importes son fruto de errores de facturación atribuibles a Google.

### **3.3 Pedidos de Compra.**

a. Obligatorio. Si el Cliente quiere que aparezca un número de Pedido de Compra en su factura, deberá informar a Google al respecto y emitirá un Pedido de Compra a Google. Si el Cliente debe presentar un Pedido de Compra y no se lo proporciona a Google, Google no estará obligado a prestar los Servicios hasta que haya recibido el Pedido de Compra. Los términos y condiciones que rigen un pedido no se aplican a este Acuerdo y se consideran nulos de pleno derecho.

b. No es Obligatorio. Si el Cliente no necesita que se incluya un número de Pedido de Compra en la factura, el Cliente comunicará a Google su renuncia del requisito de Pedido de Compra, que podrá ser, a tal efecto, un correo electrónico. Si el Cliente renuncia al requisito de Pedido de Compra: a) Google facturará al Cliente sin un Pedido de Compra y el b) Cliente aceptará pagar facturas sin un Pedido de Compra.

**3.4 Impuestos.** El Cliente es responsable de pagar los Impuestos correspondientes y abonará a Google los Servicios sin ninguna reducción de Impuestos. En caso de que Google se vea en la obligación de recaudar o de pagar Impuestos, estos serán facturados al Cliente, excepto que este proporcione a Google un certificado de exención tributaria válido emitido por la autoridad fiscal pertinente. Si las leyes aplicables requieren que el Cliente retenga Impuestos de sus pagos a Google, este deberá facilitar a Google un recibo tributario oficial o cualquier otra documentación relevante para justificar dichos pagos.

**3.5 Conflictos Relacionados con Facturas.** Los conflictos que puedan surgir en relación con facturas deben comunicarse antes de la fecha de vencimiento de dichas facturas. Si las partes determinan que existen errores de facturación atribuibles a Google, Google no emitirá una factura rectificativa, sino una nota de crédito en la que especificará la cantidad incorrecta de la factura en cuestión. Si dicha factura todavía no se ha abonado, Google le aplicará la cantidad de la nota de crédito y el Cliente será responsable de pagar el saldo neto resultante.

**4. Facturación y tarifas.** Si alguno de los Servicios se adquiere por una Cuota, las condiciones de esta Sección 4 se aplicarán a dichos Servicios. Durante o después de la Fecha de Inicio de Facturación, Google facturará al Cliente las siguientes Cuotas por cada Servicio aplicable: pago adelantado por el Cargo Mensual, Cargo Anual o Cargo del Periodo de Vigencia Inicial (según sea aplicable). Todo esto se especificará en el Formulario de Pedido.

## 5. Servicios de Asistencia Técnica.

**5.1 Por parte del Cliente.** El Cliente deberá, bajo su propia responsabilidad, responder a las preguntas y reclamaciones planteadas por los Usuarios Finales o por terceros que guarden relación con el uso que el Cliente o sus Usuarios Finales hagan de los Servicios. El Cliente realizará los esfuerzos necesarios comercialmente razonables para resolver cualquier incidencia de asistencia antes de solicitar la ayuda de Google.

**5.2 Por parte de Google.** Si el Cliente no puede resolver una incidencia de asistencia técnica de acuerdo con lo expuesto anteriormente, podrá solicitar ayuda a Google de acuerdo con las Directrices de servicio de asistencia técnica (TSS). Google proporcionará el servicio de asistencia técnica al Cliente de acuerdo con las Directrices de TSS.

## 6. Suspensión.

**6.1 Cuentas de Usuario Final por parte de Google.** Si Google tiene conocimiento de algún incumplimiento del presente Acuerdo por parte de una Cuenta de Usuario Final, podría solicitar al Cliente la Suspensión de la cuenta en cuestión. En caso de que el Cliente no satisfaga dicha solicitud de Google, será Google quien podrá llevar a cabo la Suspensión de la Cuenta de Usuario Final. La duración de cualquier Suspensión por parte de Google se prolongará hasta que el Usuario Final en cuestión haya subsanado el incumplimiento causante de la Suspensión.

**6.2 Problemas de Seguridad Urgentes.** Sin perjuicio de lo indicado anteriormente, en caso de producirse un Problema de Seguridad Urgente, Google podría suspender de forma automática el uso ofensivo. La Suspensión tendrá la duración y el alcance mínimos necesarios para evitar o resolver el Problema de Seguridad Urgente. En caso de que Google suspenda una Cuenta de Usuario Final por cualquier motivo sin previa notificación

al Cliente, por solicitud de este, Google informará al Cliente sobre los motivos de la Suspensión tan pronto como sea razonablemente posible.

## **7. Información Confidencial.**

**7.1 Obligaciones.** Cada una de las partes: a) protegerá la Información Confidencial de la otra parte con las mismas medidas de protección estándar que utilice para proteger su propia Información Confidencial y b) no divulgará la Información Confidencial, excepto a Afiliados, empleados y agentes que necesiten conocerla y que hayan aceptado por escrito mantener la confidencialidad. Cada una de las partes (y todos los Afiliados, empleados y representantes a los que se haya revelado Información Confidencial) puede utilizar la Información Confidencial únicamente para ejercer sus derechos y cumplir las obligaciones establecidas en este Acuerdo, al tiempo que emplea las medidas razonables para protegerla. Cada una de las partes es responsable de las acciones de sus Afiliados, empleados y representantes que infrinjan esta Cláusula.

**7.2 Excepciones.** La Información Confidencial no incluye información a) que ya sea conocida por el destinatario, b) que se haga pública sin responsabilidad del destinatario, c) que el destinatario genere de forma independiente o d) que un tercero le transmita legítimamente.

**7.3 Divulgación Necesaria.** Cada una de las partes puede divulgar la Información Confidencial de la otra parte cuando sea requerido por ley, aunque, si la ley lo permite, solo después de que: a) ejerza todos los esfuerzos comercialmente razonables para informar a la otra parte y b) conceda a la otra parte la oportunidad de recusar la divulgación.

**7.4 FERPA.** Las partes reconocen que a) los Datos del Cliente pueden incluir información personal de identificación de registros de educación sujetos a FERPA ("Registros FERPA") y b) en la medida que los Datos del Cliente incluyan Registros FERPA, Google se considerará un "Centro de enseñanza oficial" (de acuerdo con el uso del término en FERPA y sus normativas de implementación) y cumplirá lo estipulado en FERPA.

## **8. Derechos de Propiedad Intelectual y Elementos de Marca.**

**8.1 Derechos de Propiedad Intelectual.** A excepción de lo establecido de forma expresa en este documento, este Acuerdo no garantiza a ninguna de las partes ningún derecho, ya sea implícito o de cualquier otro tipo, sobre el contenido o la propiedad intelectual de la otra parte. Conforme a lo acordado entre las partes, el Cliente es el titular de todos los Derechos de Propiedad Intelectual correspondientes a los Datos del Cliente y Google es el titular de todos los Derechos de Propiedad Intelectual correspondientes a los Servicios.

**8.2 Exhibición de Características de Marca.** Google puede mostrar solamente aquellas Características de Marca del Cliente que este último haya autorizado y únicamente dentro

de las áreas designadas de las Páginas de los Servicios (el Cliente proporcionará dicha autorización subiendo sus Características de Marca a los Servicios). El Cliente puede especificar la naturaleza de este uso mediante la Consola de Administración. Google también puede mostrar Características de Marca de Google en las Páginas de los Servicios para indicar que los Servicios los proporciona Google. Ninguna de las partes puede mostrar ni utilizar las Características de Marca de la otra más allá de lo permitido en este Acuerdo sin el consentimiento previo por escrito de la otra parte.

**8.3 Limitación de Características de Marca.** El uso de las Características de Marca de una parte irá en beneficio de la parte que posea los Derechos de Propiedad Intelectual de dichas Características de Marca. Una parte puede revocar el derecho de la otra parte a usar sus Características de Marca en virtud de este Acuerdo mediante aviso por escrito a la otra parte y con un tiempo razonable para detener el uso.

**9. Publicidad.** El Cliente acepta que Google puede incluir el nombre o los Elementos de Marca del Cliente en una lista de clientes de Google, ya sea online o en material publicitario. Además, el Cliente también acepta que Google puede hacer referencia verbal a él como un cliente de productos o Servicios de Google, conforme a lo estipulado en este Acuerdo. Esta sección está sujeta a la Sección 8.3.

## **10. Declaraciones, Garantías y Renuncias de Responsabilidad.**

**10.1 Declaraciones y Garantías.** Cada una de las partes garantiza que cumplirá con todas las leyes y normativas aplicables para el suministro o uso de los Servicios, según corresponda (incluida la ley aplicable de notificación de infracción de la seguridad). Google garantiza que proporcionará Servicios de conformidad con el Acuerdo de Nivel de Servicio aplicable. El cliente reconoce y acepta que es el único responsable del cumplimiento de la Ley de Protección de la Privacidad Online de los Niños de 1998 (Children's Online Privacy Protection Act) incluyendo, entre otros, la obtención del consentimiento parental en relación a la recopilación de información personal de los Estudiantes en lo que respecta a la provisión y el uso de los Servicios por parte del Cliente y de los Usuarios Finales.

**10.2 Renuncias de Responsabilidad.** EN LA MEDIDA EN QUE LO PERMITA LA LEY, A MENOS QUE QUEDA EXPRESADO DE OTRO MODO EN ESTE DOCUMENTO, NINGUNA DE LAS PARTES OFRECE NINGUNA OTRA GARANTÍA DE NINGÚN TIPO, IMPLÍCITA O EXPLÍCITA, OBLIGATORIA O DE OTRA CLASE, INCLUIDAS, ENTRE OTRAS, LAS GARANTÍAS DE COMERCIABILIDAD, ADECUACIÓN PARA UN FIN PARTICULAR Y NO INFRACCIÓN. GOOGLE NO SE HACE RESPONSABLE DEL CONTENIDO NI DE LA INFORMACIÓN A LA QUE SE PUEDA ACCEDER A TRAVÉS DE LOS SERVICIOS. EL CLIENTE RECONOCE QUE LOS SERVICIOS NO SON UN SERVICIO TELEFÓNICO Y QUE ESTOS NO PUEDEN ESTABLECER NI RECIBIR LLAMADAS, INCLUIDAS LAS LLAMADAS A SERVICIOS DE EMERGENCIA, A TRAVÉS DE REDES DE TELEFONÍA DE USO PÚBLICO.

## **11. Periodo de Vigencia y Cuotas.**

**11.1 Periodo de Vigencia** Este Acuerdo tendrá validez durante todo el Periodo de Vigencia.

**11.2 Periodo de Vigencia de los Servicios y Compras durante el Periodo de Vigencia de los Servicios.** Google proporcionará los Servicios al Cliente durante el Periodo de Vigencia de los Servicios. A menos que las partes acuerden lo contrario por escrito, las Cuentas de Usuario Final adquiridas durante el Periodo de Vigencia de los Servicios tendrán un periodo prorrateado que finalizará el último día de dicho Periodo de Vigencia de los Servicios.

**11.3 Renovación Automática.** Al final de cada Periodo de Vigencia de los Servicios, los Servicios (y todas las Cuentas de Usuario Final adquiridas anteriormente por una Cuota determinada) se renovarán de forma automática durante un Periodo de Vigencia de los Servicios adicional de 12 meses. Si una de las partes no desea renovar los Servicios, deberá notificarlo por escrito a la otra parte por lo menos 15 días antes de que finalice el Periodo de Vigencia de los Servicios. Dicha notificación de no renovación entrará en vigor al concluir el Periodo de Vigencia de los Servicios en ese momento.

**11.4 Cuotas.** Durante el Periodo de Vigencia Inicial, Google no aplicará Cuota alguna al Cliente por el uso de los Servicios (con excepción de Google Vault o el almacenamiento de pago, si es aplicable). Tras el acuerdo escrito mutuo de las partes, a) Google podrá aplicar Cuotas al Cliente por el uso de los Servicios una vez finalizado el Periodo de Vigencia de los Servicios inicial y b) Google podrá aplicar Cuotas al Cliente por el uso de una versión premium de los Servicios o para poder disfrutar de una funcionalidad adicional o mejoras que podría añadir Google a los Servicios (como Google Vault o almacenamiento de pago, si es aplicable).

**11.5 Uso de los Servicios.** El Cliente no tiene ninguna obligación de utilizar los Servicios y puede dejar de utilizarlos en cualquier momento con o sin motivo.

**11.6 Revisión de Tarifas.** Para aquellos Servicios que haya adquirido el Cliente por una Cuota, Google podrá revisar sus tarifas para el siguiente Periodo de Vigencia de los Servicios notificándose por escrito al Cliente (se permite por correo electrónico) al menos 30 días antes de que comience el siguiente Periodo de Vigencia de los Servicios.

## **12. Rescisión.**

**12.1 Rescisión por Incumplimiento.** Cada una de las partes puede suspender el uso o rescindir este Acuerdo si i) la otra parte incumple de forma sustancial el Acuerdo y no lo subsana antes de treinta días después de la recepción de la notificación por escrito, ii) la otra parte cesa sus operaciones empresariales o se ve sometida a procedimientos de

insolvencia y dichos procedimientos no se desestiman antes de noventa días o iii) la otra parte incumple este Acuerdo de forma sustancial más de dos veces, sin perjuicio de la subsanación de dichos incumplimientos.

**12.2 Otro tipo de Rescisión.** El Cliente podrá rescindir este Acuerdo con o sin motivo mediante notificación previa por escrito enviada a Google 30 días antes, siempre que, no obstante, se mantenga la obligación del Cliente de abonar cualquier Cuota por los Servicios que el Cliente haya adquirido aplicable al resto del Periodo de Vigencia de los mismos.

