*Artículo original/ Original article*
*ISSN 2953-6553*

# Lista de Comprobación para verificar que un Service Level Agreement (SLA) de servicio de la nube firmado por una PYME en Ecuador garantiza la seguridad y protección de datos

# Checklist to verify that a Cloud Computing Service Level Agreement (SLA) signed by an PYME in Ecuador guarantees data security and protection

Mónica Galarza Rodas [1] 0009-0003-4416-8550, Boris Suquilanda Villa [1] 0000-0002-7033-3156

monica.galarza@tecazuay.edu.ec , boris.suquilanda@tecazuay.edu.ec

[1] Instituto Superior Universitario Tecnológico del Azuay, Azuay/Cuenca, Ecuador.

DOI 10.36500/atenas.2.004

***Resumen***

**La seguridad y protección de datos en la contratación de servicios en la nube realizada por las PYMES ecuatorianas, requiere conocer una serie de parámetros necesarios que le permitan al usuario identificar un proveedor apto con la finalidad de minimizar los riesgos que implica almacenar información fuera de su propia infraestructura, por lo que como resultado del presente estudio se proporciona a las PYMES ecuatorianas una Lista de Comprobación para verificar los Niveles de Acuerdos de Servicios de tal manera que el proveedor garantice la seguridad y protección de sus datos sin que esto implique un conocimiento técnico explícito.**

**Para la elaboración de la lista de comprobación se han analizados aspectos como: Tipos de servicios de la nube, análisis de los principales riesgos a los que han estado expuestas las empresas ecuatorianas en la contratación de servicios en la nube, mapeo de la normativa Ecuatoriana vigente vs las principales riesgos de seguridad identificados (disponibilidad, control de acceso, arquitectura, cumplimiento de la norma) y finalmente se han analizado diferentes estándares internacionales relacionados a la seguridad de la información centrándonos en los controles recomendados en la seguridad de la información general así como la seguridad de la información del servicio de *cloud computing.***

***Abstract***

**Data security and protection in the contracting of cloud services carried out by Ecuadorian (SMEs), requires knowing a series of necessary parameters that allow the user to identify a suitable provider in order to minimize the risks involved in storing information outside their own infrastructure, so as a result of this study, Ecuadorian SMEs are provided with a Checklist to verify the Levels of Service Agreements in such a way that the provider guarantees the security and protection of their data without implying explicit technical knowledge.**

**To prepare the checklist, aspects such as: Types of cloud services, analysis of the main risks to which Ecuadorian companies have been exposed when contracting cloud services, and mapping of current Ecuadorian regulations have been analyzed vs. the main security risks identified (availability, access control, architecture, compliance with the standard) and finally, different international standards related to information security have been analyzed, focusing on the recommended controls in general information security as well as the information security of the cloud computing service.**

***Palabras Claves – Cloud Computing, Ciberseguridad, Acuerdos de Nivel de Servicio Computación en la Nube, SLA Cloud Computing***

***Keywords – Cloud Computing, Cybersecurity, Service Level Agreements Cloud Computing, SLA Cloud Computing***

Recibido: 2023-05-05, Aprobado tras revisión: 2023-11-10

## I. INTRODUCCIÓN

En la actualidad, en nuestra sociedad se evidencia un incremento del uso de las tecnologías de la información y comunicación (TIC) y la popularización de la arquitectura informática de prestación de servicios conocida como computación en la nube o cloud computing (en inglés), que es un conjunto de tecnologías que se encuentran en expansión, en las que se puede encontrar cada vez mayor variedad de servicios disponibles para usuarios individuales y sobre todo para empresas.

Considerando que cuando una empresa decide contratar a un proveedor de servicios en la nube la responsabilidad de implementar los mecanismos adecuados para resguardar la seguridad de la información recaen en el proveedor de servicios y, que adicional a esto, no existe una ley o norma dentro del Ecuador que regule el servicio de la nube; la creación de una lista de comprobación para verificar el nivel de seguridad y protección de los datos será un apoyo para que las empresas y/o clientes individuales negocien adecuadamente las cláusulas que incluyan los Service Level Agreements (SLA) al respecto.

Por otro lado, según el Boletín Nro 01-2022-DIEE del Instituto Nacional de Estadística y Censos (INEC) del Ecuador, se destaca que las PYMES tienen una participación significativa en la economía del país. De acuerdo con los datos proporcionados, las PYMES representan el 99,5% del total de empresas y establecimientos en Ecuador en el año 2021. Además, el informe revela que las actividades económicas más destacadas dentro de las PYMES se encuentran en los sectores de servicios y comercio. El sector de servicios abarca el 44,8% de las PYMES, mientras que el sector de comercio representa el 34,5%.

Estos datos subrayan la importancia y la relevancia de las PYMES en la economía ecuatoriana, ya que desempeñan un papel fundamental tanto en la prestación de servicios como en el sector comercial del país. Sin embargo, el factor común que comparten todas las empresas de este tipo es la falta de recursos financieros y tecnológicos que poseen las grandes empresas. El aprovechamiento de la computación en la nube se presenta como una gran oportunidad para las PYMES del país, ya que les permite reducir las inversiones iniciales en tecnologías de la información y comunicación, lo cual les permite ingresar rápidamente al mercado y, por lo tanto, aumentar su productividad y competitividad.

La investigación se centra en desarrollar una Lista de Comprobación para verificar que un Service Level Agreement (SLA) de servicio de la nube firmado por una PYME en Ecuador garantiza la seguridad y protección de datos, esta investigación se basa en la revisión de literatura existente en el campo de la seguridad de datos en la nube, incidentes de seguridad ocurridos en el Ecuador, los estándares y mejores prácticas relacionados con los SLAs, así como los marcos normativos y regulatorios aplicables en

Ecuador. Esta fundamentación teórica permitirá contextualizar la investigación y respaldar los criterios y la metodología utilizada en la creación de la lista de comprobación.

## II. Marco teórico

Al contratar servicios en la nube es necesario tener claro los recursos computacionales requeridos según las necesidades empresariales ya que el precio del servicio variará dependiendo de los recursos seleccionados, por lo tanto, es importante conocer las principales características de los servicios:

**Auto-Servicio bajo demanda:** el consumidor puede abastecer recursos computacionales en forma unilateral según el requerimiento con el proveedor e incluso sin la interacción humana.

**Permitir el acceso desde la red (pública, privada, híbrida, comunitaria):** En este tipo de plataforma, los recursos disponibles en la nube pueden ser accedidos a través de la red, mediante el cual, el consumidor puede acceder por medios tradicionales o a través dispositivos tales como: teléfonos móviles, laptops, tablets entre otros.

