UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
SANTIAGO-CHILE

GUÍA METODOLÓGICA PARA EL USO DE CLOUD COMPUTING EN INSTITUCIONES PÚBLICAS CHILENAS

DIEGO ALONSO QUIROZ ARÁNGUIZ

MEMORIA PARA OPTAR A TÍTULO DE
INGENIERO CIVIL INFORMÁTICA

PROFESRO GUÍA: MAURICIO SOLAR

NOVIEMBRE 2016

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
SANTIAGO-CHILE

GUÍA METODOLÓGICA PARA EL USO DE CLOUD COMPUTING EN INSTITUCIONES PÚBLICAS CHILENAS

DIEGO ALONSO QUIROZ ARÁNGUIZ

MEMORIA PARA OPTAR A TÍTULO DE
INGENIERO CIVIL INFORMÁTICA

PROFESRO GUÍA: MAURICIO SOLAR

PROFESOR CORREFERENTE: RAUL MONGE

NOVIEMBRE 2016

AGRADECIMIENTOS

De manera particular, agradezco a mis padres y hermanos por el apoyo y la motivación entregada. Agradezco a mi pareja Coni por animarme y apoyarme cuando el tiempo, las ganas y la energía eran escasas. Agradezco la comprensión de mis compañeros de trabajo y socios de la empresa SGD, sin las facilidades entregadas no podría haber logrado todos mis objetivos. Agradezco a mis compañeros de universidad y amigos, en especial a Jorge Dinator, Nicolás Madariaga y Felipe Godoy por su buena disposición cuando necesite ayuda. Agradezco a Andrés Arellano, Jonny Heiss, Flavia Gomez, Juan Pablo Reyes, Manuel Suarez y Mario Araneda por regalarme un poco de su tiempo para poder construir los fundamentos de esta memoria. Agradezco al profesor Mauricio Solar por guiar este trabajo.

En general, agradezco a mis amigos y familia. Difícilmente me encontraría en este momento y lugar si no fuera por todos ustedes, gracias.

Esta memoria va dedicada a mi familia. A mis padres por toda la sabiduría y guía entregada a través de los años. A mis hermanos, para que logren todo lo que se propongan en la vida.

RESUMEN EJECUTIVO

Esta guía metodológica pretende entregar un paso a paso para facilitar y/o evaluar una posible implementación de tecnologías Cloud dentro del sector público chileno. En una primera instancia se establecen criterios y conceptos relacionados a la tecnología Cloud, en función de contextualizar al lector. En una segunda instancia, a partir de investigación y entrevistas a individuos relacionados al rubro, se levantan los fundamentos sobre los cuales la guía metódica será construida. En una tercera instancia se confecciona la guía metodológica en base a las conclusiones del paso anterior. Finalmente se presentan conclusiones sobre el trabajo realizado.

ABSTRACT

This guide intents to give a step by step procedure to facilitate the integration of Cloud Computing technology in the Chilean public sector. The first phase of this project involves explanation of concepts and criteria regarding Cloud Computing Technology in order to provide a better understanding of the subject. Afterwards, investigation and interviews are performed in order to build the foundations in which this guide relies upon. The conclusions established in the last step will be used as foundations to build the Guide. In the final phase, conclusions are presented regarding the overall work

Tabla de contenido

AGRADECIMIENTOS i
RESUMEN EJECUTIVO iii
ABSTRACT iv
1. Capítulo 1 1
1.1. Introducción 1
1.2. Definición del problema 3
1.3. Objetivos 4
1.3.1. Objetivos Generales 4
1.3.2. Objetivos Específicos 5
1.3.3. Solución 5
1.4. Metodología 6
2. Capítulo 2: Estado del arte 8
2.1. Infraestructuras Cloud 8
2.1.1. Nube Pública 8
2.1.2. Nube Privada 9
2.1.3. Nube Híbrida 10
2.1.4. Nube Comunitaria 10
2.2. Servicios Cloud 11
2.2.1. Software como servicio (SaaS) 11
2.2.2. Plataforma como servicio (PaaS) 11
2.2.3. Infraestructura como servicio (IaaS) 12
2.4. Servicios Cloud V/S servidores “in house” 13
2.4.1. Pros y contras 13
2.4.2. Costos 15
2.5. Cloud Computing e instituciones públicas alrededor del mundo 19
2.5.1. Cloud Computing e IP en Europa 20
2.5.2 Cloud Computing y el gobierno federal en EE.UU 23
2.5.3. Cloud Computing contexto nacional 24
2.6. Licitaciones actuales 27
3. Capítulo 3: Aspectos relevantes a considerar al contratar un servicio Cloud ... 30
3.1. Tipo de Nube 30
3.2. Tipo de servicios 31

3.3. Disponibilidad y clasificación Tier. 32
3.4. Seguridad de Información y confidencialidad 36
3.4.1. Confidencialidad 36
3.4.2. Integridad de información..... 38
3.4.3. Certificaciones de datacenters. 38
3.4.4. Proveedores en el extranjero. 39
3.5. Relación con proveedor..... 41
3.6. SLA 42
3.6.1. Disponibilidad 43
3.6.2. Tiempos de respuesta 44
3.6.4. Códigos, conductas y estándares para la protección de información 46
3.6.5. Reversibilidad y Terminación de servicios 46
3.7. Contrato Cloud 48
3.7.1. Estructura Contrato..... 48
3.7.3. Terminación de contrato 49
4. Capítulo 4: Antecedentes..... 50
4.1. Complemento Bibliográfico..... 51
4.1.1. Nivel de desarrollo de las tecnologías Cloud en los organismos del Estado 51
4.1.2. Correlación entre Inversión en TI y Madurez Tecnológica en Instituciones Públicas..... 55
4.1.3. Costos almacenamiento Local v/s Cloud 57
4.2. Entrevistas 61
4.2.1. Entrevistas a proveedores 64
4.2.2. Entrevistas a Instituciones Públicas 74
4.2.3. Análisis de los 10 puntos de la guía Practical Guide to Cloud..... 82
5. Capítulo 5: Guía Metodológica para el uso de Cloud Computing para instituciones públicas chilenas..... 86
5.1. Aclaraciones legales 87
5.1.1. Ley N°19.886, sobre Protección de la Vida Privada o Protección de Datos de Carácter Personal..... 87
5.1.2. Datos personas naturales (Ley N° 19.628 y Dictamen N° 43.866) 88
5.1.3. Ley N°20.285, sobre Acceso a la Información Pública 90
5.1.4 Ley N° 17.336, sobre Propiedad Intelectual 90

5.1.5 Proveedores en el extranjero 91
5.2. Estrategia Cloud 92
5.2.1 Visión 92
5.2.2 Estrategia 93
5.3. Equipo Asesor 94
5.3.1. Convenio Marco de Data Center y Servicios Asociados 94
5.3.2. Asesorías UMGD 96
5.4. Evaluación económica Cloud (TCO) 96
5.4.1. Revisión de presupuestos 97
5.4.2. Análisis de Costos (TCO) 97
5.4.3. Modelo TCO 98
5.4.4. Implementación de solución Cloud 101
5.4.5. Implementación de sistema inhouse 103
5.4.6. Migración de sistema inhouse a Cloud 104
5.5. Diseño de Solución 106
5.5.1. Análisis de la información a tratar. 109
5.5.2. Identificar al usuario 113
5.5.3. Niveles de servicio 116
5.5.4. Análisis de costo y presupuestos 117
5.5.5. Perfil tecnológico institución pública 120
5.6. Contratación Cloud 122
5.6.1. Confidencialidad de la información 123
5.6.2. Seguridad de la información 124
5.6.3. Propiedad Intelectual 125
5.6.4. Modificación Unilateral 126
5.6.5. Vendor lock in 127
5.6.6. Terminación del contrato 127
5.6.7. SLA 128
5.7. Resumen: Guía Metodológica para el uso de Cloud Computing para instituciones públicas chilenas 135
6. Conclusiones 138
Bibliografía 141
Anexos 145

Anexo 1: Tabla de instituciones públicas según nivel de madurez y segmento de inversión TI. 145
Anexo 2: Tablas de comparación de costos para Cloud v/s Local para mediana y gran organización..... 148
Anexo 3: Resultado encuesta sobre la relevancia de los 10 puntos de la guía Practical Guide to Cloud Computing a los entrevistados. 151

Índice de Figuras

Figura 3.1: Esquema de clasificación Tier para datacenters. 35
Figura 3.2: Comparación de Downtime entre 4 principales proveedores internacionales de servicios Cloud..... 35
Figura 4.1: Nivel de desarrollo del dominio Habilitantes de gobierno digital, desglosado en sus subdominios. 53
Figura 4.2: Nivel de desarrollo del dominio Software Público y Cloud Computing, desglosado en sus subdominios. 53

Índice de Tablas

Tabla 2.1: Ventajas y desventajas de Nube Pública. 9
Tabla 2.2: Ventajas y desventajas de Nube Privada. 9
Tabla 2.3: Comparación entre arquitecturas Cloud. 10
Tabla 2.4: Pros y Contras de tecnología Cloud. 14
Tabla 2.5: Pros y Contras de TI Tradicional. 14
Tabla 4.1: Niveles de desarrollo del Modelo de Madurez de Gobierno Digital..... 52
Tabla 4.2: Nivel de desarrollo especifico al domino Software Público y Cloud Computing 54
Tabla 4.3: Segmentos correspondientes al nivel de inversión de TI con respecto al presupuesto total de una institución pública..... 55
Tabla 4.4: Comparación Costo Hardware/Software entre ambiente Local y Cloud . 59
Tabla 4.5: Comparación costo de implementación entre ambiente Local y Cloud… 59
Tabla 4.6: Comparación costos de mantenimiento entre ambiente Local y Cloud... 59
Tabla 4.7: Comparación costos proyectados a 3 años para ambiente local y Cloud. 60

Tabla 4.8: Comparación costos proyectados a 3 años para ambiente local y Cloud para una organización mediana. 60
Tabla 4.9: Comparación costos proyectados a 3 años para ambiente local y Cloud para una organización grande. 61
Tabla 4.10: Listado de entrevistas realizadas 63
Tabla 4.11: Pros y contras de los proveedores de Cloud local desde el punto de vista de una institución pública 74
Tabla 4.12: Pros y contras de los proveedores de Cloud Extranjeros desde el punto de vista de una institución pública 74
Tabla 4.13: Calificaciones promedio otorgadas por los entrevistados a los 10 puntos de la guía Practical Guide to Cloud Computing..... 83
Tabla 5.1: Escenarios Cloud en base confidencialidad de la información. 111
Tabla 5.2: Escenarios Cloud en base al tipo de dato a tratar. 113
Tabla 5.3: Escenarios Cloud en base al foco del sistema a utilizar. 116
Tabla 5.4: Escenarios Cloud en base a la exigencia de los niveles de servicio..... 117
Tabla 5.5: Escenarios Cloud en base a la capacidad de la institución de manejar costos variables. 118
Tabla 5.6: Costos de proveedores internacionales en base a los 3 escenarios establecidos..... 119
Tabla 5.7: Escenarios Cloud en base a la capacidad de presupuesto de la institución..... 120
Tabla 0.1: Comparación costo de implementación entre ambiente Local y Cloud para un organización mediana. 148
Tabla 0.2: Comparación costos de mantenimiento entre ambiente Local y Cloud para una organización mediana. 148
Tabla 0.3: Comparación Costo Hardware/Software entre ambiente Local y Cloud para una organización mediana. 149
Tabla 0.4: Comparación costo de implementación entre ambiente Local y Cloud para una organización grande. 149
Tabla 0.5: Comparación costos de mantenimiento entre ambiente Local y Cloud para una organización grande. 150
Tabla 0.6: Comparación Costo Hardware/Software entre ambiente Local y Cloud para una organización grande. 150

Tabla 0.7: Resultados de la encuesta con respecto a la importancia de los puntos planteados en la guía Practical Guide To Cloud Computing 151

Índice de Ecuaciones

Ec. 5.1 98
Ec. 5.2 101
Ec. 5.3 102
Ec. 5.4 102
Ec. 5.5 103
Ec. 5.6 103
Ec. 5.7 104
Ec. 5.8 104
Ec. 5.9 105
Ec 5.10 106
Ec 5.11 106

1. Capítulo 1

1.1. Introducción

El concepto Cloud Computing es un término muy utilizado día a día, no solo por personas relacionadas a TI, sino que cada vez son más las empresas, instituciones públicas, organizaciones e incluso personas naturales los que hacen uso de la tecnología. Ya sea de manera directa o indirecta, consciente o inconsciente, las soluciones Cloud se encuentran presentes, y las tendencias indican que su crecimiento es inminente. Existen grandes beneficios en torno al uso de esta tecnología puesto que su utilización puede implicar importantes ahorros de costos económicos y de tiempo en la gestión de plataformas electrónicas. Además, dependiendo del prestador del servicio, la computación en nube puede potencialmente entregar beneficios tales como la escalabilidad, elasticidad, alto rendimiento, resistencia y seguridad (Agencia Europea de seguridad de las redes y de la información, 2011). Pero, ¿Qué es el Cloud Computing?, ¿Cuáles son sus beneficios?, ¿Cuáles son sus riegos?, ¿A qué tipo de cliente este modelo apunta?, ¿Puedo yo o mi institución utilizar este modelo?, y de ser así ¿Son los beneficios entregados por el modelo superiores al gasto involucrado?

Para proporcionar una contextualización previa a la definición formal de la tecnología, se introducirá con una breve historia de los orígenes de la tecnología. Las tecnologías Cloud nacen de la visualización de una oportunidad de negocio por parte de las empresas, a partir de sus necesidades de almacenamiento de datos e infraestructura. El escenario es el siguiente; empresas de gran envergadura se ven en necesidad de almacenamiento de datos en grandes volúmenes, por lo cual se hace necesario el desarrollo de un datacenter interno. Obviamente este datacenter requiere suplir las necesidades de almacenamiento de la empresa de tal manera que justifique la relación precio/durabilidad, por lo cual se construyen datacenters con gran

capacidad de cómputo y almacenamiento. Luego de un tiempo de uso, los encargados del datacenter caen en cuenta que el datacenter construido sobrepasa el tamaño necesario con creces. A raíz de esta situación nace la brillante idea de ofrecer el datacenter como servicio de almacenamiento a través de internet a otras empresas que no poseen la capacidad económica de desarrollar su propia infraestructura TI, dando nacimiento al concepto de Cloud Computing. Dado el atractivo comercial que el servicio genera, principalmente por los múltiples beneficios que la adopción del modelo proporciona para sus clientes, el modelo logra consolidarse, permitiendo aumento de tamaño en los datacenters, calidad de servicio y alcance.

¿Qué es el Cloud Computing?

Actualmente Cloud Computing es la clara evolución e inclusión de diversas tecnologías que han llegado a converger en lo que hoy llamamos como la Nube. ¿Por qué nube? Son varios los factores que crean la "ilusión" o metáfora de la nube como tal, ya sea por la transmisión "aérea" de datos otorgada por la columna vertebral o canal de transmisión que es el internet, o por la intangibilidad de dispositivos de almacenamiento, la abstracción de información otorga la denominación al servicio. Una definición más concisa es la que entrega el "NIST" (National Institute of Standards and Technology, 2011) "Cloud Computing es un modelo que otorga acceso de red ubicuo, conveniente y on-demand a un pool de recursos computacionales configurables compartidos. (Ejemplo: redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente asignados y liberados, fácilmente administrables y de baja interacción con el proveedor del servicio".

A partir de esta definición se desprenden algunas de las principales características de la tecnología Cloud: posee capacidad elástica para asignar recursos, entrega acceso a hardware, software o ambos, es remota, y fácil de configurar (no requiere de conocimientos técnicos avanzados para su uso).

También esta definición levanta interrogantes, tales como: ¿dónde están almacenados físicamente los datos?, ¿quién tiene acceso a estos datos?, ¿bajo qué nivel de seguridad estos datos están resguardados?, En caso de catástrofe ¿qué nivel de resguardo tiene la información en caso de pérdida?

Son estas interrogantes las que en muchas ocasiones limitan a posibles clientes de aprovechar los beneficios de esta tecnología. Bajo esta idea nace la motivación para el desarrollo de esta memoria. Específicamente, tomando el caso de las instituciones públicas en Chile, en donde más que interrogantes, son necesidades que requieren ser cubiertas por el modelo, por lo cual la decisión de implementar tecnologías Cloud para estas instituciones es de extremo cuidado. En esta memoria se busca guiar a instituciones públicas en la toma de decisión sobre la implementación de modelos Cloud en base a los criterios de mayor impacto en relación al sector público y el tipo de información que estos manejan.

1.2. Definición del problema

La gestión de datos y las necesidades con respecto a estos son aspectos considerablemente diferentes entre las múltiples organizaciones que caen en la categoría de instituciones públicas, algunas de estas instituciones necesitan mayor capacidad de procesamiento en fechas específicas del año (servicio electoral, DEMRE). Otras requieren capacidad de almacenamiento para datos históricos (municipios, hospitales). Otras buscan mantener un despliegue de información pública, estable y asequible para miles de personas (SII, servicio de registro civil) y otras necesitan confidencialidad en su información (Instituto de salud pública, policía de investigaciones). En muchos casos, varias de las características mencionadas son requeridas por tan solo una institución. A pesar de estas necesidades, muchas veces predecibles y claras, muchas de estas instituciones carecen de la tecnología para cubrirlas, ya sea por falta de experiencia en los departamentos de TI, baja inversión en TI, bajos

presupuestos en TI, o simplemente falta de información sobre la situación actual o posibles soluciones. Estas falencias pueden derivar en una mala performance de sus sistemas, lo que implica un mal funcionamiento de sus servicios. Dado a la cantidad de variables que las instituciones manejan, cada una necesita tomar sus propias decisiones con respecto a infraestructura, buscando cubrir sus necesidades específicas. Tomando en cuenta las necesidades expresadas, las tecnologías Cloud y sus servicios asociados nacen como una solución a varias de las problemáticas expuestas. Elasticidad, infraestructura, capacidad de almacenamiento para grandes volúmenes de datos, disponibilidad, son algunas de las múltiples características que las tecnologías Cloud tienen para ofrecer, de las cuales múltiples instituciones públicas podrían beneficiarse.

Al parecer la solución a la problemática es evidente, por lo cual nace la pregunta: ¿por qué las tecnologías Cloud no son predominantes o tendencia entre las instituciones públicas? El problema va más allá, incluso cuando alguna institución tiene noción de la existencia de la tecnología, nacen problemáticas como ¿Cómo puedo contratar este servicio?, ¿Estos servicios ayudarán a mejorar mi situación actual?, de ser así, ¿Qué servicios Cloud son adecuados para mi institución? Y ¿Qué proveedor contratar?, ¿Qué aspectos legales deben ser cubiertos para la utilización de esta tecnología? Tomando en cuenta el conocimiento de la tecnología, la problemática se transforma en si adoptar o no tecnologías Cloud en sus instituciones y de ser así, cual es el escenario más conveniente para realizarlo.

1.3. Objetivos

1.3.1. Objetivos Generales

Generar una guía metodológica para el uso de tecnologías Cloud por instituciones Públicas chilenas. Entregar un documento que facilite la toma de

decisión para implementar modelos Cloud acorde a las necesidades específicas de la institución en cuestión, tomando en cuenta los diferentes servicios y arquitecturas que las tecnologías Cloud ofrecen, además de las diferentes opciones disponibles en el mercado, utilizables por instituciones públicas.

1.3.2. Objetivos Específicos

- Identificar los principales aspectos de la tecnología Cloud que conciernen a las instituciones públicas, requerimientos y necesidades que buscan ser cubiertas.
- Analizar los aspectos identificados y agruparlos en puntos secuenciales que aborden la lógica del proceso de implementación Cloud.
- Estructurar y desarrollar los puntos identificados para generar un documento de apoyo para los encargados de evaluar y/o implementar tecnologías Cloud en las instituciones públicas.
- Validar el desarrollo de los puntos consolidados con expertos en temática.

1.3.3. Solución

La solución a esta problemática es la realización de una guía metodológica para el uso de Cloud Computing, enfocada específicamente en las instituciones públicas chilenas. El objetivo de esta guía es facilitar la toma de decisión con respecto a la implementación de esta tecnología para las instituciones públicas chilenas, entregando la información necesaria que compete a estas con respecto a la tecnología. Además de guiar a la institución en el proceso de selección de servicios y proveedores acorde a las distintas necesidades, buscando cubrir las singularidades que implique la implementación de la tecnología.

Para cumplir con su cometido, la guía metódica incluye tópicos que buscan facilitar la contratación de tecnología Cloud. Estos tópicos son nutridos a partir de una investigación y entrevistas a expertos relacionados con la temática. Además de la guía en sí, el documento general proporciona información necesaria para un mayor entendimiento de la tecnología en cuestión, ventajas generales e investigación con respecto a la temática Cloud en instituciones públicas.

1.4. Metodología

Para el desarrollo de una guía metodológica para el uso de tecnologías Cloud, se hace necesario entregar claras definiciones y explicaciones acerca de la temática en discusión. Se tiene en consideración que no todo lector tendrá el conocimiento necesario para hacer uso de la guía, por lo cual se contextualizará en el presente documento para un mayor entendimiento de la guía en sí. El desarrollo mismo de la guía se sustenta en investigación sobre la situación actual chilena con respecto a instituciones públicas y el uso de tecnologías Cloud, además de investigación con respecto a la relación institución pública y Cloud Computing.

Por otro lado, entrevistas a personas involucradas en la temática serán desarrolladas en función de identificar las principales necesidades y requerimientos que las instituciones públicas chilenas debiesen tener en consideración al momento de evaluar y/o implementar servicios Cloud, para así poder guiar a los usuarios en los aspectos más complejos o desconocidos con respecto a la tecnología. A posterior, un análisis de información será realizado y utilizado para la construcción de la guía tomando en cuenta los aspectos críticos canalizados y relacionándolos a la situación actual que las tecnologías Cloud tienen para ofrecer a las instituciones públicas chilenas. Cabe destacar que el foco de la entrevistas serán los encargados de TI de

múltiples y diversas instituciones públicas chilenas y proveedores de tecnología Cloud.

Los siguientes capítulos se pueden estructurar en 2 partes. El capítulo 2 y 3 sirven de introducción a la temática en cuestión. En particular, el capítulo 2 abarca el estado del arte o principalmente temáticas contemporáneas a la tecnología Cloud y el impacto en gobiernos de diferentes países. En el capítulo 3 se presentan aclaraciones con respecto a la tecnología Cloud.

La siguiente mitad de este trabajo se enfoca en la guía en cuestión. El capítulo 4 contiene los fundamentos en los cuales la guía se construye para luego dar paso a la guía en cuestión (capítulo 5). Para finalizar, el capítulo 6 establece conclusiones con respecto al trabajo.

2. Capítulo 2: Estado del arte

¿Qué es la nube?

Reutilizamos la definición otorgada por el NIST (National Institute of Standards and Technology, 2011) *"Cloud Computing es un modelo que otorga acceso de red ubicuo, conveniente y on-demand a un pool de recursos computacionales configurables compartidos. (Ejemplo: redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente asignados y liberados, fácilmente administrables y de baja interacción con el proveedor del servicio."*. Dado que el tema es amplio, corresponde abordarlo con respecto a sus diferentes categorizaciones. Una manera de categorizar a la nube es con respecto al tipo de infraestructura y servicios que estas ofrecen. A continuación se profundiza en cada uno de los aspectos importantes.

2.1. Infraestructuras Cloud

2.1.1. Nube Pública

La nube pública, como su nombre lo indica, posee infraestructura y recursos que son de carácter público, disponibles de manera general a través de internet. Las nubes públicas pertenecen a un proveedor o host que se encarga de operar la infraestructura y servicios que esta provee. La característica principal de esta infraestructura es que los recursos ofrecidos a los clientes son compartidos entre todos, es decir, los recursos provistos por la infraestructura se comparten entre todos los clientes. Este modelo trae múltiples beneficios y también desventajas, establecidas en la tabla 2.1.

Tabla 2.1: Ventajas y desventajas de Nube Pública.

Ventajas	Desventajas
Ahorro en costos dado a las economías de escala y modelo pay as you go (se paga lo que se usa).	Infraestructura compartida entre múltiples usuarios.
Alta escalabilidad. Típicamente de mayor escala que in-house Cloud, lo que implica mayor escalabilidad on-demand.	Más vulnerables que una nube privada.
Eficiencia en recursos compartidos.	Seguridad depende del proveedor.

2.1.2. Nube Privada

Una nube privada es una infraestructura dedicada específicamente a la organización que la solicita. Pueden ser administradas de manera interna o por terceros, y puede ser alojada interna o externamente. Cabe destacar que la infraestructura de una nube privada es creada con los propios recursos del organismo que la solicita. Las ventajas y desventajas del uso de nube privada se encuentran en la tabla 2.2.

Tabla 2.2: Ventajas y desventajas de Nube Privada.

Ventajas	Desventajas
Más segura que una nube pública.	Escalabilidad limitada por la infraestructura adquirida.
Mayor control que nube pública.	Mayor costo que una nube pública.
No se comparten los recursos con terceros.	

2.1.3. Nube Híbrida

Las nubes híbridas son una combinación de los modelos mencionados, manteniéndolos como entidades únicas pero trabajando juntas para obtener el mayor provecho de ambas estructuras. Con la combinación de ambas estructuras se puede mantener alta seguridad de una nube privada y al mismo tiempo aprovechar la escalabilidad y recursos on-demand de una nube pública, para momentos de sobrecarga.