**12.3 Efectos de la Rescisión.** En caso de rescisión del presente Acuerdo, i) los derechos otorgados por una parte a la otra cesarán con efecto inmediato (a menos que se disponga de otro modo en esta Cláusula), ii) Google proporcionará al Cliente o al Distribuidor acceso a los Datos del Cliente, así como la capacidad de exportarlos, durante un periodo de tiempo comercialmente razonable y a las tarifas de Google vigentes en ese momento para los Servicios aplicables, iii) tras un periodo de tiempo comercialmente razonable, Google eliminará los Datos del Cliente mediante la supresión de redireccionamientos que hagan referencia a estos en los servidores activos y de replicación de Google y sobreescrivéndolos conforme transcurra el tiempo, iv) cada una de las partes realizará de inmediato todos los esfuerzos comercialmente razonables para devolver o destruir cualquier otra Información Confidencial de la otra parte, si así se solicita.

### **13. Indemnización.**

**13.1 Por parte de Google.** Google indemnizará, defenderá y eximirá al Cliente de y con respecto a todas las responsabilidades, daños y costes (incluidos los costes de establecimiento y minutas de abogados que correspondan) que se deriven de la demanda de un tercero en la que se alegue que la tecnología de Google utilizada para proporcionar los Servicios o cualquier Elemento de marca de Google infringe o se apropiá de forma indebida de cualquier patente, derecho de copyright, secreto comercial o marca comercial de terceros. Sin perjuicio de lo mencionado anteriormente, en ningún caso Google tendrá obligación ni responsabilidad alguna, según se establece en esta Sección, derivadas del i) uso de los Servicios o las características de marca de Google de forma modificados o en combinación con otros materiales no facilitados por Google y ii) contenido, información o datos proporcionados por el Cliente, Usuarios Finales u otros terceros.

### **13.2 Posible Infracción.**

a. Reparar, Sustituir o Modificar. Si Google tiene sospechas razonables de que los Servicios infringen los Derechos de Propiedad Intelectual de un tercero, entonces Google: a) obtendrá el derecho para el Cliente, a cargo de Google, para que pueda seguir usando los Servicios, b) proporcionará un sustituto funcionalmente equivalente que no los infrinja o c) modificará los Servicios para que ya no haya infracción.

b. Suspensión o Rescisión. Si Google considera que las opciones anteriores no son comercialmente razonables, puede suspender o cancelar el uso de los Servicios afectados por parte del Cliente. Si Google rescinde los Servicios afectados, Google notificará de ello al Cliente, al Distribuidor o a ambos. Si Google rescinde el uso de los Servicios afectados, deberá proporcionar una devolución prorrata de los Importes no devengados ya pagados por el Cliente aplicables al periodo siguiente a la rescisión del uso de dichos Servicios.

**13.3 General.** El Cliente notificará inmediatamente a Google de la demanda y cooperará con Google en la defensa de la misma. Google tiene el control total y la autoridad sobre la defensa, excepto por lo siguiente: a) toda resolución que requiera que el Cliente admita responsabilidades o efectúe algún pago requerirá el consentimiento previo por escrito de esa parte, y dicho consentimiento no se retendrá ni retrasará sin motivo, y b) el Cliente podrá unirse a la defensa con su propio abogado, a su propio cargo. LA INDEMNIZACIÓN DESCRITA ANTERIORMENTE SERÁ, SEGÚN ESTE ACUERDO, EL ÚNICO RECURSO LEGAL DEL CLIENTE POR LA INFRACIÓN DE GOOGLE DE LOS DERECHOS DE PROPIEDAD INTELECTUAL DE UN TERCERO.

#### **14. Limitación de responsabilidades.**

**14.1 Limitación de las Responsabilidades Indirectas.** SEGÚN ESTE ACUERDO, NINGUNA DE LAS PARTES SERÁ RESPONSABLE DE LOS INGRESOS PERDIDOS NI DE NINGÚN DAÑO INDIRECTO, ESPECIAL, IMPREVISTO, DERIVADO, EJEMPLAR O PUNITIVO, AUNQUE LA PARTE SUPIERA O DEBIERA HABER SABIDO QUE DICHOS DAÑOS ERAN POSIBLES E INCLUSO SI LOS DAÑOS DIRECTOS NO SATISFACEN UNA COMPENSACIÓN.

**14.2 Limitación sobre el Importe de Responsabilidad.** LA RESPONSABILIDAD DE CUALQUIERA DE LAS PARTES BAJO ESTE ACUERDO NO PODRÁ SER SUPERIOR A: (I) MIL DÓLARES O (II) EL IMPORTE ABONADO POR EL CLIENTE A GOOGLE CONFORME A ESTE ACUERDO DURANTE LOS DOCE MESES ANTERIORES AL EVENTO QUE OCASIONARA LA RESPONSABILIDAD.

**14.3 Excepciones a las Limitaciones.** Las limitaciones de responsabilidad anteriores se ejecutarán en la medida permitida por la ley aplicable, pero no se aplicarán en caso de infracción de las obligaciones de confidencialidad, en caso de infracción por una de las partes de los Derechos de Propiedad Intelectual de la otra parte o de las obligaciones de indemnización.

#### **15. Otras disposiciones.**

**15.1 Avisos.** A menos que se especifique lo contrario en el presente documento, a) todos los avisos se harán por escrito y se enviarán a la atención del departamento jurídico de la

otra parte y a la persona de contacto principal, y b) un aviso se considerará entregado i) cuando se verifique mediante acuse de recibo por escrito, si se ha enviado por mensajero, con entrega urgente en menos de 24 horas, o cuando se reciba, en el caso de haberse enviado por correo, sin que se verifique la recepción, o ii) cuando se verifique mediante acuse de recibo automático o por registros electrónicos, si se ha enviado por fax o por correo electrónico.

**15.2 Asignación.** Ninguna de las partes puede asignar ni transferir ninguna parte de este Acuerdo sin el consentimiento por escrito de la otra parte, excepto a un Afiliado, aunque solo si a) el beneficiario acepta por escrito estar vinculado a las condiciones de este Acuerdo y b) la parte que efectúa la asignación sigue siendo responsable de las obligaciones contraídas mediante el Acuerdo antes de la asignación. Cualquier otro intento de cesión o traspaso se considerará nulo de pleno derecho.

**15.3 Cambio de Control.** La parte que experimente el cambio de control (debido por ejemplo a una compra de acciones, a una venta, fusión u otro tipo de transacción corporativa): a) proporcionará un aviso por escrito a la otra parte antes de treinta días después de producirse dicho cambio y b) la otra parte puede cancelar inmediatamente este Acuerdo en cualquier momento entre el cambio de control y antes de treinta días desde que se reciba el aviso por escrito del subapartado a).

**15.4 Fuerza Mayor.** Ninguna de las partes será responsable de rendimiento inadecuado siempre que esté causado por una circunstancia (por ejemplo, desastre natural, acto de guerra o terrorismo, disturbio, condición laboral, actuación del Gobierno y fallos de Internet) que estuviera fuera del control razonable de la parte.

**15.5 Sin Renuncia.** La no ejecución de alguna de las disposiciones del presente Acuerdo no constituirá la renuncia a la misma.

**15.6 Divisibilidad de las Condiciones.** Si alguna disposición del presente Acuerdo se considera inaplicable, las disposiciones restantes del Acuerdo permanecerán en pleno vigor.

**15.7 Inexistencia de Representación.** Las partes contratantes son independientes y el presente Acuerdo no constituye ninguna representación, asociación o empresa conjunta.

**15.8 Inexistencia de Terceros Beneficiarios.** Este Acuerdo no contempla como beneficiario a ningún tercero.

**15.9 Compensación Equitativa.** En ningún caso, lo establecido en este Acuerdo limitará la capacidad de ninguna de las partes para solicitar una compensación equitativa.

**15.10 Legislación Aplicable.**

a. Para entidades gubernamentales municipales, autonómicas y estatales. Si el Cliente es una entidad gubernamental municipal, autonómica o estatal, las partes acuerdan guardar silencio en lo que respecta a la ley aplicable y la competencia territorial.

b. Para Todas las demás Entidades. Si el Cliente es una entidad no incluida en el subapartado a) de la Sección 15.10, se aplica lo siguiente: las leyes californianas rigen este Acuerdo, dejando sin efecto cualquier conflicto de leyes que pudiese suscitar. LAS PARTES ACUERDAN QUE CUALQUIER DISPUTA QUE SURJA EN RELACIÓN CON EL PRESENTE ACUERDO DEBERÁ RESOLVERSE ÚNICA Y EXCLUSIVAMENTE EN LA JURISDICCIÓN DEL CONDADO DE SANTA CLARA, CALIFORNIA.

**15.11 Enmiendas.** Toda enmienda debe hacerse por escrito e indicar expresamente que se trata de una enmienda de este Acuerdo.

**15.12 Supervivencia a la Rescisión.** Las siguientes Secciones sobrevivirán al vencimiento o rescisión de este Acuerdo: 7 (Información Confidencial), 8.1 (Derechos de Propiedad Intelectual), 12.3 (Efectos de rescisión), 13 (Indemnización), 14 (Limitación de responsabilidad), 15 (Varios) y 16 (Definiciones).

**15.13 Acuerdo Completo.** Este Acuerdo y todos los documentos que se indican por la presente constituye el Acuerdo completo de las partes en relación con el objeto del mismo y reemplaza a todos los acuerdos actuales relativos a ese objeto. Si se le presenta al Cliente un acuerdo similar con el mismo objeto al registrarse para utilizar los Servicios, este Acuerdo anulará y reemplazará a dicho acuerdo. Las condiciones que se encuentran en una URL y que se mencionan en este Acuerdo se incorporan al presente documento mediante esta mención.

**15.14 Interpretación de Condiciones en Conflicto.** Si existe un conflicto entre los documentos que conforman este Acuerdo, la prioridad de los documentos será la siguiente: el Formulario de Pedido (si corresponde), el Acuerdo y los términos que se encuentran en cualquier URL.

**15.15 Copias.** Las partes podrán quedar vinculadas en este Acuerdo ejecutando el Formulario de Pedido aplicable (si existe) o este Acuerdo a través de copias, lo que incluye fax, PDF u otras copias electrónicas, que reunidas constituirán un instrumento legal.

## **16. Definiciones.**

"Política de Uso Aceptable" se refiere a la política de uso aceptable de los Servicios disponible en [https://www.google.com/apps/intl/es/terms/use\\_policy.html](https://www.google.com/apps/intl/es/terms/use_policy.html) o en cualquier otra URL que Google pueda facilitar a tal efecto.

"Cuentas de Administrador" se refiere a las cuentas administrativas que Google suministra al Cliente con el fin de administrar los Servicios. El uso de las Cuentas de Administrador requiere una contraseña, que Google proporcionará al Cliente.

"Consola de Administración" hace referencia a la herramienta online que Google proporciona al Cliente para que la utilice en la elaboración de informes o en determinadas funciones administrativas.

"Administradores" se refiere al personal técnico designado por el Cliente que administra los Servicios para los Usuarios Finales en nombre del Cliente.

"Anuncios" se refiere a los anuncios online, excluidos los anuncios ofrecidos por cualquier producto publicitario que no forme parte de los Servicios (por ejemplo, Google AdSense), que el Cliente elige utilizar en conexión con los Servicios y que Google muestra a los Usuarios Finales.

"Afiliados" hace referencia a cualquier entidad con control directo o indirecto, que es controlada por una parte o que está controlada por una parte conjuntamente con un tercero.

"Acuerdo" se refiere, según sea aplicable, a este Acuerdo de G Suite for Education o a la combinación de un Formulario de Pedido y este Acuerdo de G Suite for Education.

"Ex Alumnos" se refiere a titulados o a antiguos Estudiantes del Cliente.

"Cargo Anual" se refiere al cargo anual de los Servicios establecidos en el Formulario de Pedido (si es aplicable).

"Fecha de Inicio de Facturación" se refiere a la fecha en la que el Cliente comenzará a pagar a Google los Servicios (si es aplicable).

"Elementos de Marca" son los nombres comerciales, marcas comerciales, marcas de servicio, logotipos, nombres de dominio y otros Elementos de Marca distintivos de cada una de las partes, respectivamente, protegidos por dicha parte cuando corresponda.

"Información Confidencial" se refiere a la información revelada por una parte a la otra parte según este Acuerdo y que se marca como confidencial o que se consideraría normalmente confidencial según las circunstancias. Los Datos del Cliente se consideran Información Confidencial del Cliente.

"Datos del Cliente" se refiere a los datos (incluido el correo electrónico) provistos, generados, transmitidos o mostrados a través de los Servicios por el Cliente o los Usuarios Finales.

"Nombres de Dominio del Cliente" hace referencia a los nombres de dominio que el Cliente posee o controla, que se utilizarán en relación con los Servicios, tal como se identifica en el Formulario de Pedido. El Cliente puede prestar los Servicios a cualquiera de sus subdominios (por ejemplo, si el Nombre de Dominio del Cliente es "edu.com", un subdominio puede incluir "exalumnos.edu.com") sin el consentimiento escrito de Google.

"Fecha de Vigencia" se refiere a la fecha en que se refrendó este Acuerdo.

"Problema de Seguridad Urgente" significa que: a) el uso del Cliente de los Servicios infringe la Política de Uso Aceptable, que podría afectar a: i) los Servicios, ii) el uso de otros clientes de los Servicios, iii) los servidores o la red de Google utilizada para proporcionar los Servicios; o bien b) el acceso de terceros no autorizado a los Servicios.

"Usuarios Finales" son las personas a las que el Cliente permite usar los Servicios.