**Asignación de recursos en modo multiusuario**. El proveedor tiene la posibilidad de proveer a todos los usuarios servicios de computación en la nube, facilitando recursos de acceso y prestaciones distintas.

**Capacidad de rápido crecimiento**: las unidades de capacidad pueden ser rápidas y fácilmente aprovisionadas (en algunos casos en forma automática), escaladas (crecimiento) o liberadas. Para el consumidor, estos recursos suelen parecer ilimitados, y pueden ser adquiridos en cualquier cantidad y momento.

**Servicio medido**: los sistemas de la nube controlan de forma automática y optimizada la utilización de los recursos. Este uso de los recursos puede ser monitoreado y controlado, además, es posible realizar reportes para ambas partes, a fin de establecer la facturación del servicio.

**Elasticidad y escalabilidad**. Las aplicaciones en cloud son totalmente elásticas en cuanto a su rapidez de implementación y adaptabilidad. Además, son totalmente escalables con tan solo comunicarlo al proveedor y modificar la tarifa de suscripción.

**Seguridad**. En las aplicaciones en Internet, es importante comprender que los datos no están desprotegidos en la red, lo cual puede ser una preocupación común para las empresas. En realidad, los datos de las aplicaciones en la nube se almacenan en DATA CENTERS, empresas especializadas en la custodia y protección de datos. Es fundamental encontrar un proveedor o un DATA CENTER que brinde garantías y servicios acordes al valor de los datos almacenados.

**Tipos de Servicio:** Una vez claras las características de los servicios de la nube, es importante también conocer sus tipos de servicios, Según (Polze, 2009) las instalaciones de la computación en la nube se pueden clasificar de acuerdo a tres estrategias generales:

**Cloud Software as a Service (SaaS):** La aplicación SaaS es ofertada por un fabricante de software o proveedor de servicios informáticos a través de Internet. En el cual puede ser utilizado por varios usuarios. En este tipo de aplicación, el fabricante es el encargado del mantenimiento de la privacidad de los datos y de su personalización. En este modelo de servicio, por lo general el usuario se encarga del pago por el uso y por la infraestructura requerida para el correcto funcionamiento de la aplicación y se restringe a emplear la herramienta y las funciones que ésta ofrece.

**Cloud Platform as a Service (PaaS):** Este modelo de nube amplía las prestaciones de **SaaS**, de forma que el consumidor de servicios, pueda desplegar aplicaciones desarrolladas o adquiridas por el usuario, para ampliar las funcionalidades de dicha nube.

**Cloud Infrastructure as a Service (IaaS):** Las IaaS contempla la externalización de servidores para espacio en disco, base de datos entre otros, Este aplicativo permite al usuario tener un control completo a través del DATA CENTER dentro de la empresa. Por el contrario, podrá disponer de un centro de datos o administrarlo. Bajo este concepto, este modelo de despliegue en la nube, representa una solución basada en la virtualización. En el cual, el usuario deberá cancelar por el consumo de los recursos, la utilización del espacio en disco, el tiempo de CPU, el espacio en base de datos y la transferencia de datos.

## III. METODOLOGÍA

La metodología de investigación utilizada en este estudio es el mapeo sistemático, que incluye la etapa de recolección de datos y el método de análisis. Con el fin de alcanzar este objetivo, se llevó a cabo un estudio de mapeo sistemático para explorar investigaciones relevantes existentes sobre directrices y recomendaciones para los acuerdos de nivel de servicio (SLA) aplicados a los servicios en la nube.

Los estudios de mapeo utilizan una metodología similar a las Revisiones Sistemáticas de la Literatura, pero tienen como objetivo identificar y clasificar toda la investigación relacionada con un tema amplio de ingeniería en lugar de responder preguntas sobre los méritos relativos de las tecnologías competidoras que las Revisiones Sistemáticas de la Literatura convencionales abordan. El mapeo sistemático revisa un tema de ingeniería de software más amplio y clasifica los trabajos de investigación primarios en ese dominio específico (Budgen D., Turner M., Brereton P., Kitchenham B., 2008), siendo el dominio del presente trabajo los SLA.

Los procedimientos de estudios de mapeo sistemático muestran cinco etapas (B. Kitchenham, D., Budgen, and B. Pearl, 2011):

1. Definición de las preguntas de investigación;

¿Cuáles son los principales estándares de seguridad de la información y ciberseguridad en el cloud computing?

2. Realización de la búsqueda de estudios primarios;
3. Documentos de selección basados en criterios de inclusión / exclusión;
4. Clasificación de los trabajos;
5. Extracción y agregación de datos.

Para desarrollar la estrategia de búsqueda, fue necesario considerar el título, resumen y palabras clave de los artículos en las bases de datos electrónicas incluidas y actas de congresos.

1) Palabras clave: 2) Grafías y acrónimos alternativos para los términos principales: 3) Cadena de búsqueda: se forma la siguiente cadena de búsqueda general. La razón para formular una cadena genérica es que en el estudio de mapeo queremos cubrir toda la literatura en la que se reporta el trabajo SLA.

## IV. Resultados y Discusión

### Incidentes de seguridad ocurridos en Ecuador y Latinoamérica

Al ser el estudio dirigido a las Pymes Ecuatorianas fue importante conocer primero los principales incidentes de seguridad presentados en las empresas ecuatorianas y latinoamericanas, lo cual sirvió como punto de partida para entender la problemática que atraviesan las empresas que contratan servicios en la nube con respecto a la seguridad.

Los ciberataques que han sufrido las empresas públicas y privadas, en los últimos años, han dejado en evidencia la débil conciencia que existe en Ecuador en el tema de ciberseguridad.

En un estudio reciente acerca de las tendencias que conlleva los ciber riesgos y seguridad de la información realizado por Deloitte a nivel Latinoamérica presenta algunas estadística de interés:

- 4 de cada 10 instituciones afirman haber sufrido ciberataques en los últimos 24 meses, sin embargo, solo 2 de cada 10 han podido validar la efectividad del proceso de respuesta a los ciber incidentes y evitar que ocurran nuevamente.
- 8 de cada 10 instituciones afirman no generar nuevas estrategias frente a las amenazas, lo cual no garantiza una protección frente ataque y poder minimizar su impacto.

- 4 de cada 10 empresas cuentan con un plan de continuidad del negocio.
- 1 de cada 10 empresas que cuentan con un plan de continuidad del negocio, han incluido a los ciberataques como escenarios a ser considerados para definir sus estrategias de continuidad.

Este estudio analizó la participación de 150 instituciones públicas y privadas, de las cuales 84 instituciones pertenecen al Ecuador. Los ciberataques son los incidentes de seguridad más comunes mientras las empresas apuestan más a la tecnología para mejorar su participación en el mercado, así como para optimizar sus costos de operación (Chávez, R., 2019).