2.1.4. Nube Comunitaria

Una nube comunitaria ocurre cuando 2 o más organizaciones forman una infraestructura Cloud compartida entre ellos y con objetivos similares. Esta infraestructura es construida específicamente para este grupo, pudiendo ser administrada por el grupo en cuestión o un tercero. La arquitectura de una nube comunitaria puede ser privada tanto como híbrida.

En la Tabla 2.1 (Gsoedl, 2011) se establece una comparación entre las diferentes arquitecturas mencionadas.

Tabla 2.3: Comparación entre arquitecturas Cloud.

Publica vs Privada Vs Híbrida			
Características	**Publica**	**Privada**	**Híbrida**
Escalabilidad	Alta	Limitada	Alta
Seguridad	Buena, pero depende del proveedor Cloud	La más segura	Muy segura: opciones de integración agregan una capa de seguridad adicional
Performance	Baja a media	Muy Buena	Buena
Confiabilidad	Media, depende de la conectividad a internet y la disponibilidad del proveedor	Alta, dado que todo el equipo es on premise (infraestructura local)	Media a alta. Cache es almacenado on premise pero también sigue dependiendo de la conectividad y de la disponibilidad del proveedor
Costo	Muy Bueno. Modelo pay-as-you-go, sin necesidad de infraestructura local.	Bueno pero necesita infraestructura local, espacio para datacenter, electricidad, etc.	Mejorada, dado que permite utilizar recursos del modeo pay-as-you-go

2.2. Servicios Cloud

Los servicios Cloud son servicios disponibles para usuarios a través de la internet entregados por proveedores Cloud. Estos se clasifican en servicios de infraestructura, de software y de plataformas. A continuación se profundiza en cada uno de ellos.

2.2.1. Software como servicio (SaaS)

Este modelo SaaS (del inglés Software as a Service) es una forma de distribuir software que permite al cliente la utilización de este a través de internet, sujeta a una mensualidad y bajo demanda, permitiendo reemplazar aplicaciones tradicionalmente instaladas en infraestructura propia. Se accede a este servicio a través de un proveedor el cual se ocupa del hospedaje, mantención y seguridad de la aplicación.

Este modelo ofrece a los clientes múltiples beneficios, tales como: reducción de costos en hardware y software (pago por uso), conectividad en cualquier momento y lugar (mediante conexión internet), todo el soporte, actualizaciones y mejoras están controladas por el proveedor.

Cabe destacar que el usuario posee un acceso limitado a configuraciones del software, las aplicaciones ofrecidas mediante este modelo están altamente estandarizadas.

2.2.2. Plataforma como servicio (PaaS)

Este modelo PaaS (del inglés Plataforma as a Service) el proveedor entrega una plataforma con herramientas de hardware y software, permitiendo a los clientes desarrollar, correr y mantener aplicaciones, liberando a los clientes de necesidades de infraestructura, software y hardware. Generalmente este servicio es utilizado por desarrolladores de software.

El cliente tiene un control parcial sobre las configuraciones del entorno y las mismas aplicaciones, ya que la infraestructura y recursos aun dependen del proveedor que las despliega. Desde el punto de vista de la seguridad, esta es compartida entre el proveedor y el cliente, ya que las aplicaciones desarrolladas o “hosteadas” en la plataforma corren por parte del cliente.

2.2.3. Infraestructura como servicio (IaaS)

Este modelo IaaS (del inglés Infrastructure as a Service) el proveedor proporciona al cliente infraestructura computacional (servidores, equipamiento de red) como un servicio, el cual es accesible y configurable mediante una interfaz web. Este servicio entrega al cliente la libertad de poder realizar cualquier acción que se pudiese llevar a cabo en una infraestructura propia, tener servicios corriendo, desarrollo de aplicaciones, hosting, almacenamiento de datos, todo esto sin la necesidad de preocuparse por la gestión de los servidores físicos. La finalidad de este servicio es evitar la compra de infraestructura por parte de los clientes, buscando reducir costos de equipos, mantención y personal de TI, dado que todo esto es proporcionado por la empresa proveedora.

A diferencia de tener infraestructura física in-house, IaaS proporciona recursos on-demand, permitiendo a la infraestructura escalar de ser necesario sin la necesidad de realizar complejos procedimientos.

Otra característica que destaca este modelo es el alto alcance de replicación y disponibilidad del servicio. Dependiendo del proveedor y del SLA (Service Level Agreement) correspondiente, los servicios IaaS pueden garantizar una altísima disponibilidad gracias a la capacidad para suplir puntos de fallo, en específico, la capacidad de “Uptime” o disponibilidad depende de la clasificación de los Datacenters de los proveedores (Tier I,II,III y IV, ver sección 3.3). Muchos proveedores poseen replicaciones en múltiples continentes,

manteniendo la integridad de datos incluso en situaciones catastróficas que afecten algún datacenter en particular.

2.4. Servicios Cloud V/S servidores “in house”

Una de las principales interrogantes a la hora de implementar una infraestructura o servidor para el almacenamiento de datos en una organización/empresa es si implementar una infraestructura “in house” conocida como tradicional, o adoptar una opción Cloud. En el modelo tradicional, el cliente es el dueño de la infraestructura, es el encargado de comprar y mantener toda la infraestructura necesaria para el funcionamiento de esta. En el modelo Cloud, el usuario posee una interfaz donde hace manejo de los recursos y algunas configuraciones de su infraestructura, la cual se encuentra mantenida por un proveedor que es dueño de esta. La cuestión no es que modelo es superior al otro, sino que modelo es el que se adapta de mejor manera a los requerimientos y necesidades.

2.4.1. Pros y contras

Cada una de las alternativas presenta diferentes ventajas con respecto a la otra. Lógicamente, una implementación de tipo tradicional permite un mayor control de la infraestructura. Por otro lado, proveedores Cloud de alta categoría pueden garantizar una disponibilidad difícilmente alcanzable por un modelo in-house. Como esta, existen múltiples diferencias que hacen particulares a ambas implementaciones, y que dependiendo de lo que se requiera, ambas opciones pueden ser una buena opción para el cliente. En la tabla 2.3 se establecen los pros y contra de la tecnología Cloud y en la tabla 2.4 se establecen los pros y contra de una implementación de infraestructura tradicional.

Tabla 2.4: Pros y Contras de tecnología Cloud.

Cloud Computing	
Pros	**Contras**
Accesibilidad remota mediante internet	Al ser el internet el único canal de acceso a los servicios Cloud, sin internet no hay accesibilidad al servidor Cloud.
Alta capacidad de recuperación de datos en caso de catástrofes.	Costos de mensualidades constantes y permanentes.
Provee un ambiente de fácil cooperación entre usuarios.	La seguridad corre completamente por parte del proveedor. No es posible realizar cambios o implementar protocolos de seguridad sobre esta infraestructura.
Soluciones Cloud reducen huella de carbono y uso de energía en un 30% (Accenture, 2010).	Terceros poseen acceso a la información almacenada.
Posee una interfaz que permite al cliente asignar recursos fácilmente.	

Tabla 2.5: Pros y Contras de TI Tradicional.

TI Tradicional	
Pros	**Contras**
Completo control y propiedad sobre la infraestructura.	Altos costos en relación al hardware/software. Altos costos operacionales y de mantención.
Acceso limitado a terceros.	Mayor complejidad y costos asociados a cambio/upgrade de recursos.
Control sobre la seguridad y sus protocolos.	En caso de incorrecta estimación de recursos, la infraestructura puede tener recursos de sobra o limitados que perjudiquen la operatividad del sistema.
No depende de conectividad de internet para su operatividad.	Si no cuenta con protocolos de respaldo o alguna solución híbrida para la redundancia de datos, puede ser un trabajo difícil o imposible recuperar datos en caso de catástrofe.

2.4.2. Costos

Uno de los factores de mayor importancia a la hora de tomar la decisión de implementar una infraestructura interna de almacenamiento o un servicio Cloud, son los costos asociados a estas alternativas. Usualmente se escucha hablar de los bajos costos de los servicios Cloud en comparación a alternativas in-house, pero ¿Es en todos los casos más rentable implementar soluciones Cloud?

La situación es la siguiente, por un lado se encuentran las soluciones Cloud, que comúnmente ofrecen sus servicios bajo una mensualidad. Existe una amplia gama de proveedores Clouds con diferentes estándares de desempeño, lo que implica una cartera de precios diferentes disponibles para los clientes. Por otro lado, se encuentran las opciones “in-house” o servidores propios, lo que implica una adquisición de parte del cliente de toda la implementación necesaria para poder hacer funcionar un datacenter, desde la infraestructura hasta todos los costos asociados con el funcionamiento del mismo.

En general, los costos asociados a estos servicios se pueden categorizar en 3 tipos: costos de hardware/software, costos de implementación, costos de operación y mantención. A partir de estos costos se calcula el costo total asociado a cualquiera de las alternativas en cuestión. Factores como el tamaño/magnitud del cliente y la proyección del servicio, son parámetros a tomar en consideración en la posible variación de costos entre ambas soluciones. A continuación se presentan los costos asociados a cada una de las alternativas.

- **Costos asociados a solución tradicional “in-house”**

Con el enfoque tradicional o “in-house” de servidores el usuario debe costear por completo el datacenter a utilizar, además de todos los costos asociados al funcionamiento del mismo. Estos costos pueden ser dividos en tres categorías:

Hardware/software: corresponde a todo el hardware necesario para establecer la infraestructura más el software necesario para su funcionamiento. (Eje: servidores, rack, cables, switches, etc.)

Implementación: Corresponde a todos los costos asociados con la implementación del infraestructura, ya sea traslado, mano de obra, configuración de hardware y software, etc. Cabe destacar que en general, una infraestructura necesita un espacio físico en donde localizarse, por lo cual esto debe estar definido y listo previamente a la implementación de la infraestructura.

Mantención: Corresponden a todos los costos asociados con la mantención física y operacional de la infraestructura. Dentro de estos costos podemos encontrar los costos de personal asociado al mantenimiento y operatividad, costos de renovación y mejora de equipos de la infraestructura, electricidad. Cabe destacar que es necesario considerar los posibles costos asociados a reparación o compra de nuevos equipos en caso de fallas u obsolescencia dado a antigüedad del mismo.

Cabe destacar que estos costos están siempre involucrados en el establecimiento de una infraestructura interna.

- **Costos asociados a solución Cloud**

Uno de los principales atractivos de la tecnología Cloud son los costos asociados a esta. Se habla mucho de la reducción de costos al implementar soluciones Cloud, pero ¿Es en todos los casos más rentable implementar soluciones Cloud? Esta interrogante varía dependiendo del tipo de organización que desea acceder al servicio, además de los requerimientos por parte de la misma.

Como fue mencionado anteriormente, los costos asociados a soluciones Cloud corresponden a una mensualidad al cliente por el servicio solicitado. Cabe destacar que no todos los costos asociados a la infraestructura in-house son cobrados directamente al cliente en servicios Cloud. Por ejemplo, en una implementación Cloud no existen costos asociados a la compra de hardware/software, ni costos asociados a la mantención y operatividad del sistema. Todos estos costos se ven cubiertos por el proveedor, mediante las economías de escala aplicada a los recursos que estos manejan, por lo cual los costos pasan de manera abstracta al cliente mediante una mensualidad. Esta situación es práctica para el cliente ya que no es necesario preocuparse por los aspectos involucrados en una solución tradicional, todos son suplidos por el proveedor Cloud. En muchos casos, se realiza un cobro de implementación, asociado al software a utilizar por el cliente para administrar el servicio y las posibles configuraciones relacionadas a servidor. También en términos de implementación, se puede incurrir en costos asociados a la capacitación de personal, costos que pueden variar dependiendo del número de capacitaciones necesarias.

En algunos casos, estas mensualidades asociadas a la operatividad del sistema pueden ser altamente costosas, y que proyectadas en cierto tiempo, no sean costo efectivas en comparación a una situación tradicional. Por otro lado, estos costos son muchas veces asumidos por organizaciones/empresas que necesitan una presencia internacional de alta disponibilidad y replicación.

Los costos asociados a una contratación Cloud pueden ser tanto más altos, como más bajos que una implementación de tipo tradicional. Son múltiples los factores que afectan en los costos relacionados al servicio. El tamaño/envergadura de la empresa/organización cliente es uno de los factores más importantes al analizar el costo entre ambas situaciones. Es muy común que empresas de gran envergadura (empresas de presencia internacional)

construyan su propia infraestructura para el manejo de datos, también es común que estas empresas implementen soluciones Cloud o híbridas dado los altos requerimientos en disponibilidad. Por otro lado, es poco frecuente que empresas de pequeña envergadura puedan acceder a infraestructuras de buen nivel dado los costos asociados a esta.

Otro factor significativo a la hora de realizar una comparación de costos entre ambas situaciones es la longevidad del periodo de comparación de los servicios. En el caso tradicional, es necesario tener en cuenta la renovación de infraestructura en caso de obsolescencia y en caso de fallas, en cambio en la situación Cloud la tarifa es el único costo involucrado. Por otro lado, al pasar el tiempo la inversión en términos de infraestructura puede ser cubierta en caso el caso tradicional, en cambio la mensualidad siempre será requerida para la mantención del servicio.

A pesar de los diferentes factores que puedan inferir en la variación de costos entre las dos alternativas, la pregunta se mantiene, ¿Qué alternativa es más rentable? Con la intensión de aterrizar esta incógnita el grupo Leviathan Security Group (Leviathan Security Group, 2015) realiza un análisis de costos entre 3 años de infraestructura propia para el almacenamiento de información v/s 3 años utilizando servicios de almacenamiento Cloud. Cabe destacar que los costos considerados en este análisis no son la totalidad involucrada a futuro. Se obvia los costos relacionados al remplazo completo de infraestructura por renovación. Es evidente que en algún momento dado, será necesario remplazar en gran parte o quizás en su totalidad la infraestructura, debido a la imposibilidad de mantener sistemas antiguos. Por otro lado, se obvia los pronósticos de decrecimiento de costos en servicios Cloud. Dado los grandes avances en la tecnología Cloud, es posible evidenciar el descenso de costos que estos servicios han experimentado con la evolución de la tecnología.

Para el cálculo de costos, se utilizaron precios referenciales de mercado para la infraestructura como para los proveedores Cloud. Se realiza la comparación de las 2 opciones para 3 escenarios diferentes: pequeña, mediana y gran empresa/organización. Para el cálculo completo del costo se tomaron en cuenta los costos de hardware y software, costos de implementación y costos operacionales.

Los resultados del estudio arrojan que bajo ninguno de los escenarios presentados es más económico utilizar servicios Cloud. En términos de Hardware y software, siempre es más económico la utilización Cloud. En relación a los costos de implementación, también es más económico realizar una implementación Cloud. Por otro lado, en los costos de operación el estudio arroja que es más costoso la utilización Cloud. Cabe destacar que este estudio no considera el costo en mano de obra en los costos operacionales, solo toma en consideración los costos de mantención de equipos (ver resumen completo en estudio Leviathan), por lo cual claramente el servicio Cloud se escapa en costos operacionales, dado que considera la mensualidad a pagar en los costos operacionales. A pesar de este detalle, el estudio entrega una buena aproximación sobre los aspectos relevantes a tener en consideración al realizar una comparación de costos.

2.5. Cloud Computing e instituciones públicas alrededor del mundo

A través del mundo, son múltiples los países que han sabido identificar el potencial que las tecnologías Cloud poseen y los múltiples beneficios que este modelo ofrece para el sector público y privado. En esta sección se aborda algunas situaciones que ameritan mención con respecto a la relación sector público, servicio Cloud.

2.5.1. Cloud Computing e IP en Europa

En septiembre del 2012, la comisión Europea lanzó un programa estrategias para el fomento de Cloud Computing denominado “Unleashing the Potential of Cloud Computing in Europe” (European Comssion, 2012) con el fin de promover tanto en el ámbito público como privado, la utilización de servicios Cloud. La comunidad europea ve el impacto del uso de Cloud Computing sustancial en materias económicas tanto como sociales, permitiendo una mayor conectividad y eficiencia social. La estrategia nace del resultado de múltiples análisis en función de identificar maneras de maximizar el potencial que la nube ofrece, ya sea en materia económica como práctica/funcional para instituciones.

Este documento, entre otras cosas, busca facilitar el uso de Cloud Computing para instituciones públicas y privadas mediante estandarizaciones en los servicios Cloud para garantizar a los usuarios interoperabilidad, portabilidad de data y reversibilidad. Por otro lado, el documento busca entregar un set de regulaciones unificado para toda la comunidad europea, con el objetivo de acelerar el uso de Cloud Computing, entregando un contrato modelo que regula las preocupaciones especificas con respecto al Cloud Computing que no se encuentran cubiertas por las leyes comunes europeas.

La Asociación Cloud Europea (ECP), es otro punto clave de la estrategia Cloud, donde se establece un mercado digital de herramientas Cloud para Europa. Nube confiable Europa es un documento formulado por ECP con el fin de promover ideas que ayuden a instituciones europeas a comprar y vender servicios Cloud en un ambiente seguro y confiable (European Comission, 2014).

Existe otra institución financiada por la Comisión Europea denominada “Cloud For Europe”, comunidad que se enfoca principalmente en entregar una visión

clara en los requerimientos de instituciones públicas para el uso de tecnologías Cloud. Basándose en los principios de ECP y la estrategia Cloud Europea, “Cloud for Europe” tiene como objetivos: Identificar obstáculos para el uso del Cloud Computing en el sector público, definir servicios que superen estos obstáculos y realizar investigación en favor de la innovación Cloud.

Por otro lado, no solo la Comisión Europea ha Estado fomentando el uso de tecnologías Cloud, la gran mayoría de países de la comunidad Europea se han sumado a esta iniciativa, buscando obtener ventajas económicas y mejorar su eficiencia en instituciones. A continuación se presentan algunos casos específicos de diversos países, ya sea en materia de estudios o programas de fomento.

- **Cloud Computing en España**

El instituto nacional de tecnologías de la comunicación (INTECO) actual instituto nacional de ciberseguridad (INCIBE), realizó un estudio (noviembre-diciembre 2011) sobre el uso de Cloud Computing en el sector público español (INTECO , 2011). Los principales objetivos de este estudio fueron conocer el posicionamiento y percepción de las entidades públicas españolas respecto al Cloud Computing en términos de: conocimiento y uso, modelo de decisión sobre la adopción, resultado de implantación e intención de uso futuro.

La metodología del estudio se basa en un análisis documental sobre estudios nacionales e internacionales con respecto al Estado de tecnologías Cloud con respecto a instituciones públicas. Además de encuestas a 500 responsables de TI en entidades del sector público, local, autonómico o estatal.

A partir de este estudio, INTECO obtuvo algunas de las siguientes conclusiones.

- La extensión del Cloud Computing entre las entidades del sector público español es todavía limitada, y es más frecuente entre administraciones locales que entre organismos de ámbito autonómico o estatal.
- En cualquier caso, el modelo de despliegue más habitual es el privado.
- La búsqueda de ahorro, eficiencia y sencillez, son las motivaciones que empujan a las administraciones a contratar servicios Cloud Computing.

- **Francia**

El año 2011, Francia comenzó su primer intento por desarrollar una G-Cloud (nube gubernamental) denominada “Andromeda”, plataforma Cloud de IaaS para instituciones gubernamentales, apuntando a entregar servicios Cloud acordes con la legislatura Francesa con respecto al manejo de datos. En otras palabras, una nube especialmente diseñada para cumplir con todas las leyes con respecto a datos y la seguridad de estos. Lamentablemente esta plataforma no se llevó a cabo. El año 2012 el directorio legal y administrativo de información (DILA) otorgo un contrato por 3 años para la empresa ACCENTURE para diseñar y construir lo que sería la primera G-Cloud en Francia.

- **Reino Unido**

El Reino Unido actualmente tiene un mercado digital (Digital Market Place) para encontrar trabajadores y tecnologías para proyectos del sector público, en donde distintos proveedores de Cloud Computing promueven sus servicios bajo el marco o framework llamado G-Cloud, el cual es un acuerdo entre el gobierno y proveedores que mantiene todas las normativas necesarias para el uso de Cloud Computing por parte de IP en el Reino Unido. Actualmente se utilizan los marcos G-Cloud 6 y 5, y se está trabajando en el nuevo G-Cloud 7 (Digital Market Place, 2015).

El mercado digital ofrece alrededor de 19,000 servicios Cloud divididos en las categorías IaaS, PaaS, SaaS y SCS. Servicios como Amazon Web Service

(AWS) pueden ser encontrados en esta lista de proveedores. El mercado proporciona una guía para compradores con todo lo necesario para poder contratar alguno de estos servicios. Además, el mercado provee de estadísticas con respecto a las ventas, gastos, etc.
El año 2013 la empresa ORACLE se une al proyecto G-Cloud instalando su primer datacenter dedicado para uso gubernamental.

2.5.2 Cloud Computing y el gobierno federal en EE.UU

Como nación, los Estados Unidos poseen los principales proveedores a nivel mundial de servicios Cloud, además de ser una de las naciones con mayor aporte a la comunidad tecnológica/informática a nivel mundial. A pesar de esto, la inclusión de tecnologías Cloud en el sector público ha sido dilatada en comparación a la comunidad europea. El primer intento por parte del gobierno federal para la inclusión de tecnologías Cloud fue denominado “Cloud first” o “Federal Cloud Computing Strategies”, en donde se promulgaba el uso de tecnologías Cloud para nuevos proyectos de las agencias federales. Hasta hoy en día, las agencias federales se encuentran “tímidas” con respecto al uso de tecnologías Cloud.

Actualmente el gobierno de EE.UU ha certificado ciertos proveedores de servicios Cloud bajo Fedramp, donde se asegura que la documentación de proveedores Cloud cumple con los requisitos y estándares mínimos para instituciones públicas. Además posee un Marketplace donde se encuentran todos los proveedores aprobados.

A finales del año 2014 la empresa Meritalk (government IT network) realizó un reporte (Cloud Tech, 2015) sobre el uso de Cloud Computing en agencias federales. Se estableció que las agencias federales están tomando en cuenta el concepto de Cloud pero resisten a migrar todos sus recursos IT a la

tecnología. Actualmente 1 de cada 5 agencias (de las 150 entrevistadas por Meritalk) entrega sus servicios a través de la nube. Los servicios más comunes a migrar son: email, seguido de web-hosting y luego servidores y almacenamiento. Por otro lado, servicios financieros y de contabilidad fueron los menos migrados a la nube. La encuesta arrojó que muchas veces no es que las agencias no deseen migrar a la nube, sino que alrededor del 30% de la información que poseen es de carácter confidencial. Un quinto de los entrevistados asegura que ni siquiera entregarían su información confidencial a los proveedores autorizados por Fedramp.

Por otro lado, a pesar del revelador reporte realizado por Meritalk, agencias gubernamentales de gran envergadura han decidido optar por tecnologías Cloud, como es el caso de la CIA. Con el fin de lograr mayor interconectividad entre sus diferentes agencias, el año 2014 la CIA firmó un millonario contrato ($600 millones) con Amazon por la utilización de su servicio Amazon Web Services para cubrir las necesidades de 17 agencias internas. Otro caso es la creación de CalCloud, plataforma Cloud para todos los municipios, agencias estatales y gubernamentales en el Estado de California. A través de CalCloud el Estado de California provee IaaS permitiendo que las instituciones de california compartan una pool de recursos computacionales, almacenamiento, redes y servicios de recuperación ante desastres. Cabe destacar que la infraestructura y redes utilizadas son llevadas por IBM y AT&T respectivamente. La plataforma CalCloud cumple con los estándares Fedramp.

2.5.3. Cloud Computing contexto nacional

Tomando como ejemplo países con alto desarrollo tecnológico a nivel mundial, Chile ha logrado posicionarse como el país con mayor desarrollo tecnológico a nivel Sudamericano, y el desarrollo en la nube no ha sido la excepción.

Chile es un país, que actualmente ha sabido reconocer los beneficios que la tecnología Cloud potencialmente puede brindar al sector público. Tal es el alcance, que la UMGD (Unidad de Modernización y Gobierno Digital), iniciativa del Ministerio Secretaria General de la Presidencia, recomienda la adopción de soluciones Cloud al interior de los órganos de la administración del Estado como regla general. De la mano de Chilecompras (sistema de licitaciones estatales) y UMGD, Chile se convirtió en el primer país a nivel Sudamericano en ofrecer servicios Cloud a instituciones estatales a través de una tienda virtual. El objetivo del convenio marco Cloud y Datacenter es facilitar a organismos públicos la adquisición de servicios Cloud a través de una tienda virtual ubicada en el portal Mercadopublico, en donde los 850 organismos públicos tienen acceso a un listado de 42 proveedores previamente licitados, los cuales ofrecen tanto Cloud Computing como, Hosting, Housing, enlaces de datos e internet, y servicios complementarios de Data Center. Cabe destacar que todos los proveedores cumplen y siguen los reglamentos considerados como necesarios para poder ofrecer servicios Cloud a instituciones gubernamentales.

El Mercadopublico hace una descripción más detallada sobre las funcionalidades, servicios y etapas del convenio marco Cloud Computing: “El convenio marco de Servicios de Data Center y Asociados, ID 2239-17-LP11, congrega en esta primera etapa a 42 proveedores adjudicados, los cuales se encuentran diferenciados en dos categorías, el primero de Data Center y Servicios Complementarios y el segundo de Software como Servicio (SaaS), Plataforma como Servicio (PaaS) e Infraestructura como Servicio (IaaS)” (Mercado Público , 2015).

Entre los servicios disponibles para instituciones públicas dentro de este convenio marco para esta categoría SAAS (Software as a Service) se pueden encontrar por una parte soluciones integrales en la nube para administrar

contenidos y framework de sitios y productos para la web, y también soluciones para mantener repositorios institucionales con contenidos y documentación oficial.