"Cuenta de Usuario Final" es la cuenta alojada por Google y configurada por el Cliente a través de los Servicios para un Usuario Final.

"Leyes de Control sobre Exportación" hace referencia a todas las leyes y normativas de control de exportación y de reexportación aplicables, incluidas las Normativas de administración de exportación ("EAR") del Departamento de Comercio de los Estados Unidos, las sanciones económicas y comerciales de la Oficina de control de activos extranjeros del Departamento del Tesoro de los Estados Unidos y los Reglamentos Internacionales del Tráfico de Armas ("ITAR") del Departamento de Estado de los Estados Unidos.

"Cuotas" se refiere a los importes que factura Google al Cliente por los Servicios (si es aplicable) tal y como se describe en este Acuerdo.

"FERPA" corresponde a la Family Educational Rights and Privacy Act (ley de privacidad y derechos educativos de la familia) de EE. UU. (20 U.S.C. 1232g) y a las normativas de dicha ley (34 CFR Part 99), según las enmiendas y modificaciones realizadas periódicamente.

"Aviso de Privacidad de G Suite for Education" se refiere al aviso que se puede consultar en [https://www.google.com/intl/es/work/apps/terms/education\\_privacy.html](https://www.google.com/intl/es/work/apps/terms/education_privacy.html) o en cualquier otra URL que Google pueda facilitar a tal efecto.

"Centro de Ayuda" hace referencia al Centro de Ayuda de Google al que se accede a través de <https://www.google.com/support/> o de cualquier otra URL que Google pueda proporcionar a tal efecto.

"Actividades de Alto Riesgo" implica usos tales como el funcionamiento de instalaciones nucleares, control del tráfico aéreo o sistemas de asistencia vital, donde un error de los Servicios podría provocar la muerte, lesiones personales o daños al medio ambiente.

"HIPAA" (Health Insurance Portability and Accountability Act) es la ley estadounidense sobre portabilidad y responsabilidad de seguros médicos, de 1996, con sus eventuales modificaciones posteriores y cualquier otra normativa emitida en virtud de aquella.

"Derechos de Propiedad Intelectual" se refiere a derechos actuales y futuros a nivel mundial según la legislación de patentes, legislación de derechos de autor, legislación de secreto comercial, legislación de marcas comerciales, legislación de derechos morales y otros derechos similares.

"Periodo de Vigencia de los Servicios Inicial" es el periodo para los Servicios aplicables que empieza en la Fecha de Comienzo del Servicio y continúa con el "Periodo de Vigencia de los Servicios actual", tal y como se establece en el Formulario de Pedido en la Fecha de Inicio de Facturación (si se aplica un Formulario de Pedido a los Servicios); o bien, si no se aplica ningún Formulario de Pedido a los Servicios, es el plazo que empieza en la Fecha de vigencia y continúa durante un año.

"Cargo de Periodo de Vigencia Inicial" es el cargo de los Servicios correspondiente al Periodo de Vigencia de los Servicios Inicial (con excepción de las cuotas puntuales aplicables), tal y como se establece en el Formulario de Pedido (si es aplicable).

"Cargo Mensual" se refiere al cargo mensual para los Servicios establecidos en el Formulario de Pedido (si es aplicable).

"Productos No Pertenecientes a G Suite" se refiere a los productos de Google que no forman parte de los Servicios, pero a los cuales pueden acceder los Usuarios Finales mediante el nombre de usuario y la contraseña de inicio de sesión de sus Cuentas de Usuario Final. Los Productos No Pertenecientes a G Suite son los que se indican en <https://www.google.com/support/a/bin/answer.py?hl=es&answer=181865> o en cualquier otra URL que Google pueda facilitar a tal efecto.

"Condiciones de los Productos No Pertenecientes a G Suite" se refiere a las condiciones que aparecen en [http://www.google.com/apps/intl/es/terms/additional\\_services.html](http://www.google.com/apps/intl/es/terms/additional_services.html) o en cualquier otra URL que Google pueda facilitar a tal efecto.

"Dirección de Correo Electrónico de Notificación" se refiere a la dirección de correo electrónico designada por el Cliente para recibir notificaciones por correo electrónico de

Google. El Cliente puede cambiar esta dirección de correo electrónico a través de la Consola de Administración.

"Formulario de Pedido" se refiere a un formulario de pedido que es el documento escrito facilitado por Google y en el que se especifican los Servicios de Google que el Cliente adquirirá por una Cuota (si hay) de acuerdo con lo estipulado en el Acuerdo. El Formulario de Pedido contendrá: i) un bloque de firma para el Cliente o para el Cliente y Google; ii) SKU de servicio aplicables; iii) Cuotas (si es aplicable) y iv) el número y el Periodo de Vigencia actual para las Cuentas de Usuario Final.

"Orden de Compra" hace referencia a la orden de compra emitida por un Cliente.

"Servicios" se refiere a los Servicios Principales de G Suite for Education, a Google Classroom y, si es aplicable, a los Servicios de Google Vault facilitados por Google y utilizados por el Cliente de conformidad con este Acuerdo. Los Servicios se describen en [https://www.google.com/apps/intl/es/terms/user\\_features.html](https://www.google.com/apps/intl/es/terms/user_features.html) o en cualquier otra URL que Google pueda facilitar a tal efecto.

"Fecha de Comienzo del Servicio" es la fecha en que Google pone los Servicios a disposición del Cliente.

"Páginas de los Servicios" se refiere a las páginas web que muestran los Servicios a los Usuarios Finales.

"Periodo de Vigencia de los Servicios" se refiere al Periodo de Vigencia de los Servicios inicial y a todos los periodos de renovación para los Servicios aplicables.

"SLA" hace referencia al Acuerdo de Nivel de Servicio disponible en <https://www.google.com/apps/intl/es/terms/sla.html> o en cualquier otra URL que Google pueda facilitar a tal efecto.

"Plantilla" hace referencia a cualquier persona (incluido un cuerpo docente) que esté o haya sido empleado por el Cliente. Los Estudiantes o Ex alumnos que también formen parte de la Plantilla, se considerarán Plantilla de conformidad con este Acuerdo (y quedarán excluidos de la definición de Estudiante o Ex alumno) si han sido empleados por el Cliente en los últimos doce meses.

"Estudiante" se refiere a la persona que se registra para recibir clases ofrecidas por el Cliente durante los últimos doce meses.

"Suspensión" es la inhabilitación inmediata del acceso a los Servicios o a componentes de los Servicios, según corresponda, para impedir el uso posterior de estos.

"Impuestos" se refiere a los aranceles, derechos de aduana o impuestos (excluido el impuesto de la renta de Google) asociados con la venta de los Servicios, lo que incluye cualquier multa o interés relacionado.

"Periodo de Vigencia" hace referencia al periodo del Acuerdo, que abarcará desde la Fecha de Entrada en Vigor hasta i) la finalización del último Periodo de Vigencia de los Servicios o ii) la rescisión del presente Acuerdo en virtud de lo estipulado en este documento, lo que ocurra primero.

"Solicitud de Terceros" hace referencia a una solicitud de un tercero al acceso a registros relacionados con el uso de los Servicios por parte de un Usuario Final. Las Solicitudes de Terceros pueden ser una orden de búsqueda judicial, un auto, una citación, otra orden judicial válida o el consentimiento por escrito del Usuario Final mediante el que se permite la divulgación.

"Servicios de Asistencia Técnica (TSS)" son los servicios de asistencia técnica que brinda Google a los Administradores durante el Periodo de Vigencia, conforme a las Directrices de TSS.

"Directrices para los Servicios de Asistencia Técnica (TSS)" se refiere a las directrices para los servicios de asistencia técnica de Google vigentes para los Servicios. Las Directrices para TSS están disponibles en <https://www.google.com/apps/intl/es/terms/tssg.html> o en cualquier otra URL que Google pueda facilitar a tal efecto.

"Condiciones de URL" hace referencia a la Política de Uso Aceptable, al Acuerdo de Nivel de Servicio (SLA) y a las Directrices de TSS.

*Anexo 4 Acuerdo proporcionado por Google a la UTI*

**Anexo 6:** Guía para construir Estados del Arte

## **GUÍA PARA CONSTRUIR ESTADOS DEL ARTE**

**Olga Lucía Londoño Palacio  
Luis Facundo Maldonado Granados  
Liccy Catalina Calderón Villafáñez**



**Bogotá, 2014**

## Contenidos

	Página
Introducción	4
1      ¿Qué es un Estado del Arte?	6
2      Objetivos de un Estado del Arte	11
3      Fundamentos para la construcción de estados del arte	13
4      Alcances y límites de un Estado del Arte	15
5      Diferencia entre Estado del Arte, Marco Teórico, Estado de Conocimiento y Estado de la Investigación	18
6      Competencias Investigativas para la elaboración de estados del arte	20
7      La Heurística y la Hermenéutica como metodologías para la construcción de Estados del Arte	23
8      Fases para elaborar Estados del Arte	29
9      Escritura de un artículo que contiene un estado del arte	32
Conclusión	35
Referencias	36
Anexo: Modelo de ficha bibliográfica	38

## **Figuras**

<b>Figura</b>		<b>Página</b>
1	El inicio de un estado del arte	7
2	Requisitos para iniciar un estado del arte	9
3	Un estado del arte exige una revisión constante	10
4	Concepto de estado del arte desde los objetivos principales	12
5	Interrogantes que contribuyen a delimitar los alcances de un estado del arte	15
6	El “Círculo hermenéutico” como ruta investigativa	24
7	Ruta para construir estados del arte	31

## **Tablas**

<b>Tabla</b>		<b>Página</b>
1	Principios que orientan la construcción de estados del arte	14
2	Ejemplo de búsqueda usando como escenario PROQUEST	17
3	Competencias y habilidades investigativas	21
4	Estrategias metodológicas utilizadas para la construcción de estados del arte	28

## Introducción

En cualquier proceso de investigación es necesario seguir diversos pasos, todos ellos fundamentales, para abordar cualquier problema. Uno de ellos es el estado del arte, cuya elaboración es necesaria para afianzar la formulación del problema o tema investigativo, aunque generalmente se inicia cuando se está planteando el problema. La realización de estados del arte permite compartir la información, generar una demanda de conocimiento y establecer comparaciones con otros conocimientos paralelos, ofreciendo diferentes posibilidades de comprensión del problema tratado o por tratar, debido a que posibilita múltiples alternativas en torno al estudio de un tema.

Una versión generalmente aceptada de la expresión *Estado del Arte* es la de seguirle las huellas a un proceso hasta identificar su estado de desarrollo más avanzado. Es una forma de investigación que apoya otras estrategias también de investigación. Como resultado se tiene un conocimiento sobre la forma como diferentes actores han tratado el tema de la búsqueda, hasta dónde han llegado, qué tendencias se han desarrollado, cuáles son sus productos y qué problemas se están resolviendo. Un artículo del estado del arte resume y organiza los avances del conocimiento en una forma novedosa y apoya la comprensión de un campo específico de conocimiento.

Como producto de lo dado en el presente, el estado del arte responde a la lógica de la investigación que precede a un trabajo pero que, mediante distintos abordajes y metodologías, busca llegar a resultados, conclusiones, respuestas y productos diferentes. La búsqueda necesaria para consultar trabajos ya realizados, se torna hoy en día en una obligación en cualquier proceso de investigación. Para la gestión del conocimiento, la elaboración de estados del arte es un proceso fundamental que cumple varios propósitos: delimita el objeto de estudio y las relaciones con otros objetos de estudio; identifica actores y una red social de referencia, los mecanismos de comunicación vitales para la actualización del conocimiento, usuarios y productores de conocimiento, los parámetros espaciales y temporales – dimensiones históricas de un dominio de conocimiento, producciones tecnológicas y documentales; y compara métodos de producción, acceso, aplicación y valoración específicos.

En el campo de la tecnología la expresión *estado del arte* hace referencia al nivel más alto de desarrollo conseguido en un momento determinado sobre una técnica o un dispositivo tecnológico (Collins English Dictionary, 2003) y que ha sido aprobado – patentados – y acogidos por varios fabricantes. Un sinónimo es la expresión *tecnología de punta* – en inglés *state-of-the-art technology*.

La elaboración de estado del arte se considera una etapa en los procesos de investigación convencionales, como se presenta en los manuales de metodología de la investigación científica. En este sentido, se pueden identificar dos procesos generales: a) la búsqueda, selección, organización y disposición de fuentes de información para un tratamiento racional; b) la integración de la información a partir del análisis de los mensajes contenidos en las fuentes, que corresponde a la dimensión hermenéutica del proceso, muestra los conceptos básicos unificadores. En consecuencia, un estado del arte estudia una porción substancial de la literatura y fuentes relevantes de información en un área y desarrolla un proceso de comprensión que converge en una visión global e integradora y en una comunicación de este resultado para otros.

La lectura y la escritura son las herramientas claves para generar un producto investigativo de calidad. Por ser un proceso de construcción escrita que surge de la lectura significativa, se requiere de un manejo adecuado de ambas herramientas para que la actividad de elaborar estados del arte sea no solo eficaz, sino también comprensible para quienes se interesen en él. Así, el estado del arte permite el desarrollo de un pensamiento claro y productivo sobre un tema específico, en el cual se asuma analítica e interpretativamente los textos que acumulan conocimientos para integrarlos coherentemente a través de la adopción del lenguaje como instrumento de comunicación y medio fundamental para el desarrollo del pensamiento.