**Análisis de Riesgos de uso de Cloud Computing**

A continuación, se identificaron los principales riesgos a los que están expuestos los servicios de computación en la nube contratados por las Pymes ecuatorianas, teniendo en cuenta que existen diferentes formas de implementación de servicios en la nube fue importante en primera instancia conocer cuáles de estas opciones son las más adoptadas por las pymes. Aunque es innegable la tendencia de las Pymes ecuatorianas en adoptar el cloud computing, hay una escasa cantidad de investigaciones que analizan los factores que afectan esta adopción, por lo cual se toma como referencia el estudio publicado en (Celleri J-Pacheco, Rivas Asanza W, Andrade Garda J, Rodríguez Yáñez S, 2019), donde incluye un estudio exploratorio aplicado a través de encuestas a una muestra de 331 empresas de la provincia del Oro, siendo el 86% Micro, Pequeñas y Medianas Empresas, dentro de los resultados del estudio en la parte pertinente a la identificación a los servicios más optados por las Pymes, se puede identificar que el 68% de las empresas han optado por el modelo de despliegue privado, el 16% a la nube Pública y el 8% a la nube Híbrida y Comunitaria. En relación al modelo de servicio, las empresas han demostrado una preferencia de un 75% por los denominados Software como servicio (SaaS), un 25% para el nivel Plataforma como servicio (PaaS) y un reducido 16,7% para la Infraestructura (IaaS), considerando que existen empresas que usan más de un modelo (Aguilar, J. M.).

El riesgo de los servicios en la nube se evaluó mediante los incidentes de seguridad ocurridos desde dos perspectivas: la probabilidad y el impacto de los incidentes. Para el proceso de evaluación del riesgo se utilizaron los criterios definidos por el NIST (Instituto Nacional de Normas y Tecnología, USA) en su publicación “800-30: Risk Management Guide for Information Technology Systems”.

**Tabla 1.**

*Escala de Medición de la Probabilidad.*

| Nivel | Significado | Descripción |
|---|---|---|
| 5 | Muy Alto | Es casi seguro que el incidente ocurra |
| 4 | Alto | Es muy probable que el incidente ocurra |
| 3 | Medio | Es probable que el incidente ocurra |
| 2 | Bajo | Es poco probable que el incidente ocurra |
| 1 | Muy Bajo | Es muy poco probable que el incidente ocurra |

**Tabla 2.**

*Escala de Medición del Impacto.*

| Nivel | Significado | Descripción |
|---|---|---|
| 5 | Muy Alto | Si ocurre un incidente es casi seguro que generará un impacto adverso. |
| 4 | Alto | Si ocurre un incidente es muy probable que genere un impacto adverso. |
| 3 | Medio | Si ocurre un incidente es probable que se generará un impacto adverso |
| 2 | Bajo | Si ocurre un incidente es poco probable que se genere un impacto adverso |
| 1 | Muy Bajo | Si ocurre un incidente es muy poco probable que se produzca un impacto adverso |

Por tanto, la evaluación de los riesgos de seguridad en la implementación de la computación en la nube se realizó mediante el análisis de la probabilidad e impacto de los incidentes identificados.

Cada empresa o Pyme que decide contratar diferentes servicios del cloud computing es diferente y por ende las principales vulnerabilidades a las que pueden estar expuestas pueden variar entre ellas, el presente estudio identificó las vulnerabilidades más relevantes y comunes entre las empresas de tal manera que sirva de una guía estándar para las Pymes ecuatorianas.

**Tabla 3.**

*Valoración del impacto y probabilidad de las vulnerabilidades identificadas.*

| ID | Vulnerabilidad | Riesgo | I | P |
|---|---|---|---|---|
| **1** | Se desconoce la reputación, trayectoria, cartera de clientes y sostenibilidad del proveedor, por lo que no se tiene la garantía de contar con el respaldo de una empresa sólida, así como la disponibilidad del servicio y de la información. | Confidencialidad, Integridad, Disponibilidad, Arquitectura, Cumplimiento de la Normativa | 3 | 3 |
| **2** | Los acuerdos del nivel de servicio no presentan las garantías necesarias con respecto a los tres ejes fundamentales de la seguridad de la información como son: confidencialidad, la integridad y disponibilidad, por lo cual la operación del negocio se puede ver comprometida. | Confidencialidad, Integridad, Disponibilidad, Arquitectura, Cumplimiento de la norma | 5 | 4 |

| | | | | |
|---|---|---|---|---|
| **3** | No se tiene claro en donde reside la información y cuál es la normativa legal que rige en el país que custodia la información. | Confidencialidad, Integridad, Disponibilidad, Cumplimiento de la Norma, Localización de los datos | 3 | 2 |
| **4** | Inadecuado proceso que maneja el proveedor con respecto al acceso a la información por parte de terceros, lo que puede comprometer la confidencialidad de la misma. | Confidencialidad, Integridad | 4 | 3 |
| **5** | Infraestructura compartida entre varios clientes puede provocar la mezcla de información. | Confidencialidad, Integridad, Disponibilidad, Arquitectura, Aislamiento de Datos | 5 | 2 |
| **6** | La falta de un plan de recuperación ante cualquier desastre que pueda suceder, el cual además debe estar correctamente documentado, probado, incluir los tiempos de recuperación es otro aspecto. que deben estar especificados en el contrato. | Disponibilidad, Respuesta a incidentes | 4 | 2 |
| **7** | Configuración incorrecta y un inadecuado control de cambios. | Integridad, Disponibilidad | 3 | 3 |
| **8** | Interfaces y APIs inseguras, a través de las cuales se realizan varias tareas como la autenticación, acceso, cifrado de datos, etc. | Confidencialidad, Integridad, Disponibilidad | 2 | 2 |
| **9** | Falta de una estrategia de seguridad en el cloud computing | Confidencialidad, Integridad Disponibilidad, Arquitectura | 5 | 5 |
| **10** | Sistemas débiles de administración y gestión de usuarios por parte del proveedor del servicio | Confidencialidad, Integridad | 4 | 3 |

Luego de valorar la probabilidad e impacto de las principales vulnerabilidades identificadas en los tipos de nubes, se calculó el riesgo el cual se obtuvo de multiplicar la probabilidad y el impacto y ubicarlo en la tabla de valoración de riesgo.