Otros servicios contemplados en la categoría SaaA permitirán por ejemplo a las instituciones públicas la compra de servicios para administrar en la nube carteras de proyecto de la organización, la compra de servicios en la nube de correo electrónico de acuerdo a las necesidades y requerimientos institucionales como cantidad de usuarios y capacidad de almacenamiento, etc.

Al tratarse de servicios de alta disponibilidad y recambio en el mercado, este convenio marco, que tendrá una duración de 72 meses, permite realizar nuevos llamados permitiendo la incorporación de nuevos proveedores a contar del sexto mes de vigencia.
Por último, este convenio marco cuenta con una amplia gama de servicios complementarios para administrar, gestionar, instalar, configurar, respaldar, migrar, infraestructura de Data Center y Cloud Computing, además de la posibilidad de contratar servicios PMO."

Cabe destacar que la tienda Cloud posee un asistente en línea, en donde se responden a interrogantes como: Leyes relacionadas a la contratación del servicio, particularidades presentes en Cloud Computing y IP, definiciones propias de la tecnología y sus derivados, contrato SLA.

El convenio marco de Cloud Computing se encuentra vigente desde febrero del presente año, por lo cual es temprano para poder establecer resultados concretos pero para Claudio Loyola Loyola (jefe de la división tecnología y negocios de Chilecompra), "el resultado principal es validar que hoy en día existe una posibilidad real para las agencias públicas de moverse a la nube"

(Datacenter Dynamics, 2015). Además indicó que “Ése es el principal resultado en estos seis meses de trabajo, más allá de que se hayan ejecutado muchos procesos”. En el mismo documento Rodrigo Fernández, gerente comercial de Grupo GTD indica “se está entrando en un ciclo de mayor madurez de este tipo de soluciones, donde las empresas públicas y financieras están viendo con mayor naturalidad alojar sus servicios en la nube”.

2.6. Licitaciones actuales

Cabe destacar que a pesar de la existencia del convenio marco Cloud Computing and Datacenter, instituciones públicas siguen recurriendo a licitaciones en el Mercadopublico para suplir sus necesidades Cloud. En concreto, desde la puesta en marcha del marco Cloud, la corporación administrativa del Poder Judicial y el Metro S.A han licitado servicios Cloud.

Tomando la licitación del Metro (Empresa de transporte de pasajeros Metro SA, 2015) como ejemplo, la licitación constituye básicamente la estructura solicitada por Chilecompra, donde se sigue el siguiente esquema.

Contenido de las bases

1. Características de la licitación
2. Organismo demandante
3. Etapas y plazos
4. Antecedentes para incluir en la oferta
5. Requisitos para contratar al proveedor adjudicado
6. Criterios de evaluación
7. Montos y duración del contrato
8. Garantías requeridas
9. Requerimientos técnicos y otras cláusulas

Con lo que compete con la temática Cloud, se establecen los requerimientos técnicos y condiciones de cotización en la etapa 4 de la licitación.

Dentro de las condiciones de cotización se establece que las instituciones y/o empresas que pueden participar de dicha licitación, deben cumplir con las condiciones estipuladas en la misma. Se establece la forma de ofertar, participando a través del Mercadopublico e ingresando una OFERTA TECNICA rellenando los formularios adjuntos dentro de la licitación. A posterior, una OFERTA ECONOMICA es solicitada llenando un formulario de oferta económica adjunto en la licitación. Cabe destacar los artículos 16, 17, 18 y 19, artículos ligados al tipo de servicio solicitado. Se estipula la confidencialidad solicitada, aludiendo al no uso de información a la que tenga acceso el proveedor. Cualquier tipo de divulgación de información se considera un incumplimiento grave a este artículo, por lo cual acciones judiciales serán tomadas. Se establecen las normativas con respecto a la propiedad intelectual del producto, estableciendo que cualquier tipo de propiedad industrial o intelectual que se derive de la realización del servicio son propiedad exclusiva del Metro S.A, prohibiendo cualquier uso de estas propiedades al oferente. El artículo 19 establece la no-exclusividad del contrato, explicitando que la celebración del contrato no entrega exclusividad al proveedor, permitiendo a Metro S.A la posibilidad de celebrar un contrato similar con otro tercero.

Con respecto a las especificaciones técnicas, “Metro S.A requiere la adquisición de servicio de respaldo en la nube para 90 usuarios, el cual permita el respaldo de información online con un volumen de 500 GB por usuario”. Otras particularidades de las especificaciones técnicas son las siguientes.

- Respaldos diarios.
- Duplicación de datos.
- Acceso remoto.

- Encriptación al transferir con nivel de 256bits o superior (no específica algoritmos ni tipo de encriptado).
- Almacenamiento de la información sea en territorio nacional y con un datacenter de categoría TIER II como mínimo.
- Soporte telefónico de lunes a viernes entre las 8:30AM y 19:00 durante la vigencia del servicio, con multas asociadas a no respuesta.

Se vuelve a tocar la temática de la confidencialidad, especificando que “La empresa deberá asegurar que los datos administrados no serán accesibles por terceros y se ejecutará un proceso de borrado seguro de la data almacenada una vez que finalicen los servicios contratados por Metro S.A., una vez adjudicado, el proponente deber proporcionar un certificado en el cual se establezca que la información respaldada es de absoluta confidencialidad y no podrá ser reproducida por ningún medio ni en ningún formato por el Proponente”.

3. Capítulo 3: Aspectos relevantes a considerar al contratar un servicio Cloud

Para todo cliente que desea acceder a un servicio Cloud, existen ciertas consideraciones que el cliente debe tener previo a la elección y contratación de un proveedor para sus servicios. Estas son de carácter global para todo tipo de cliente, pero en el caso de las instituciones públicas, estas singularidades se ven esquematizadas en base a legalidades y políticas generales que las instituciones públicas deben cumplir dado su estatus de públicas, además de sus políticas internas. Es por esto que se hace necesario, además de entender las consideraciones correspondientes, y a posterior contextualizarlas en base a las particularidades en las que estas se aplican para una institución pública. A continuación, aspectos relevantes a considerar en un servicio Cloud previamente a su contratación.

3.1. Tipo de Nube

El tipo de nube se relaciona directamente con el tipo de información que la institución pública desea almacenar en la nube. De ser información de carácter público, el uso de una **nube pública** no debiese ser inconveniente alguno para la institución, ya que esta información tiene la finalidad de ser expuesta, por lo cual, no es una preocupación posibles filtraciones de información o uso de la información por terceros.

Por otro lado, si la información a almacenar es de carácter privado o sensible, ya sea porque el contenido es relacionado a personas naturales o de carácter gubernamental, el almacenamiento en una nube pública puede ser un problema si es que esta nube no cumple con los requisitos necesarios para poder operar información de este tipo. Otro posible inconveniente con nubes públicas es las limitaciones técnicas que estas pudiesen llegar a tener con respecto a los requisitos necesarios que debe cumplir una institución pública

como tal (disponibilidad, redundancia). Cabe destacar que el uso de nubes públicas para instituciones públicas no se encuentra prohibido por ninguna legislación. Además que existen múltiples nubes públicas con altos estándares en relación a disponibilidad y seguridad de información.

Por otro lado, la utilización de una **nube privada** puede ser una buena opción con respecto a la seguridad, ya que la información no se encuentra en manos de terceros, ni se comparte infraestructura con otros clientes, sino que se la información se encuentra en una nube privada donde el acceso a los recursos de esta nube es particularmente para la institución en cuestión. Además, por ser una nube privada, el cliente posee completo control sobre la misma, permitiendo control sobre la seguridad y sus protocolos implementados. Por otro lado, la escalabilidad de recursos se relaciona a la capacidad de inversión que la institución posea. Para un óptimo funcionamiento de una nube privada, se requiere una inversión considerablemente mayor a la contratación de una nube pública. Las **nubes híbridas** ofrecen lo mejor de ambos mundos, permitiendo mezclar ambos tipos de nubes en búsqueda de una combinación que se acomode a las necesidades del cliente.

3.2. Tipo de servicios

Es primordial que la institución pública en cuestión tenga claridad de qué servicio Cloud desea. En términos generales, los servicios que tienen mayor relación a las actividades y/o necesidades de las instituciones públicas son los servicios de infraestructura y Software.

En términos de **software**, este servicio puede entregar una gran potencialidad y ahorro a instituciones públicas. Permitiendo a las Instituciones públicas ahorros en mantención, licencias, horas hombre de personal TI y tiempos de actualizaciones. Además de proveer una mayor accesibilidad e interconectividad para sus usuarios.

En términos de **infraestructura**, este servicio brinda altas capacidades de almacenamiento y procesamiento, características que actualmente muchas instituciones públicas en Chile no pueden costear de manera física, ya sea por la infraestructura en sí o por el personal de TI necesario para poder mantener estas estructuras. Además este servicio brinda la posibilidad de obtener recursos bajo demanda, lo cual puede ser beneficioso para instituciones públicas que posean un errático comportamiento en relación a la demanda de recursos, o por altas demandas en períodos claves del año, que no justifiquen una constante capacidad durante todo el año.

Por lo general, el servicio de plataformas tiene cavidad en las instituciones públicas cuando éstas desarrollan, corren y/o mantienen aplicaciones WEB.

3.3. Disponibilidad y clasificación Tier.

Un punto de evaluación significativo al momento de contratar un servicio Cloud, es la disponibilidad o **uptime** que el servicio posee. Para múltiples instituciones la disponibilidad de información es un requisito de alta prioridad, dado que el servicio que se necesita establecer lo demanda. Por otro lado, muchas instituciones necesitan una disponibilidad aceptable, ligada a un requisito menor de disponibilidad que permita satisfacer sus necesidades. Dado los diferentes escenarios posibles, es necesario establecer alguna convención o estandarización de los servicios en base a su disponibilidad.

El **Uptime** (bajo el contexto Cloud) se define como la cantidad de tiempo que el servicio Cloud provisto por el proveedor Cloud se encuentra accesible para el usuario/cliente. Por otro lado, el **Downtime** es el tiempo que el servicio Cloud se encuentra no disponible para el usuario/cliente.

A partir de estos conceptos, y con el esfuerzo de poder evaluar de una manera más efectiva la infraestructura de los datacenters en función de la disponibilidad que estos proveen, el Uptime Institute creó el sistema Tier Classification estándar (Uptime Institute, 1990) “El sistema Tier Classification ofrece a la industria de los centros de datos un método coherente para comparar las instalaciones personalizadas y normalmente únicas en función del rendimiento o el tiempo de productividad esperado de la infraestructura del sitio. Además, los Tiers les permiten a las compañías alinear las inversiones en la estructura de su centro de datos con los objetivos comerciales específicamente relacionados con las estrategias tecnológicas y de crecimiento”.

Los diferentes niveles de Tiers varían en los componentes de su infraestructura y como estos posibilitan un mejor desempeño, lo cual se relaciona directamente con el uptime que estos datacenters pueden garantizar a sus clientes. A continuación se abordan los diferentes tipos de Tiers.

- **Tier I Datacenter Básico:** Datancenters Tier 1 proveen un mejor ambiente en comparación a instalaciones de oficina. Incluyendo espacio dedicado para sistemas TI, fuente de poder continua mitigando cualquier tipo de corte momentáneo, equipos de enfriamiento dedicados previniendo sobrecalentamiento en horarios de trabajo, y un motor generador para mitigar los cortes de energía prolongados. Generalmente son empresas de pequeña/mediana envergadura las que pueden sacar el mejor provecho de estas instalaciones.

- **Tier II Componentes Redundantes**: A diferencia del Tier I, las infraestructuras Tier II poseen componentes extra de energía y enfriamiento para aumentar el margen de seguridad en contra de fallas de hardware de la infraestructura. El tipo de instituciones que utilizan

Tier II son organizaciones gubernamentales, educacionales y empresas de mediano tamaño.

- **Tier III Mantenimiento Concurrente:** Además de los equipos redundantes del Tier II, las infraestructuras Tier III poseen todos los equipos necesarios para que los equipos principales de la infraestructura puedan ser completamente apagados, y la infraestructura siga en funcionamiento, lo que se denomina mantenimiento concurrente. Este tipo de infraestructura es utilizado por clientes que buscan maximizar su disponibilidad, generalmente por negocios 24/7, o clientes que han identificado significativos costos en momentos de no disponibilidad.

- **Tier IV Tolerante a Fallas:** Infraestructura construida sobre Tier III, agregando el concepto de tolerancia de fallas a la topología de la infraestructura. Esto significa que cuando un equipo individual falla o caminos de distribución son interrumpidos, el sistema sigue en funcionamiento. Esto requiere de dos líneas de distribución simultáneamente activas. Organizaciones que tienen requerimientos de alta disponibilidad para negocios/instituciones/organizaciones. Se recomienda Tier IV para organizaciones con presencia internacional 24/7, y que sus servicios o información son altamente utilizadas.

En la figura 3.1 se puede observar una comparación de los aspectos específicos de los diferentes Tiers (Uptime Institute, 1990).

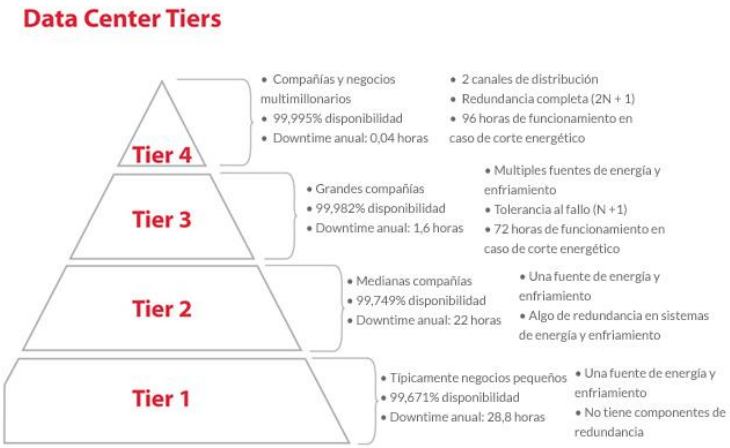

Figura 3.1: Esquema de clasificación Tier para datacenters.

Actualmente la demanda de servicios Cloud es alta, lo cual implica un amplio abanico de proveedores. Para tener una mejor idea de las mediciones de uptime de proveedores Cloud, la empresa CloudHarmmony (Network World, 2015) monitoreo el rendimiento de los principales proveedores Cloud a nivel mundial durante todo el año 2014. Dentro de estos proveedores se encuentran: Amazon Elastic Compute Cloud (EC2), Google Cloud Platform, Racketspace, entre otros. La figura 3.2 establece el downtime de los principales proveedores internacionales de Cloud durante el año 2014.

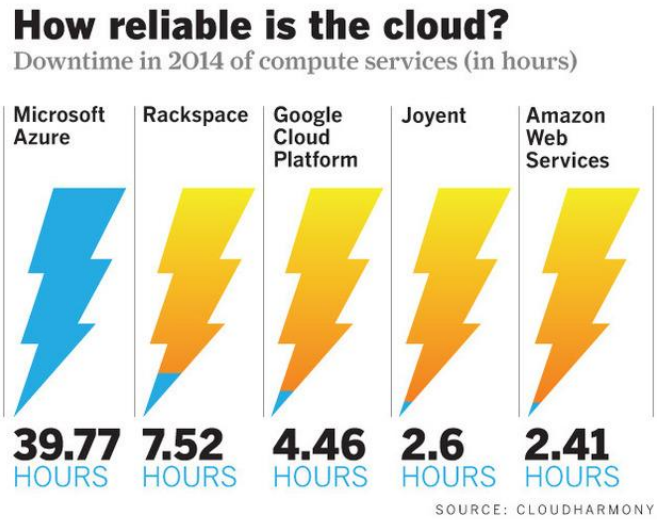

Figura 3.2: Comparación de Downtime entre 4 principales proveedores internacionales de servicios Cloud.

Como se puede apreciar, el proveedor Cloud con el menor downtime es Amazon web service, entregando un porcentaje de uptime de 99.9974%. Cabe destacar que AWS posee la infraestructura más grande de estos proveedores, superando en casos 5 veces el tamaño de sus competidores, lo cual hace aún más sorprendente su desempeño. Por otro lado, Microsoft Azure, el proveedor Cloud más nuevo en el listado, mantuvo un downtime de 39,77 horas en todo el año 2014, lo cual deja mucho que desear en comparación a sus competidores. A partir de esta captación de información, se establece que varios de estos proveedores están alcanzando el estándar de “five-nines” o 99,999% de disponibilidad en algunos aspectos específicos de sus datacenters. Por ejemplo, la plataforma de google, en su servicio de almacenamiento, experimentó tan solo 14 minutos de downtime en todo el año 2014, lo cual representa un 99,9996% de disponibilidad. Este estudio deja en evidencia los avances de la tecnología en comparación a años anteriores, y como los proveedores van avanzando en entregar un servicio cada vez mejor, cada día más cercano a entregar un servicio “five-nines”.

3.4. Seguridad de Información y confidencialidad

La seguridad de la información es uno de los temas más polémicos a la hora de hablar de tecnologías Cloud. El contraste con respecto al uso de sistemas inhouse es que el manejo a nivel de almacenamiento, procesamiento y control se le entrega a una empresa tercera, que utiliza sus propios protocolos e infraestructura para realizar estas tareas. Esta situación deja interrogantes como ¿qué se hace con la información almacenada? y ¿quiénes tienen acceso a la información almacenada?

3.4.1. Confidencialidad

Como concepto, la confidencialidad es la garantía de que cierta información catalogada como confidencial será protegida para que no sea divulgada sin consentimiento del entendido o propietario de la misma. Esta temática es

esencialmente controversial a la hora de hablar de Cloud Computing dado que es el proveedor Cloud es el encargado de mantener la confidencialidad de la información del cliente. Dada la naturaleza de la tecnología Cloud, toda la información a almacenar, procesar o transferir es responsabilidad del proveedor Cloud, lo cual se traduce en completo acceso a esta.

La privacidad y confidencialidad de la información es un tema importante a la hora de delegar el almacenamiento de la información a una empresa tercera. En el contexto Cloud, el proveedor debe garantizar la confidencialidad de la información del cliente tanto desde su propio accionar con respecto a esta información, como desde el accionar de terceros que intenten ganar acceso a esta información de manera desautorizada.

La manera en la que el proveedor entrega garantías sobre la confidencialidad es el set de reglas a las que este se compromete, lo cual se define en el contrato vinculante. Es aquí donde el proveedor debe estipular su completo accionar con la información, las personas o entidades que tendrán acceso a esta información almacenada y los protocolos y mecanismos utilizados para resguardar dicha información de posibles violaciones de terceros.

El énfasis que una institución pública debiese poner en esta temática va netamente ligado al tipo de información que la institución pública pretende almacenar en los servicios Cloud. En el caso de ser netamente información de carácter pública, la confidencialidad de la información puede no resultar una temática relevante. No así en el caso en que se trabaje con información de personas naturales o confidenciales a nivel institucional. Independiente de esto, los proveedores Cloud debiesen asegurar confidencialidad en el contrato a celebrar con el cliente.

3.4.2. Integridad de información

Tal como lo sugiere la ENISA, "la *integridad y la disponibilidad de los datos son elementos esenciales en la prestación de los servicios de computación en la nube*" (ENISA, 2011). La integridad de la información se define como la seguridad de que la información almacenada o transportada sea modificada por quienes están autorizados a hacerlo. Esto implica que no se debiese perder o corromper información ni por errores del sistema ni por terceros.

La integridad de la información se encuentra asociada a diferentes medidas que los proveedores Cloud deben cumplir para poder garantizarla. Para esto, protocolos y política de protección de infraestructura son aplicadas, redes se deben mantener seguras e impenetrables, y hardware debe ser protegido en caso de sobrecargas o alguna otra causa que interfiera en su correcto funcionamiento. Estas medidas se confirman a través de certificados que los proveedores adquieren para validar la calidad de sus instalaciones. Un ejemplo de certificación seria la norma ISO 27000 sobre la seguridad de la información.

3.4.3. Certificaciones de datacenters.

Las siguientes certificaciones son estándares de calidad de datacenter que buscan asegurar que las infraestructuras y servicios provistos desplegados en datacenters, tanto para proveedores Cloud como proveedores de otro tipo de infraestructura, cumplan con ciertas normas que aseguren estándares de calidad. En el capítulo anterior se menciona la certificación Tier, que corresponde a la elite en certificaciones. A continuación se abordan otras alternativas que permiten asegurar buenas prácticas y procedimientos.

- **TIA 942:** Es el principal estándar en normas de certificación de datacenters. Este estándar producido por TIA (Telecommunications Industry Association) entrega exigencias a nivel de arquitectura de red, diseño electrónico, redundancia de hardware, control del entorno,

copias de seguridad, etc. Al igual que las certificaicones del Uptime Institute, se clasifican los datacenters en 4 categorias.

- **Certificacion ISO/IEC:** La Organización Internacional de Normalización (ISO), es una organización para la creación de estándares internacionales. Con este objetivo, en conjunto con la Comisión Electrotécnica Internacional (IEC), formaron en 1987 el Comité Técnico ISO/IEC 1 (JTC 1) para desarrollar, mantener, promover y facilitar los estándares relacionados con la Tecnología de la Información. Existen una serie de certificaciones ISO que pueden ser aplicadas a empresas que prestan servicios de datacenter, tales como la serie **ISO 9001, la ISO 27001, y las normas ISO/IEC 14763-2, 11801-5**, entre otras (Asicom Data Center, 2016). Múltiples proveedores de servicios Cloud chilenos cuentan con esta certificación. Entre ellos se encuentra Entel, Claro, Intesis, Sonda, entre otros.

- **Certificación ICREA:** Norma similar a TIER, de origen latinoamericano. Esta norma resalta aspectos de seguridad y confiabilidad que involucran las siguientes especialidades; instalación eléctrica, aire acondicionado, seguridad, comunicaciones y Entorno. También segmenta sus certificaciones, pero esta vez en 5 niveles de acuerdo a la disponibilidad.

3.4.4. Proveedores en el extranjero.

Existe una gran gama de proveedores de carácter internacional, ya sea como una empresa internacional (amazon, google) o una empresa chilena con datacenters nacionales o que posee sus servidores externalizados fuera del territorio nacional. Cualquiera sea el caso, esta situación abre nuevas variables con respecto a la confidencialidad y seguridad de la información.

El hecho de tener la información fuera de territorio nacional implica que esta posiblemente sea regulada por normas del país correspondiente, normas que en muchos casos no ofrecen la protección necesaria. Un ejemplo de esto son los datacenters en los Estados Unidos y la ley “Patriot Act”, que en caso de sospecha de terrorismo, el Estado demanda acceso a información a cualquier entidad perteneciente al país. Son estas situaciones en donde información de carácter personal o gubernamental puede ser comprometida e intervenida por terceros.

Es por estas situaciones que países optan por regular al sector público con respecto a contrataciones internacionales. Por ejemplo, rígidos límites han sido aplicados para mover información fuera de los límites de los 27 países de la Unión Europea. Sector público y privado que deseen procesa información fuera del territorio deben negociar y realizar acuerdos legales para asegurar que información personal de ciudadanos de la Unión Europea serán tratadas de acuerdo a regulaciones correspondientes (CISCO, 2011).

Tal como el ejemplo anterior, no se sugiere descartar por completo el uso de nubes públicas fuera de territorio nacional. La Unidad de Modernización y Gobierno Digital recomienda que el órgano contratante adopte la decisión sobre la base de los siguientes pasos.

- Determinar el tipo de información que se quiere subir a los servidores de los servicios *cloud* de conformidad a lo indicado en el punto 2.4. No se ve mayor inconveniente de contratar a proveedores extranjeros en aquellos casos en que la información que se pretende almacenar es eminentemente pública.
- Revisar la legislación en materia de protección de datos y privacidad que rige al prestador del servicio *Cloud* y determinar si dichos marcos regulatorios establecen estándares de protección que son o no lo

suficientemente robustos como para proteger adecuadamente los intereses del órgano contratante.

Si se está frente a un régimen que garantiza la reserva de los datos de forma adecuada, no se ve inconveniente de contratar servicios de computación en la nube extranjeros.

- De preferencia, se sugiere en estos casos encriptar siempre la información que será alojada en las infraestructuras del prestador del servicio Cloud.

3.5. Relación con proveedor

Dado el carácter del servicio, se genera la necesidad de una relación directa con el proveedor para la contratación de los servicios, dado que existen diversas variaciones dependiendo del cliente en específico. Para establecer un contrato con un proveedor, se recomienda una exhaustiva investigación sobre este en base a diferentes materias. En lo posible, obtener información con respecto a otras experiencias que hayan tenido instituciones del Estado en relación a este proveedor.

Existen diferentes tipos de proveedores de servicios Cloud. Están los proveedores que poseen y utilizan sus propias infraestructuras, las cuales gestionan y administran para brindar el servicio a los clientes. Por lo general, estos proveedores ofrecen además de la infraestructura, diferentes servicios de migración a estas y diversos SaaS. Por otro lado, existen proveedores que actúan como un reseller de servicios de otros proveedores Cloud, los cuales compran los servicios Cloud de empresas con infraestructura propia y luego los venden a clientes. En esta categoría se pueden encontrar 2 tipos de resellers, aquellos que integran diferentes sistemas Cloud, adquiridos de diferentes proveedores para establecer un sistema. La otra categoría son los resellers con valor agregado, los cuales se encargan de vender, instalar, mantener las aplicaciones Cloud, evitando que el cliente tenga relación con

estas tareas. Por lo general, estos resellers utilizan el hardware de un tercero para así montar aplicaciones creadas por ellos mismos (TechTarget, 2011).