# 1

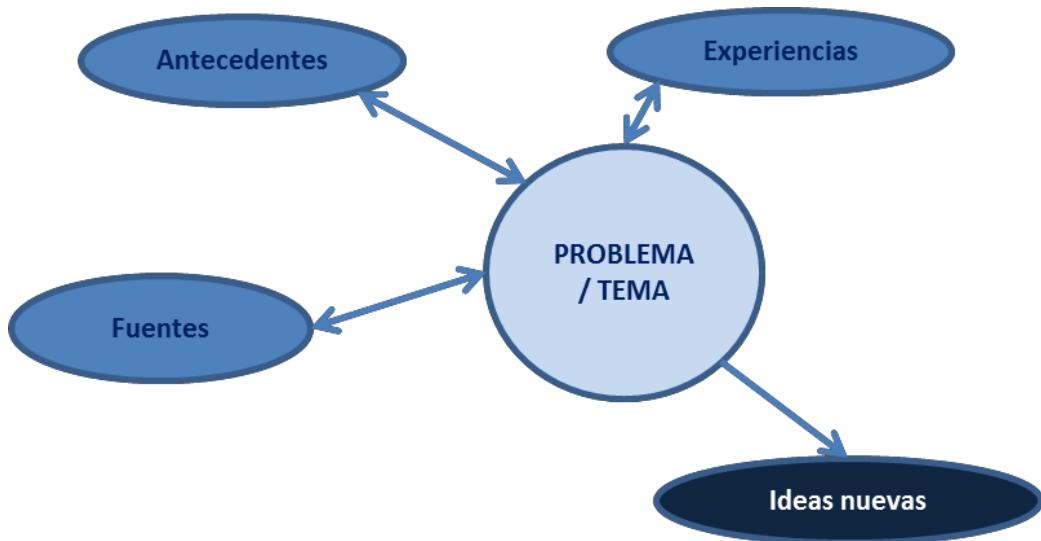
## ¿Qué es un Estado del Arte?

Una de las primeras etapas que debe desarrollarse dentro de una investigación es la construcción de su estado del arte, ya que permite determinar la forma como ha sido tratado el tema, cómo se encuentra el avance de su conocimiento en el momento de realizar una investigación y cuáles son las tendencias existentes, en ese momento cronológico, para el desarrollo de la temática o problemática que se va a llevar a cabo.

El estado del arte le sirve al investigador como referencia para asumir una postura crítica frente a lo que se ha hecho y lo que falta por hacer en torno a una temática o problemática concreta, para evitar duplicar esfuerzos o repetir lo que ya se ha dicho y, además, para localizar errores que ya fueron superados. Esto explica que no puede considerarse como un producto terminado, sino como una contribución que genera nuevos problemas o nuevas hipótesis de investigación y representa el primer y más importante insumo para dar comienzo a cualquier investigación.

Según lo anterior, un estado del arte representa la primera actividad de carácter investigativo y formativo por medio de la cual el investigador se pregunta, desde el inicio de su trabajo, qué se ha dicho y qué no; cómo se ha dicho; y, a quién se ha dicho, con el fin de develar el dinamismo y la lógica que deben estar presentes en toda descripción, explicación o interpretación de cualquier fenómeno que ha sido estudiado por teóricos o investigadores (Vélez y Galeano, 2002). Explica Vargas (1999) que una necesidad primaria para el desarrollo de competencias en investigación, consiste en mantener actualizado un estado del arte, al que entiende como un dispositivo de saber que contribuye a la formación crítica, así como al conocimiento disciplinar, temático y metodológico.

El estado del arte se puede definir como una modalidad de la investigación documental que permite el estudio del conocimiento acumulado escrito dentro de un área específica; su finalidad es dar cuenta del sentido del material documental sometido a análisis, con el fin de revisar de manera detallada y cuidadosa los documentos que tratan sobre un tema específico (Figura 1). Esto significa que es una recopilación crítica de diversos tipos de texto de un área o disciplina, que de manera escrita, formaliza el proceso cognitivo de una investigación a través de la lectura de la bibliografía hallada durante la indagación del problema, los temas y los contextos.



**Figura 1:** El inicio de un estado del arte

Fuente: Elaboración propia

Afirman Vargas y Calvo (1987) que un estado del arte consiste en inventariar y sistematizar la producción en un área del conocimiento, ejercicio que no se puede quedar tan solo en inventarios, matrices o listados; es necesario trascender cada texto, cada idea, cada palabra, debido a que la razón de ser de este ejercicio investigativo es lograr una reflexión profunda sobre las tendencias y vacíos en un área o tema específicos.

Es importante aclarar que todo estado del arte se construye como un marco conceptual y que no existen estados del arte universales. Por ello, Delgado y otros (2005) recomiendan a quien se compromete con su elaboración, tener en cuenta tres interrogantes básicos:

- |  |
|--|
| <ul style="list-style-type: none"> <li>• ¿Qué campos de indagación se han definido y reconocido como directamente relacionados con el tema de la investigación?</li> <li>• ¿Qué conceptos se evidencian como esenciales en los documentos seleccionados para construir el estado de arte?</li> <li>• ¿Qué contenidos, tópicos o dimensiones, se han definido como prioritarios?</li> </ul> |
|--|

Cuando se realiza un estado del arte con base en un problema específico, esto es, cuando se tiene definida “la pregunta investigativa” y lo que se busca es contextualizar la información, para establecer algunos límites para definir los parámetros de análisis y sistematización, y se encuentra que ese tema que ya ha sido investigado, según Calvo y Castro (1995), simultáneamente a la segmentación o análisis de dicho problema, las preguntas básicas que es necesario responder, son:

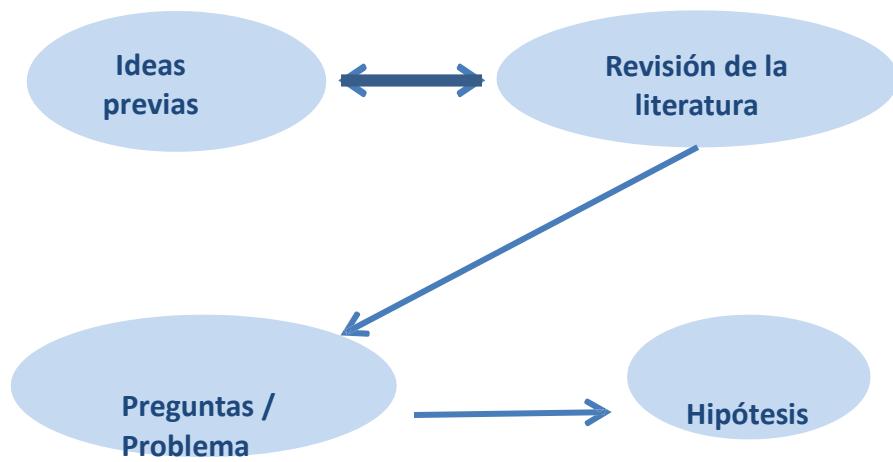
- |  |
|--|
| <ul style="list-style-type: none"><li>• <b>¿Qué problemas se han investigado?</b></li><li>• <b>¿Cómo se definieron esos problemas?</b></li><li>• <b>¿Qué evidencias empíricas y metodológicas se utilizaron?</b></li><li>• <b>¿Cuál es el producto de las investigaciones?</b></li></ul> |
|--|

Por su parte, la Asociación Americana de Psicología (American Psychological Association APA) (2003), define los estados del arte como,

... las evaluaciones y sistematizaciones críticas de toda la literatura científica que ha sido publicada sobre una temática o problema específico [...]. La organización, integración y evaluación del material previamente publicado tiene en cuenta: el progreso de la investigación en la clarificación del problema o temática; resume las investigaciones previas; identifica relaciones, contradicciones, lagunas e inconsistencia en la literatura; y sugiere los siguientes pasos o etapas en la posible solución del problema o comprensión de la temática revisada.

Según Molina (2005), debido a que una forma de generar conocimiento es la investigación, un estudio previo y sistemático de las investigaciones precedentes para elaborar estados del arte, contribuye a mejorar la teoría y la práctica de un tópico determinado, además de plantear conclusiones y respuestas nuevas que se proyecten a futuro. La importancia de realizar estados del arte, afirma Torres (2001) es tener presente que el requisito principal para comenzar a elaborarlo está en establecer el tema o el problema que se va a investigar; esto implica el reconocimiento de los límites de lo que ya ha sido dado a conocer, para encontrar las preguntas inéditas, susceptibles de ser pensadas e investigadas desde el acumulado en ese campo del conocimiento.

De una manera gráfica (Figura 2), estas ideas pueden representarse así:



**Figura 2:** Requisitos para iniciar un estado del arte

**Fuente:** Elaboración propia

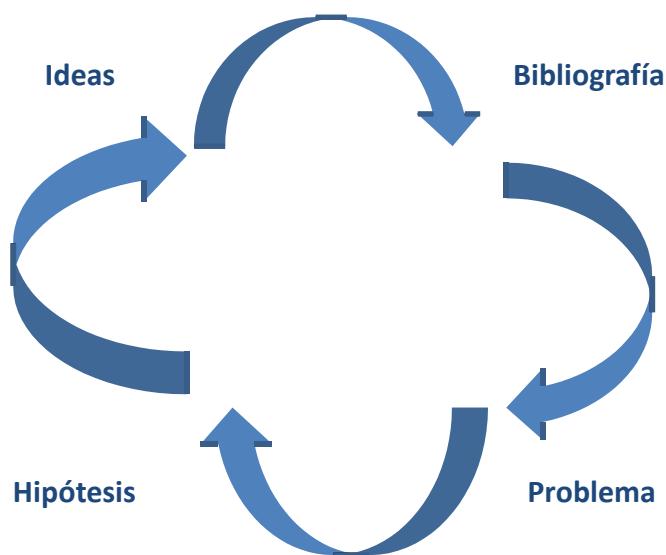
Al respecto, dice Jiménez (2006) que, cuando hablamos de estado del arte para el abordaje de un problema o un tema [...], estamos hablando de la necesidad hermenéutica de remitirnos a textos que a su vez son expresiones de desarrollos investigativos, dados desde diversas percepciones de las ciencias y escuelas de pensamiento, [...] tarea emprendida y cuyo objetivo final es el conocimiento y la apropiación de la realidad para disertarla y problematizarla. Ciertamente, con los estados del arte se comprueba que sólo se problematiza lo que se conoce, y para conocer y problematizar un objeto de estudio es necesaria una aprehensión inicial mediada por lo ya dado, en este caso el acumulado investigativo condensado en diversos textos e investigaciones que antecedieron mi inclinación temática (p. 32).

La pretensión de todo estado del arte es construir los antecedentes a partir de ellos mismos; realizar un sondeo descriptivo, sinóptico y analítico; alcanzar un conocimiento crítico y una comprensión de sentido de un tema específico; generar nuevas comprensiones surgidas de las existentes; e, ir más allá de la descripción y la explicación, acerca del nivel de comprensión que se tiene de un tema.

Son diversas las fuentes que se utilizan para la construcción de estados del arte, entre las más comunes están los libros, artículos, ensayos, tesis, monografías, entre otros. Dice Martínez (1999) que “al confluir todas estas miradas, estructuran un tejido nuevo de sentidos y significados, surgido de la reflexión crítica y que permite hacer nuevas comprensiones del objeto de estudio” (p. 13).

Es importante resaltar que los estados del arte hoy se han constituido en un insumo necesario para toda investigación. De ahí que siempre se inicie revisando y cimentando lo que otros han hecho y escrito para definir rumbos, cotejar enunciados y reconocer perspectivas novedosas, tanto relativas a los objetos de estudio, como a las maneras de abordarlos, las percepciones generadas durante el proceso investigativo, las metodologías utilizadas, sin desconocer las soluciones o respuestas que en ellos se proponen.

Cuando se está llevando a cabo una investigación, la construcción de su estado del arte es un trabajo permanente (Figura 3). Resumiendo las palabras de Sandoval (1996), se puede afirmar que la revisión constante de la literatura es importante y necesaria, debido a la misma dinámica que de suyo posee la investigación cuando está en curso, pues es normal que durante el ejercicio investigativo se presenten cambios y refinamientos, relacionados con el avance que va emergiendo del proceso investigativo.