**Tabla 4.**

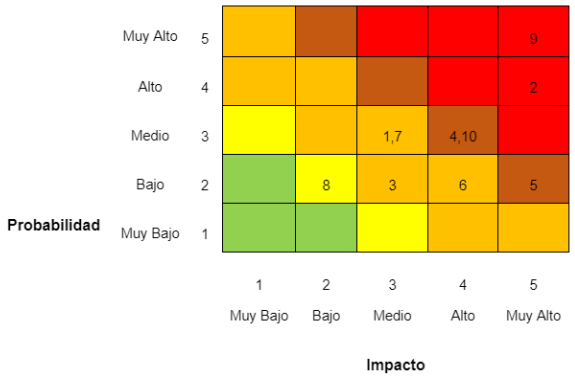
*Valoración del riesgo inherente de las vulnerabilidades identificadas*

| Vulnerabilidad | Impacto | Probabilidad | Riesgo |
|---|---|---|---|
| 1 | 3 | 3 | 9 |
| 2 | 5 | 4 | 20 |
| 3 | 3 | 2 | 6 |
| 4 | 4 | 3 | 12 |
| 5 | 5 | 2 | 10 |
| 6 | 4 | 2 | 8 |
| 7 | 3 | 3 | 9 |
| 8 | 2 | 2 | 4 |
| 9 | 5 | 5 | 25 |

| | | | |
|---|---|---|---|
| 10 | 4 | 3 | 12 |

**Figura 1.**

*Valoración del riesgo inherente de las vulnerabilidades identificadas*




Derivado de este análisis se obtiene que entre los principios de seguridad mayormente afectados en los diferentes tipos de cloud computing en las Pymes Ecuatorianas están:

- Confidencialidad: enfocándonos en la Identidad y Control de Acceso.
- Integridad: centrado en la Identidad y Control de Acceso con el fin de garantizar que la información almacenada en la nube no pueda ser manipulada por personas no autorizadas.
- Disponibilidad.
- Cumplimiento de la normativa
- Marco Arquitectónico o Arquitectura
- Respuestas a incidentes

**Controles, Estándares de Seguridad y Legislación Ecuatoriana.**

La seguridad de la información se alcanza mediante la implementación de un conjunto adecuado de controles, que incluyen políticas, procesos, procedimientos de software y funciones del hardware. Estos controles deben establecerse, implementarse, supervisarse, revisarse y mejorarse según sea necesario, con el fin de asegurar el cumplimiento de los objetivos de seguridad y los objetivos estratégicos de cada PYME. Por lo tanto, es importante establecer los controles de seguridad necesarios en los acuerdos de nivel de servicio con el proveedor de servicios en la nube. Esto asigna la responsabilidad al proveedor de garantizar la seguridad de la información y del servicio en sí.

La especificación de los acuerdos de servicio garantiza la calidad de los servicios en un entorno de contratación o subcontratación. Si bien el SLA no garantiza el cumplimiento de todas las especificaciones, define los mecanismos de seguimiento necesarios y establece responsabilidades, sanciones y compensaciones en caso de incumplimiento.

Una vez identificados los riesgos de mayor impacto y/o probabilidad de ocurrencia, se establecen los controles necesarios y la forma de gestionarlos, basándose en las recomendaciones de estándares de seguridad y en la legislación y regulaciones nacionales aplicables.

En una organización los objetivos de seguridad y privacidad de una organización son de vital importancia para tomar decisiones de externalización de servicios de tecnología de la información y, en particular, en las decisiones de migración de recursos a la nube. Lo que funciona para una PYME no necesariamente funciona para otra.

Este estudio se basó en una serie de estándares internacionales de seguridad de la información actualmente vigentes. Es importante destacar que no existe un modelo superior a los demás, sino que la selección se basó en la pertinencia y el alcance pretendido. Para este estudio, se trabajó principalmente con las normas ISO 27017 e ISO 27018, ya que se centran específicamente en la aplicación de controles y recomendaciones en función de la evolución de los riesgos y los requisitos de seguridad de la información, legales, contractuales y regulatorios que los proveedores de servicios en la nube deben cumplir.

Otro aspecto importante considerado en la presente investigación fue el análisis de la legislación ecuatoriana en el modelo de prestación de servicios de la Computación de la Nube para las PYMES. Las leyes y reglamentaciones desempeñan un papel crucial al establecer lineamientos y directrices necesarias para la celebración de diferentes tipos de contratos. Aunque actualmente Ecuador no cuenta con un marco legal específico que regule las contrataciones entre clientes y proveedores en los modelos de servicios de Cloud Computing, se pudo observar que la falta de seguridad jurídica es uno de los principales obstáculos para una mayor adopción de esta tecnología en el sector empresarial, especialmente en las pequeñas y medianas empresas. Existe una necesidad clara de establecer acciones, responsabilidades y sanciones de manera precisa en los contratos, con el objetivo de generar acuerdos justos.

A pesar de no existir una normativa específica que regule los servicios de cloud computing es importante reconocer que ha existido un avance en la regularización de aspectos que pudieran adaptarse a los servicios del cloud computing.

Es importante considerar que a pesar que ciertos aspectos están respaldados en la legislación ecuatoriana vigente, al momento de escoger un proveedor que se encuentre físicamente ubicado en otro país, la regulación del servicio estará bajo la normativa del país en donde reside físicamente el servicio.

El análisis de la legislación ecuatoriana se basó en disposiciones de las siguientes normativas:

- Constitución de la República del Ecuador.
- Ley Orgánica de Protección de Datos Personales (LOPD) y su reglamento.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Código Integral Penal.
- Ley Orgánica de Telecomunicaciones.
- Ley Orgánica de Transparencia y Acceso a la Información Pública.
- Ley del Sistema Nacional de Registro de Datos Públicos.
- Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación.

Para este análisis se consideró cada uno de los aspectos del cloud computing que son objeto del presente estudio relacionados al cumplimiento de la normativa, arquitectura, disponibilidad, respuesta a incidentes, identidad y control de acceso del servicio con las diferentes normativas ecuatorianas, por lo que, en el Anexo 1 se presenta una comparativa de cada uno de los artículos de las diferentes leyes y reglamentos que respaldan el servicio tomando en cuenta los principios de seguridad mayormente afectados y que fueron detectados en el presente estudio.

En el Ecuador, el crecimiento del Cloud Computing ha sido evidente, pero ha carecido de criterios claros de estandarización. En lugar de ello, los proveedores han optado por diferenciar sus servicios mediante especificaciones propias. Esto ha llevado a la creación de contratos estáticos y predefinidos para todos los usuarios del servicio, que protegen los intereses de los proveedores incluyendo términos ambiguos que dificultan la evaluación de las ofertas de servicio y los riesgos asociados a los mismos.