Por otro lado, es necesario establecer un SLA (acuerdo de nivel de servicio), en donde se establecen los servicios y la calidad de estos entre proveedor y cliente. Por lo general, estos pueden ser encontrados en los sitios web de cada proveedor bajo nombres como términos y condiciones, acuerdos de servicio o políticas.

3.6. SLA

SLA o ANS (acuerdo de nivel de servicio) es un vínculo importante en la relación Cliente, proveedor. "Un acuerdo de nivel de servicio, es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. El ANS es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc." (Wikipedia, 2015). Los SLAs son medidos a través de métricas denominadas SLO (service level objective).

Es en este documento donde el cliente debe especificar (o en su defecto encontrar) las necesidades y estándares que requiere del servicio que se busca suplir. Dependiendo del cliente y del objetivo del sistema a desplegar, algunos niveles de requerimientos resaltan más que otros. En el caso de los organismos del Estado, dado su carácter público, tienen el deber legal de atender las necesidades públicas en forma continua y permanente, por lo cual la **disponibilidad** es una necesidad que debe ser tratada dentro de este documento. Lo mismo aplica con la **confidencialidad** e **integridad** de datos, por lo cual estándares deben ser establecidos frente a estas temáticas. Estos deben ser reflejados en el contrato mediante un acuerdo de nivel de servicio

(SLA) en el que se especifiquen los indicadores de calidad de servicio que van a ser medidos y los valores mínimos aceptables de los mismos. Sanciones deben ser establecidas en caso de no respetar estos estándares. Estas sanciones pueden ser de carácter monetario o incluso de terminación de contrato en caso de falta grave. Dada la naturaleza de las instituciones, los estándares de SLA deben ser altos, al igual que las sanciones.

Una manera conveniente de estructurar los SLAs para un servicio Cloud es agruparlos en 3 grupos distintivos: en relación al **desempeño**, relación a la **seguridad**, en relación al **manejo de información** y la **protección de información personal** (European Commission, 2014). A continuación se detallan algunos SLAs destacables con sus respectivos SLOs relevantes para una institución pública.

3.6.1. Disponibilidad

Es de suma importancia para una institución pública la disponibilidad de su información, ya sea de manera interna o para el público en general. El concepto disponibilidad cae en la categoría de desempeño, y va más allá de que la información se encuentre disponible para su uso, además es necesario que estas sean desplegadas bajo estándares de uso, en un tiempo de respuesta aceptable y sin errores. No es de utilidad información disponible pero no accesible dado la mala performance del sistema, por lo cual niveles de disponibilidad y accesibilidad deben ser establecidos.

Los siguientes son objetivos deben ser cuantificados (porcentajes) con respecto a la disponibilidad en un SLA.

- **Uptime o tiempo disponible:** Se debe definir el tiempo en que la aplicación necesita estar disponible. Es claro que sería ideal que se tuviera un 100% de disponibilidad, pero ningún servicio de Cloud

Computing puede garantizar este tipo de performance, por lo cual es necesario establecer que parámetro es considerado correcto para la institución. Cabe destacar que certificaciones respaldan los uptimes de los proveedores, por lo cual es necesario revisar esto en la documentación de los proveedores. Cabe destacar que algunos proveedores no especifican como downtime los tiempos de mantención.

- **Porcentaje de solicitudes exitosas:** Este punto hace referencia a la cantidad de respuestas exitosas con respecto a la cantidad de solicitudes realizadas. Se diferencia del tiempo disponible ya que va ligado específicamente al uso que se le da al servicio. Por ejemplo, si una institución realiza uso de sus servicios Cloud durante el día sin ninguna solicitud fallida, el porcentaje de solitudes exitosas será alto, mientras que el tiempo disponible puede que no se correlacione dado que ocurrió durante periodos de inactividad.

- **Porcentaje de solicitudes procesadas en el tiempo:** Describe la cantidad de solicitudes procesadas completamente sobre todas las solicitudes procesadas en un tiempo determinado.

3.6.2. Tiempos de respuesta

El tiempo de respuesta es el tiempo que demora el proveedor Cloud en entregar el servicio en respuesta a una solicitud enviada por el usuario Cloud. Es de suma importancia para una institución pública tiempos de respuesta acorde con la velocidad necesaria que el servicio busca cumplir. Tiempo de respuesta se categoriza como un estándar de desempeño Por ejemplo, si se desea tener una plataforma en línea donde personas naturales realicen algún tipo de trámite, es esencial para estos un buen performance de la plataforma, por lo cual el tiempo de respuesta debe ser bajo. Por otro lado, si se desea

tener un servicio Cloud que respalde información de manera nocturna y el tiempo apremia con respecto a las horas de no actividad de la institución, quizá un tiempo de respuesta óptimo en relación a las horas que se tenga sea suficiente. Cabe destacar que los tiempos de respuesta son variables a la naturaleza del servicio solicitado, por lo cual raramente se encuentran certificados.

Objetivos Relevantes (SLO)

- **Tiempo de respuesta promedio:** Promedio del tiempo de respuesta de un número de solicitudes de un mismo tipo.
- **Tiempo de respuesta máximo:** Tiempo de respuesta máximo de una solicitud específica.

Cabe destacar que no es necesario establecer los tiempos de respuesta para todo tipo de solicitud. Una buena opción es revisar los tiempos de respuesta propuestos por el servicio, y si es necesario especificar alguno en particular.

3.6.3. Confiabilidad del servicio

Es la capacidad del servicio de funcionar sin ningún error sobre un periodo de tiempo. Generalmente se relaciona a controles de seguridad que mantengan la continuidad del negocio y la capacidad de recuperación en caso de desastre. Dentro de esta capa se cubre la capacidad que tiene el proveedor Cloud de lidiar con fallas del sistema y pérdida e integridad de información, aspectos claves para una institución pública dado que la información en muchos casos es de importancia, por lo cual deben existir los respaldos necesarios para que esta se mantenga en caso de cualquier falla del sistema.

Objetivos medibles

- **Nivel de redundancia:** Describe el nivel de redundancia de la información a tratar. Este nivel depende del tipo de servicio que se provee.

- **Confiabilidad del servicio:** Es la capacidad que tiene el servicio de mantenerse funcionando establemente en un periodo de tiempo determinado.

3.6.4. Códigos, conductas y estándares para la protección de información

Los proveedores Cloud tienen la responsabilidad de mantener la información segura y evitar que esta caiga en manos de personal no autorizado. Tema de especial cuidado con respecto a instituciones públicas ya que en muchos casos, estas poseen información privada de personas naturales e información relevante en materias gubernamentales. Para esto, los proveedores de servicios Cloud deben poseer información transparente con respecto a los protocolos, estándares y códigos que permiten mantener la información segura en sus servidores. Bajo esta situación, el objetivo de este SLA es transparentar e informar al cliente con respecto a los protocolos, mecanismos y estándares que el proveedor Cloud posee en función de proteger la información.

3.6.5. Reversibilidad y Terminación de servicios

Es importante para cualquier cliente tener la capacidad de elegir algún otro proveedor en caso de que la relación proveedor cliente no esté funcionando. Es en este caso que el prestador de servicios debe entregar la información a la institución en su totalidad, por lo cual se necesita completa colaboración de este para poder retribuir la información o migrarla a otro proveedor. Una vez finalizada la terminación del servicio y la entrega de datos al cliente, es necesario que el proveedor de servicio elimine los datos del cliente. Para estas situaciones, es necesario establecer SLOs de acuerdo con lo apropiado para cada institución.

SLOs relevantes

- **Periodo de recuperación de información:** Describe el periodo en el cual el cliente puede adquirir una copia de la información almacenada por los servicios Cloud.

- **Periodo de retención de datos:** Establece el periodo en el cual el proveedor de servicios Cloud retiene la información a posterior de finalizado el servicio y la entrega de los respaldos de información al cliente. El propósito es en caso de que el cliente necesite nuevamente la información o en caso en que por alguna situación legal se necesite la información mencionada.

La estructura utilizada para la categorización de los SLO en los puntos del SLA mencionado están hechos en base al documento “Guía de estandarización de SLA para servicios Cloud” formulado por la Comisión Europea (European comisión 2014) bajo su programa de agenda digital. Cabe destacar que la estructura presentada y los SLOs mencionados no son de carácter obligatorio, sino que van acorde a la estandarización presentada en la guía mencionada. Esta estandarización busca simplificar lo variado que pueden ser los SLAs entre diferentes proveedores, estandarizar los SLAs para una mejor canalización de necesidades y establecer un mejor entendimiento de rendimientos y necesidades entre proveedor y cliente.

Los SLOs mencionados en este documento son considerados importantes para una institución pública, pero cabe destacar que la guía de estándares proporciona un framework que abarca todos los posibles ángulos de un SLA en materias Cloud, por lo cual se recomienda revisar (European comisión 2014).

3.7. Contrato Cloud

En términos generales, el contrato Cloud se compone de cláusulas que estipulan los servicios y sus condiciones entre proveedor y Cliente Cloud. El contrato debe contener las responsabilidades del proveedor y del cliente. En general, todo lo mencionado anteriormente debiese estar especificado bajo alguna cláusula del contrato con el proveedor.

Cabe destacar que muchos proveedores, en especial proveedores a nivel internacional, poseen sus propios contratos que no son sujetos a modificaciones por parte de clientes. En estos casos la tarea se torna en una revisión sobre las diferentes condiciones que los proveedores ofrecen y ver si estas se ciñen a lo requerido por el cliente, es por esto que es importante entender qué tipo de cláusulas deben ser estipuladas en un contrato Cloud.

3.7.1. Estructura Contrato

La UMGD en los anexos del documento (UMGD, 2014) proporciona una serie de cláusulas que pueden ser empleadas (con libre opción de modificación) para estructurar un contrato Cloud. Dentro de estas cláusulas se encuentran temáticas como la confidencialidad y protección de datos, seguridad de información, responsabilidad civil, etc. Cabe mencionar que los órganos de administración del Estado son completamente libres de determinar la estructura y modalidades de sus cláusulas.

Desde el punto de vista de los servicios, la prestación de estos y su rendimiento, una sección con acuerdo de niveles de servicio (SLA) debe ser agregada a este contrato, en el que se especifiquen los indicadores de calidad de servicio que van a ser medidos y los valores mínimos aceptables de los mismos. En la sección de SLA (referencia) del presente documento, se establece la idea principal y temas relevantes que deben ser tomados en

cuenta en la redacción de los SLA. Por otro lado, la Comisión Europea, bajo su programa de agenda digital, proporciona una estandarización de SLA para facilitar la redacción y alcance de estos.

3.7.3. Terminación de contrato

Es esencial para el cliente tener la posibilidad de terminar la relación con el proveedor de servicios. Es por esto que bajo el contrato se debe estipular una cláusula que establezca la libertad del cliente de terminar el contrato en caso de insatisfacción de servicios, y en los niveles de servicio las correspondientes métricas que gobiernan este comportamiento.

Otro aspecto importante es revisar las consideraciones en relación a la migración a un nuevo servicio Cloud para garantizar la continuidad del servicio (temática en detalle en punto 5.6.5). Por último es necesario establecer los protocolos de entrega de la información almacenada en el servicio, una vez terminado el contrato, es necesario que el prestador de servicios entregue una copia de toda la información acumulada durante la prestación de servicios, además de eliminar todo rastro de la información almacenada durante el periodo de servicios.

Cabe destacar que todo lo mencionado en este punto debe ser establecido en la cláusula de Terminación de contrato y medido a través los SLA que se relacionen con este punto.

4. Capítulo 4: Antecedentes

La relación entre los servicios Cloud y los organismos del Estado no es algo nuevo. Son muchos los países que han identificado los potenciales beneficios que estos servicios pueden brindar tanto al sector público como privado. Un impedimento importante a la hora de realizar contrataciones Cloud es el conocimiento con respecto al proceso mismo y a la tecnología en sí. Existe mucha información en internet con respecto a esta temática, lo cual en muchos casos resulta contraproducente dado la naturaleza del tema. Ocurre que las tecnologías Cloud no son blanco o negro, sino que existen matices que varían dependiendo de las necesidades del cliente, lo que puede tornar un simple proceso en una situación compleja. Es por esto que se han desarrollado guías enfocadas a ciertos nichos para poder entregar información específica y simplificar el proceso.

Para el desarrollo de esta guía se han estudiado y re-utilizado múltiples conceptos que guías anteriores han establecido. Muchas de estas guías entregan un paso a paso de los puntos relevantes que el cliente foco debiese realizar para la contratación Cloud, otras son más específicas a ciertos aspectos de la tecnología. La idea del estudio de estas guías es poder utilizar los puntos más relevantes, analizar sus paso a paso, para luego contextualizas y poder aplicarlos a la situación estatal chilena en relación a las tecnologías Cloud.

Por otro lado, dado la naturaleza del cliente y la especificidad que esta guía busca alcanzar, se ha hecho necesario estudiar el caso particular de Chile. Para esto, resulta interesante obtener la perspectiva tanto de las instituciones públicas como de los proveedores de servicios Cloud chilenos. Es por esto que se han realizado entrevistas tanto a instituciones como proveedores chilenos, con el fin de alimentar esta guía con información contextualizada a

la situación país y así identificar los puntos claves que realmente conciernen a las instituciones en materia de contratación Cloud.

Este capítulo establece las bases conceptuales en que la guía metodológica será construida. En otras palabras, las bases de donde se desprende la estructura y los puntos a abordar en la guía. Como fue mencionado anteriormente, la estructura y el contenido de esta guía son enfocados a los organismos públicos chilenos, por lo cual es necesario establecer los puntos de interés de la temática en cuestión en relación al sujeto al que va dirigida. Para esto, se realizaron una serie de **entrevistas** a diferentes organismos, tanto instituciones públicas del Estado como proveedores o prestadores de servicios relacionados a la tecnología Cloud, para así obtener cierta información relevante sobre qué temas conciernen a los organismos públicos con respecto a la tecnología y cómo abordarlos.

Además, se busca complementar la información recopilada mediante las entrevistas con información bibliográfica disponible en función de obtener un mejor estudio del sujeto en cuestión. Este capítulo es dividido en 2 partes, la primera siendo el complemento bibliográfico mencionado, y la segunda enfocada a las entrevistas realizadas a los distintos organismos más ciertas conclusiones derivables de las mismas.

4.1. Complemento Bibliográfico

4.1.1. Nivel de desarrollo de las tecnologías Cloud en los organismos del Estado

Resulta interesante para el desarrollo de esta guía metodológica tener una aproximación del nivel de penetración que han tenido las tecnologías Cloud en los organismos públicos chilenos. Esta información es valiosa para poder dimensionar el nivel de experiencia y entendimiento que los encargados de TI de las diversas instituciones públicas poseen con respecto a la tecnología, y

así poder orientar la guía de manera focalizada en función de los conocimientos previos de lector en cuestión.

Para esto, se revisó el modelo de madurez MMGD (Centro de Gobierno Electrónico, 2015). Este modelo busca encontrar una medición para el desarrollo de las capacidades de gestión en tecnología en los diferentes organismos públicos. En el trabajo realizado, 121 instituciones fueron sometidas al modelo mediante una autoevaluación del mismo. Lo interesante del modelo es que subdivide sus dominios de análisis llegando específicamente a la temática en cuestión, Software Público y Cloud Computing, el cual queda clasificado como una subcategoría del dominio Habilitantes de Gobierno Digital. La tabla 4.1 establece los 4 niveles de madurez que el modelo establece.

Tabla 4.1: Niveles de desarrollo del Modelo de Madurez de Gobierno Digital.

	Descripción
Nivel 1: no existe desarrollo	• No ha considerado abordar el tema al que se refiere cada variable, y/o es abordado de forma reactiva, tiende a ser aplicado de forma individual caso a caso. • Sin embargo, se sabe que el problema debe ser abordado
Nivel 2: desarrollo incipiente	• La institución ha iniciado el trabajo en el tema en un caso específico. • El trabajo responde a una solicitud concreta más que a la necesidad de contar con un trabajo para toda la institución
Nivel 3: desarrollo intermedio	• La institución cuenta con un proceso formalizado para hacerse cargo del tema. • Se hace una gestión básica para que el proceso sea aplicado regularmente. • La aplicación evidencia que se han logrado resultados positivos en el tema.
Nivel 4: desarrollo avanzado	• Los procesos han alcanzado un alto nivel en su funcionamiento. • Hay una práctica de seguimiento y mejoramiento continuo. • Se ha logrado un nivel de automatización y digitalización en la gestión del tema. • Se han alcanzado altos niveles de eficiencia y eficacia. Los resultados alcanzados así lo evidencia.

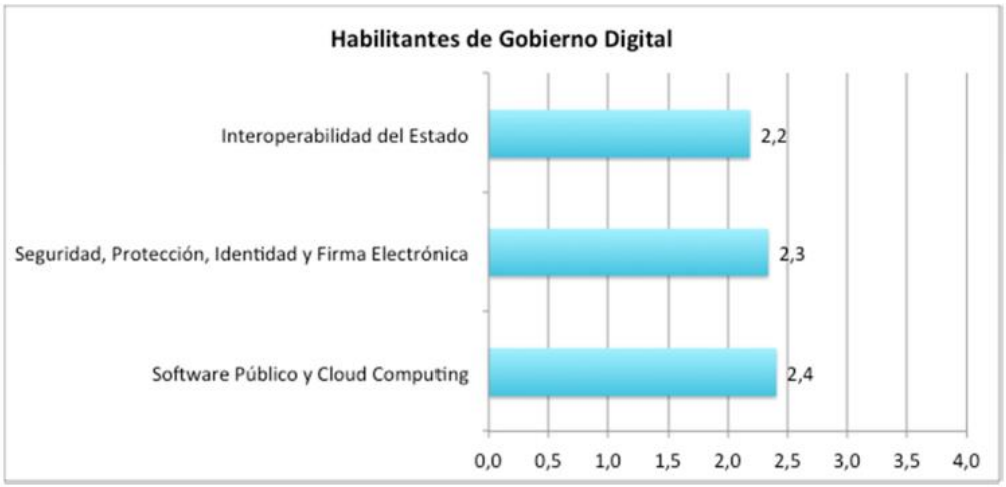

Figura 4.1: Nivel de desarrollo del dominio Habilitantes de gobierno digital, desglosado en sus subdominios.

Como es posible evidenciar, el subdominio Software Público y Cloud Computing es el subdominio con mayor índice de madurez. A la vez, se divide el subdominio de Software Público y Cloud Computing en la figura 4.2.

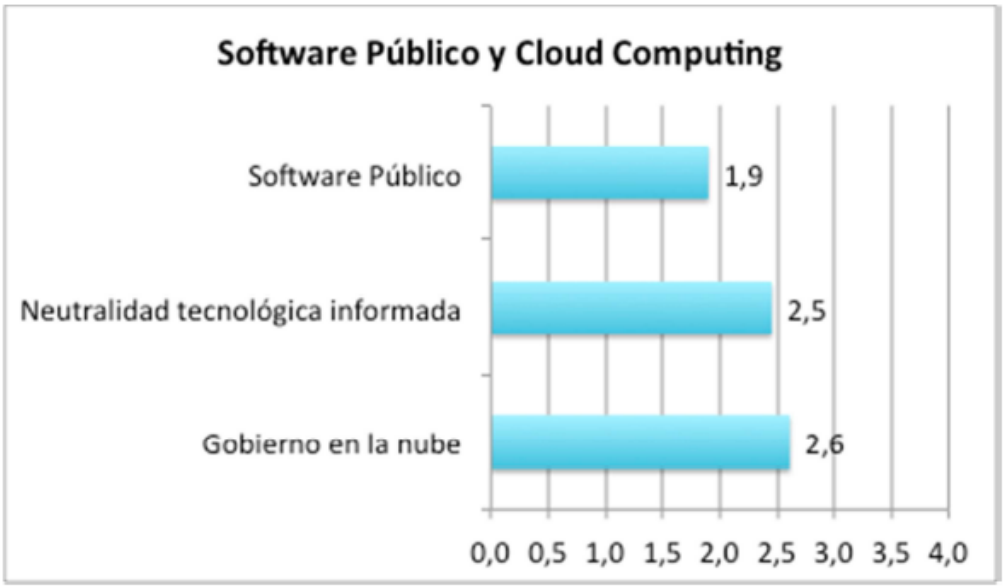

Figura 4.2: Nivel de desarrollo del dominio Software Público y Cloud Computing, desglosado en sus subdominios.

Donde se define:

- **Gobierno en la nube:** Permite verificar si la institución ha evaluado los beneficios, ahorros y mejoras de la eficiencia al incorporar un plan de virtualización y Cloud Computing

Sobre el dominio Software Público y Cloud Computing, se definen niveles de desarrollo específicos explicados en la tabla 4.2.

Tabla 4.2: Nivel de desarrollo especifico al domino Software Público y Cloud Computing

Nivel de Desarrollo	Descripción
1	La institución no ha identificado la necesidad de integrar información para realizar trámites.
2	La institución ha identificado la necesidad de integrar información para realizar trámites, pero aún no lo realiza a través de la plataforma de interoperabilidad del Estado
3	La institución ha identificado la necesidad de integrar información para realizar trámites, y lo ha implementado a través de la plataforma de interoperabilidad del Estado
4	La institución ha integrado información para realizar trámites a través de la plataforma de interoperabilidad del Estado, la cual actualiza en forma permanente

Como es posible evidenciar, el gobierno en la nube es la subdivisión con mayor grado de madurez de los subdominios. Por otro lado, el grado de desarrollo del gobierno en la nube corresponde al nivel 2. En otras palabras, las instituciones públicas chilenas tiene un desarrollo a Cloud bajo, remitiéndose a entender que debería existir una iniciativa para incorporar tecnologías Cloud pero sin un mayor entendimiento de lo que significa esta tecnología y sus implicancias. Cabe destacar los talleres realizados a las instituciones públicas (85 participantes), de donde se derivó que no todas las instituciones públicas siquiera comprenden el concepto de Cloud Computing.

En base a este estudio, es evidente concluir que el nivel de madurez de las organizaciones públicas con respecto a las tecnologías Cloud es bajo. Punto a considerar en el desarrollo de esta guía, para así orientar su contenido de manera que sea entendible y claro

4.1.2. Correlación entre Inversión en TI y Madurez Tecnológica en Instituciones Públicas

En base a los resultados del estudio de modelo de madurez mencionado en el punto anterior, se estableció una correlación entre la inversión de TI y el nivel de madurez de las instituciones (Correlación entre Inversión en TI y Madurez Tecnológica en Instituciones Públicas). En este estudio se establece que las instituciones con mayor presupuesto dedicado a TI en relación al presupuesto general que manejan, son las instituciones con mayor índice de madurez tecnológica.

El estudio establece 4 segmentos (tabla 4.3) en relación al porcentaje de inversión en TI con respecto al presupuesto total.

Tabla 4.3: Segmentos correspondientes al nivel de inversión de TI con respecto al presupuesto total de una institución pública.

Segmento I	Instituciones con presupuesto dedicado a TI mayor al 5% de su presupuesto total.
Segmento II	Instituciones con presupuesto dedicado a TI mayor que 2% y menor o igual al 5% de su presupuesto total.
Segmento III	Instituciones con presupuesto dedicado a TI mayor que 0,5% y menor o igual al 2% de su presupuesto total.
Segmento IV	Instituciones con presupuesto dedicado a TI menor o igual que 0,5% de su presupuesto total.

En el anexo 1 se puede encontrar los organismos pertenecientes a este estudio, segmentados según esta clasificación y el nivel de madurez correspondiente.

La información con respecto a los presupuestos de TIC corresponde al presupuesto vigente del año 2013, otorgada por la Dirección de Presupuesto del Ministerio de Hacienda para realizar el estudio.

De los resultados obtenidos, se puede verificar que el segmento I, es donde están las instituciones con mayor inversión en TIC con respecto a su presupuesto. Es el segmento donde se encuentran la mayor cantidad de instituciones maduras, considerando que se tiene 4 instituciones con nivel de madurez superior al nivel 3.

El segmento II tiene una única institución con promedio superior a 3, siendo ésta en realidad la de mayor madurez entre todas las instituciones encuestadas, con un nivel promedio de 3,4. Los otros dos segmentos, III y IV, no tienen ninguna institución con nivel de madurez mayor a 3.

Es posible verificar que 70,8%, que corresponden a 17 instituciones de las 24 que componen el segmento I tienen una madurez inferior a 2,5. Esta relación, en el segmento II sube a 79,4% (27 de 34 instituciones), y en los segmentos III y IV, la relación se incrementa a 94% (33 de 35 instituciones) y 93% (26 de 28 instituciones).

De hecho, los promedios de madurez en cada segmento es de 2,4, para el segmento I, 2,2 para el segmento II, y para los segmentos III y IV, los promedios de madurez son de 2,0 y 2,1 respectivamente, recordando que son los segmentos con niveles de inversión menor de 2% en TIC.

4.1.3. Costos almacenamiento Local v/s Cloud

Una temática bastante controversial son los costos asociados a la tecnología Cloud en comparación a una solución inhouse. Es clara que la inversión a corto plazo de una infraestructura inhouse resulta ser más costosa a momento que la utilización de soluciones Cloud, pero ¿es este comportamiento consistente en el tiempo? Es importante analizar todos los costos que se incurren en ambas soluciones a través de un periodo de tiempo determinado, dado por lo general las soluciones que las instituciones buscan abordar son de un carácter más longevo ya que buscan entregar un servicio público. Otro punto a considerar en esta discusión es el tamaño de la institución u organización que pretende implementar estos servicios. Esta temática es importante dado que los costos de infraestructura y mantenimiento para soluciones de menor envergadura afectan al comparativo de ambas situaciones.