**Figura 3:** Un estado del arte exige una revisión constante

**Fuente:** Elaboración propia

## 2

### Objetivos de un Estado del Arte

Con base en la definición que Hoyos (2000) expresa en la presentación de su libro sobre el término “investigar”, es posible deducir los objetivos de los estados del arte. Dice la autora que

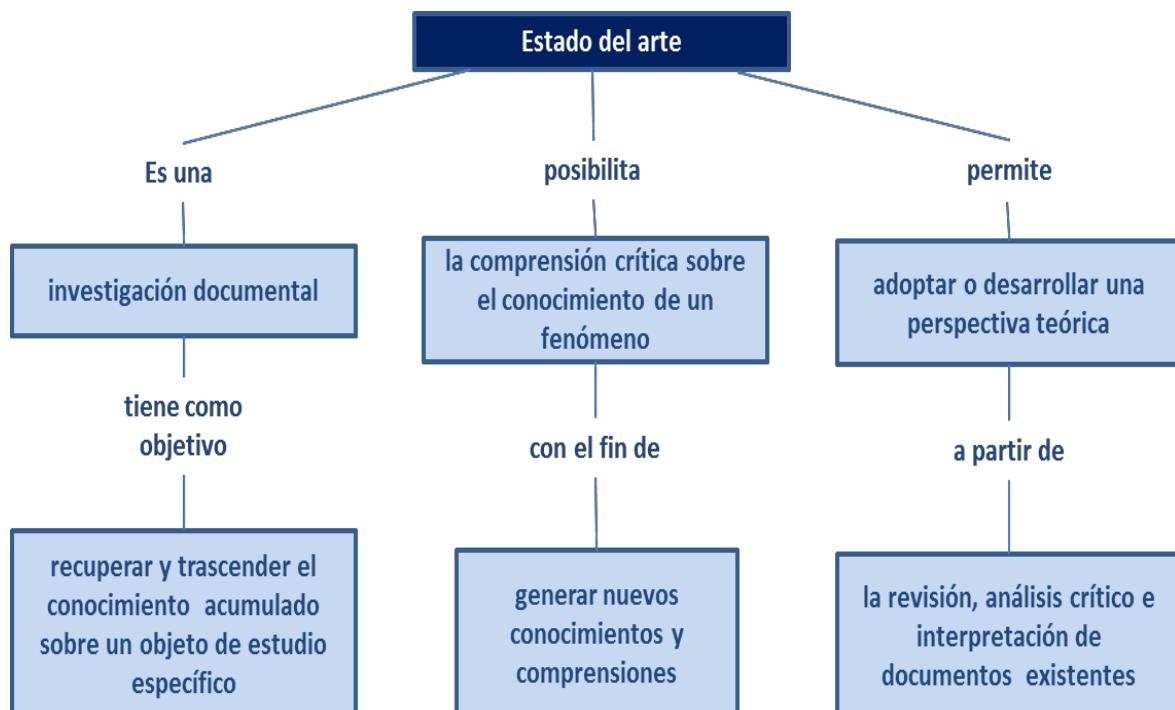
...investigar, no es ni puede ser un “acto”, es un “proceso” que implica secuencialidad en sus fases, donde cada paso es útil para la construcción del siguiente. Pero el proceso solo nada dice si no es en íntima conexión con el otro eje de esa unidad dialéctica el colectivo de investigadores. Este remite indudablemente a un equipo comprometido, donde lo teórico, lo práctico y lo contextual se conjuguen con el ejercicio de profundos y reconocidos valores éticos (p. 15).

Es decir, construir estados del arte significa adquirir una responsabilidad ética de asumir el reto de trascender el conocimiento existente. Como ya se dijo, un estado del arte no es un inventario de textos, sino una manera de crear un nuevo enfoque contextualizado, a partir de documentos existentes. Teniendo esto en mente, los objetivos de un estado del arte, bien pueden ser:

- Obtener datos relevantes acerca de los enfoques teóricos y disciplinares dados al objeto de estudio, de las tendencias y de las perspectivas metodológicas.
- Describir el estado de desarrollo alcanzado en torno a un tema, un área o una disciplina.
- Ampliar el conocimiento sobre lo estudiado con el fin de aportar argumentos que contribuyan a justificar y definir el alcance de una investigación.
- Aportar a la construcción de un lenguaje común que permita una comunicación transparente, efectiva, ágil y precisa entre estudiosos o interesados en el tema objeto de estudio.

- Estudiar la evolución del problema, área o tema de una investigación.
- Generar nuevas interpretaciones y posturas críticas en torno a un tema, área o disciplina.
- Determinar y cotejar los diversos enfoques que se le han dado a un problema.
- Identificar los subtemas pertinentes.
- Organizar el material existente para una posterior sistematización que conlleve a una mejor y más profunda comprensión.
- Identificar vacíos o necesidades referidas a la producción documental en el campo del saber objeto de investigación.

De acuerdo con sus objetivos, en general y gráficamente (Figura 4), un estado del arte puede definirse como:



**Figura 4:** Concepto de estado del arte desde los objetivos principales

**Fuente:** Elaboración propia

### 3

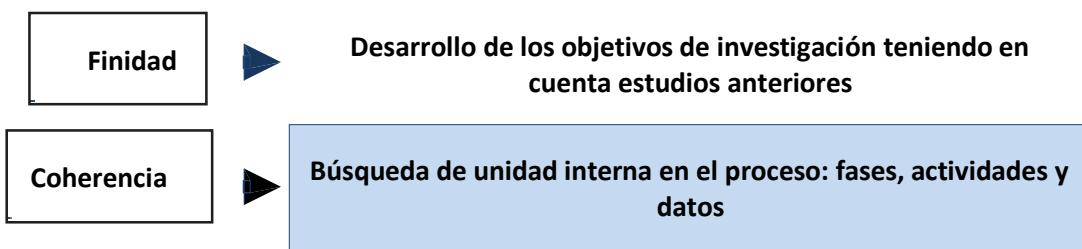
## Fundamentos para la construcción de estados del arte

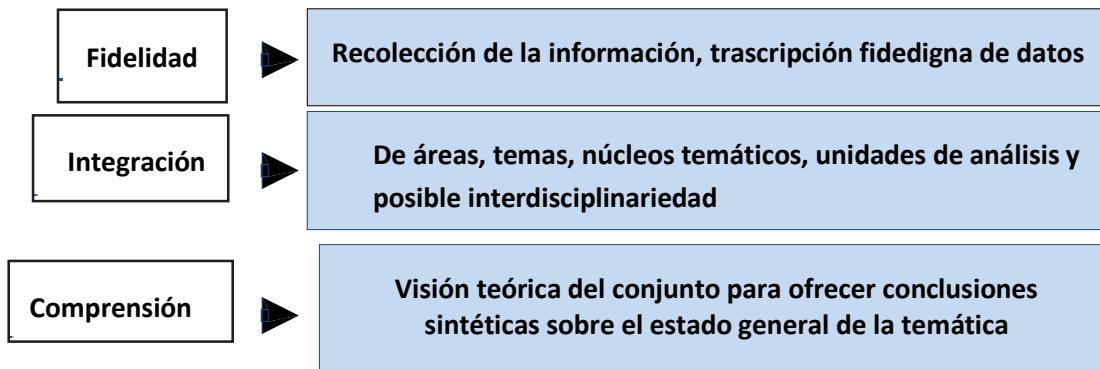
Lo que se pretende al construir estados del arte es alcanzar un conocimiento crítico acerca del nivel de comprensión que se tiene de un fenómeno específico, con el fin de presentar hipótesis interpretativas o surgidas desde la interdisciplinariedad que conlleva el trabajo en equipo, sin prescindir de una fundamentación teórica.

Siguiendo a Eco (2000) una hipótesis interpretativa se produce como resultado de la acción cooperativa de un colectivo de investigadores; su planteamiento brinda una explicación relativa a la variación expresiva en su vinculación con aspectos más profundos de la estructura de un texto y permite considerarlo como un todo. La define como un “producto cuya suerte interpretativa debe formar parte de su propio mecanismo generativo: generar un texto significa aplicar una estrategia que incluye las previsiones de los movimientos del otro” (p.90).

Según Hoyos (2000) este trabajo colaborativo implica un sondeo completo de carácter descriptivo, sinóptico y analítico para llegar a construir sentidos, a definir los logros, los avances, las limitaciones, las dificultades y vacíos que ofrece una investigación sobre determinado objeto, sondeo que tiene desarrollo propio e implica una metodología mediante la cual se procede progresivamente por fases diferenciadas para el logro de unos objetivos delimitados, que guardan relación con el resultado del proceso.

Lo anterior explica los principios orientadores para su construcción (Tabla 1), los que según Hoyos (2000) están basados en los fines que se persiguen (finalidad), en hallar una estructura que le dé unidad (coherencia), en el respeto y la ética del investigador frente al manejo de los datos (fidelidad), en lograr una unidad dentro de la diversidad de los documentos analizados (integración), en alcanzar un resultado final en el que se demuestre una visión de totalidad de los fundamentos teóricos como conjunto (comprensión).





**Tabla 1:** Principios que orientan la construcción de estados del arte

**Fuente:** Contextualización de Hoyos (2000).

El insumo para los estados del arte son las diferentes formas de objetos portadores de conocimiento como son los documentos o los productos tecnológicos. Un estado del arte requiere una dirección y foco, además de un escenario de búsqueda. La utilidad del resultado está en proporción directa a su nivel de especificidad. Esto significa que entre más general sea el estado del arte, será menos útil.

Definir la muestra documental es punto básico en la elaboración de un estado del arte. Con ella se garantiza la base de identificación suficiente y válida de los resultados obtenidos en el campo de investigación y de los procesos asociados a la obtención de los resultados. El investigador parte de la determinación de los criterios para seleccionar la muestra documental. Este paso le permite ordenar los procesos de búsqueda.

## 4

### Alcances y límites de un Estado del Arte

El desarrollo de los objetivos planteados para un estado del arte, permite elaborar nuevas comprensiones sobre las explicaciones e interpretaciones que los teóricos e investigadores han construido; da lugar a una recreación sobre los desarrollos existentes en un área, tema o problema del conocimiento; contribuye a la comprensión del objeto de estudio que, en últimas, es el encargado de motivar el estado del arte; favorece la identificación de tendencias y de vacíos de conocimiento; y, propicia el planteamiento de perspectivas y líneas de trabajo en el campo objeto de estudio.

De ahí que el alcance de un estado del arte sea la definición de los aportes que alimentan las investigaciones existentes y, por ello, se recomienda tener en mente las siguientes preguntas (Figura 5):



**Figura 5:** Interrogantes que contribuyen a delimitar los alcances de un estado del arte

**Fuente:** Elaboración propia

Las bibliotecas, hemerotecas, las bases de datos y la Internet son escenarios de búsqueda de información para la elaboración de estados del arte. Los criterios de búsqueda se expresan, en primer lugar, en palabras claves, cuya debida combinación permite la identificación de fuentes. La organización actual de estos escenarios ofrece posibilidades muy dinámicas para el manejo de criterios de selección. En la selección de términos de búsqueda o palabras claves, la consulta a expertos en el dominio de conocimiento es fundamental. Son también de utilidad los *thesaurus* disponibles que estandarizan palabras claves. Las bases de datos bibliográficas, como han sido diseñadas permiten hacer búsquedas combinando una variedad de criterios.

En cuanto a los límites que pueden presentarse cuando se está trabajando en la construcción de un estado del arte, se puede afirmar que, en general, están relacionados con el tiempo y el espacio de la investigación, razón por la cual su dinámica exige una estricta disciplina de trabajo; con la dificultad para adquirir el material bibliográfico necesario y la puesta en común con el colectivo investigador, en especial debido a que es necesario delimitar y acordar los “qué...”, los “cuánto...”, los “cómo...”, los “de qué manera...” y, los “cuáles parámetros, enfoques, metodologías, tendencias...”.

Es importante sumar a estos límites las diferencias en los estilos de escritura, fundamentalmente cuando se trabaja de manera colaborativa y se hace necesaria la escritura de textos con la intervención de más de dos manos. Este último aspecto conlleva la necesidad de asignar a una sola persona para efectos de unificar la redacción del escrito final.

## 5

### Diferencia entre Estado del Arte, Marco Teórico, Estado de Conocimiento y Estado de la Investigación

Una vez definido el estado del arte, es importante diferenciar su concepto de los denominados marco teórico, estados de conocimiento y estados de la investigación, pues según afirma Weiss (2005) entre ellos hay diferencias importantes, ya que los estados del arte van dirigidos a la formulación y justificación específica de problemas de investigación; los estados de conocimiento se encaminan hacia un público más amplio de estudiantes, académicos y tomadores de decisiones interesados en el ámbito educativo; los estados de la investigación, están dirigidos a un sector más restringido, es decir, a investigadores especializados en la temática y a los tomadores de decisiones; y, los marcos teóricos en los que, según Hernández y otros (1998) “lo importante es explicar claramente la teoría y la forma en que se aplica a nuestro problema de investigación” (p. 46).

- Un **marco teórico** se dirige a establecer los modelos explicativos que pueden ser utilizados para analizar y, de manera eventual, intervenir en los problemas investigados (Castro y Calvo, 1995). Según Vélez y Galeano (2002) la diferencia entre estado de arte y marco teórico es que en el primero se da cuenta de las investigaciones recientes respecto a las categorías de análisis de la investigación, partiendo de un lectura y análisis intra e intertextual en un tiempo y espacio geográfico determinado. El marco teórico hace alusión al análisis de diferentes posturas epistemológicas y/o disciplinas respecto a las categorías de análisis.

Explica Schwarz (2013) que el marco teórico corresponde al conocimiento mínimo necesario que se requiere para comprender un problema de investigación, es decir es la base teórica de referencia que permite comprender el problema y sus principales aspectos de detalle en toda su extensión. Por su parte, el estado del arte se concentra en rescatar el conocimiento existente y necesario más actualizado para resolver el problema de investigación, debido a que se compone de todos los conocimientos e investigaciones más recientes que han sido formulados en torno a la solución de un problema o problemática de investigación o bien, han contribuido sustancialmente con algún aspecto de la solución del mismo.

- Un **Estado de Conocimiento** es un análisis sistemático y valorativo del conocimiento y de su producción, surgido de un campo de investigación durante un periodo específico, que permite identificar los objetos de estudio y sus referentes conceptuales, las principales perspectivas teórico-metodológicas, tendencias y temáticas abordadas, el tipo de producción generada, los problemas de investigación y ausencias, así como su impacto y condiciones de producción (Weiss, 2005).
- Un **Estado de la Investigación** según López y Mota (2003: 26), consiste en “dar cuenta de la distribución de los grupos que la realizan, las condiciones de trabajo de la misma, la formación de investigadores, la existencia de programas de posgrado, entre otros aspectos”. A estas características, Weiss (2003) agrega los diagnósticos, panoramas y estados de conocimiento; reflexiones sobre la epistemología y los métodos de la investigación, generalmente dentro del área de educación; comunicación de la investigación; políticas de financiamiento; e impactos de la investigación.