A pesar de todos los beneficios que aportan las organizaciones para la estandarización del servicio de Cloud Computing, debemos tener claro que como usuarios de estos servicios conllevan responsabilidad, principalmente en un profundo análisis de las listas de comprobación SLA para escoger el proveedor del servicio según las necesidades, luego el correcto uso dentro de la empresa y como usuario final.

Es de vital importancia que en los acuerdos entre proveedores y clientes en una contratación de los servicios de cloud computing se incorporen distintas cláusulas para garantizar la seguridad de la

información y preferiblemente éstas se deriven de controles recomendados por diferentes estándares de seguridad, así como estén acorde a la normativa legal vigente, lo que permitirá a las PYMES ecuatorianas seleccionar la mejor alternativa de servicio ofertados por los proveedores. Antes de realizar la evaluación de la mejor alternativa es importante que la empresa conozca los requerimientos del servicio, de tal manera se comparan los criterios requeridos por los usuarios versus los parámetros del servicio ofertado por los proveedores, para esto el presente estudio propone como resultado de la investigación la siguiente la lista de comprobación que ayuda a verificar que un Service Level Agreement (SLA) de servicio de la nube firmado por una PYME en Ecuador se garantice la seguridad y protección de los datos, ésta herramienta se la puede encontrar que lo puede encontrar en el Anexo 2.

## V. CONCLUSIONES

- La lista de comprobación de Niveles de Acuerdos de Servicios contratados en la nube propuesta en el presente estudio, representa una sustancial contribución de la academia al sector productivo ecuatoriano (PYMES), el cual pretende ayudar a las empresas a evaluar los requisitos de seguridad al contratar los diferentes tipos de servicios en la nube, debido a que fue construida tomando como referencia controles recomendados por diferentes estándares de calidad asociados a la seguridad de la información así como a requisitos legales de protección de datos de la legislación ecuatoriana, brindando mayor confianza a los clientes al momento de tomar la decisión de dar el salto a la computación de la nube o realizar el cambio de proveedor de los servicios contratados, en el cual se incluye exigencias en la gestión y monitoreo del servicio, por lo tanto la lista de comprobación en mención se convierte en un documento sencillo que ayuda a las PYMES a negociar un SLA que se ajuste a sus objetivos empresariales.
- La lista de comprobación pretende establecer una compresión mutua de los parámetros del servicio según las áreas de seguridad priorizadas en concordancia a los principales riesgos que han impactado a las empresas ecuatorianas en temas de seguridad de la información y protección de datos; así como las responsabilidades y garantías en caso de incumplimiento de algún acuerdo de nivel de servicio pactado.
- El SLA pactado debe formar parte del contrato del servicio de computación en la nube para proteger a ambas partes en el acuerdo.
- Es importante considerar que los requisitos del servicio, así como las capacidades de los proveedores son variantes, por lo se debe considerar en la negociación un mecanismo para que los acuerdos de nivel de servicio se mantengan actualizados.

- El SLA propuesto fue construido en base a la normativa legal vigente, así como a las versiones actuales de los estándares de seguridad de la información existentes, por lo cual, se recomienda que la lista de comprobación sea revisada y actualizada en base a los nuevos cambios en materia legal, así como a nuevas versiones de los estándares aplicados.

# APÉNDICE 1

## MAPEO REQUISITOS LEGALES Y REGLAMENTARIOS

| Alcance | Constitución de la República del Ecuador | Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos | Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos | Código Integral Penal | Ley Orgánica de Telecomunicaciones | Ley Orgánica de Transparencia y Acceso a la Información Pública | Ley del Sistema Nacional de Registro de Datos Públicos | Código orgánico de la economía social de los Conocimientos, Creatividad e Innovación | Ley Orgánica de Protección de Datos Personales (LOPD) |
|---|---|---|---|---|---|---|---|---|---|
| **Cumplimiento de la Normativa** | Art 322 | Disposiciones Generales: 5ta | Art. 21 | Art 178 | Art. 82 | | Art 4 | Art 85 | Art 2 |
| | Art 22 | | | Art 179 | | | | Art 86 | Art 3 |
| | | | | Art 180 | | | | Art 150 | |
| | | | | Art 233 | | | | Art 141 | |
| | | | | | | | | | |
| **Arquitectura** | | | | Art 195 | | | | Art 83 | |
| | | | | | | | | | |
| **Identidad y control de acceso** | Art 66 | Art 5 | | Art 190 | Art 77 | Art 10 | Art 6 | | Art 10 |
| | Art 92 | Art 9 | | Art 234 | | | | | Art 33 |
| | | | | Art 229 | | | | | Art 34 |
| | | | | Art 230 | | | | | Art 35 |
| | | | | Art 231 | | | | | Art 45 |
| | | | | | | | | | |
| **Disponibilidad** | | | | Art 232 | Capítulo II Art 24 | | Art 26 | | Art 17 |
| | | | | | Art 22 | | | | |
| | | | | | | | | | |
| **Respuesta a Incidentes** | | | | | | | | | Art 44 |