El grupo de seguridad Leviatan, el año 2015 realizó un análisis general comparativo entre soluciones locales v/s Cloud. En específico, se realizó un análisis de costos (Leviathan Security Group, 2015). Este análisis toma 3 escenarios en relación a tamaños de organizaciones con las siguientes características.

1. **Organización de tamaño pequeño:** 50 empleados, generalmente una locación física. Promedio de almacenamiento de información por usuario es de 200gb-300gb, por lo que se requiere un total de 15TB de espacio de almacenamiento.
2. **Organización de tamaño medio:** 500 empleados, distribuidos ente una oficina principal y 4 sedes. Consumo de almacenamiento por usuario de 250gb promedio, por lo que se requiere un total de 150TB.
3. **Organización de tamaño grande:** 2500 empelados, distribuidos en 2 oficinas corporativas, 6 oficinas sede y múltiples empleados realizando teletrabajo. Además la organización tiene rentado datacenters.

Almacenamiento promedio por usuario es de 300GB, resultando en 750TB para la organización completa.

En base a las necesidades de cada escenario, se establecieron soluciones a nivel de hardware para poder comparar con los escenarios Cloud. El estudio tomó hardware y software específico para poder realizar un análisis de costos real, pero esto no significa que el equipo Leviatan haya seleccionado estos componentes por alguna relación comercial con los específicos proveedores. La selección fue realizada en base a los precios más precisos que se pudieron obtener. Por otro lado, los proveedores Cloud seleccionados para esta comparación de costos no constituyen una lista exhaustiva de proveedores, pero si son una muestra representativa de los precios, modelos de cobro y capacidades. Se postula que esta utilización de proveedores representa los servicios de almacenamiento Cloud como un entero. Este análisis se puede encontrar en los anexos del documento de estudio (Leviathan Security Group, 2015).

Los costos analizados se clasifican en 3 tipos:

1. Costos de Hardware/Software
2. Costos de implementación
3. Costos de mantenimiento

Cabe destacar que a través de los 3 escenarios, algunos valores o costos se mantendrán constantes. En esto encontramos costo de mano de obra, tiempos de implementación, ingeniería de procesos, costos de parches y costos Cloud.

Se presentan cuadros comparativos segmentados por los 3 escenarios, en comparación a una infraestructura inhouse vs Cloud, proyectado a 3 años.

Escenario 1: Organización pequeña

Tabla 4.4: Comparación Costo Hardware/Software entre ambiente Local y Cloud

		Local		Cloud	
Item	Price ($)	Quantity	Cost ($)	Quantity	Cost ($)
Dell PowerVault NX400,[6] including: 2 x 500G mirrored disks (Operating System) 8 x 3TB disk (storage) RAID5 Card Gigabit NIC 8G RAM 1.8GHz Xeon Processor	6,680	1	6,680	0	0
Backup Hardware (locally attached)[7]	1,649	1	1,649	0	0
Windows 2012 R2 Server[8]	882	2	1,764	1	882
Backup Server Software (Symantec Backup Exec Small Business)	728	1	728	0	0
Anti-Virus Software - Server Hardware (PowerEdge R320)	2,529	1	2,529	1	2,529
Anti-Virus Software - Client Licenses (including year 2 and 3 maintenance)[9]	2,205	1	2,205	1	2,205
Total Hardware and Software			15,555		5,616

Tabla 4.5: Comparación costo de implementación entre ambiente Local y Cloud.

		Local		Cloud	
Item	Price ($)	Quantity	Cost ($)	Quantity	Cost ($)
Installation Costs (per server / per hour)	125	16	2,000	8	1,000
Workstation Configuration (per server / per hour)	125	100	12,500	100	12,500
Total Implementation Costs			14,500		13,500

Tabla 4.6: Comparación costos de mantenimiento entre ambiente Local y Cloud.

		Local		Cloud	
Item	Price ($)	Quantity	Cost ($)	Quantity	Cost ($)
Power & Cooling - NAS[10][11]	241	1	241	0	0
Power & Cooling - AV Server	153	1	153	1	153
Patching (per event / per server)	149	24	3,576	12	1,788
Maintenance Agreement (15% of hard-ware/software cost)	2,334	1	2,334	1	2,334
Yearly Cloud Subscription - see Table 15	9,299	0	0	1	9,299
Total Operations Costs			6,304		13,574

Tabla 4.7: Comparación costos proyectados a 3 años para ambiente local y Cloud.

	Local ($)	Cloud ($)
Hardware and Software Costs	15,555	5,616
Implementation Costs	13,500	13,550
Operations Costs (3 years)	6,304	13,574
	6,304	13,574
	6,304	13,574
Total Costs Over 3 Years	47,967	59,888

Escenario 2: Organización Mediana

Para este escenario solo se muestra el cuadro resumen con los resultados de los 3 tipos de costos. Las tablas con los resultados específicos de los costos se encuentran en el anexo 2. La tabla 4.8 resume para los resultados del escenario 2.

Tabla 4.8: Comparación costos proyectados a 3 años para ambiente local y Cloud para una organización mediana.

	Local ($)	Cloud ($)
Hardware and Software Costs	116,802	34,025
Implementation Costs	66,500	63,500
Operations Costs (3 years)	31,016	93,371
	31,016	93,371
	31,016	93,371
Total Costs Over 3 Years	276,350	377,638

Escenario 3: Organización Grande

Para este escenario solo se muestra el cuadro resumen con los resultados de los 3 tipos de costos. Las tablas con los resultados específicos de los costos se encuentran en el anexo 2. La tabla 4.9 resume para los resultados del escenario.

Tabla 4.9: Comparación costos proyectados a 3 años para ambiente local y Cloud para una organización grande.

	Local ($)	Cloud ($)
Hardware and Software Costs	1,131,936	164,718
Implementation Costs	317,500	314,500
Operations Costs (3 years)	99,660	460,739
	99,660	460,739
	99,660	460,739
Total Costs Over 3 Years	1,748,416	1,861,435

A partir de estos resultados es posible evidenciar que para los 3 escenarios propuestos por el grupo Leviatan, proyectando los costos a 3 años, siempre resulta más económico la utilización de infraestructura local. Es importante considerar que todos los precios utilizados son referentes a Estados Unidos, lo cuales difieren a los precios chilenos ya que los servicios Cloud y los componentes de infraestructura son más económicos, también los sueldos de empleados son más altos.

Los resultados obtenidos son de notable importancia ya que a simple vista las tecnologías Cloud pueden parecer un ahorro significativo en comparación a realizar una compra de infraestructura, y en algunos casos lo son. Para muchos proyectos de menor longevidad, o de uso intermitente de infraestructura, no tiene sentido la compra de una infraestructura. Pero para proyectos de mayor duración, el estudio indica que debiese ser más económico el uso de infraestructura local.

Es importante destacar que el análisis es netamente económico, no contempla los beneficios de una tecnología sobre otra, ni como estos podrían llegar a afectar a los 3 escenarios contemplados.

4.2. Entrevistas

El principal foco de estas entrevistas fue identificar los puntos que esta guía debiese contener según el criterio de proveedores Cloud e instituciones

públicas. Se buscó extraer información concreta con respecto a puntos específicos y como estos se interrelacionan, para lograr un enfoque lineal (paso a paso) y una coherencia global entre los mismos.

Como objetivo secundario, estas entrevistas buscan obtener información relevante respecto a la temática general, sin una necesaria estructura, para luego poder nutrir el compilado de puntos a desarrollar en la guía misma. Dentro de esta clasificación se puede encontrar temáticas como: relación cliente-proveedor, casos de éxito, comparación Cloud con otras tecnologías, información con respecto a los proveedores de la tecnología, experiencia en TI con instituciones públicas chilenas, etc.

Al finalizar las entrevistas, se realizó un análisis en conjunto con los entrevistados, sobre los 10 pasos para el camino al Cloud Computing postulados en la guía Practical guide for Cloud Computing (Cloud Standards Customer Council, 2014). La idea de este análisis fue utilizar los puntos que nos entrega esta guía como una base, y evaluar su relevancia enfocándose en las instituciones públicas chilenas. Esta evaluación fue medida con notas del 1 al 5, siendo 5 la más alta en relevancia. Por otro lado, el debate generado en torno a estos puntos fue aprovechado para obtener información sobre otras temáticas derivables de ellos. La elección de estos puntos para analizar con los entrevistados se basa en lo bien abordados que estos están y lo diverso que son, abarcando de buena manera los principales tópicos Cloud. Originalmente estos puntos están enfocados a una empresa u organización privada. En el caso de la entrevista, estos puntos fueron enfocados a las instituciones públicas chilenas y como estos son relevantes a ellas. Cabe destacar que no se pudo hacer este análisis con todas las entrevistas realizadas debido a los cursos que tomaron las entrevistas y los tiempos que los entrevistados disponían, pero se realizó en la gran mayoría de ellas. Los resultados de estas mediciones se pueden encontrar en el anexo 3.

Las entrevistas fueron realizadas tanto a instituciones públicas como a proveedores Cloud chilenos. La idea de enfocar las entrevistas a estos actores es obtener ambas perspectivas de la relación proveedor y cliente Cloud. En el caso de las instituciones públicas, se realizaron entrevistas con los respectivos encargados o coordinadores de TI. Para el caso de los proveedores, se entrevistaron consultores y gerentes de las empresas.

La tabla 4.10 contiene el listado de todos los entrevistados, con la correspondiente información de su relación con la organización perteneciente.

Tabla 4.10: Listado de entrevistas realizadas

Nombre	Cargo	Tipo Organismo	Organización
Andrés Arellano	Coordinador área de tecnología y desarrollo	Institución Pública perteneciente al Ministerio Secretaria General de la Presidencia	Unidad de modernización y gobierno Digital (UMGD)
Jonny Heiss	Coordinador Nacional de Tecnología	Institución Pública	Ministerio de Educación
Flavia Gomez	Jefe Unidad Sistemas y Tecnologías de Información	Institución Pública	Hospital Roberto del Rio
Juan Pablo Reyes	Gerente	Empresa, Proveedor	LINETS
Manuel Suarez	Gerente General	Empresa, Proveedor	Synaptic
Mario Araneda	Consultor Senior	Empresa, Proveedor	INTESIS

Cabe destacar que a pesar del bajo espacio muestral, las entrevistas fueron realizadas en profundidad y con personal capacitado y altamente experimentado con la tecnología y la relación cliente-proveedor a nivel estatal.

4.2.1. Entrevistas a proveedores

Cuando se comenzó a realizar el análisis para encontrar una forma de generar el contenido de esta guía, una respuesta natural fue realizar entrevistas a instituciones públicas. Obviamente, esta guía está orientada a ser usada por los organismos públicos, por lo cual la opinión de estos con respecto a cómo facilitar la integración de tecnologías o que temáticas son las que más complica a la hora de evaluar y contratar servicios tecnológicos, es clave. Pero ¿son las instituciones públicas los organismos más capacitados para poder identificar los puntos de mayor complicación a la hora de contratar servicios Cloud?

Los proveedores Cloud poseen vasta experiencia tratando con cliente dado que es parte del núcleo de su negocio, por lo cual naturalmente desarrollan metodologías de trabajo y procesos en los cuales, dado la repetición de los mismos, se logra identificar dificultades o impedimentos que lógicamente les gustaría agilizar y solucionar.

Las empresas proveedoras fueron seleccionadas en base a su trabajo previo con instituciones públicas, ya sea mediante asesorías, consultorías, implementación o administración de ambientes Cloud. Además 2 de los 3 proveedores pertenecen al convenio marco de **Datacenter y servicios asociados** (el tercero inscrito en el nuevo proceso de captación de proveedores del convenio), lo que certifica la capacidad de estos para lidiar con instituciones públicas.

Cabe destacar que las empresas entrevistadas abarcan un amplio espectro de soluciones informáticas, tanto como resellers como proveedores directos de tecnologías Cloud (Ver punto 3.5). Estas empresas utilizan las tecnologías Cloud para dar una mejor performance a una problemática. En algunos casos el uso de la tecnología Cloud se aplica de manera directa, y en otros como complemento para dar una mejor performance a la solución principal. Esto implica que estas empresas no ofrecen simplemente sus servicios a nivel de

infraestructuras propias (en el caso de tener), sino que utilizan las herramientas que mejor se acomoden a las problemáticas. Situación que resulta interesante ya que estos proveedores poseen experiencia con diferentes tipos de nubes, tanto locales como extranjeras, privadas o públicas, propias o tercerizadas, etc.

Dentro de los principales trabajos realizados por los proveedores para instituciones públicas se puede encontrar la plataforma de entrega de puntajes PSU, optimización y administración de la plataforma de postulación al Fondart nacional, desarrollo de la infraestructura de la Super Intendencia de Insolvencia y Reemprendimiento, Servicios de Datacenter e Infraestructura completa para soportar sistemas Web de Fonasa, ClickEduca, entre otros.

A continuación se exponen las temáticas más relevantes y concurrentes captadas en las entrevistas a empresas.

4.2.1.1. Servicios de Cloud chilenos

- **Cloud chileno en comparación a servicios extranjeros**

Un consenso alcanzado entre las empresas entrevistadas son las limitantes que los proveedores de servicios Cloud con infraestructura en Chile (Claro, Entel, Sonda, etc) poseen en comparación a los grandes proveedores en el extranjero (AWS, Google Platform, Azure). Uno de los conceptos más atractivos de la tecnología Cloud es el uso bajo demanda y la capacidad de escalar la infraestructura a tiempo real, concepto asociado a las nubes públicas. La mayoría de las grandes empresas que prestan infraestructura Cloud localizada en Chile ofrecen nubes compartidas, las cuales permiten escalar pero en base a levantamientos de procesos. Esto implica que no poseen la facultad de levantar infraestructura de manera inmediata utilizando una plataforma, ni manejar costos variables de acuerdo al uso de recursos. Esto resulta contraproducente a la hora de levantar infraestructuras por periodos menores a un mes o aplicaciones con tráfico impredecible.

Manuel Suarez, gerente de la empresa **Synaptic,** comenta sobre las empresas que lideran hoy en día en servicios Cloud en Chile, "*No son malos desde el punto de vista de cómo fueron construidos, tienen todos los estándares, la infraestructura es buena, el problema son los servicios accesorios, los servicios de ingeniería*". Manuel relata que la plataforma de entrega de puntajes PSU (realizada por su empresa Synaptic) sería un proyecto inviable o con muchos gastos asociados innecesarios en caso de haber utilizado alguna de estas infraestructuras Cloud chilenas. Actualmente la plataforma de entrega de resultados PSU se encuentra alojada en AWS. Esta aplicación lleva operando 4 años, y se mantiene durante el año prácticamente deshabilitada hasta 3 meses previos a la entrega de puntajes. Durante estos 3 meses, se realizan pruebas de funcionamiento. Un par de semanas antes de la entrega, se levanta la infraestructura completa para entregar los resultados. Manuel nos comenta que esto hubiese sido muy difícil de trabajar con una infraestructura Cloud local dado que el cobro variable y los recursos bajo demanda son claves para el funcionamiento de la aplicación, y ninguno de los grandes proveedores chilenos brinda este servicio.

Juan Pablo Reyes, gerente de la empresa **LINETS**, respalda lo postulado por Manuel. Juan comenta que los servicios Cloud ofrecidos por los proveedores grandes chilenos (SONDA, ENTEL, CLARO), no proveen Clouds públicas sino que ambientes virtualizados mediante vmware que no permiten escalabilidad bajo demanda, sino que cobran un fijo mensual y se entrega una infraestructura fija con la capacidad de crecer bajo levantamiento de procesos y aumento del fee mensual. Mario Araneda, consultor senior en la empresa **INTESIS** nos comenta el mismo fenómeno. Señala que los grandes proveedores de Cloud en Chile no proveen el mismo tipo de nube pública que los grandes proveedores a nivel mundial, sino que proveen infraestructura mediante levantamientos de procesos en una mesa de ayuda.

A pesar de los comentarios con respecto a los grandes proveedores Cloud, Linets e Intesis están trabajando actualmente en nubes públicas chilenas. Linets se encuentra ad portas de lanzar su nube **BEEBOP**, Cloud chileno con datacenter en Santiago (Tier II) que vende un paquete fijo lo cual reserva una cantidad de recursos en el datacenter y del cual se puede escalar bajo demanda (BASE + OnDemand). Es similar al servicio que entrega Amazon mediante su servicio Reserved Instances. Por otro lado, INTESIS mediante la empresa internacional GIGAS, se encuentra en proceso de implementación de una nube pública en Chile, además Mario señala que Microsoft se encuentra en proceso de implementar su servicio Cloud de Azure en territorio nacional.

- **Performance Nacional vs Extranjero**

Uptime: En temas de **Uptime**, todos los entrevistados están de acuerdo con que los mejores resultados corresponden a empresas internacionales, en específico Amazon Web Service. Dependiendo de las necesidades de la institución, el uptime puede ser un factor decisivo a la hora de migrar servicios al extranjero. Mario comenta que muchas veces las instituciones (de manera interna), solicitan 100% de uptime para sus servicios, por lo cual es importante identificar qué componentes de este sistema realmente necesitan ese 100% dado que generalmente este no es el caso. Por otro lado Mario comenta que importante sería hacer una clasificación en término de exigencia de acuerdo de los diversos servicios que prestan las instituciones. (bajo, medio, alto).

Latencia: Otro punto fundamental en la performance nacional vs extranjero es la Latencia. Los tiempos de latencia con nubes chilenas son significativamente mejor al del extranjero. Juan Pablo nos comenta que las nubes públicas en desarrollo serán un gran avance en temas de latencia, ya que se podrá tener las ventajas de las nubes públicas extranjeras pero con menor latencia. Actualmente los proveedores locales llevan la ventaja en términos de latencia.

Tráfico: Un tercer factor identificado por los entrevistados es el **Tráfico** nacional vs internacional**.** En muchas situaciones ocurre que los enlaces internacionales se colapsan debido al alto uso de aplicaciones internacionales**,** en estas situaciones el uso de plataformas o sistemas con infraestructura fuera del país pueden resultar inviables. Juan Pablo nos comenta que el Banco Estado tiene exactamente este problema. LINETS desarrolló y mantiene una intranet del Banco Estado donde fue necesario alojarla en servidores chilenos dado que en las oficinas todo el enlace internacional contratado estaba copado por otro tipo de aplicaciones (youtube, spotify, viemo, etc). Mario comenta que una de las principales problemáticas de las nubes públicas fueras de Chile es el tema del tráfico internacional, indicando que Chile es uno de los pocos países que aun hace distinción entre tráfico nacional/internacional.

Otro punto relevante mencionado por Juan Pablo en relación al **tráfico** es el corte de enlace internacional. En el eventual caso de un corte de enlace internacional, Chile queda aislado de cualquier conectividad al extranjero. En este caso las opciones son o mantener el sistema en cuestión dentro del país o manejar un ambiente replicado con las instancias de alta disponibilidad en proveedores extranjeros y una como backup en Chile.

Es evidente que en la actualidad chilena existe un trade-off en términos de performance con las opciones nacional/extranjero, es por esto que es importante identificar las necesidades del cliente para poder obtener la performance más adecuada con respecto a sus requisitos.

- **Relación cliente/proveedores**

Manuel comenta que otra problemática de trabajar con proveedores Cloud chilenos tiene que ver con lo engorroso que es entablar una relación de trabajo, sobre todo para emprendedores. Las negociaciones con empresas chilenas de Cloud son engorrosas, costosas y duraderas. No así con empresas

extranjeras como Amazon o Google, donde ni siquiera es necesario celebrar un contrato para poder utilizar sus servicios Cloud.

4.2.1.2. Problemáticas de las Instituciones Públicas y los servicios Cloud

- **Datos fuera del territorio nacional**

Los 3 entrevistados enfatizaron la preocupación de las instituciones públicas con respecto a la tenencia de datos fuera del territorio nacional. Mario señala "Existe un temor historico en relación a los datos, dónde se encuentran y quiénes tiene accesos a estos". La preocupación con mantener datos fuera de Chile tiene relación con performance de sistemas y con la seguridad de la información.

Mario sugiere que el **primer punto a tratar por esta guía** debiese ser la aclaración de que no existe ninguna restricción legal que limite el almacenamiento de datos fuera del territorio nacional para instituciones públicas. La decisión de manejar datos dentro o fuera del país recae en la institución misma, en sus políticas internas y en el criterio de poder identificar qué tipo de datos requieren un mayor cuidado.

Manuel señala que es importante identificar qué **data** es la que se puede mantener fuera de Chile. En el caso de la plataforma de entrega de resultados PSU, poca relevancia tiene que la información se encuentre fuera del país en términos de seguridad, dado que es información pública. Pero mucha relevancia tiene que esté fuera dado los niveles de performance y escalabilidad que el proveedor Cloud ofrece y que la plataforma de entrega necesita para mantener un buen funcionamiento.

- **Seguridad de la información**

"El principal problema de las instituciones públicas es la privacidad de sus datos", Juan Pablo comenta. Independiente de si la información está dentro o fuera del país, si esta información es de carácter sensible, es necesario

mantenerla segura. Los entrevistados comentan diferentes maneras como mitigar este problema.

Manuel también abarca este tópico, en búsqueda de poder obtener los beneficios de los servicios Cloud internacionales para aquellas instituciones que no pueden sacar datos fuera del país. Manuel comenta “entendiendo la información o el sistema que se quiere implementar, se pueden llegar a realizar mezclas de arquitecturas para poder resguardar la información necesaria.”

Juan Pablo cuenta que en casos donde un cliente solicita un ambiente donde los datos necesariamente tengan que estar en Chile y son de carácter sensible, generalmente se implementa una **nube privada.** En contraparte a una nube pública, donde no se sabe realmente quien tiene acceso a la información. Otra buena solución es la utilización de **nubes híbridas**, donde la data de mayor sensibilidad se almacena en nubes privadas locales y el resto no sensible o a nivel de plataforma, se maneja fuera del país en función de obtener los múltiples beneficios (escalabilidad, reducción de costos, redundancia) que los proveedores internacionales de Cloud pública pueden ofrecer.

¿Es más seguro mantener la información en Chile que en el extranjero?

Manuel responde “*En general los sistemas acá están mal hechos, súper vulnerables, las redes de Entel son vulnerables, en general los proveedores no son expertos en ese sentido, el 95% de las instituciones públicas tienen datacenter, y datacenters que ni siquiera son datacenters, más bien closetcenters, sucuchos donde tiene los servidores lo que es mucho más riesgoso*”.

Por otro lado, Juan Pablo postula no se tiene una real certeza con respecto a qué ocurre con la información en caso de estar en manos de un proveedor extranjero en una nube pública.

- **Asignación de presupuestos**

Los presupuestos destinados a las instituciones públicas en base a consumo de servicios son considerablemente menores a los asignados a compra de infraestructura. Juan Pablo comenta que es un trabajo difícil invitar a las instituciones públicas a sumarse a tecnologías Cloud desde el punto de vista de presupuestos. A las instituciones públicas se les asigna bajo presupuesto para servicios pero un alto presupuesto para Hardware (dado que son activos). Lo cual las instituciones justifican mediante la compra de servidores y hardware relacionado. Juan Pablo comenta "la misma superintendencia me decía que no tiene plata para servicios, tengo que gastar la plata en hardware… ¿Qué me compro?"

Mario comenta que dada esta situación mencionada, es necesario revisar el esquema presupuestal que la institución pública tiene. Siempre los presupuestos de inversión son mayores a los gastos operacionales dado que se privilegian las inversiones medibles en tangibles. Mario señala que este análisis debiese ser realizado por la institución **como un segundo punto de la guía**, en conjunto con un análisis de costos.

Otra problemática que afecta a las instituciones públicas en materia de presupuestos son los **costos variables que una infraestructura Cloud pública involucra**. Las instituciones funcionan con presupuestos fijos, por lo cual el costo variable se transforma en una problemática, comenta Juan Pablo. Una solución a esta problemática es subcontratar el servicio Cloud mediante un tercero, donde el tercero cobra un fijo. El problema de esto es que claramente esta situación resulta de mayor costo.

4.2.1.3. Sugerencias sobre el desarrollo de la guía

A partir del ejercicio de la entrevista, los entrevistados entregaron información concreta en relación a como moldear la guía, ya sea directamente con qué

puntos ellos creen que son claves a mencionar o como estructurar estos puntos para generar una mejor coherencia.

Mario directamente sugirió los 2 primeros puntos que según su experiencia como consultor, son pasos necesarios e iniciales para pensar en comenzar a utilizar Cloud. Como fue mencionado anteriormente, Mario señala que **el primer punto de la guía es aclarar las legalidades a las instituciones públicas,** despejar cualquier duda con respecto a lo legal sobre el uso de las tecnologías Cloud por instituciones públicas, datos de terceros, etc. **El segundo punto es verificar la factibilidad de presupuesto que la institución maneja en relación a servicios a contratar**. A posterior, Mario sugiere realizar un **análisis de costos,** comparando las tecnologías Cloud vs el TCO (coste total de propiedad). Mario ha podido ver con el tiempo que "algún proyecto proyectado a menos de 24 meses, es un sí a la nube. De ser más, es muy probable que convenga comprar infraestructura a 5 años", refiriéndose al costo y no a los posibles beneficios de ambas opciones.

Manuel sugirió lograr plasmar **la diferencia entre migrar una infraestructura a la nube y utilizar la nube para un desarrollo en específico.** Gran parte de las instituciones públicas poseen datacenters propios, los cuales podrían llegar a ser migrados de manera completa o parcial a la nube. Por otro lado, las instituciones públicas constantemente están desarrollando soluciones informáticas para ser utilizadas por la ciudadanía, las cuales podrían ser alojadas en la nube. Manuel señala que estas 2 vertientes del tema competen diferentes puntos al momento de realizar una guía.