Por lo anterior, afirma Schwarz (2013), el estado del arte contiene la base más profunda de la investigación que permite descubrir conocimiento nuevo al revisar la literatura asociada al tema de investigación de manera que pueda determinarse quienes, cómo, cuándo, dónde y por qué han tratado de resolver el problema de investigación, determinar su actualización y verificar si el tema sigue vigente así como descubrir hasta dónde ha avanzado el conocimiento validado más reciente sobre el tema en el que se está trabajando. De acuerdo con este concepto, cuando se elabora un estado del arte, se identifican de una forma rápida y acertada las fronteras del conocimiento respecto al problema de investigación, lo que significa que cualquier desviación y aspecto por estudiar traslada casi directamente al investigador al desarrollo de los nuevos conocimientos.

## 6

### **Competencias Investigativas para la elaboración de estados del arte**

“Una noción amplia de competencias permite reconocerlas como: los conocimientos, habilidades, destrezas y actitudes, que desarrollan las personas y que les permiten comprender, interactuar y transformar el mundo en el que viven” (Ministerio de Educación Nacional MEN, 2006). De este concepto se deduce que las competencias investigativas se refieren a las capacidades que tienen las personas para leer, escribir, analizar, interpretar, explicar, argumentar y, plantear alternativas y soluciones frente a un problema de investigación.

Así mismo, afirma Moreno (2005) que presuponen y requieren unos dominios y habilidades de diversa naturaleza que se desarrollan mucho antes de que las personas hagan parte a procesos sistemáticos de formación para la investigación, pues inherentes a la formación educativa básica, que a su vez, es y debe ser la encargada de potencializarlas.

Aunque el conocimiento en los estados del arte se encuentra desde un inicio mediado por los documentos y los textos, es importante tener en cuenta que las habilidades investigativas se constituyen en un proceso en el que intervienen diversas prácticas investigativas y, necesariamente, debe estar presente la intervención de distintos actores. Su concreción está en el quehacer académico, el cual consiste, según Rojas (2007: 6) en “promover, facilitar, preferentemente de manera sistematizada, el acceso a los conocimientos, la construcción y reconstrucción de competencias”, actitudes y la internalización de valores, necesarios para la práctica denominada investigación. Por su parte, Delgado (2012) plantea en su trabajo de tesis de Maestría que,

La ciencia moderna se centra en la resolución de problemas prácticos, que procuren conocimientos con utilidad social, lo cual se consigue de dos formas: por un lado elaborando conceptos y categorías que implican un importante grado de abstracción, y por el otro, aplicando estas teorías a la mayor cantidad de problemas posibles. El resultado es una mejora conjunta de la tecnología y las teorías científicas. En consecuencia estas aplicaciones transforman la vida cotidiana, por ende, la superioridad del saber científico radica en que ofrece una verdad de uso práctico (p. 37).

Para la elaboración de estados del arte, siguiendo a Moreno (2005) se consideran como competencias investigativas las siguientes (Tabla 3):

Competencias	Habilidades
<b>Básicas</b>	<b>Capacidad para indagar, confrontar, contextualizar, conjeturar, preguntar y plantear hipótesis.</b>
<b>Observación y percepción</b>	<b>Sensibilidad frente a fenómenos, intuición, capacidad para describir e identificar características de objetos, eventos o fenómenos en diversos contextos.</b>
<b>De pensamiento</b>	<b>Capacidad de análisis, reflexión, interpretación, crítica y lógica; pensar de manera autónoma y flexible.</b>
<b>De construcción de conceptos</b>	<b>Capacidad para apropiarse y reconstruir las ideas de otros, generar ideas, organizar lógicamente y exponer ideas, problematizar, desentrañar y elaborar semánticamente (construir) un objeto de estudio, sintetizar conceptos.</b>
<b>Instrumentales</b>	<b>Dominio formal del lenguaje (leer, escribir, escuchar, hablar), de operaciones cognitivas básicas de inferencia (inducción, deducción, abducción), análisis, síntesis, interpretación.</b>
<b>Textuales y discursivas</b>	<b>Capacidad para analizar e interpretar un texto escrito, inferir, comunicar y socializar resultados en forma oral y escrita, argumentar y defender conceptos, identificar intencionalidades en textos narrativos, explicativos, argumentativos e informativos.</b>
<b>Sociales</b>	<b>Capacidad para trabajar en equipo, socializar el conocimiento y su proceso de construcción.</b>
<b>Metodológicas</b>	<b>Capacidad para diseñar instrumentos, buscar, recuperar o generar información, diseñar metodologías y técnicas para organizar, sistematizar y analizar la información.</b>

**Tabla 3. Competencias y habilidades investigativas**

Fuente: Contextualización de Moreno (2005)

Además de las anteriores, una de las competencias que debe desarrollar un investigador es saber cómo afrontar la lectura de los artículos científicos. Schwarz (2012) considera que este ejercicio requiere de un entrenamiento especializado, el cual puede lograrse con la siguiente secuencia:

1. Leer y comprender el título de la investigación y el resumen, entendido como la síntesis del artículo. La lectura de las palabras clave facilita la identificación de los referentes semánticos durante la lectura.
2. Identificar las partes que componen el artículo.
3. Analizar y entender cómo se ha realizado el estado del arte, pues en este apartado es posible identificar soluciones que otros autores han planteado, analizar la manera como exponen cada solución y cuáles son las deficiencias halladas en cada solución revisada.
4. Entender la manera como el(los) autor(es) del artículo proponen una nueva solución a partir de las deficiencias encontradas en el análisis anterior, de forma tal que el nuevo aporte corrija las deficiencias y proponga algo nuevo.
5. Comprender cómo el(los) autor(es) del artículo someten a prueba la nueva solución propuesta para probar y verificar las bondades de la nueva solución encontrada con respecto a las anteriores existentes en la literatura.
6. Entender cómo el(los) autor(es) plantean las conclusiones a partir de los resultados y la manera de expresarlos, con el fin de identificar las consecuencias del aporte bajo la óptica de los investigadores.
7. Revisar con detalle las referencias bibliográficas para reconocer a los autores en los que se basaron al fundamentar las ideas y argumentos del artículo.

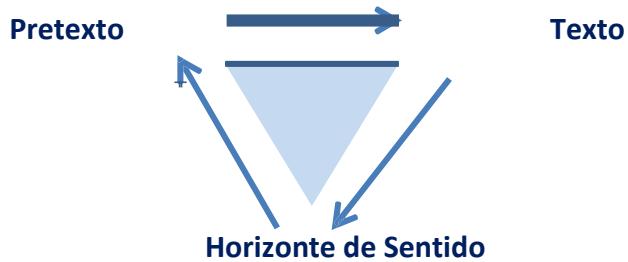
## 7

### **La Heurística y la Hermenéutica como metodologías para la construcción de Estados del Arte**

Referirse a la construcción de un estado del arte para estudiar un tema, remonta a un trabajo, inicialmente heurístico y, posteriormente, hermenéutico. Es decir, el proceso consta de dos momentos, que desde la acepción filosófica se definen como:

- a) La **heurística**, del griego *heuriskein*, significa descubrir, encontrar e indagar en documentos o fuentes históricas, la información necesaria para procesos investigativos y la resolución de problemas en diversos ámbitos científicos, con el fin de describir procedimientos sin rigurosidad o no formales que se llevan a cabo con el propósito de resolver una dificultad o solucionar una determinada cuestión. Se compone de una suma de procedimientos que pueden aplicarse con el mismo éxito tanto para demostrar una aseveración como para refutarla, al calificar una hipótesis provisional o una actitud epistemológica, como principio rector de una investigación (Polanyi, 1994).
- b) La **hermenéutica**, del griego *hermeneutiké tejne*, es la capacidad para explicar, traducir, interpretar y explicar las relaciones existentes entre un hecho y el contexto en el que acontece. En tanto de la interpretación busca determinar la expresión y representación del pensamiento. Tiene dos dimensiones: por un lado, es la reflexión filosófica sobre la estructura y condiciones del ‘comprender’ (forma única de conocimiento, que aprehende la existencia como realización de sentido, de valor y de posibilidades [poder-ser]). Por otro lado, es la teoría-práctica de un método que incluye orientaciones para comprender e interpretar la realidad. Explica Gadamer (1977) que el lenguaje es su medio universal, pues lo que se busca es la comprensión de textos y, a su vez, comprender significa interpretar.

Como método, la hermenéutica explica las bases de la comprensión, determinando sus posibilidades y configuraciones a partir del círculo hermenéutico, condición de toda interpretación por ser el que determina la ruta investigativa. Comienza con el pretexto, cediendo paso al sentido del texto para luego configurar el horizonte de sentido o interpretación. (Figura 6):



**Figura 6:** El “Círculo hermenéutico” como ruta investigativa  
**Fuente:** Elaboración propia

- **El Pretexto:** es el primer momento de todo trabajo hermenéutico que Gadamer (1977) resume al decir que “la comprensión sólo alcanza sus verdaderas posibilidades cuando las opiniones previas con las que se inicia no son arbitrarias. Por eso es importante que el intérprete [...] examine tales opiniones en cuanto a su legitimación, esto es, en cuanto a su origen y validez” (pp. 333 y 334).

El reconocimiento de todo aquello que se dirige a indagar la realidad como objeto de interpretación, surge de su mismo ser, de lo que tiene en sí mismo. Una investigación hermenéutica nace de una propuesta conceptual y metodológica, a partir de la cual se define lo que se **es** y se **tiene** como ejercicio que precede al desarrollo del trabajo. Este conjunto de ser y tener se entiende como todo aquello que conforma el horizonte previo y permite ubicar no sólo el mundo desde el cual se genera el interrogante central, sino también, la necesidad de darle un sentido y una razón de ser a las preguntas que junto a él surgen.

Los presupuestos nacen de quienes se involucran en la investigación; no son sólo actos subjetivos u objetivos, sino también desplazamientos hacia las formas expresadas a través de conceptos, definiciones, nociones, lenguajes, movilidades, acciones, métodos, objetos y artefactos, que son emitidos, creados, recreados o sugeridos por diversos autores y saberes.

- **El texto:** Como segundo peldaño de la hermenéutica está la dimensión del texto, conformado por lenguajes, narrativas, imágenes, acciones y acontecimientos, así como por la escucha y la observación, siendo éstos los que finalmente hacen posible la tarea interpretativa. Es el momento del análisis de lo que luego se interpretará. Se puede decir que es el ‘objeto’ que conduce a la interpretación, teniendo en cuenta que para la hermenéutica ese ‘objeto’ no se

encuentra distanciado del sujeto que interpreta, debido a que el pretexto también contribuye, implícita o explícitamente, a la construcción del texto.

La realidad descrita debe ser vista como un texto con sentido. Dice Eco (1997), al enumerar las características del enfoque hermenéutico que “un texto es un universo abierto en el que el intérprete puede descubrir infinitas interconexiones” (p. 50), pues es en él donde se hace visible el reconocimiento de las actuaciones y, con base en herramientas metodológicas pertinentes, se puede construir el sentido del texto.

Una de las principales reglas de la hermenéutica, dice Gadamer (1977) proviene de la retórica y consiste en “comprender el todo desde lo individual y lo individual desde el todo” (p. 360). El todo del texto es su sentido, es la complejidad de su construcción. Lo individual, que vendría a ser una equivalencia de las partes, es la configuración del texto que casi siempre actúa como referente de investigación. Pero esas partes, no son formas ni estructuras que se ensamblan para formar un todo, son horizontes personales que conforman un sentido para recomponer otro horizonte como totalidad.

El texto está definido desde su ‘contexto’, en tanto escenario social objetivado a través del cual se muestran las reglas de actuación de los sujetos sociales, formado también por aquello que se dice en ese ámbito determinado: esto es, texto es ‘lo dicho’, ‘lo escuchado’, ‘lo visto’, ‘lo olido’, ‘lo palpado’, ‘lo sentido’; en una palabra, es la circulación de las diversas formas de lenguajes que permiten percibir y comprender los significados del contexto.

- **El horizonte de sentido:** Se puede definir el ‘sentido’, como una actitud particular o colectiva para percibir el orden, la armonía en el espacio, en el tiempo o en el espacio-tiempo, en cuanto en él están involucrados tanto imaginarios como concepciones y percepciones, considerando que su representación es la instancia más elaborada y consciente del saber del sujeto. De acuerdo con la semiótica, el sentido es una forma individual y particular de significar (De Saussure, 1969), es un proceso en el cual se ‘da’ una significación. En otras palabras, es llevar a cabo una acción, pero sin limitarse a ello, pues para que esa acción se dé, se hace necesario un campo de significaciones, un horizonte en el cual sea posible establecer relaciones estructurantes entre unos significados, para de esta forma construir un mundo simbólico desde unas estructuras significativas.

Dar sentido es manifestar de una manera responsable, un criterio, un conocimiento, un sentimiento, un pensamiento, o cualquier expresión discursiva formalizada, teniendo en cuenta un interés o una motivación. El sentido siempre es de orden discursivo, debido a que su construcción exige la actividad textual; es decir, el sujeto da sentido a través de un nuevo texto surgido de otros textos. Es captar esencias que permitan descifrar la realidad, interpretando un texto desde su misma comprensión y a partir de una pregunta surgida de sus mismas entrañas. Es saber capturar un sentido a partir de la lectura; “leer es encontrar sentidos” (Barthes, 1980: 7).

El modelo de análisis hermenéutico trabaja desde un único núcleo significativo al que denomina “unidad de sentido”, el cual comprende tanto una actividad interpretativa por parte del lector, como la acción del texto; es en el diálogo establecido entre ambos, donde se encuentra expresado el horizonte de sentido; es el sujeto social quien hace posible el conocimiento de la realidad como una construcción colectiva de sentido.