# MAPEO ESTÁNDARES INTERNACIONALES SEGURIDAD CLOUD COMPUTING VS RIESGOS IDENTIFICADOS PARA PYMES ECUATORIANAS

| Organizaciones de estandarización de Cloud Computing orientadas a la seguridad | Estándares más relevantes en seguridad | Riesgo | | | | |
|---|---|---|---|---|---|---|
| | | Confidencialidad | Integridad | Disponibilidad | Arquitectura | Cumplimiento de la Normativa |
| **International Telecommunication Union (ITU)** | **ITU-T Y.3501**: Proporciona un marco de referencia para Cloud Computing mediante la identificación de requisitos de alto nivel para la computación en nube | | | | | X |
| | **UIT-T Y.3510:** Identifica los requisitos para las capacidades de infraestructura en la nube para apoyar los servicios de nube. | | | | | X |
| | **UIT-T Y.3520:** Describe la plataforma de computación en nube necesaria para la gestión de recursos de los usuarios finales. | | | | | X |
| | **UIT-T Y.3511**: Marco de la computación en nube para la comunicación inter-redes y la infraestructur | | | X | | X |
| | **UIT-T X.1600:** Marco de seguridad para el Cloud Computing. | X | | | | X |
| **ISO (Organización Internacional de Normalización** | **ISO/IEC 17203:2017** Tecnología de la información: especificación del formato de virtualización abierta | | | | | X |
| | **ISO/IEC 17788:2014** Tecnología de la información - Computación en la nube | | | | | X |
| | **ISO/IEC 17789:2014** Tecnología de la información - Computación en la nube - Arquitectura de referencia | | | | X | X |
| | **ISO/IEC 17963:2013** Especificación de servicios web para administración (WS-Management) | | | | X | X |
| | **Serie ISO/IEC 18384** Tecnología de la información - Arquitectura de referencia para arquitectura orientada a servicios. | | | | X | X |
| | **Serie ISO/IEC 19086**: Tecnología de la información - Computación en la nube - Marco del acuerdo de nivel de servicio | X | | | X | X |
| | **ISO / IEC 19086-1**: 2016 es para el beneficio y uso tanto de los proveedores de servicios en la nube como de los clientes de servicios en la nube | | | X | | X |
| | **ISO/IEC 19941:2017** Tecnología de la información - Computación en la nube - Interoperabilidad y portabilidad | X | | X | | X |
| | **ISO/IEC 19944:2017** Tecnología de la información - Computación en la nube - Servicios y dispositivos en la nube | | | X | | X |
| | **ISO / IEC 27001: 2013** Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información | X | X | X | X | X |
| | **ISO / IEC 27701: 2019** Técnicas de seguridad - Extensión a ISO / IEC 27001 e ISO / IEC 27002 para la gestión de la información de privacidad | X | | | | X |
| | **ISO / IEC 27002: 2013:** Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información | X | X | X | X | X |
| | **ISO / IEC TS 27110:2021:** Tecnología de la información, ciberseguridad y protección de la privacidad | X | X | | | X |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **ISO/IEC 27017:2015:** Tecnología de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información basado en ISO / IEC 27002 | X | X | X | X | X |
| | **ISO / IEC 27018: 2019** Tecnología de la información - Técnicas de seguridad | X | X | X | X | X |
| | **ISO / IEC 27032: 2012** Tecnología de la información - Técnicas de seguridad - Directrices para la ciberseguridad | X | X | | | X |
| | **ISO/IEC TR 22678:2019** Este documento proporciona orientación sobre el uso de estándares internacionales | | | | | X |
| | **ISO/IEC TR 23186:2018** Tecnología de la información - Computación en la nube - Marco de confianza para el procesamiento de datos de múltiples fuentes | X | | | | X |
| | **ISO/IEC TR 30102:2012** Tecnología de la información - Plataformas y servicios de aplicaciones distribuidas | X | | | X | X |
| | **ISO/IEC DIS 22624** Tecnología de la información - Computación en la nube - Manejo de datos basado en taxonomía para servicios en la nube | | | | | X |
| | **ISO/IEC PDTS 23167** Tecnología de la información - Computación en la nube - Tecnologías y técnicas comunes | X | | | | X |
| | **ISO/IEC NP TR 23187** Tecnología de la información - Computación en la nube - Interacción con socios de servicios en la nube (CSN) | X | | | | X |
| | **ISO/IEC PDTR 23188** Tecnología de la información - Computación en la nube - Panorama de la computación perimetral | | | | | X |
| | **ISO / IEC TR 23951: 2020** Tecnología de la información - Computación en la nube - Orientación para usar el modelo métrico de SLA en la nube | X | | | | X |
| | **ISO/IEC NP TR 23613** Tecnología de la información - Computación en la nube - Elementos de medición de servicios en la nube y modos de facturación | | | | | X |
| | **ISO/IEC AWI 23751** Tecnología de la información - Computación en la nube y plataformas distribuidas | | | | | X |
| **IETF (Internet Engineering Task Force),** | **RFC 6208** describe los tipos de medios para las interfaces de Gestión de Datos de Nubes | | | | | X |
| **Cloud Security Alliance (CSA)** | **CSA Cloud Controls Matrix** es un marco de control de ciberseguridad para la computación en la nube | X | | | X | X |
| **El comité Técnico GRID de la ETSI** | **ETSI SR 003 391 V2.1.1 (2016-02):** Fase 2 de coordinación de estándares en la nube; Interoperabilidad y seguridad en la nube | X | X | | | X |
| | **ETSI SR 003 392 V2.1.1 (2016-02)**: Fase 2 de coordinación de estándares en la nube | | | | | X |
| | **ETSI SR 003 382 V2.1.1 (2016-02):** Fase 2 de coordinación de estándares en la nube; Estándares de Computación en la Nube y Código Abierto | | | | | X |
| | **ETSI SR 003 381 V2.1.1 (2016-02)**: Fase 2 de coordinación de estándares en la nube; Identificación de las necesidades de los usuarios de la nube | | | | | X |
| | **ETSI TR 101567 V1.1.1 (2016-01)**: Intercepción legal (LI); Servicios virtuales / en la nube para interceptación legal (LI) y datos retenidos (RD) | | | | | X |
| | **ETSI TR 102 997 V1.1.1 (2010-04):** NUBE; Análisis inicial de los requisitos de estandarización para los servicios en la nube | | | | | X |
| | **ETSI TR 103126 V1.1.1 (2012-11):** NUBE; Recomendaciones de usuarios del sector privado de la nube | | | | | X |

## APÉNDICE 2

# Lista de comprobación para verificar que un Service Level Agreement (SLA) de servicio de la nube firmado por una PYME en Ecuador garantiza la seguridad y protección de datos

| Riesgo | Dominio | Control recomendado | Cumple si [1] / no [0] |
|---|---|---|---|
| Identidad y Control de Acceso | Control de acceso a la información e instalaciones | Dispone de una política de control de acceso a los sistemas e instalaciones | |
| | | Socializa la política de control de acceso en la organización. | |
| | Gestión de acceso al usuario (Garantizar el acceso a usuarios autorizados e impedir el acceso no autorizado a sistemas de información y servicios) | Posee un procedimiento para la creación y eliminación de usuarios. | |
| | | Cuando se usen contraseñas como información secreta de autenticación, se seleccionan contraseñas de calidad con número mínimos de caracteres, caracteres alfanuméricos, así como caracteres especiales. | |
| | | Posee un procedimiento para la gestión de derechos de acceso con privilegios especiales. | |
| | | Encripta la información confidencial de autenticación de los usuarios. | |
| | | Los empleados firman un acuerdo de confidencialidad antes de que se le entreguen las credenciales de acceso. | |
| | Responsabilidades de los usuarios. | Respalda la entrega de las credenciales del usuario mediante un acta entrega recepción o símil, en donde conste que el usuario se responsabiliza el uso correcto de sus credenciales. | |
| | | Se solicita el cambio de contraseña en el primer acceso al sistema. | |
| | Control de acceso a sistemas y aplicaciones | Controla la restricción de acceso a la información, asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados. | |
| | | Dispone de procedimientos fiables de inicio de sesión. | |
| | | Manera interactiva y eficiente para la gestión de contraseñas de usuario. | |
| | | Control de acceso al código fuente de las aplicaciones de software. | |
| | | Cuenta con registros de accesos de los usuarios de la nube. | |
| | Acceso a redes y servicios de red | Identifica y documenta los equipos que se encuentran en las redes debidamente autorizados. | |
| | | Monitorear continuamente el uso de los servicios de la red, con alertas sobre aquellos recursos que se consideren críticos. | |
| | Separación de entornos virtuales. | El entorno virtual de un cliente del cloud computing está protegido de otros clientes del servicio en la nube y personas no autorizadas. | |