Otra sugerencia fue la implementación de algún tipo de base de datos o índice de referencias sobre **casos de éxito.** Una buena manera de abordar un proyecto Cloud es asesorarse por alguna otra institución que ya haya realizado el proceso, que ya conozca la tecnología y que pueda entregar un veredicto real de cómo enfrentar la situación.

4.2.1.3. Conclusiones

A partir de las entrevistas realizadas a las empresas de servicios Cloud se obtienen las siguientes conclusiones.

1. Identificar el **tipo de dato** que se quiere tratar es crucial para obtener una óptima **performance** y **seguridad** de la información.
2. Es necesario identificar los **niveles de servicio** que el sistema en cuestión necesita (disponibilidad, latencia, tráfico) para un óptimo funcionamiento.
3. A partir del entendimiento del tipo de dato (punto 1) y de los niveles de servicios (punto 2), evaluar las posibilidades de servicios Cloud en términos de los diferentes proveedores, servicios y arquitecturas que se encuentran disponibles.
4. Existe un **trade-off** entre el uso de Cloud local o extranjero que hay que tener en consideración al momento de seleccionar proveedores
5. Es necesario esclarecer los aspectos legales que conciernen a una institución pública al momento de utilizar tecnologías Cloud.
6. Es necesario realizar algún tipo de análisis de costo y revisión de presupuestos institucionales, en función de identificar la viabilidad económica de llevar a cabo la implementación Cloud que se desea evaluar.

A partir de lo mencionado por los proveedores, fue posible concluir pros y contras tanto para el trabajo con proveedores locales y extranjeros. Las tablas 4.11 y 4.12 establecen dicha comparación.

Tabla 4.11: Pros y contras de los proveedores de Cloud local desde el punto de vista de una institución pública

Proveedor Local	
Pros	**Contras**
Datos dentro de territorio nacional	Menor control de recursos
Menores tiempos de latencia	Escalabilidad de recursos bajo levantamiento de proceso
Conexión nacional menos colapsada (menor tráfico nacional)	Menor disponibilidad
Costo fijo	Mayor costo
	Engorrosa relación con cliente (contratos, levantamiento de
	datacenters hasta Tier 3

Tabla 4.12: Pros y contras de los proveedores de Cloud Extranjeros desde el punto de vista de una institución pública

Proveedor Extranjero	
Pros	**Contras**
Mayor disponibilidad	Enlace extranjero colapsado
Mayor control de recursos	Datos fuera de territorio nacional
Escalabilidad de recursos bajo demanda y en tiempo real	Mayor latencia
Simple de entablar relación con proveedor	Costos variables
Datacenters de mejor nivel (hasta Tier 4)	

4.2.2. Entrevistas a Instituciones Públicas

En contraste a las entrevistas a empresas relacionadas a los servicios Cloud, se realizaron entrevistas a instituciones públicas chilenas. Las instituciones

públicas además de ser el cliente en la relación, son el foco del desarrollo de esta guía, por lo cual obtener información de primera fuente de los coordinadores de tecnología de estas instituciones en relación a servicios Cloud es de suma importancia para el desarrollo de esta guía.

Son los coordinadores de tecnología de los organismos estatales los encargados de evaluar, contratar y muchas veces implementar las diferentes tecnologías disponibles para mejorar el servicio a la comunidad, por lo cual su experiencia es de suma importancia para encontrar los puntos de inflexión con respecto a la contratación de tecnologías Cloud.

Existen diversos tipos de organismos estatales, diferentes tamaños y enfoques, lo que repercute en el tamaño de los departamentos de tecnología. El tamaño de la institución es relevante, no para determinar la cantidad de recursos tecnológicos que podrían llegar a requerir, sino para poder evidenciar como un equipo pequeño, mediano o grande enfrentan contratar o no un servicio de esta naturaleza.

La muestra de instituciones fue pequeña, solo 3 instituciones fueron participes del proceso. Se seleccionaron 3 instituciones de diferentes tamaños para poder tener una muestra heterogénea en relación a esta característica. A pesar de la pequeña muestra, se realizó una entrevista al coordinador de la Unidad de Modernización y Gobierno Digital (UMGD) **Andrés Arellano**. Esta institución es la encargada de incentivar el uso de tecnologías a nivel estatal para mejorar procesos y entregar mejores servicios. La UMGD lanzó el año 2013 un documento para incentivar el uso de tecnologías Cloud a nivel estatal, con recomendaciones para la contratación de servicios. Esta entrevista sirvió para en cierta manera obtener una mejor idea del global de las instituciones públicas ya que son ellos los encargados de analizar las diferentes necesidades de las instituciones y cómo las tecnologías de la información pueden ayudar a estas problemáticas.

Para abarcar a las instituciones con departamentos de TI de menor envergadura, se entrevistó a **Flavia Gómez**, Jefe Unidad Sistemas y Tecnologías de Información del **Hospital Roberto del Rio**. Y para cubrir una institución de gran tamaño, se entrevistó a **Johnny Heiss,** coordinador de tecnología **del Ministerio de Educación.**

A continuación se exponen las temáticas más relevantes y concurrentes captadas en las entrevistas a organismos el Estado.

4.2.2.1. Instituciones públicas y servicios Cloud

- **Servicios Cloud e infraestructuras Contratadas**

Las 3 instituciones entrevistadas tienen diferentes experiencias con las tecnologías Cloud. Jonny comenta que actualmente en el ministerio tienen diferentes servicios Cloud corriendo, tanto mediante proveedores locales como proveedores internacionales. Jonny comenta que todos los sitios web del ministerio están alojados en datacenters de **SONDA.** También comenta que tienen contratado los servicios de infraestructura de **Azure** de la empresa Microsoft**.** También el Ministerio tiene **SaaS** provisto por la empresa chilena de Cloud Computing **Zona Nube**. Jonny señala que está a favor del aumento del uso de tecnologías Clouds. “mientras más Cloud computing, mejor”. Jonny también menciona el caso del Centro de Perfeccionamiento, Experimentación e investigaciones Pedagógicas (CPEOP) donde se han adquirido sistemas de apoyo a la docencia, principalmente mediante SaaS, con lo cual entregan apoyo a más de 200.000 mil profesores.

Flavia comenta que para ellos es inviable poder acceder a un servicio de Cloud Computing dado que el enlace de conexión a internet es de muy mala calidad, por lo cual tener funcionalidades dependientes de internet es inviable para ellos. La razón de este enlace es debido a que ellos como institución no poseen la facultad de seleccionar proveedores, esto depende del Ministerio de Salud, el cual a partir de políticas, regula datacenters y servicios que sus

subdivisiones manejan. Situación compleja, ya que ellos como hospital evidencian las ventajas de los servicios Cloud, especialmente para los pacientes, los cuales se podrían ver beneficiados con las ventajas que estos servicios ofrecen. Actualmente manejan un datacenter interno.

Andrés no comenta sobre su propia institución, sino que de casos de otras instituciones. Relata la situación de las instituciones de mayor tamaño, donde estas son capaces de implementar servicios Cloud con gran facilidad dado lo experimentado de sus departamentos de TI, y el caso de instituciones más pequeñas donde la tarea resulta más completa. Actualmente la UMGD proporciona asesorías a estas instituciones para poder facilitar la contratación de estos servicios.

Por otro lado, Andrés comenta que la UMGD busca centralizar ciertos servicios para así entregar soluciones SaaS a las instituciones públicas de manera estandarizada, aprobadas y listas para utilizar. A raíz de la ley del lobby, la UMGD **desarrolló una plataforma para cumplir con las regulaciones de transparencia**. Este proceso es necesario para todas las instituciones públicas, por lo cual la unidad desarrolló un software para ser utilizado a modo SaaS por todos los organismos del Estado. Como detalle, Andrés comenta que esta plataforma está alojada en Amazon Web Services, para aprovechar todos los beneficios de escalabilidad de este proveedor.

- **Contratación de servicios Cloud**

Andrés señala que la opción por defecto para adquirir servicios Cloud por los organismos públicos es el “Convenio Marco de servicios de datacenter y asociados”, mediante este proceso las instituciones públicas se pueden asegurar que los proveedores seleccionados están calificados a nivel gubernamental para ser utilizados por organismos públicos. Andrés califica al convenio marco como “el avance más sustantivo para utilizar la nube”.

Jonny señala que todas las contrataciones realizadas por el Ministerio de Educación se han hecho a través del convenio marco. Proceso que facilita el proceso de licitación que anteriormente se realizaba.

- **Proveedores nacionales vs internacionales**

Jonny comenta que él no tiene ninguna preocupación con mantener la información fuera de Chile, lo cual no es lo normal ni en el Ministerio ni en Chile. "*A la gente le da susto que los datos estén alojados afuera…Hay gente en el Ministerio que se pone nerviosa teniendo los datos en el extranjero, lo cual me parece absurdo*". Jonny argumenta que las empresas extranjeras no tienen ningún interés en leer la información que almacenan y que por lo contrario, él no tiene ninguna desconfianza de estos proveedores. Actualmente Jonny ha implementado múltiples servicios Cloud, tanto local como en el extranjero. Jonny comenta que en su caso, la principal razón del uso de Cloud extranjero tiene que ver con las licencias de los softwares que se requerían utilizar (Licencias ERP de Microsoft), por lo cual Azure era la opción.

Desde el punto de vista de Andrés, ellos en la UMGD promueven el uso de Cloud Computing, ya sea nacional o extranjero. Andrés señala que es necesario aclarar que la normativa de seguridad de la información indica que cada institución debe tener sus propios protocolos para el resguardo de información. Protocolos de almacenamiento y resguardo de información, disponibilidad de sistemas, etc. En otras palabras, de manera general no existe ninguna prohibición del uso de tecnologías Cloud, ya sea nacional o extranjera para las instituciones públicas. Postula que cualquier proveedor que se encuentre en el **Convenio Marco Servicios de Data Center y Asociados**, independiente que utilice infraestructura en el extranjero, el convenio marco asegura a las instituciones públicas que la contratación que se está realizando está bien normada con respecto a las leyes generales que gobiernan a las instituciones del Estado. El convenio marco es el método por defecto que los

organismos del Estado debiesen utilizar para la contratación de servicios Cloud.

- **Seguridad de la información**

Jonny comenta que para poder establecer una buena seguridad de la información con el proveedor es clave entender primeramente qué tipo de información es la que se está tratando. Una vez “catalogada” el tipo de información que se desee tratar, el trabajo de identificar qué tipo de proveedor o arquitectura utilizar es considerablemente más fácil. En general, existe información con el objetivo de ser compartida y pública, por lo cual Jonny se queda tranquilo con respecto a la seguridad de esta información. En caso de ser información de carácter privado, Jonny realiza contratos con las cláusulas de seguridad correspondientes al grado de seguridad necesaria para la información. Con respecto a la posibilidad de los proveedores de utilizar la información, Jonny no considera relevante este tema.

Andrés comenta respecto del apartado de seguridad de la información de la guía Cloud de la UMGD. Para darle clasificación de tipo de seguridad a la información, la guía proporciona un cuestionario con el fin de poder identificar el grado de seguridad que la información necesita. También la guía proporciona todas las leyes involucradas en el uso de Cloud Computing por las instituciones públicas referentes al trato de información de personas naturales por terceros.

Una temática que es clara, es el establecimiento de cláusulas de seguridad con respecto a la información. Andrés señala que además la guía proporciona un anexo con un modelo de contrato con cláusulas estándar a nivel de institución pública, para que los organismos utilicen al momento de realizar contrataciones Cloud.

Con respecto a las normas de seguridad o protocolos que las instituciones públicas debiesen seguir, Andrés aclara que la normativa de seguridad de la

información indica que cada institución debe tener sus propios protocolos de resguardo de la información.

Flavia comenta que el tema de la seguridad para ellos como hospital es de extremo cuidado. A nivel de organización, el hospital maneja información confidencial de personas naturales, la cual de ser difundida, podría perjudicar a los pacientes involucrado (utiliza como ejemplo los pacientes con VIH). Para Flavia es complejo mantener sistemas donde no se tiene conocimiento o regulaciones con respecto a qué se hace con la información almacenada en estos sistemas, especialmente con proveedores internacionales donde a pesar de las cláusulas establecidas, existen diferentes leyes con respecto al acceso a la información. Por otro lado, los beneficios de plataformas de difusión de información a pacientes mediante internet sería un gran servicio a la comunidad ya que facilitaría la entrega de resultados, reduciendo el número de visitas y tiempos de espera.

- **Documento "Buenas prácticas en materia de contratación de Servicios de Computación en la Nube (Cloud Computing) al interior de la Administración del Estado"**

Andrés postula que este documento fue un muy buen avance en la relación Cloud y organismos del Estado. No obstante, el documento deja mucho análisis a realizar por parte de las instituciones, por lo cual la UMGD reconoce la necesidad de generar nuevos documentos de apoyo a adopción de tecnologías Cloud.

Andrés señala que documentos futuros debiesen establecer **criterios concretos y taxativos,** que busquen disminuir el análisis a realizar por los organismos de Estado. El documento ideal permitirá a una institución ingresar ciertos criterios o inputs, con respecto a la necesidad de la institución, y entregar un output con una solución concreta. Para lograr esta tarea sería necesario tener categorizados sistemas "tipo", y estos poder asociarlos a una

solución Cloud pre-aprobada, para así facilitar el trabajo de las instituciones públicas, trabajo que la UGMD aún no ha realizado.

- **Tipos de instituciones Públicas**

Existen distintos niveles de madurez en los equipos de TI de las instituciones públicas. Muchos de ellos tienen un nivel de expertise bastante alto, el cual les permitiría implementar una estrategia Cloud por si solos. Otras instituciones tienen departamentos de TI de mediana envergadura, los cuales se apoyan mucho en los proveedores. Estos equipos tienen la capacidad de ser una buena contraparte a los proveedores, sacando provecho y valor a lo que los proveedores tienen para entregar. En el caso de las instituciones de menor envergadura, Andrés señala que es aquí donde se producen las mayores brechas, tanto como de presupuesto como de malas asesorías por falta de conocimiento.

El otro criterio tiene que ver con el nivel de seguridad requerida en base al tipo de información que las instituciones manejan. Existen rubros como los hospitales donde la gran mayoría de la información de personas naturales es de carácter privado. Otras, donde la información de personas y el procesamiento de la misma tienen fines públicos. En común las instituciones comparten los datos a nivel interno, que naturalmente son privados, pero dependiendo de la institución pueden tener diferente grado de privacidad.

4.2.2.2. Conclusiones.

A partir de las entrevistas realizadas a las Organizaciones estatales se obtienen las siguientes conclusiones.

1. Existen **diferentes tamaños de organizaciones públicas**, las cuales requieren diferente tipo de soporte para ayudar la implementación de tecnologías Cloud.

2. Son las instituciones con departamentos de TI de menor y mediana envergadura las que necesitan mayor asesoría con respecto a contratación de servicios Cloud.
3. **Se necesita un documento taxativo** que reduzca el análisis que los organismos públicos deben realizar para la decisión sobre contratación de servicios Cloud.
4. Sería útil tener una **categorización de sistemas "tipo**", asociados a una solución Cloud predeterminada.
5. Actualmente son múltiples las organizaciones públicas que están utilizando servicios Cloud, tanto de proveedores nacionales como internacionales.
6. Existe motivación e interés por parte del gobierno y de los mismos organismos públicos por promover el uso de tecnologías Cloud.
7. No existen prohibiciones a nivel gubernamental con respecto al uso de tecnologías Cloud o del almacenamiento de información fuera de territorio nacional por organismos públicos. Son las propias instituciones las encargadas de generar sus propios protocolos y políticas con respecto a la seguridad de su información.
8. El método por defecto de **contratación de servicios** Cloud para las instituciones públicas es el **Convenio Marco de datacenter y servicios asociados**.

4.2.3. Análisis de los 10 puntos de la guía Practical Guide to Cloud

A cada uno de los entrevistados se les realizó un cuestionario sobre los 10 puntos postulados en la guía Practical Guide to Cloud Computing, en función de la relevancia en cómo estos puntos se podrían aplicar a la situación de los organismos públicos chilenos, que deberían saber o manejar a nivel de conocimiento y preparación para poder implementar servicios Cloud.

Se les solicitó a los entrevistados evaluar del 1-5 cada uno de estos puntos (siendo 1 lo menos significativo) y que se comentara el punto en cuestión. La tabla 4.13 contiene las calificaciones promedio de los entrevistados en relación a los 10 puntos de la guía.

Tabla 4.13: Calificaciones promedio otorgadas por los entrevistados a los 10 puntos de la guía Practical Guide to Cloud Computing

Puntos	Calificación Promedio
1. Preparación de un equipo	**4**
2. Desarrollar una estrategia Cloud	**4**
3. Tipo de Arquitectura Cloud	**1**
4. Tipo de servicio Cloud	**1**
5. Encargado de desarrollar, implementar y desplegar el ambiente Cloud	**3**
6. Acuerdos de servicio	**4**
7. Resolución de problemas de Seguridad de la información	**5**
8. Integración de servicios Cloud con sistemas pre-existentes	**3**
9. Realizar una prueba de concepto	**2**
10. Administración del ambiente Cloud	**3**

A partir de los comentarios de los entrevistados con respecto a los puntos y su vínculo con la situación a tratar, se llegaron a las conclusiones que se presentan a continuación.

4.2.3.1. Conclusiones

1. En general se requiere la mayor participación de proveedores en el proceso Cloud e involucrar lo necesario a los organismos públicos. Los

organismos públicos deben focalizarse en generar soluciones que mejoren los servicios públicos y dejar a los proveedores que se enfoquen en lo específico.

2. Con respecto a la Preparación de un equipo (**punto 1**) se re-enfoca el propósito original del punto en función de establecer una dinámica de trabajo en conjunto del organismo público con un posible asesor/consultor, el cual aborde los puntos de diseño de solución, análisis de costos, desarrollar, implementar y desplegar el servicio y a futuro posiblemente administrarlo (de ser necesario). Lo anterior, enfocado a las instituciones sin el departamento de TI de suficiente envergadura para abordar el proyecto. Los organismos con grandes departamentos de TI como el Ministerio de Educación poseen equipos capacitados para abordar este tipo de implementaciones.
3. Se concluye que en general, los puntos mencionados en la guía deben ser abordados de manera diferente dependiendo del tamaño de los departamentos de TI de las diferentes instituciones públicas.
4. Los puntos de la guía van enfocados a realizar un cambio radical de paradigma de almacenamiento de información. Migración completa de infraestructura física a Cloud. A partir de lo comentado por los entrevistados, **la orientación de guía a realizar debiese ser en función de implementación de tecnología en torno a proyectos**, para así orientar a una futura migración completa de los sistemas que ameriten.
5. En general, todos los puntos que trata la guía son relevantes y necesarios. La diferenciación está en si estos puntos son realmente relevantes para la institución o corresponden a análisis a realizar por el proveedor de apoyo.
6. Juan Pablo señala que existe un tópico que debiese ser tratado en la guía bajo el nombre de **diseño de la solución**, en el cual se pueden englobar los puntos **3, 4, 8**. Estos puntos son resultados del análisis de los requerimientos de la institución y del diseño que se propone para abordar la solución.

7. Los puntos técnicos **3 y 4**, sobre la tecnología Cloud (**arquitectura y servicios**), obtuvieron la calificación de relevancia más baja. Esto se explica dado que la tendencia de los participantes, en especial las empresas, se enfoca a que las instituciones se concentren en generar soluciones y utilizar las herramientas que mejoren sus servicios públicos, dejando a las empresas proveedoras encargadas de diseñar la solución.
8. El punto 9, en relación a la prueba de concepto catalogado fuera de lugar dado que los sistemas Cloud deben funcionar y no ameritan una prueba de concepto, a menos que sea la migración de una infraestructura completa y compleja. Testing es tan necesario como en cualquier otro tipo de implementación.
9. Para todos los entrevistados los acuerdos de servicio son un punto necesario. Cabe destacar que los grandes proveedores internacionales no manejan acuerdos de servicio en base a requerimientos del cliente ya que estos poseen sus propios acuerdos de servicio.

5. **Capítulo 5:** Guía Metodológica para el uso de Cloud Computing para instituciones públicas chilenas

Para poner en práctica una iniciativa Cloud a nivel estatal es necesario establecer ciertos procedimientos comunes para que las instituciones públicas hagan uso de. Esta guía metodológica establece los pasos a seguir para facilitar el proceso de contratación Cloud para una institución pública. Estos pasos también pueden ser utilizados para identificar si es o no posible utilizar un ambiente Cloud para una posible solución que se desee abordar. La siguiente guía está construida a partir de material bibliográfico referente a la temática complementada con entrevistas a involucrados en el tema (ver capítulo 4). A partir de este material se extrajeron los puntos abordados en la guía.

Esta guía va dirigida a los encargados de TI o responsables de implantar posibles mejoras a nivel informático dentro de las instituciones públicas.

Índice Guía

5.1. Aclaraciones legales 87
5.2. Estrategia Cloud 92
5.3. Equipo Asesor 94
5.4. Evaluación económica Cloud (TCO) 96
5.5. Diseño de Solución 106
5.6. Contratación Cloud 122
5.7. Resumen: Guía Metodológica para el uso de Cloud Computing en instituciones públicas chilenas 135

5.1. Aclaraciones legales

Existe incertidumbre respecto a qué limitantes legales existen en la utilización de servicios Cloud por parte de los organismos del Estado. Las organizaciones públicas en muchos casos manejan información de carácter sensible, la cual se encuentra regida por ciertas leyes que deben ser consideradas al momento de realizar una implementación Cloud. Este primer punto busca aclarar estas dudas, entregando un resumen de las leyes que involucran el uso de tecnologías Cloud y sus correspondientes implicancias.

5.1.1. Ley N°19.886, sobre Protección de la Vida Privada o Protección de Datos de Carácter Personal

El **primer aspecto legal** a cubrir (por obvio que lo parezca) es el cumplimiento de la **ley N° 19.886,** o ley de **Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios** (Ley 19.866, 2003)**.** Ley que regula los contratos en relación a suministro de bienes muebles, y de los servicios que requieran los organismos para el desarrollo de sus funciones. Dado que la contratación de tecnologías Cloud cae en la materia de servicios, el contrato celebrado entre las partes debe estar normado por esta ley.

Frente a cualquier duda sobre la materia, conviene destacar que la Dirección de Compras y Contratación Pública tiene, dentro de sus funciones, el deber de asesorar a los organismos públicos en la planificación y gestión de sus procesos de compras y contrataciones y promover la máxima competencia posible en los actos de contratación de la Administración. En este sentido, siempre es factible que, frente a cualquier duda sobre el alcance de esta normativa, se efectúen consultas a dicho órgano.

Con respecto a esta ley, es importante destacar los **artículos 14 y 15 de la Ley N° 19.886** y los **artículos 74 y 76** del reglamento de dicha ley, disposiciones que, en general, señalan que no se permite que el contratista ceda total o parcialmente del contrato y que sólo permiten una subcontratación

parcial de los servicios. Este caso es común en materias Cloud ya que muchos prestadores de servicios chilenos son “resellers” o asociados de los prestadores de los servicios Clouds, por lo cual es necesario que el tercer oferente represente legalmente al prestador del servicio Cloud para efectos de suscribir el contrato a nombre de este último. Lo anterior se debe al hecho que es el prestador del servicio Cloud –y no el tercer oferente− quien realmente ejecuta la obligación de llevar adelante el servicio, almacena información, protege la confidencialidad de los datos del órgano contratante, etcétera (UMGD, 2014).

5.1.2. Datos personas naturales (Ley N° 19.628 y Dictamen N° 43.866)

En muchos casos es necesario almacenar información de personas naturales en los servicios Cloud en cuestión, la **Ley N° 19.628** permite que los órganos pueden tratar datos personales respecto de las materias de su competencia y sin consentimiento del titular, en la medida que cumplan con los principios y normas que establece dicha ley. También la ley permite “[los] órganos o servicios públicos, en conformidad a lo dispuesto en el artículo 8° de la Ley N° 19.628, [pueden] encargar el tratamiento de los datos a un tercero, que tendrá la calidad de mandatario” (Ley 19.628, 1999).

En función de aplicar la **ley 19.628**, es necesario que el contrato celebrado con el proveedor contemple las siguientes consideraciones (UMGD, 2014):

- Obliguen al prestador a adoptar “[…] los resguardos necesarios para que tal información no sea utilizada en finalidades distintas a las deseadas por el servicio”[1].

[1] CONTRALORÍA GENERAL DE LA REPÚBLICA, Dictamen N° 43.866 de 3 de octubre de 2003 y Dictamen
N° 57.623 de 22 de noviembre de 2004.

- Protejan la debida confidencialidad de los datos, a fin de que "…no se vulneren, además, las disposiciones que regulan la información de carácter secreto o reservado"[2]. Particular atención se debe poner al artículo 7 de la Ley N° 19.628, el que obliga a las personas que están en el tratamiento de los datos (en este caso, el prestador del servicio Cloud), a guardar reserva o secreto de los datos que están siendo objeto de tratamiento; y
- Ordenen al prestador del servicio adoptar, en su calidad de mandatario, "[…] todas las medidas, tanto organizativas como técnicas, para resguardar la integridad, confidencialidad y disponibilidad de los datos contenidos en sus registros con la finalidad de evitar la alteración, pérdida, transmisión y acceso no autorizado de los mismos"[3]. Lo anterior, atendido al deber legal del responsable de las bases de cuidar de tales datos con la debida diligencia, haciéndose responsable de los daños (artículo 11 de la Ley N° 19.628)
- Que hagan civilmente responsable al prestador del servicio Cloud acerca de la filtración o uso inadecuado de los datos personales que le son confiados.
- Que obliguen al prestador del servicio y sus empleados cumplir con las disposiciones establecidas por la Ley N° 19.628.