Entonces, seguir el proceso hermenéutico para construir estados del arte, asegura una primera aprehensión a partir de estudios existentes y de acumulados investigativos desde diversos textos e investigaciones que antecedieron el estudio que se está iniciando (pretexto). Esos estudios se someten a un proceso de análisis e interpretación (texto), proceso que da lugar a un nuevo texto (horizonte de sentido). Aclara Jiménez (2006: 35) que “la tarea metodológica no solamente se centra en una ampliación de la documentación, sino en la conversión de la investigación en sí, en consecuencia se puede hablar de *la investigación de la investigación*”.

Siguiendo a Pantoja (2006: 106) “en investigación no se parte de cero sino de lo acumulado y de su reconocimiento depende la proyección del trabajo y, por qué no, del aporte que se haga a la construcción social de conocimiento”. Como propuesta hermenéutica un estado del arte está enfocado desde tres perspectivas fundamentales y se utiliza como herramienta para el reconocimiento e interpretación de la realidad, como propuesta metodológica documental y como base para la toma de decisiones en el campo de la investigación (Hoyos, 2000).

En un estudio realizado por Vélez y Calvo (1992), las autoras encontraron que aunque pueden adoptarse diversas metodologías cuando se está construyendo un estado del arte, hay tres momentos o pasos que son comunes y están relacionados íntimamente con el círculo hermenéutico; dichos pasos los nominan y presentan de la siguiente forma:

- **Contextualización:** se tienen en cuenta el planteamiento del problema de estudio y sus límites, el material documental que se utilizará en la investigación y algunos criterios para contextualizarlos.

- **Clasificación:** en este paso se determinan los parámetros que deben tenerse presentes para la sistematización de la información, la clase de documentos que se estudian, sus objetivos, la cronología, las diversas disciplinas que enmarcan los trabajos, las líneas de investigación, el nivel de las conclusiones y el alcance; estos están definidos en cada uno de los estudios. Esta información se clasifica tipológicamente y según el interés que requiera el análisis.
- **Categorización:** para este momento se tiene en cuenta la jerarquización y generación de la información para su correcto manejo, lo que implica recuperar lo que se conciba como esencial, facilitando así el estudio del fenómeno a investigar, debido a que permite el desarrollo de la práctica hermenéutica con respecto a las prácticas investigativas, dentro del área en la que se enmarca el objeto de estudio. Este paso puede, a su vez, organizarse dentro de dos categorías:
  - a) **Internas**, derivadas directamente del estudio de la documentación bajo el enfoque de las temáticas, metodologías, hallazgos, teorías, estudios prospectivos o retrospectivos.
  - b) **Externas**, consideradas como práctica hermenéutica al relacionar aquellas temáticas que permiten establecer una contribución socio-cultural al interior de la investigación en el área en la que se desarrolla.

A partir del anterior estudio, Cabra y otros (2003) proponen añadir una nueva fase que conduzca a obtener un resultado más significativo para que los resultados de las investigaciones sean aplicables al entorno y transferibles a otros. Dicha fase consiste en establecer asociaciones analíticas al estado del arte para desentrañar la esencia creativa del conocimiento, identificar las perspectivas y tendencias de la investigación y, reconocer el devenir hermenéutico como cardinal para la toma de decisiones.

En síntesis, en un inicio, se hace una lectura rápida y transversal para descartar aquellos trabajos que no tengan una relación directa con el tema de la investigación. Es necesario hacer explícita la estrategia de búsqueda que se utilizó, la relación con el objeto de estudio de la investigación, así como las fuentes que se consultaron. Esta revisión documental es la que permite un acercamiento a conceptos, teorías, metodologías y perspectivas, que sirven como base a la investigación que se está construyendo.

De manera simultánea a la lectura, normalmente se elaboran fichas que permitan sintetizar las ideas centrales de cada lectura analizada, lo cual supone establecer una relación precisa de las categorías (indicadores) que se van reseñando, las cuales se caracterizan por ser pertinentes, estar disponibles, ser accesibles, ser medibles, específicas, confiables, unívocas (no ser redundantes) y fáciles de replicar.

Entendiendo que una investigación es un proceso compuesto por diversas actividades en las que se busca definir el “qué se va a hacer”, el “cómo hacerlo” y la precisión de lo que se proyecta como “producto final”, Hoyos (2000) propone unas estrategias metodológicas, todas ellas relacionadas con las fases consecutivas de dicho proceso y con el compromiso, sentido de pertenencia y la ética del colectivo de investigadores.

Es importante aclarar que a partir de estas fases se realiza el cronograma de actividades en el cual se distribuye y organiza en forma de secuencia temporal el conjunto de experiencias y actividades diseñadas a lo largo de la investigación, organizadas básicamente en torno a dos ejes: la duración del ejercicio investigativo y el tiempo que previsiblemente el investigador dedicará al desarrollo de cada una de las actividades.

Hoyos (2000) propone cinco etapas como estrategias metodológicas: la preparatoria, la descriptiva, la constructiva, la interpretativa y la extensión, las cuales se encuentran sintetizadas y consignadas a continuación en la Tabla 4:

Preparatoria	► <b>Definir objeto de estudio, tema, tipos de lenguaje, pasos y etapas (se trata de fijar las “reglas del juego”)</b>
Descriptiva	► <b>Tipos de estudio, referentes disciplinares, poblaciones y muestras, delimitaciones, metodologías</b>
Constructiva	► <b>Identificación de tendencias, logros, vacíos, limitaciones, dificultades</b>
Interpretativa	► <b>Proporcionar hipótesis interpretativas: Ampliación del horizonte de estudio</b>
Extensión	► <b>Buscar la mejor estrategia para dar a conocer la investigación (publicación, conferencia, congreso, etc.)</b>

**Tabla 4:** Estrategias metodológicas utilizadas para la construcción de estados del arte

**Fuente:** Contextualización de Hoyos (2000)

## 8

### Fases para elaborar Estados del Arte

En términos generales, el primer paso para elaborar un estado del arte es recopilar la mayor información posible y pertinente sobre el tema seleccionado y consignar dicha información en fichas, lo que permite estudiar la bibliografía seleccionada para tener una mayor comprensión del tema que se está estudiando. En dichas fichas es necesario anotar los conceptos básicos y unificadores, para luego pasar a su interpretación y a elaborar la estructura de lo que será el texto final.

Una vez realizado el proceso anterior, se pasa a la presentación del estado del arte, para la que se debe tener en cuenta la utilización de un lenguaje claro y conciso, ser breve y directo; evitar el uso de la primera persona. En el proceso de escritura, explica Correa (2007) es importante utilizar palabras precisas, que posean significados exactos y prescindir del uso de lenguaje coloquial y los modismos.

El proceso para llevar a cabo un estado del arte desde la heurística y la hermenéutica implica seguir una serie de fases, a saber:

1. **Heurística:** es la búsqueda y compilación de las fuentes de información, las cuales pueden ser de diversas características y naturaleza, como por ejemplo, bibliografías, anuarios, monografías, artículos, trabajos especiales, documentos oficiales o privados, testamentos, actas, cartas, diarios, trabajos de investigación, tesis, monografías, filmaciones, audiovisuales, grabaciones, multimedios.

Es en esta fase cuando se leen las fuentes encontradas, se seleccionan los puntos fundamentales y se indican el o los instrumentos diseñados por el investigador para sistematizar la información. A través de la recopilación de la información es posible contextualizar las temáticas, clasificar los tipos de texto, los autores, las metodologías, los marcos de referencia, los conceptos y las conclusiones, ya que permiten elaborar y organizar el material consultado, además de establecer convergencias y divergencias.

Para realizar el estado del arte, es necesario que el investigador realice un proceso de búsqueda de la información, el que por lo general, se lleva a cabo en seis subfases:

- **Preparatoria o iniciación:** identificación y selección del área o tema que será investigado, lo que implica definir el objeto de investigación, las áreas temáticas comprendidas en el tema central, el lenguaje básico común que se va a utilizar y los pasos a seguir. En esta primera fase se busca:
  - a) Establecer los elementos teóricos que sustentan la construcción de un estado del arte, las fases y su relación.
  - b) Identificar y contextualizar el objeto de estudio.
- **Exploración:** lectura analítica y comprensión del problema para precisar la necesidad de la información que se requiere.
- **Descriptiva:** con el fin de extractar de las unidades de análisis del material documental, los datos pertinentes y someterlos a un proceso de revisión, reseña y descripción, es necesario establecer:
  - a) Los referentes disciplinarios y teóricos.
  - b) Los autores que los han realizado.
  - c) Las delimitaciones espaciales, temporales y contextuales.
  - d) Los diseños metodológicos utilizados.
- **Formulación:** generación de ideas bases o indicadores, a partir de la información encontrada.
- **Recolección:** compilación de la información que se conciba como pertinente en fichas bibliográficas. Estas fichas son instrumentos que permiten el registro e identificación de las fuentes de información, así como el acopio de datos o evidencias. Su diligenciamiento facilita el registro de información, la organización y la clasificación de la información de manera eficiente, permiten el procesamiento de la información, son un medio adecuado para el registro técnico de las fuentes de información y la elaboración de las referencias bibliográficas. Como anexo de este documento se muestra un modelo de ficha en el que se consignan los datos necesarios.
- **Selección:** organización del material para determinar si algo falta o se da por terminada la búsqueda.

2. **Hermenéutica:** consiste en la lectura, análisis, interpretación, correlación y clasificación de la información, según el grado de interés y necesidad frente a la nueva investigación. Como en todo trabajo hermenéutico, es necesario realizar el

ejercicio de pasar de la fragmentación realizada en las fichas, a la síntesis del texto y de la pluralidad del pensamiento a la reflexión crítica. Igualmente, con base en transcripción de la información es necesario definir la forma como se hará su sistematización.

Este segundo momento comprende tres fases:

- **Interpretación:** es proceder al análisis de los documentos por áreas temáticas de manera integrada, lo que permite ampliar el horizonte del estudio por unidades de análisis y proporcionar datos nuevos integrativos por núcleos temáticos.
- **Construcción Teórica:** comprende la revisión de conjunto de la interpretación de los núcleos temáticos con el fin de formalizar el estado actual del tema. Es la construcción del documento que contiene el estado del arte.
- **Publicación:** es dar a conocer a la comunidad científica los resultados finales del estado del arte ya consolidado.

Graficando lo anterior, la ruta para construir estados del arte es: (Figura 7)



**Figura 7.** Ruta para construir estados del

arte

**Fuente:** Elaboración  
propia

## 9

### **Escritura de un artículo que contiene un estado del arte**

Un artículo sobre el estado del arte, resume, organiza y compendia la construcción teórica de una investigación, enfocándose en el problema, los objetivos, la metodología y los resultados de una manera novedosa que integre y agregue claridad al trabajo en un campo o área de conocimiento específico. Lo que se busca es dar a conocer el desarrollo de un conocimiento, haciendo énfasis en la clasificación de la literatura existente, desde una perspectiva del área en la que su ubica el objeto de estudio y, principalmente, evaluar las principales tendencias halladas durante la revisión bibliográfica.

La apariencia visual y estética del artículo es muy importante. La presentación formal debe tener una estructura y organización lógica y sus títulos y subtítulos deben ser claros. Si contiene figuras (gráficos, esquemas, fotografías) y tablas (matrices, cuadros) deben estar bien diseñadas, ser muy claras y didácticas. Es indispensable verificar que el artículo se adapte al formato requerido por quien va a realizar la publicación (tipo de letra, numeración de secciones, número de columnas, estilo de las normas de las referencias, ubicación y requerimientos técnicos de figuras y tablas).

Hoyos (2000), realiza algunas recomendaciones para su escritura, que pueden sintetizarse de la siguiente forma:

- Aclarar el tipo de documentos que se eligieron para ser analizados.
- Es importante responder tácitamente las siguientes preguntas: ¿cómo surgió la investigación?, ¿cuándo se inició?, ¿quiénes trabajaron?
- Contextualizar el material documental utilizado y establecer una relación con la nueva investigación.
- Sistematizar los resultados obtenidos, donde se demuestre que hay una congruencia de los datos.
- Realizar una delimitación conceptual; es decir, organizar el artículo a manera de un marco conceptual, con la coherencia que este ejercicio requiere.
- Determinar las maneras de concebir el estado en el que se encuentra el conocimiento del tema que se está trabajando, definiendo si el nivel de la investigación es descriptivo o explicativo.
- Es necesario hacer explícitos tanto los problemas como las problemáticas que se trabajaron.

- Es obligatorio manifestar los resultados concebidos como sobresalientes.
- Manifestar de manera muy clara cómo se deconstruyeron las temáticas propuestas.
- El escrito debe apuntar a la comprensión del proceso.
- Es preciso manifestar los avances logrados en relación con otras investigaciones.
- Es muy importante decir qué no se logró y por qué, al igual que expresar si quedan lagunas, vacíos o limitaciones.
- Emitir recomendaciones; esto es, qué se debe hacer, hacia dónde se debe apuntar, qué preguntas no se respondieron, qué controversias surgieron o pueden llegar a surgir.
- Es posible, aunque no necesario, dar a conocer si hubo cambios de actitudes, de valores, de comportamientos en torno al tema de la investigación.