| | | | |
|---|---|---|---|
| | Virtual Machine harderin | El administrador de infraestructura instala permanentemente las actualizaciones del sistema operativo de las máquinas virtuales. | |
| | Criptografía | Proporciona protección criptográfica a los datos en reposo y en tránsito utiliza bibliotecas criptográficas certificadas según los estándares aprobados | |
| Disponibilidad | Responsabilidades y procedimientos de operación (Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.) | Posee documentación de procedimientos de operación y éstos estén al alcance de los usuarios que lo requieran. | |
| | | Gestiona los cambios que afectan la seguridad de la información y procesos del negocio, instalaciones y sistemas de procesamiento de la información. | |
| | | Gestiona las capacidades a través del seguimiento y ajuste del uso de recursos a través de proyecciones necesarias para el futuro. | |
| | | Separa los entornos de prueba, desarrollo y producción. | |
| | Copias de seguridad (El objetivo es alcanzar un grado de protección deseado contra la pérdida de datos) | Realiza copias de seguridad de la información, además evidencia pruebas regulares de las copias de información, del software y de las imágenes del sistema en relación a una política de respaldo. | |
| | | Entrega en un periodo determinado una copia de seguridad al cliente. | |
| | | Cuenta con un procedimiento para la restauración de datos. | |
| | Registro de actividad y supervisión (Registrar los eventos relacionados a la seguridad de la información y generar evidencias) | Registra y gestiona eventos de seguridad de la información, actividad, excepciones y fallas. | |
| | | Sincronización del reloj. | |
| | Garantía de disponibilidad | Específica explícitamente el porcentaje de disponibilidad durante los días laborales, noches y fines de semana. | |
| | | Posee acuerdos de intercambio de información con entidades externas si el servicio así lo amerita | |
| | | Asegurar los servicios de aplicaciones en redes públicas. | |
| | | Especifica las sanciones aplicadas en caso del no cumplimiento del porcentaje de disponibilidad. | |
| | Auditoría | Posee controles de auditoría en los sistemas de información. | |
| | Protección contra código malicioso. | Garantiza la infiltración de código malicioso en los servicios que el ofrece. | |
| Cumplimiento de la normativa | Mapeo regulatorio del sistema de información | Identifica y documenta todos los estándares, regulaciones, legales / contractuales,<br>y requisitos legales, que son aplicables a su organización. | |
| | Ubicación | Ubicación de los datos de acuerdo a la normativa legal. | |
| | Normativa Legal Vigente | Manifiesta el incumplimiento de la legislación en materia de protección de datos y especifica que puede dar lugar a la imposición de sanciones administrativas, civiles e incluso penales, que varían en función del país | |
| | | Garantiza los derechos de propiedad intelectual de acuerdo a la normativa legal vigente. | |

| | | | |
|---|---|---|---|
| | | El contrato del servicio identifica claramente los diferentes actores involucrados: Consumidor, Proveedor, Transportador (intermediario que ofrece conectividad y transporte de los servicios y los datos desde los entornos del proveedor a los del consumidor) y/o Broker (intermediario que se encarga de negociar la relación entre el consumidor y el proveedor) | |
| | | El proveedor cuenta con herramientas de mediciones y monitoreo del servicio para asegurar que el nivel de servicio está en los rangos aceptables. | |
| | | Especifica quien posee o controla la infraestructura o si es subcontratada a terceros. | |
| | | Específica en donde se encuentran las instalaciones. | |
| | | Actúa en concordancia de la normativa legal como la ley de protección de datos, ley de telecomunicaciones, etc. y aquellas que al momento se encuentren vigentes. | |
| | | El proveedor especifica las garantías en caso de que se violó las leyes con relación a la protección de datos incluso si los datos se almacenan en un país con ninguna ley de protección de datos. | |
| | Fin de la contratación del servicio | Especifica el procedimiento a seguir para migrar los datos a un proveedor competidor al momento de terminar el contrato. | |
| Arquitectura | Infraestructura y Seguridad de la Virtualización | Utiliza canales de comunicación seguros y encriptados al migrar servidores, servicios, aplicaciones o datos a entornos de nube. Dichos canales deben incluir solo protocolos actualizados y aprobados. | |
| | Infraestructura y Seguridad de la Virtualización | Documenta las técnicas de protección, detección y respuesta oportuna a los ataques basados en la red y tiene registros que los evidencia. | |
| | Security Data Center | Posee procesos establecidos para la reubicación o transferencia de hardware, software, o datos / información a una ubicación externa o alternativa. La solicitud requiere la autorización escrita o verificable criptográficamente. | |
| | | Posee procesos establecidos para el transporte seguro de medios físicos, revisar y actualizar las políticas y procedimientos al menos una vez al año. | |
| | | Clasifica y documenta los activos físicos y lógicos (por ejemplo, aplicaciones), basado en el riesgo empresarial organizacional. | |
| | | Implementa perímetros de seguridad física para salvaguardar los datos, y sistemas de información. | |
| | | Posee las medidas necesarias que garantizan la protección de la energía y las telecomunicaciones. | |
| | | Tiene implementado algún control físico de entrada al Data Center y evidencia los registros de acceso. | |
| | | Posee operando óptimamente sistemas de control ambiental en el centro de datos y monitorea la efectividad continua de la temperatura y condiciones de humedad, evidencia los registros de los monitoreos. | |
| | | Mantiene los equipos críticos de la empresa lejos de ubicaciones sujetas a altas probabilidades de eventos de riesgo ambiental. | |