Cabe destacar que el cumplimiento de estas leyes es a nivel país. Cualquier proveedor fuera del territorio nacional no se vería implicado en esta legislatura.

---

[2] CONTRALORÍA GENERAL DE LA REPÚBLICA, Dictamen N° 43.866 de 3 de octubre de 2003.
[3] CONSEJO PARA LA TRANSPARENCIA, 'Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la Administración del Estado'. *Op.Cit.*,p. 15.

5.1.3. Ley N°20.285, sobre Acceso a la Información Pública

En muchos casos los organismos públicos manejan información confidencial respectiva al artículo 21 de la **Ley N°20.285.** Esta información se considera dentro de la ley en las siguientes causales (Ley 20.285, 2008):

- Su publicidad, comunicación o conocimiento afecte el debido cumplimiento de las funciones del órgano requerido, particularmente.
- Cuando su publicidad, comunicación o conocimiento afecte los derechos de las personas, particularmente tratándose de su seguridad, su salud, la esfera de su vida privada o derechos de carácter comercial o económico.
- Cuando su publicidad, comunicación o conocimiento afecte la seguridad de la Nación, particularmente si se refiere a la defensa nacional o la mantención del orden público o la seguridad pública.
- Cuando su publicidad, comunicación o conocimiento afecte el interés nacional, en especial si se refieren a la salud pública o las relaciones internacionales y los intereses económicos o comerciales del país.
- Cuando se trate de documentos, datos o informaciones que una ley de quórum calificado haya declarado reservados o secretos, de acuerdo a las causales señaladas en el artículo 8º de la Constitución Política.

En caso de haber información de estas características, se debe asegurar la confidencialidad de esta información mediante clausulas en el contrato vinculante.

5.1.4 Ley N° 17.336, sobre Propiedad Intelectual

Se debe velar por que el prestador de servicios respete lo establecido por la ley chilena con respecto a la propiedad intelectual (LEY N° 17.336, 1970). Es importante destacar que tanto propiedad intelectual de terceros como de la misma institución, podrán ser utilizados por el prestador de servicio para

efectos de la ejecución de las obligaciones emanadas en virtud de lo establecido bajo contrato.

5.1.5 Proveedores en el extranjero

En el caso de la utilización de proveedores que almacenan datos en el extranjero, las leyes mencionadas en los puntos anteriores, no tienen validez dado que predominan las leyes extranjeras del país donde se encuentren los datacenters. Como consecuencia, esta situación puede dejar información confidencial expuesta en base a diferentes leyes que permitan el acceso a esta información confidencial. Un ejemplo de esto es la **ley USA PATRIOT,** donde en sospecha de terrorismo, el gobierno de los Estados Unidos puede solicitar acceso a información de privados. Este ejemplo no deja de ser relevante ya que los proveedores de servicios Cloud de mayor envergadura se encuentran localizados en este país.

Cabe destacar que **no existe ninguna prohibición desde el ámbito legal sobre las organizaciones públicas para el uso de tecnologías Cloud alojadas fuera del territorio nacional.** Mientras las consideraciones abarcadas en los puntos anteriores sean contempladas, el uso de infraestructura extranjera queda a libre criterio de las propias instituciones. La toma de esta decisión debe ser basada en el tipo de información que se desea almacenar, los términos y condiciones que el proveedor en cuestión implementa, y si estos abarcan los resguardos necesarios a dicha información (ver punto 5.5.1). No es recomendable descartar a los proveedores Cloud extranjeros sin revisar y entender que información es la que se desea guardar y si estos proveedores satisfacen los requerimientos en base a la información.

Por otro lado, **la normativa de la seguridad de la información establece que cada servicio público debe tener sus propios protocolos de resguardo de información**. Esto implica que internamente muchas de las instituciones puedan tener como política la no utilización de datacenters fuera

del país, por lo cual es necesario revisar los protocolos particulares de la organización para verificar el posible uso de proveedores en el extranjero. Para obtener un ejemplo, revisar las política seguridad de información del Ministerio de Salud (Seguridad de la Información, 2015).

5.2. Estrategia Cloud

La necesidad de infraestructura a nivel público ha ido en crecimiento a través de las últimas décadas. Son múltiples las instituciones que a través de los años han adquirido infraestructura que hoy en día se encuentra obsoleta, lo cual se traduce en una increíble acumulación de hardware y altos costos de mantención asociados a este. Por otro lado, existen organismos que por razones de presupuestos, no han podido financiar infraestructuras o software potencialmente beneficioso para su operación. Esta proliferación de compra de infraestructura, sumada al poco desarrollo tecnológico Cloud a nivel país, ha perjudicado la adaptación de nuevas posibilidades en materia Cloud a nivel gubernamental.

Como fue mencionado en el capítulo 4 (punto 4.1.1), las organizaciones del Estado poseen un nivel de madurez insipiente en relación al uso de tecnologías Cloud. Por lo tanto, si existe una intención de promover el uso de tecnologías Cloud, es necesario introducir a las organizaciones en el tema, y los potenciales beneficios asociados a su utilización.

5.2.1 Visión

Existe una visión a nivel gobierno, establecida por la Unidad de Modernización y Gobierno Digital (UMGD), la cual busca promover el uso de tecnologías Cloud en función de aprovechar los posibles ahorros de costos económicos, tiempo en gestión de plataformas electrónico, escalabilidad, elasticidad, alto rendimiento, resistencia y seguridad. “La Unidad de Modernización y Gobierno Digital recomienda, como regla general, la adopción de este tipo de soluciones

tecnológicas al interior de los órganos de la Administración del Estado. Ello atendido a que dicha tecnología impacta positivamente en la forma en que tales órganos ejercen sus funciones, con plena consonancia con los principios de eficacia y eficiencia que considera el artículo 3° de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado" (UMGD, 2014).

Parte de la visión que toma esta guía, en función a las entrevistas realizadas a los proveedores Cloud, es fomentar la focalización de los organismos del Estado en el core de su negocio. Parte del paradigma Cloud refleja esta postura. La idea es lograr que las organizaciones del Estado se focalicen en entregar un servicio de calidad a la ciudadanía, proponiendo y mejorando sistemas que permitan facilitar accesibilidad, disponibilidad y mejores rendimientos a las herramientas utilizadas por la ciudadanía. Para esto es necesario confiar y dejar a empresas terceras, expertas en tecnología, tomar cargo de ciertos aspectos tecnológicos. En el caso específico de esta memoria, las tecnologías Cloud.

5.2.2 Estrategia

La estrategia que busca fomentar esta guía postula una adopción de modelos Cloud por parte de los organismos públicos del Estado, mediante una migración paulatina de sus servicios, en base a proyectos específicos y la utilización de tecnologías Cloud para los mismos. En respuesta al nivel incipiente de desarrollo Cloud a nivel institucional (ver punto 4.1.1), se entiende que una migración completa de infraestructura es una tarea compleja. El camino que busca esta guía va en función de comenzar a realizar proyectos específicos, ya sea una nueva solución o la migración de una existente, mediante la utilización de **IaaS** y **SaaS**.

5.3. Equipo Asesor

Es importante que los organismos públicos definan un diseño, implementación y mantenimiento de una futura solución Cloud. También es necesario lograr identificar la viabilidad desde el punto de vista económico y de implementación de dicha solución y poder compararla con otras disponibles en el mercado. Existen ciertos departamentos de TI a nivel estatal que poseen el “know how” suficiente para llevar a cabo estas tareas, pero este no es el escenario predominante a nivel global.

Esta guía promueve el uso de una tecnología que por esencia busca externalizar ciertos servicios, permitiendo a los organismos concentrarse en el “core” de su negocio. En el caso de los organismos públicos, su principal objetivo es entregar servicios de calidad a la ciudadanía, donde el adjetivo calidad mantiene un nivel de subjetividad el cual se busca mejorar. Es por esto que se sugiere la utilización de proveedores o asesores para abordar una solución Cloud, buscando mejorar la calidad del servicio mediante diseño, implementación y mantención de soluciones desarrolladas por expertos en la temática.

Existen diferentes formas en la cual una organización pública puede acceder a asesorías o apoyo de expertos en la temática en cuestión, ya sea mediante soporte estatal o mediante soporte de empresas especializadas. A continuación se presentan algunas opciones mencionadas.

5.3.1. Convenio Marco de Data Center y Servicios Asociados

Este convenio marco contempla una serie de empresas relacionadas a la temática Cloud, las cuales se encuentran pre-aprobados a nivel gubernamental para el uso estatal de los servicios que estas entregan. Mediante el portal Mercadopublico, los organismos del Estado tienen acceso

a un listado de proveedores Cloud disponibles, los cuales se encuentran diferenciados en dos categorías, el primero de Data Center y Servicios Complementarios y el segundo de Software como Servicio (SaaS), Plataforma como Servicio (PaaS) e Infraestructura como Servicio (IaaS).

Mediante este convenio es posible acceder a diferentes proveedores Cloud sin necesidad de levantar un proceso de licitación, lo cual facilita su accesibilidad. Más allá de la categorización de los mismos, el convenio permite mediante una plataforma a través del Mercadopublico, acceso a proveedores de servicios que utilizan la tecnología Cloud para complementar la solución de un sistema. Es entre estos proveedores donde se debe buscar un aleado para el análisis, diseño de solución, y posiblemente implementación y mantenimiento del sistema. Cabe destacar que dentro del espectro de proveedores disponible, existen diferentes niveles de expertise. Algunos de proveedores actúan como “resellers” de servicios Cloud, otros prestan servicios Cloud con infraestructura propia. También existen proveedores que poseen servicios Cloud propios y además implementan soluciones como “resellers”, en búsqueda de satisfacer los requerimientos del cliente de mejor manera. Idealmente se sugiere relacionarse con un proveedor diverso, que contemple diferentes herramientas para poder entregar un mejor diseño de la solución a la problemática planteada.

En las entrevistas realizadas se entrevistaron a 3 proveedores de soluciones TI (todos parte del convenio marco) que calzan con el perfil que se busca para llevar a cabo el apoyo a una implementación Cloud. La empresa **SYNAPTIC** realiza soluciones informáticas utilizando diferentes herramientas. No poseen su propio servicio de Cloud Computing, pero realizan implementaciones de diversos proveedores Cloud de acuerdo a las necesidades del cliente SYNAPTIC es la empresa por detrás de la plataforma de entrega de puntajes PSU. La empresa **LINETS**, se encuentra en participación del segundo llamado

a licitación para ser parte del convenio marco. LINETS posee un servicio Cloud propio denominado BeeBop (Cloud pública y privada chilena) y además realizan implementaciones a nivel internacional. La empresa **INTESIS** ofrece servicios de datacenter, Cloud público chileno mediante la empresa GIGAS y servicios de asesoría. Son este tipo de empresas las que se sugiere asesorarse para llevar a cabo una implementación Cloud, empresas con experiencia con organismos del Estado con diferentes herramientas que permitan obtener un mejor diseño de solución.

5.3.2. Asesorías UMGD

La Unidad de Modernización y Gobierno Digital ofrece asesorías a las organizaciones públicas, para así facilitar procesos de implementación de herramientas TI. En búsqueda de promover el uso de tecnologías Cloud, la UMGD busca emparejar la cancha para los distintos tamaños de organizaciones públicas, brindando apoyo a las de mediana y pequeña envergadura mediante su área de Asesoría y estudios.

La UMGD posee conocimientos en tema de soluciones Cloud para problemáticas estatales, muchos de estos expuestos en la guía Buenas prácticas en materia de contratación de Servicios de Computación en la Nube (Cloud Computing) al interior de la Administración del Estado, guía que también puede ser usada como fuente asesora para una implementación Cloud.

5.4. Evaluación económica Cloud (TCO)

El siguiente punto busca proporcionar un modelo de cálculo de costos para obtener una estimación de los costos involucrados en la adquisición de un servicio y también realizar una comparación económica entre una solución inhouse y su versión Cloud.

5.4.1. Revisión de presupuestos

Un punto relevante, previo a la realización de un TCO, es revisar la distribución de presupuestos TI. Por lo general, los departamentos de TI tienen presupuestos orientados a la adquisición de activos, lo que en TI se traduce en infraestructura/hardware y software. Dado que las tecnologías Cloud son un servicio, es necesario revisar los presupuestos asignados a servicios y ver si estos permiten algún tipo de financiamiento Cloud.

Otro factor a tener en consideración es el modo de cobro variable en que la tecnología opera. Es importante tener en mente que una de las principales ventajas de la tecnología Cloud es el uso bajo demanda de recursos, y su uso puede ser beneficioso para múltiples sistemas. En caso de no poder abordar un costo variable, es posible utilizar modelos de costo fijo y que en para casos específicos, se aplique el modelo de costo variable sobre el costo fijo. Otra manera de abordar esto es tercerizar el servicio Cloud, solución de mayor costo ya que la empresa tercera se asegura de cobrar un fee que le permita marginar independiente del costo variable que ellos pagan.

5.4.2. Análisis de Costos (TCO)

Realizar un análisis de costo entre las opciones a implementar es de vital importancia para poder dimensionar si realmente es factible la implementación de un sistema. También es necesario para poder comparar, desde un punto de vista económico, las diferentes opciones disponibles. Los escenarios que se toman en consideración para comprar, son los siguientes:

5.4.3 Implementación de solución Cloud

5.4.4 Implementación de sistema inhouse

5.4.5 Migración de sistema inhouse a Cloud

Se propone la utilización del modelo de TCO desarrollado por (Solar et al, 2012). Donde se propone un modelo de TCO orientado a las organizaciones públicas chilenas, realizado en base a un compilado de gastos en TI de ciertos

ministerios, obtenidos de la Dirección de Presupuestos (DIPRES), Chile compras y un cuestionario Web. Como complemento a este análisis TCO, se agregan algunos puntos propuestos por en el trabajo Value of Cloud Security: Vulnerability (Leviathan Security Group, 2015) que complementan el caso específico Cloud.

5.4.3. Modelo TCO

El modelo contempla los siguientes Costos a considerar:

- $\boldsymbol{Costo_{imp}}$: Costos de implementación
- $\boldsymbol{Costo_{man}}$: Costos de mantenimiento
- $\boldsymbol{Costo_{ent}}$: Costos de entrenamiento
- $\boldsymbol{Costo_{ind}}$: Costos indirectos
-

Por lo cual, el total de costos a considerar en la solución a analizar esta dado por la Ec. 5.1.

$$\boldsymbol{Costo_{total}} = \boldsymbol{Costo_{imp}} + \boldsymbol{Costo_{man}} + \boldsymbol{Costo_{ent}} + \boldsymbol{Costo_{ind}} \qquad \textit{(Ec. 5.1)}$$

Una vez realizado el análisis con los posibles escenarios en cuestión, comparar los costos totales. A continuación se presenta una descripción de cada uno de los costos del modelo.

Costos de implementación

Dentro de los costos de implementación se puede encontrar los siguientes Costos:

- **Costos de migración e implementación:** Costos de la migración de la información por migrar, instalación del nuevo sistema y restauración de data.
- **Costos de instalación y configuración:** costos de instalar los componentes necesarios para el sistema a implementar, además de los costos de configuración y customización de los ambientes.

- **Costos de licencias de software:** Costos de todas las licencias de los softwares a utilizar.
- **Costos de software adicional:** Relacionado al costo de posible incompatibilidad en aplicaciones al momento de migración, forzando a la organización a re diseñar la aplicación.
- **Costos de hardware:** Costo de todo el hardware involucrado en la implementación del sistema.

Costos de mantenimiento/operacionales

- **Costos por subscripción:** Costos involucrados en algún servicio de pago mensual/anual.
- **Costos de actualizaciones de software:** Algunas aplicaciones o SO requieren el pago de una nueva licencia al momento de actualizarse.
- **Costos de soporte y mantención de software:** Incluye los costos de realizar las actualizaciones de softwares, ya sea de manera interna o externalizada. También los costos de soporte del software.
- **Costos de actualización de Hardware:** Con el tiempo las infraestructuras se van deteriorando y resulta necesario renovar hardware.
- **Costos de mantención de hardware:** Incluye los costos de mantener operativos los dispositivos hardware involucrados en el sistema.
- **Costos de soporte y mantención de software hecho a medida:** Son los costos que se incurre en mantener y actualizar una aplicación hecha a medida para la institución. Es probable que la misma compañía que desarrolló el software provea estos servicios.
- **Costos de personal:** Corresponde a los salarios involucrados en la contratación de personal TI.

Costos de entrenamiento

- **Costos de preparación técnica:** Costos involucrados en la preparación del personal TI.
- **Costos de preparación de usuario:** Costos involucrados en la capacitación de usuarios para el uso del sistema en cuestión.

Costos indirectos

Estos costos son de carácter no cuantificable, ya que se relacionan de manera indirecta con la implementación de algún servicio. Dentro de estos costos se encuentran las horas hombres perdidas de producción de la preparación de usuarios, costos de recuperación de data por mala gestión de la misma, pérdida de productividad de la nueva plataforma dado falta de experiencia de los usuarios (en caso de ser una nueva plataforma), y el tiempo perdido de productividad durante el proceso de migración de los sistemas. Bajo el modelo planteado, los costos indirectos pueden o no ser agregados al TCO, esto depende del criterio del usuario del modelo.

El modelo presentado busca que la institución pueda hacer un diagnóstico propio aproximado sobre los posibles costos que los servicios en consideración puedan tener. Cabe destacar que en muchas ocasiones calcular estos costos puede ser complejo debido a toda la información técnica necesaria involucrada. El modelo también proporciona información sobre cómo obtener toda la información necesaria poder sobre los costos involucrados (Solar et al, 2012). En el caso de estar trabajando en conjunto con alguna empresa asesora de servicios Cloud, revisar un posible análisis de TCO que ellos realicen entorno a las opciones que se están analizando.

Utilizando este modelo se pueden calcular los TCO para las 3 situaciones que conciernen ese trabajo. Para cada caso específico se utilizan diferentes subcategorías de los costos mencionados. A continuación se segmentan los costos específicos para cada situación para así facilitar el análisis necesario a realiza.

5.4.4. Implementación de solución Cloud

A diferencia de la implementación de una solución inhouse, en una implementación Cloud no es necesario la compra de infraestructura ni preocuparse de la mantención de esta, por lo cual estos costos son reducidos del análisis de costos. Por otra parte, dado su característica de servicios, es necesario realizar el pago de este servicio de manera constante mientras el servicio se encuentre habilitado, lo cual debe ser considerado como un costo. En esta dinámica se da un trade-off que dependiendo del tamaño de la organización, el tipo de proyecto a abordar y el tiempo que este estará activo, pueden resultar más o menos atractivo los costos involucrados en una solución Cloud, para referirse a esta temática.

En este punto se consideran una implementación de software Cloud o una infraestructura Cloud para montar una solución. A continuación se aíslan los costos del modelo presentado, manteniendo solo los costos relacionados a la solución Cloud.

5.4.4.1. Costos de implementación

Tomando en cuenta que no existe hardware involucrado en la implementación de un ambiente Cloud, y que el sistema, infraestructura o software a instalar no es una migración de un sistema previo, el desglose de costos es el siguiente:

- **Costos de instalación y configuración ($\boldsymbol{Costos_{inst}}$):** costos de instalar los componentes necesarios para el sistema a implementar, además de los costos de configuración y customización de los ambientes.

Por lo cual el desglose de la componente Costos de implementación queda según la Ec 5.2.

$$\boldsymbol{Costo_{imp} = Costos_{inst}} \qquad \textit{(Ec. 5.2)}$$

5.4.4.2. Costos de mantenimiento/operacionales

- **Costos por subscripción ($\boldsymbol{Costos_{subs}}$):** Costos de la suscripción al servicio Cloud.
- **Costos de soporte y mantención de software ($\boldsymbol{Costo_{sop}}$):** En este punto solo se considera un posible soporte adicional que no fuese a estar incluido en los costos de suscripción.
- **Costos de personal ($\boldsymbol{Costo_{pers}}$):** Esto es un opcional dependiendo del tipo de servicio Cloud que se esté utilizando. En caso de ser una infraestructura donde se alojara un nuevo sistema, es posible incurrir en costos de personal para la mantención de esta de manera independiente del proveedor Cloud. En caso de contratar algún servicio de software Cloud no existía un costo a personal asociado.

Por lo cual el desglose de la componente Costo de mantenimiento/operacionales queda según la Ec. 5.3.

$$\boldsymbol{Costo_{man}} = \boldsymbol{Costos_{subs}} + \boldsymbol{Costo_{sop}}(\boldsymbol{opcional}) + \boldsymbol{Costo_{pers}}\ (\boldsymbol{opcional}) \qquad \textit{(Ec. 5.3)}$$

5.4.4.3. Costos de entrenamiento

- **Costos de preparación de usuario ($\boldsymbol{Costo_{prep}}$):** Necesario dado que el sistema a implementar no es una migración de un sistema previamente en uso (Ec. 5.4.)

$$\boldsymbol{Costo_{ent}} = \boldsymbol{Costo_{prep}} \qquad \textit{(Ec. 5.4)}$$

5.4.4.4. Costos indirectos

Se mantiene el criterio opcional del modelo con respecto a los costos indirectos propuestos por el modelo.

5.4.4.5. TCO Final

El TCO para la implementación de una solución Cloud estaría dado por la siguiente formula de la Ec. 5.5.

$$\boldsymbol{TCO} = \boldsymbol{Costos_{inst}} + \boldsymbol{Costos_{subs}} + \boldsymbol{Costo_{sop}} + \boldsymbol{Costo_{pers}}\ (\boldsymbol{opcional}) + \boldsymbol{Costo_{prep}}\ (\boldsymbol{opcional}) + \boldsymbol{Costo_{ind}} \qquad \textit{(Ec. 5.5)}$$

5.4.5. Implementación de sistema inhouse

Para la implementación de un sistema o solución inhouse, es necesario tener la gran mayoría de los costos del modelo dado que todo corre por cuenta propia de la organización. Hardware y software deben ser adquiridos, mantenidos y actualizados, y todos los costos indirectos asociados a realizar estas acciones. A continuación se presenta el desglose de costos para cada uno de los ítems del modelo presentado:

5.4.5.1. Costos de implementación

Son todos los costos del modelo, por lo cual la variable costo de implementación queda definida según la Ec. 5.6.

$$\boldsymbol{Costo_{imp}} = \boldsymbol{Costos_{migr}} + \boldsymbol{Costos_{inst}} + \boldsymbol{Costos_{soft}} + \boldsymbol{Costos_{adic}} + \boldsymbol{Costos_{hard}} \qquad \textit{(Ec. 5.6)}$$

5.4.5.2. Costos de mantenimiento/operacionales

Son todos los costos del modelo pero sin contar los costos por suscripción Cloud, por lo cual la variable costo de mantenimiento/operacionales queda definida según la Ec. 5.7.

$$\boldsymbol{Costo_{man}} = \boldsymbol{Costos_{actuSoft}} + \boldsymbol{Costo_{sop}} + \boldsymbol{Costo_{actuHard}} + \boldsymbol{Costo_{mant}} + \boldsymbol{Costo_{mantSoft}} + \boldsymbol{Costo_{pers}}\ (\boldsymbol{opcional}) \quad \textit{(Ec. 5.7)}$$

5.4.5.3. Costos de entrenamiento

En esa situación, el costo de entrenamiento se mantiene como fue definido en el modelo dado que a partir de la necesidad de mantener la infraestructura y los sistemas internos, es necesario contar con personal capacitado para la mantención del sistema (Ec. 5.8).

- **Costos de preparación técnica ($\boldsymbol{Costo_{prepTec}}$):** Costos involucrados en la preparación del personal TI. En caso de externalizar este punto, se vería reflejado en los costos de mantenimiento y no en este punto.
- **Costos de preparación de usuario ($\boldsymbol{Costo_{prepUs}}$):** Costos involucrados en la capacitación de usuarios para el uso del sistema en cuestión.

$$\boldsymbol{Costo_{man}} = \boldsymbol{Costo_{prepTec}} + \boldsymbol{Costo_{prepUs}} \quad \textit{(Ec. 5.8)}$$

5.4.5.4. Costos indirectos

Se mantiene el criterio opcional del modelo con respecto a los costos indirectos propuestos por el modelo.

5.4.6. Migración de sistema inhouse a Cloud

Este escenario es una combinación de las situaciones **5.3.5.** y **5.3.4.** Por un lado, se deja de utilizar la infraestructura inhouse, por lo cual el mantenimiento de esta desaparece, y por otro lado se asume el costo del servicio Cloud. En este escenario se tienen los posibles casos: **Migración de un sistema previamente existente, adaptación de un sistema previo a un SaaS Cloud.** A continuación se presenta el desglose de costos para cada uno de los ítems del modelo presentado:

Costos de implementación

- **Costos de migración e implementación:** Costos de migración de la información del ambiente inhouse al ambiente Cloud. Se deben considerar posibles costos de adaptabilidad del sistema a migrar. Este hito se ve en el diseño de la solución (punto 5.5). Los costos pueden ser asociados a un re-diseño del aplicativo para que se adapte al sistema.
- **Costos de instalación y configuración:** costos de instalar los componentes necesarios para el sistema a implementar, además de los costos de configuración y customización de los ambientes.