### **Esquema para la construcción de un artículo sobre un estado del arte**

Todas las revistas tienen unas “normas de autor”, la mayoría relacionadas con aspectos formales de publicación, en las que se especifica cómo desean que se les envíe el artículo. Aun así, el contenido de un estado del arte, por lo general se presenta en el siguiente orden, aunque hay que reiterar que no existe uniformidad en los procedimientos seguidos en la elaboración de estados del arte. La siguiente es una secuencia lógica y general para una investigación de estado del arte:

- Título del artículo y subtítulo (si lo tiene) en los idiomas que lo soliciten
- Nombres y datos de los investigadores
- Fecha de presentación
- Resumen y palabras clave
- Abstract y key words (resumen en inglés y/u otro idioma si lo solicitan)
- Introducción
- Desarrollo del Contenido:
  - ✓ Delimitación del problema para el estado del arte
  - ✓ Definición de parámetros y características de la muestra documental
  - ✓ Problemas de investigación investigados
  - ✓ Aproximaciones metodológicas de las investigaciones
  - ✓ Enfoques epistemológicos predominantes
  - ✓ Conclusiones validadas
  - ✓ Resultados de conocimiento: conclusiones validadas, artefactos tecnológicos, procedimientos validados, instrumentos de medición validados.
  - ✓ Los títulos de los proyectos
  - ✓ Desarrollo Tecnológico
  - ✓ Dominio de conocimiento
  - ✓ Dimensiones del aprendizaje

- Metodología
- Discusión
- Resultados de conocimiento, artefactos
- Conclusiones y recomendaciones
- Caracterización de la comunidad académica del campo
- Unidades de investigación
- Cooperación internacional
- Trayectoria de los investigadores
- Administración de recursos
- Referencias bibliográficas

## **Conclusiones**

El estado del arte es una investigación documental que busca alcanzar un conocimiento crítico acerca del nivel de comprensión que se tiene de un fenómeno, con el fin de presentar hipótesis interpretativas sin prescindir de una fundamentación teórica. Se concibe como la primera actividad que debe desarrollar toda investigación y su objetivo es dar cuenta, desde una postura crítica, de las investigaciones que se han realizado sobre un tema específico.

Los principios que orientan la construcción de un estado del arte son finalidad, coherencia, fidelidad, integración y comprensión, los que determinan los alcances, trazan las limitaciones y se constituyen en la base para el cabal desarrollo de las competencias investigativas.

Para el manejo metodológico de la construcción de estados del arte, se proponen desde su concepción filosófica, la heurística y la hermenéutica, cuya circularidad permite partir de pretextos para elaborar nuevos textos desde diversos enfoques y formas de conocimiento, desembocando en un producto final escrito, que fusiona horizontes creativos y críticos, en los que es posible demostrar una comprensión total del objeto de estudio que da origen a la investigación.

## Referencias

- American Psychological Association APA. (2003). Manual de estilo de publicaciones. México: El Manual Moderno.
- Barthes, R. (1980). S/Z. México: Siglo XXI.
- Cabra, M. et al. (2003). Estado del arte de los proyectos de Grado de los postgrados de la Facultad de Educación de la Universidad de San Buenaventura durante el periodo comprendido entre 1989 y 2002. Bogotá: Universidad de San Buenaventura.
- Castro, Y. y Calvo, G. (1995). Estado del arte sobre la investigación de la familia en  
ersidad
- Collins  
, 2000
- Correa Ramírez, A. y otros. (2007). El estado del arte. En: Leo y escribo en la Universidad: Módulo de tecnologías lectoescriturales. Medellín: Universidad de Antioquia.
- De Saussure, F. (1969). Curso de lingüística general. 7<sup>a</sup> ed. Barcelona: Losada.
- Delgado, M.H. (2012). Mejoramiento de la competencia investigativa en la formación de docentes de licenciatura en educación básica. [Tesis de Maestría]. Bogotá: Universidad Libre de Colombia.
- Delgado, R. y otros. (2005). Estado del Arte: educación para el conocimiento social y político. Facultad de Educación. Bogotá: Pontificia Universidad Javeriana.
- Eco, U. (1997). Interpretación y sobre interpretación. Madrid: Cambridge University Press, edición española.
- Eco, U. (2000). Lector in fabula. La cooperación interpretativa en el texto narrativo. Barcelona: Lumen.
- Gadamer, H.G. (1977) Verdad y método. Salamanca: Sígueme.
- Hernández, R.; Fernández, C. y Baptista, P. (1998) Metodología de la investigación. México: Mc Graw Hill.
- Hoyos Botero, Consuelo. (2000). Un modelo para investigación documental. Guía teórico-práctica sobre construcción de Estados del Arte. Medellín: Señal Editora.
- Jiménez, A. (2006) El estado del arte en la investigación en ciencias sociales. Bogotá: Universidad Pedagógica Nacional
- López y Mota, A. (2003). Saberes científicos humanísticos y tecnológicos: procesos de enseñanza y aprendizaje. México: COMIE.
- Martínez, L.A. (1999). “¿Qué significa construir un estado del arte desde una perspectiva hermenéutica?”. En: Revista Criterios, 8, p. 13-20. Pasto: Universidad Mariana.
- Ministerio de Educación Nacional MEN. (2006). Un mundo de Competencias: ¿Qué son?  
En: <http://www.colombiaaprende.edu.co/html/competencias/1746/w3-printer-249280.html>

- Molina, N.P. (2005). "Herramientas para investigar. ¿Qué es el estado del arte?". En: Revista Ciencia y Tecnología para la salud Visual y Ocular, 5: 73-75. Bogotá: Universidad de La Salle.
- Moreno, M.G. (2005). Potenciar la educación. Un currículo transversal de formación para la investigación. En: Revista Electrónica Iberoamericana sobre Calidad, Eficacia y Cambio en Educación REICE. 3 (1) 520-540. En: [http://www.ice.deusto.es/RINACE/reice/Vol3n1\\_e/Moreno.pdf](http://www.ice.deusto.es/RINACE/reice/Vol3n1_e/Moreno.pdf)
- Pantoja, M.I. (2006). Construyendo el objeto de estudio e investigando lo investigado: aplicaciones de un estado del arte. En: Revista Memorias, 4 (8) 104 – 107. Pereira: Universidad Cooperativa de Colombia.
- Polanyi, K. (1994). El sustento del hombre, Barcelona: Mondadori.
- Rojas, S. (2007). El estado del arte como estrategia de formación en la investigación. En Revista Studiositas, 2 (3) 5-10. Bogotá: Universidad Católica de Colombia.
- Sandoval, C.A. (1996) Investigación cualitativa, especialización de teorías, métodos y técnicas de investigación social. Bogotá: ICFES.
- Schwarz, M. (2012). ¿Cómo leer un paper de investigación científica? En: <http://max-schwarz.blogspot.com/2012/12/como-leer-un-paper-de-investigacion.html>
- Schwarz, M. (2013). Marco teórico vs Estado del Arte en la investigación científica. En: <http://max-schwarz.blogspot.com/2013/01/marco-teorico-vs-estado-del-arte-en-la.html>
- Torres, A. (2001). El planteamiento de problemas en la investigación social. Departamento de ciencias Sociales, Universidad Pedagógica Nacional – Instituto Colombiano para el Fomento de la Educación Superior ICFES. Bogotá: Universidad Pedagógica Nacional.
- Vargas Guillén, G. (1999). "Las líneas de investigación: de la posibilidad a la necesidad, en el desarrollo de líneas de investigación a partir de la relación docencia e investigación en la Universidad Pedagógica Nacional". Encuentro interno de investigación. Bogotá: Universidad Pedagógica Nacional.
- Vargas, G. y Calvo, G. (1987) "Seis modelos alternativos de investigación documental para el desarrollo de la práctica universitaria en educación". En: Revista Educación Superior y desarrollo Nº 5. Proyecto de extensión REDUC – Colombia. Bogotá: Universidad Pedagógica Nacional.
- Vélez, A. y Calvo, G. (1992). La investigación documental. Estado del arte y del conocimiento. Análisis de la investigación en la formación de investigadores. Maestría en Educación. Bogotá: Universidad de la Sabana.
- Vélez, O. y Galeano, E. (2002). Investigación cualitativa. Estado del arte. Medellín: Universidad de Antioquia.
- Weiss, E. (2003). La investigación educativa en México 1992-2002. México: Consejo Mexicano de Investigación Educativa.
- Weiss, E. (2005). El campo de la investigación educativa en México a través de los estados de conocimiento. Conferencia pronunciada en el VIII cine. Hermosillo, México.

## Anexo 7: Contratación SaaS con el proveedor Google Apps

En la primera pantalla que se presenta se inicia la suscripción al servicio.

G Suite

Empecemos

Obtendrás acceso al servicio de correo electrónico de empresa, videoconferencias, almacenamiento online y otras herramientas empresariales. **Empieza a probarlo gratis durante 14 días sin necesidad de introducir tus datos de pago ni descargar ningún software.**

Te indicaremos cómo crear una cuenta de G Suite para tu empresa.

SIGUIENTE

En la siguiente pantalla el proveedor pide la razón social y el número de empleados que trabajan en la empresa.

Háblanos sobre tu  
empresa

Nombre de la empresa

Transportadora Jaramillo

Número de empleados, contándote a ti

- Solo tú
- 2-9
- 10-99
- 100-299
- 300 o más

SIGUIENTE

En la siguiente pantalla se ingresa la ubicación y el número de teléfono de la empresa.

## ¿Cuál es la ubicación y el número de teléfono de tu empresa?

País

Ecuador

Número de teléfono de la empresa

+593 981632988

SIGUIENTE

En la siguiente pantalla se ingresa el correo electrónico de contacto.

## ¿Cuál es tu dirección de correo electrónico actual?

Para que podamos ponernos en contacto contigo, debes proporcionar una dirección que consultes regularmente. Podrás crear una dirección de correo electrónico de empresa más tarde.

Dirección de correo electrónico actual

elizajaramillo0502@gmail.com

SIGUIENTE

En la siguiente pantalla se establece un nuevo dominio o un dominio ya utilizado.

## ¿Tu empresa tiene un dominio?

Para configurar el correo electrónico y una cuenta de G Suite para tu empresa, necesitarás un dominio, como, por ejemplo, *example.com*.



[SÍ, TENGO UN DOMINIO VÁLIDO](#)

[NO, NECESITO UN DOMINIO](#)

En la siguiente pantalla se escribe un dominio para la empresa.

## ¿Qué nombre de dominio quieres?

Busca un dominio para tu negocio. Aunque es posible que algunos ya estén cogidos, hay muchas opciones disponibles.

Nombre de dominio

transjaramillo

.com



**BUSCAR**

[Quiero usar un dominio del que ya soy propietario](#)

*Figura 1 Dominio para las cuentas de la empresa*

El dominio que quieras  
está disponible.

transjaramillo.com

Disponible 12,00 \$/año

Compra **transjaramillo.com** te permite crear direcciones de correo electrónico empresariales como **tú@transjaramillo.com** o **ventas@transjaramillo.com**.

Puedes finalizar la compra más delante, después de crear una cuenta de G Suite.

SIGUIENTE

En la siguiente pantalla se ingresa la dirección de la empresa cliente.

Introduce la dirección de  
tu empresa

Para registrar el dominio, introduce la dirección de tu empresa. [?](#)

Dirección postal

110101

Línea de dirección 2

Código postal

110101

Ciudad

Loja

SIGUIENTE

En la siguiente pantalla se ingresa el nombre y apellido del administrador.

## ¿Cómo te llamas?

Al crear la cuenta de G Suite, te conviertes en su administrador, pero no te preocupes ya que podrás asignar esta función a otro usuario más adelante. [\(?\)](#)

Nombre

Esther Elizabeth

Apellidos

Jaramillo Malla

SIGUIENTE

En la siguiente pantalla se establece el usuario y contraseña del administrador.

## Cómo iniciarás sesión

Usarás tu nombre de usuario para iniciar sesión en la cuenta de G Suite y crear la dirección de correo electrónico de tu empresa.

Nombre de usuario

elizabeth

@transjaramillo.com

Contraseña

••••••••••••••|



8 caracteres como mínimo

SIGUIENTE

En la siguiente pantalla se acepta que el proveedor envíe mensajes al correo electrónico.

# Compartir ideas fantásticas con Google

Te enviaremos correos electrónicos puntuales con sugerencias útiles, ofertas especiales y anuncios, y te invitamos a que nos envíes tus comentarios.

[ACEPTAR](#)

[NO, GRACIAS](#)

En la siguiente pantalla muestran el link de la parte contractual, en la que se aceptan los términos del acuerdo.

## Ya casi has terminado de crear tu cuenta de G Suite

Sabemos que probablemente no eres un robot, pero tenemos que preguntártelo:

[¿Eres un robot?](#)

[No soy un robot](#)



reCAPTCHA

[Privacidad - Condiciones](#)

Al hacer clic en Aceptar y crear cuenta, aceptas el [Acuerdo de G Suite](#).

[ACEPTAR Y CREAR CUENTA](#)

Posteriormente se presenta un mensaje de confirmación de la cuenta creada.

# Se ha creado tu cuenta de G Suite

A continuación te ofreceremos instrucciones sobre cómo completar la compra de tu dominio.

[IR A CONFIGURACIÓN](#)

Al hacer click en “IR A CONFIGURACIÓN” se presenta la siguiente pantalla, en la que se establece una cuenta para cada usuario final.

The screenshot shows the Google Admin interface with a blue header bar containing the text "Google Admin". Below the header, there is a search bar with the placeholder "Buscar usuarios, grupos y ajustes (p. ej., crear usuario)". The main content area has a title "Añadir Registro del dominio" and a subtitle "Paso 1: Selecciona opciones de compra". It includes fields for "PAÍS" (set to "Ecuador") and "MONEDA" (set to "USD (\$)"). Under "PLAN DE PAGO", it says "Plan anual" and lists two bullet points: "Te comprometes a un plan de servicio de 12 meses." and "Al final del primer mes te cobraremos el precio anual completo.". To the right of this information is a price of "\$ 12,00 /dominio/año". Below this, there is a form for registering the domain "transjaramillo.com", with several checkboxes for renewal and privacy options. At the bottom of the form, it says "\$12.00 Cargo anual estimado durante 1 año a partir del 3/4/17".