| | | | |
|---|---|---|---|
| | Detección y actualizaciones | Posee, actualizar las herramientas de detección, firmas de amenazas e indicadores de compromiso semanalmente o con mayor frecuencia. | |
| | Software firewall | Configura los endpoints con firewalls de software configurados correctamente. | |
| | Capacidad de Infraestructura | Especifica el rendimiento del servicio en tiempos de respuesta mínimos. | |
| | Legalidad de software | Utiliza versiones originales de sistemas operativos y de más aplicaciones. | |
| | Portabilidad. | Especifica si garantiza la portabilidad de los datos entre proveedores, tanto formato de los datos, tamaño, política de borrado de datos. | |
| | Medición y métricas | Posee al menos las siguientes métricas:<br>Utilización del CPU.<br>Memoria utilizada.<br>Memoria disponible.<br>Tasa de la caché.<br>Tiempo de espera del servidor, etc.<br>Además por cada métrica establece límites máximos, mínimos, valores por defectos, desviaciones esperadas. | |
| | | Posee un proceso para la aplicación de cada métrica, en donde se establecen además los periodos de mediciones. | |
| Respuesta a incidentes | Política y procedimientos de gestión de incidentes de seguridad | Posee políticas y procedimientos actualizados para la gestión de incidentes de seguridad. | |
| | Notificación de violación de seguridad | Notifica a sus clientes las violaciones de seguridad. Informa brechas de seguridad e incumplimientos del nivel de seguridad basado en leyes y regulaciones. | |
| | Plan de respuesta a desastres. | Posee un plan probado de respuesta a desastres para recuperarse de desastres naturales provocados por el hombre. Actualiza el plan al menos una vez al año o ante cambios significativos. | |
| | Redundancia | Complementa los equipos y enlaces críticos para el negocio con equipos redundantes de forma independiente ubicado a una distancia mínima razonable de acuerdo con la industria aplicable normas. | |
| | Puntos de contacto | Mantiene puntos de contacto de las autoridades reguladoras de la aplicación de la ley nacional y local, y otras autoridades jurisdiccionales legales. | |
| | Mesa de servicio | Pose un proceso para identificar problemas y expectativas de resolución (por ejemplo, centro de llamadas) | |
| | Mesa de servicio | Especifica en el contrato los tiempos de respuesta a incidentes de acuerdo al tipo de incidente. | |
| | | **TOTAL:** | |

## VI. Referencias Bibliográficas


Aguilar, J. M. (2019, 5 diciembre). Hechos ciber físicos: una propuesta de análisis para ciber amenazas en las Estrategias Nacionales de Ciberseguridad. https://revistas.flacsoandes, https://revistas.flacsoandes.edu.ec/urvio/article/view/4007/3193.

Asamblea Constituyente del Ecuador (2018), Constitución de la República del Ecuador 2008, 20 de octubre de 2008.

Asamblea Nacional del Ecuador (2015), Ley Orgánica de Telecomunicaciones, 18 de febrero de 2015.

Asamblea Nacional del Ecuador (2016), Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, 9 de diciembre de 2016.

Asamblea Nacional del Ecuador (2021), Ley del Sistema Nacional de Registro de Datos Públicos, 26 de mayo de 2021.

Asamblea Nacional del Ecuador (2021), Ley Orgánica de Protección de datos personales, 26 de mayo de 2021.

Asamblea Nacional del Ecuador (2021), Código Integral Penal, 17 de febrero de 2021.

B. Kitchenham, D., Budgen, and B. Pearl (2011), "Using mapping studies as the basis for further research–a participant-observer case study. Information and Software Technology", 53(6), 638-651, Science Direct.

Braun, V., Clarke V (2006), "Using thematic analysis in psychology, Qualitative Research in Psychology", 3(2):77-101. Routledge, IEEE.

Brereton P, Kitchenham, D., Budgen, Turner M (2011), Lessons from applying the systematic literature review process within the software engineering domain. JSS 80, pp. 571-583.

Budgen D., Turner M., Brereton P., Kitchenham B. (2008), Using mapping studies in software engineering, in: Proceedings of PPIG 2008, Lancaster University, pp.195–204.

Celleri J-Pacheco, Rivas Asanza W, Andrade Garda J, Rodríguez Yáñez S (2019), Análisis del uso del Cloud Computing en empresas de Ecuador 2019, 10.23878/alternativas. v19i2.251, Alternativas.

Célere, J., Andrade, J., & Rodríguez, S. (2018). Cloud Computing para PYMEs. (Primera en Español ed.). Ediciones UTMACH.

Chávez, R. (2019), Ciberseguridad: Latinoamérica vs. Ecuador. https://datta.com.ec/. https://datta.com.ec/articulo/ciberseguridad-latinoamerica-vs-ecuador.

Congreso Nacional del Ecuador (2004), Ley Orgánica de Transparencia y Acceso a la Información Pública, 18 de mayo de 2004.

Congreso Nacional del Ecuador (2004), Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos del Ecuador, 17 de abril del 2002.

Cruzes D., Tore D (2011), Research synthesis in software engineering: A tertiary study. Inf. Softw. Technol, 53(5): 440455.

CSA, (2021), Cloud Controls Matrix and CAIQ v4, https://cloudsecurityalliance.org/. https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/

Da Silva, C. A., & Geus, P. L. (2014). An Approach to Security-SLA in Cloud Computing Environment (2014 IEEE Latin-America Conference on Communications (LATINCOM)). Institute of Computing - Unicamp Campinas, Brazil.

EINISA. (2009). Computación en la nube, Beneficios, riesgos y recomendaciones para la seguridad de la información. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish.

Feng Xie, Yong Peng, Wei Zhao, Dongqing Chen, Xiaoran Wang, Xingmei Huo, (2012), A Risk Management framework for cloud computing.

Fernandez C., Daneva M., Sikkel K., Wieringa R., Dieste O., Pastor O., (2009) "A systematic mapping study on empirical evaluation of software requirements specifications techniques", ESEM 3rd International Symposium, 502-505.

Garre, S., Segovia, A. J., Tortajada, A. (2020). Implementación de un sistema de gestión de la seguridad de la información (Tercera Edición). Fundació Universitat Oberta de Catalunya.

Gilje Jaatun, Bernsmed K, Undheim A, (2012), Security SLAs - An Idea Whose Time Has Come?, pages 123-130, Lecture Notes in Computer Science, Springer Berlin/Heidelberg.

Mannan M, Usan M, (2011), Software Engineering Curriculum: "A Systematic Mapping Study, IEEE, 2011.

NIST, (2012), NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments. Recuperado de: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Petersen R. S. M., Feldt K., Mattson (2008), Systematic mapping studies in software engineering In EASE 08, pages 1–10, Bari, Italy, 2008.

Rivas Solórzano, J. A., (2016), Estado del arte de los Servicios de Contratación y Protección de datos en la Nube. Universidad Nacional de Loja.

Staples M. , Niazi M, (2008), “Systematic review: Systematic review of organizational motivations for adopting CMM-based SPI,” Inf. Softw. Technol. 50 (7-8): 605-620.

Instituto Nacional de Estadística y Censos (2022). Boletín Nro 01-2022-DIEE "Directorio de Empresas y establecimientos 2021". https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Economicas/DirectorioEmpresas/Directorio_Empresas_2021/Boletin_Tecnico_DIEE_2021.pdf