Por lo cual la variable costo de implementación queda definida según la Ec. 5.9.

$$\boldsymbol{Costo_{imp} = Costos_{migr} + Costos_{inst}} \qquad \textit{(Ec. 5.9)}$$

Costos de mantenimiento/operacionales

- **Costos por subscripción:** Se requiere el pago de la suscripción al servicio Cloud.
- **Costos de soporte y mantención de software hecho a medida:** Son los costos que se incurre en mantener y actualizar una aplicación hecha a medida para la institución. Es probable que la misma compañía que desarrolló el software provea estos servicios. De utilizar un SaaS este costo no debiese ser considerado.

  Por lo cual la variable costo de implementación queda definida según la Ec. 5.10.

$$\boldsymbol{Costo_{imp} = Costos_{subs} + Costos_{sopr}} \quad \textit{(Ec 5.10)}$$

Costos de entrenamiento

- **Costos de preparación de usuario:** De ser una migración a un SaaS, sería necesario incurrir en un costo de preparación para los usuarios. De mantenerse en el mismo sistema pero montado en la nube, se asume que los usuarios ya manejan el funcionamiento de este, por lo cual no debiese considerarse (Ec. 5.11).

$$\boldsymbol{Costo_{entr} = Costos_{prepUs}} \quad \textit{(Ec 5.11)}$$

Costos indirectos

Se mantiene el criterio opcional del modelo con respecto a los costos indirectos propuestos por el modelo.

No es una tarea fácil comparar la compra de hardware con el modelo pay as you go Cloud, esto se debe a que calcular el costo real de levantar una infraestructura propia no es un cálculo trivial. Varios proveedores Cloud internacionales proporcionan herramientas para calcular el TCO (total cost of ownership) de utilizar sus servicios Cloud en contraste con infraestructura inhouse. AWS proporciona su propia herramienta de cálculo, AWS TCO Calculator (Amazon, 2016). La cual permite obtener un aproximado entre utilizar una infraestructura inhouse vs la utilizacion de Amazon Web Services.

5.5. Diseño de Solución

El mundo Cloud es amplio, donde múltiples variables hacen la diferencia a la hora de decidir qué solución es la correcta para la problemática presentada. Existen diferentes variantes a la hora de seleccionar una solución Cloud;

diferentes proveedores, arquitecturas, servicios, locaciones, etc. Estas variables no son ni mejores ni peores, sino que responden a diferencias necesidades del cliente. Es efectivo que existen diferentes niveles de servicio, a diferentes costos, lo cual puede interpretarse como un servicio de mejor o peor calidad. Esto no es del todo cierto dado que los requerimientos de un sistema no necesariamente deben tener la mejor calidad, estos deben ser suficientes en base a lo que el requisito necesita.

El diseño de la solución nace en respuesta a un análisis de los requerimientos del sistema que la organización en cuestión desea implementar. A partir de estos requerimientos, y contrastándolos con las variables Cloud involucradas, es posible diseñar una posible solución que se aproxime de optima manera a lo que el organismo busca.

El siguiente punto se enfoca en la búsqueda de un diseño de solución a la problemática planteada a partir de las temáticas mencionadas anteriormente. La idea de este punto es analizar los requerimientos desde diferentes puntos de vista: el tipo de dato a tratar, niveles de servicio requeridos, políticas internas de la organización, etc, y mediante una serie de pasos, lograr educar al lector para que este logre diseñar una solución a su problemática. Cabe destacar que existen diversas posibles soluciones para una problemática, y que esto queda a criterio del lector. Además, se mantiene la postura con respecto a buscar una asesoría de un experto para guiar el proceso general, este apartado busca educar al lector.

Antes de establecer los pasos para aproximar una posible solución a nivel de diseño, es necesario establecer los escenarios o variables Cloud que se busca aclarar a partir de estos puntos. Como fue mencionado antes, existen múltiples variables al momento de contratar un servicio Cloud, para este diseño de solución se consideran 3 principales variantes al momento de implementar Cloud.

Escenarios Cloud a considerar

1. **Arquitectura Cloud** (Nube pública, privada, Híbrida)
2. **Servicios Cloud** (SaaS, PaaS, IaaS)
3. **Proveedor Cloud** (Nacional, Extranjero)

En base a los escenarios Cloud mencionados, se establecen los siguientes puntos con el objetivo de guiar el diseño de la solución, orientando al organismo sobre la elección de las diferentes opciones que los escenarios Cloud mencionados presentan, y así buscar una combinación que se adapte mejor a las necesidades del organismo.

Se propone una serie de pasos para poder realizar un posible diseño de la solución

Pasos para diseñar una solución Cloud

5.5.1 Análisis de información a tratar (Tipo de dato)
5.5.2 Identificar al usuario
5.5.3 Niveles de servicio.
5.5.4 Análisis de costo.
5.5.5 Perfil tecnológico institución pública

Cabe destacar que las recomendaciones establecidas en cada uno de estos puntos son simplemente para guiar algún posible diseño de solución, no deben ser tomadas como algo absoluto, el lector es libre de establecer su propio diseño de solución. A continuación se especifica cada uno de los puntos del diseño de la solución, contemplando la relación de estos con los escenarios Cloud mencionados.

5.5.1. Análisis de la información a tratar.

La información que la organización pública busca almacenar y tratar dentro del ambiente Cloud en cuestión es la razón por la cual se busca realizar estas implementaciones. Ya sea para mejorar su accesibilidad, disponibilidad o seguridad, el entendimiento de tipo de información que se busca transar es clave. Son múltiples los aspectos que hay que considerar con respecto al tipo de data para así lograr realizar una decisión más educada, y entender de mejor manera la naturaleza de la información que se busca trabajar. A continuación se presentan los aspectos a considera.

5.5.1.1. Confidencialidad de la información a tratar

Existen 2 divisiones entre la información que una organización pública pudiese tratar. La primera tiene que ver con información pública que su finalidad es ser vista y utilizada por la ciudadanía de una manera pública y libre. Son muchos los sistemas que manejan este tipo de información. Dada la naturaleza de esta información, no existen muchas restricciones a nivel de confidencialidad de la misma dado que su finalidad es de carácter público.

El segundo tipo de información es de carácter confidencial. Son múltiples tipos de información los que pueden caer en esta categoría, ya sea información confidencial de personas naturales, gubernamental, información procesada que tiene un valor a nivel de inteligencia de datos, bases de datos de valor, etc. También esta información puede poseer diferentes niveles de confidencialidad.

Para poder identificar el tipo de información que se busca tratar, a nivel de confidencialidad de la misma, la Unidad de Modernización y Gobierno Digital (UMGD, 2014) propone el siguiente cuestionario a responder, con la idea de evidenciar a la institución si la información que se desea almacenar posee algún grado de confidencialidad importante para la misma.

Así, antes de pensar en contratar un servicio Cloud, tales órganos debieran hacérselas siguientes preguntas respecto de dicha información y servicio.

1. ¿Es esta información sensible para la Seguridad Nacional?
2. ¿Es dicha información pública o es reservada de conformidad a lo dispuesto en la Ley N° 20.285? (Ver punto 5.1.3).
3. ¿Cuán importante es para la organización mantener en reserva la información que mantengo en el servicio Cloud? ¿Cuáles son las consecuencias en caso de que esta información se filtrara?
4. ¿Tengo bases de datos de personas naturales? ¿Son estos datos sensibles? ¿Cuál es el tamaño de dichas bases de datos? ¿Cuáles son las consecuencias para las personas de que tales datos se filtraran?
5. ¿En mis bases de datos se contiene información comercial sensible o perteneciente a empresas que no han autorizado la divulgación de dicha información?
6. ¿Con la potencial divulgación de la información subida a nube se afectarían los derechos de propiedad intelectual o industrial o, en general, cualquier derecho de terceras personas en los casos en que éstas no hubiesen autorizado dicha divulgación?

Dependiendo de las respuestas a dichas preguntas, los órganos deben definir cuánta importancia le deben dar tales órganos a aspectos contractuales como la protección de datos personales, la confidencialidad y la seguridad de la información.

En general, se recomienda el uso de nubes privadas en casos que la información sea clasificada de alta confidencialidad. También se sugiere la evaluación de modelos de nubes híbridas, donde la data de mayor sensibilidad se almacena en nubes privadas locales y el resto no sensible o a nivel de plataforma, se maneja en nubes públicas en función de obtener los

múltiples beneficios (escalabilidad, reducción de costos, redundancia) que la amplia gama de proveedores ofrecen en materia de nubes públicas.

A continuación se presenta la Tabla 5.1 donde se establecen los posibles escenarios Cloud en base a la confidencialidad de la información.

Tabla 5.1: Escenarios Cloud en base confidencialidad de la información.

	1. Arquitectura Cloud	**3. Proveedor Cloud**
Información Confidencial	Privada o híbrida	Nacional
Información no confidencial	Pública	Nacional o Internacional

5.5.1.2. Identificar el tipo de dato a tratar y su comportamiento

La clasificación del dato o de la información a traficar en los sistemas es importante, especialmente para poder diseñar una solución con buenos tiempos de respuesta. El uso de tecnologías Cloud y su naturaleza a través del internet implica varios factores que inciden en los tiempos de respuesta, por lo cual desarrollar un entendimiento del tipo de dato y relacionarlo a los escenarios Cloud es de gran importancia.

A diferencia de un ambiente local, en una situación Cloud se utilizando 100% el enlace de internet para la transmisión de datos. Esto implica que múltiples factores deban ser tomados en consideración para que el funcionamiento del aplicativo sea óptimo. Existen los factores de rendimiento del proveedor, los cuales son mencionados en el punto 5.6.7, y también existen los factores relacionados a la elección del proveedor Cloud en función del tipo de dato que se busca transar en el sistema en cuestión. Existen tiempos de latencia

asociados y locación del proveedor que deben ser analizados en base al tipo de dato a utilizar.

A continuación se realizan una serie de preguntas para poder identificar qué tipo de datos o de qué manera se desean utilizar.

1. Con respecto al carácter de la información a desplegar, ¿es esta de carácter informativo, o más bien de contenidos tales como imágenes o archivos (superior a los 10Mb)?
2. ¿el sistema maneja constante subida de archivos? ¿descarga de archivos? De ser así ¿Qué tipo de información suben? ¿Qué información bajan?
3. ¿Cuál es el estimado de usuarios a utilizar la solución?

La idea es identificar la cantidad de tráfico que la solución requiere y los posibles tiempos de latencia asociados. El factor tamaño del archivo afecta considerablemente la cantidad de tráfico. A mayor tamaño de archivo, más paquetes deben ser transportados. Esto sumado con los posibles tiempos de latencia (suma de retardos en propagación de información) debido a la distancia que se encuentra el proveedor puede afectar considerablemente la velocidad del sistema.

A partir del entendimiento del tipo de dato y su comportamiento, es posible comenzar a deliberar con respecto de la locación de la infraestructura del posible proveedor Cloud a utilizar. Si la información predominante a traficar cae en la categoría de imágenes, datos pesados, subida y bajada de archivos, el factor locación de la infraestructura Cloud impactará en la performance de la herramienta. Por otro lado, si se habla de tráfico de datos meramente informativos (texto), los cambios en latencia entre utilizar infraestructura Cloud cercana o lejana del foco de consultas pueden ser imperceptible.

Es necesario reducir los tiempos de retardo en el servicio (latencia), por lo cual servicios Cloud que se encuentren con infraestructura relativamente cercanos

al foco de consulta entregaran una mejor performance, reduciendo tiempos de latencia. En esta situación, proveedores chilenos entregarían mejores tiempos de respuesta. En el caso de que el sistema a diseñar, maneje principalmente información a nivel de datos, puede que esta temática sea imperceptible.

A partir de estas preguntas se pretende evidenciar el dato a nivel de espacio y el comportamiento de mismo para así poder localizar los servicios de mejor manera. La Tabla 5.2 postula posibles escenarios Cloud en base al tipo de dato a tratar.

Tabla 5.2: Escenarios Cloud en base al tipo de dato a tratar.

	3. Proveedor Cloud
Dato multimedia (imágenes, sonido, documentos, etc)	Nacional
Dato informativo (texto)	Nacional o Internacional

5.5.2. Identificar al usuario

Es importante identificar al usuario final de la solución a implementar. Este punto hace referencia a quienes serán principalmente los usuarios encargados de la utilización de esta herramienta. Este factor es importante dado que a partir de entender quiénes son los usuarios finales del aplicativo, es posible desprender posibles locaciones para el servicio a utilizar y así lograr disminuir tiempos de latencia sobre el aplicativo o el colapso de los enlaces correspondientes.

5.5.2.1. Locación geográfica del usuario.

Debido a que el foco de esta guía son los organismos públicos chilenos, y dado la labor que estos desempeñan, es lógico concluir que el público objetivo a utilizar el sistema a implementar se encuentra localizado en Chile. A pesar de

lo obvio que esto pueda resultar, es importante identificar la locación de los usuarios para así identificar el foco de consultas a la aplicación. Los menores tiempos de latencia se darán en el caso que los servicios estén alojados en infraestructura Cloud chilena. En el caso de utilizar proveedores extranjeros (eje: Amazon, Google, servidores localizados en EE.UU) la información debe transitar mayores distancias, y dependiendo de la naturaleza de esta, puede resultar en tiempos de latencia significativos para el correcto funcionamiento del sistema.

5.5.2.2. Usuario Objetivo de la solución.

En general, los aplicativos pueden tener 2 orientaciones específicas: a nivel interno de gestión para los organismos públicos, de uso externo como un servicio para la ciudadanía. En el caso de los aplicativos de gestión, puede darse la situación que los enlaces de conectividad internacional se encuentren colapsados por el alto uso del enlace internacional (Youtube, Spotify, Facebook, etc). Esta situación es común a nivel organizacional dado que por lo general las consultas vienen desde una misma fuente, por lo cual aprovechar los enlaces nacionales (menos colapsados) implica una mejor performance del sistema. En general, la situación país es que los enlaces de conexión al extranjero se encuentran significativamente más colapsados que los enlaces nacionales, por lo cual esta recomendación está en aprovechar los enlaces nacionales, específicamente si se encuentra la situación de colapso de la conectividad extranjera mencionada anteriormente.

Por lo general, cuando se habla de un aplicativo de uso interno de alguna organización, se hace alusión a datos a nivel interno de la organización, los cuales por lo general son considerados confidenciales para la misma. Por lo cual, en base al punto 5.5.1.1, es posible considerar una arquitectura orientada a la garantizar una mayor seguridad de la información.

En el segundo caso, nos encontramos con las aplicaciones a nivel ciudadanía, donde el foco de usuarios se encuentra localizados en Chile, pero no específicamente desde el mismo lugar (no utilizando el mismo enlace). En este caso, el tema del colapso de enlace internacional provisto por el ISP, tiene menor relevancia en el caso anterior, dado que este por lo general no debiese encontrarse colapsado. Por lo cual, se podrían considerar los proveedores internacionales también.

Desde el punto de vista de la arquitectura, nos encontramos con 2 situaciones: donde el sistema es de uso público y transparente para cualquiera a consultar, y cuando la información a consultar por los ciudadanos es privada y exclusiva para cada individuo. Dada esta situación, se considera el uso de nubes públicas, y en caso de necesitar mayor seguridad, complementar con el uso de alguna arquitectura híbrida que resguarde la información confidencial específica.

Otro punto a considerar, es un posible corte del enlace internacional a nivel país. El operador VTR sufrió un percance similar el año 2015 debido a un bloqueo de enlace internacional en Brasil (Emol, 2015), en donde se perdió conectividad a través del enlace internacional de la empresa VTR. La utilización de enlaces nacionales mitiga este tipo de situaciones ante un eventual corte o sobrecarga del enlace internacional para ambos casos mencionados.

La Tabla 5.3 identifica posibles escenarios Cloud en función al foco del sistema a utilizar.

Tabla 5.3: Escenarios Cloud en base al foco del sistema a utilizar.

	3. Proveedor Cloud	**1. Arquitectura Cloud**
Sistema de uso interno organizacional	Nacional	Privada
Sistema para la ciudadanía	Nacional o Internacional	Pública o híbrida

5.5.3. Niveles de servicio

En general, son muchas los organismos públicos que solicitan de manera interna altos niveles de servicio. Es lógico, dado que se buscan aplicativos y sistemas con buen rendimiento, en especial si buscan implementar soluciones a nivel ciudadano, donde estas son esenciales para procesos o tramites. A pesar de que esta es la tónica a nivel organizacional, la realidad indica que existen diferentes soluciones que no requieren de niveles de servicios tan demandantes. Es necesario entender esta situación dado que los mejores niveles de servicio por lo general son brindados por proveedores extranjeros, por lo cual es necesario poner en la balanza todos los aspectos que afectan una solución y priorizar los de mayor importancia para así poder converger a una mejor solución a la problemática.

En términos generales, es posible encontrar proveedores de servicios Cloud con mejores niveles de servicio en el extranjero que en Chile. Esto se debe a que el desarrollo Cloud en Chile aún se encuentra en una temprana etapa, donde recientemente se están estableciendo las primeras nubes públicas con infraestructuras localizadas en Chile y respaldadas por proveedores de clase mundial.

Este retraso del desarrollo Cloud a nivel nacional se ve reflejado en nubes con menor control de la infraestructura por usuarios, menor flexibilidad de recursos on-demand, menor disponibilidad, infraestructuras con menores estándares (Tier I y II), etc. Estas condiciones implican que en muchas situaciones,

proyectos necesariamente deban utilizar infraestructuras Cloud extranjeras dado que lo ofrecido nacionalmente no cubre las necesidades básicas del requerimiento.

En base a lo postulado, es necesario que el organismo público vinculante, recopile los niveles de servicio necesarios para llevar a cabo el proyecto, y en base a la exigencia de los mismos, identificar si el proyecto se puede llevar a cabo utilizando infraestructura nacional, o si se logra un mejor resultado utilizando un proveedor extranjero. Además de los niveles de servicio del proyecto en sí, los organismos públicos muchas veces poseen estándares a nivel organizacional en relación a estos servicios, por lo cual es necesario tomarlos en consideración. Es posible encontrar los niveles de servicio oferentes por los proveedores en sus sitios web.

La Tabla 5.4 establece posibles escenarios Cloud en base a la exigencia de los niveles de servicio.

Tabla 5.4: Escenarios Cloud en base a la exigencia de los niveles de servicio.

	3. Proveedor Cloud
Alta exigencia en niveles de servicio	Internacional
Media o baja exigencia en niveles de servicio	Nacional

5.5.4. Análisis de costo y presupuestos

5.5.4.1. “Pay As you Go”

Uno de los paradigmas de la tecnología Cloud es la posibilidad de “**pay as you go”** o pago por uso. Este modelo de pago permite pagar por los recursos utilizados en cierto periodo de tiempo, por lo cual el usuario solo paga por lo

utilizado. El modelo de cobro es similar a como funciona la electricidad o la luz. A pesar de que este no es el único modelo de pricing, es predominante en las nubes públicas. El problema para los organismos públicos es como destinar presupuesto para un costo que es variable. A partir de esta problemática, para sumarse a un servicio de Cloud pública con modelo “pay as you go”, se requiere realizar una estimación en un periodo determinado de los recursos a utilizar, para así poder aproximar el presupuesto necesario. Dado que los modelos Cloud públicas son relativamente nuevos en Chile, la gran mayoría de los servicios Cloud ofrecidos no manejan costos variables (pseudo nubes, ambientes virtualizados), sino que el modelo de cobro es en base a una mensualidad, variable en función a aumento de recursos pero sobre el costo base, modificando el cobro mensual general. En una situación donde no se logra establecer una forma de pago para un modelo de cobro variable, la utilización de estos proveedores resulta favorable.

La Tabla 5.5 establece los escenarios Cloud en base a la posibilidad de costos variables.

Tabla 5.5: Escenarios Cloud en base a la capacidad de la institución de manejar costos variables.

	3. Proveedor Cloud
Posibilidad de manejo costos variables	Internacional
No manejo de costos variables	Nacional

5.5.4.2. Costos nacional vs extranjero.

Como fue mencionado anteriormente, el desarrollo de la tecnología Cloud a nivel de proveedores en Chile es significativamente inferior a los grandes proveedores a nivel internacional. Como resultado de su economía de escala, los proveedores internacionales pueden ofrecer precios significativamente

menores que los proveedores chilenos. Además, dado los costos involucrados en el mantenimiento de las infraestructuras, costos de equipos, electricidad, etc, se hace necesariamente más costoso para los proveedores nacionales llevar la operación de sus infraestructuras.

Para tener una idea de los costos de ciertos proveedores internacionales se presenta la Tabla 5.6 comparativa realizada por la empresa Leviatan (Leviathan Security Group, 2015).

Tabla 5.6: Costos de proveedores internacionales en base a los 3 escenarios establecidos.

Provider (annual costs)	Scenario 1 500 users 15 TB ($)	Scenario 2 500 users 150TB ($)	Scenario 3 2500 users 750TB ($)
Amazon - Zocalo[19]	4,776	47,706	237,306
box.com - Business[20]	9,000	90,000	450,000
copy.com - Pro[21]	4,495	44,950	449,500*
Cubby - Enterprise[22]	9,598	76,780	335,916*
DropBox - Business[23]	10,200	102,000	1,020,000
Google - Cloud Storage[24]	4,792	47,923	479,232
HP - Cloud Object Storage[25]	16,588	165,888	1,658,880
OneDrive - OneDrive For Business[26]	35,906	366,557	1,846,992
Rackspace - Cloudfiles[27]	18,432	184,320	1,843,200
SpiderOak - Blue Enterprise[28]	3,300	30,300	150,300
Mean (average cost)[29]	11,963	117,826	791,651
Median (the 'central' quote)	9,299	83,390	449,750
Range (difference between highest and lowest quotes)	32,606	336,257	1,696,692.40

La Tabla 5.7 establece los escenarios Cloud en base a capacidad de presupuesto de la institución.

Tabla 5.7: Escenarios Cloud en base a la capacidad de presupuesto de la institución.

	3. Proveedor Cloud
Presupuestos limitados	Internacional
Presupuestos Suficientes	Nacional o internacional

5.5.4.3. Costo levantar saas v/s iaas.

El siguiente punto toma el escenario en donde a partir de los requerimientos del sistema a utilizar, existe algún tipo de SaaS que satisfaga el requerimiento. En este caso, es siempre más rentable la contratación de este SaaS, que montar alguna infraestructura Cloud y luego adquirir o desarrollar un software que corra en dicha infraestructura. A pesar de lo lógico que esto suena, muchas veces no se da el tiempo para poder revisar las ofertas en el mercado en relación a SaaS.

5.5.5. Perfil tecnológico institución pública

En el **punto 4.1.2 del capítulo 4,** se estableció una relación entre el nivel de madurez de las instituciones chilenas en función de los presupuestos. Se concluye que las organizaciones con mayor presupuesto dedicado a TI poseen un mayor nivel de madurez tecnológico. En base a esto, se hace posible identificar a las instituciones en base a 4 segmentos en función de su porcentaje de inversión en TI (Ver punto 4.1.2).

En función de fomentar el uso Cloud, resulta necesario analizar el presupuesto de las instituciones para así poder recomendar ciertos tipos de servicios que se acomoden a los presupuestos manejados y al nivel de desarrollo que la institución tenga.

Para instituciones con bajo nivel de madurez (revisar anexo 1 para identificar posible nivel de madurez), se recomienda un acercamiento paulatino a las tecnologías Cloud, por lo cual el uso de **SaaS** es un buen punto de partida. En el modelo SaaS, el aplicativo viene instalado y configurado, listo para su utilización. Esto se traduce en tiempos reducidos para tener el sistema funcionando y así poder obtener los beneficios del sistema rápidamente. Por otro lado, los rápidos tiempos de operatividad permiten levantar fácilmente prototipos o demostraciones para así testear su funcionalidad y tener una evaluación del sistema más precisa. También los SaaS generalmente poseen "free trials" o instancias gratuitas, de donde también se pueden realizar pruebas de concepto o demostraciones para evaluar el sistema.

En el caso de las instituciones con mayor nivel de madurez, los SaaS son considerablemente una buena opción en caso de que se ajuste a las necesidades del sistema que se busca implementar. En caso contrario, siempre existe la posibilidad de montar algún otro tipo de sistema en una infraestructura Cloud utilizando IaaS, o desarrollar una solución a medida y montarla en una infraestructura Cloud. Las IaaS poseen un nivel de control considerablemente mayor a lo proporcionado por los SaaS, de lo cual se pueden obtener múltiples beneficios en manos de un equipo con experiencia en manejo de infraestructuras o sistemas Cloud.

Utilizando los niveles de madurez establecidos en el estudio de madurez de las instituciones públicas (capitulo 4, punto 1), se establecen las siguientes recomendaciones de arquitectura Cloud en base a los niveles de madurez TI (Tabla 5.8).

Tabla 5.8: Escenarios Cloud en base al nivel de madurez de la institución pública.

	3. Arquitectura Cloud
Institución con bajo nivel de madurez TI (nivel 1 y 2)	SaaS
Institución con medio, alto nivel de madurez TI (Nivel 3 y 4)	SaaS, IaaS

5.6. Contratación Cloud

Con los puntos anteriores cubiertos, es momento de comenzar a establecer algún posible proveedor Cloud que satisfaga los puntos establecidos en el diseño de la solución. Como fue mencionado anteriormente, es posible que la empresa asesora maneje diferentes soluciones Cloud, tanto como propias o como re-seller de otro proveedor. También se abordó en el punto 4 (preparación de un equipo) los canales de contacto a proveedores nacionales aprobados a nivel estatal, mediante el convenio marco Data Center y servicios asociados. Como último, se encuentra la gran oferta de proveedores internacionales.

Existen 2 aspectos necesarios a comparar al momento de tomar la decisión de que proveedor contratar. Lo primero es revisar que proveedores cumplen con lo establecido en los puntos anteriores, en base al diseño de la solución. Lo siguiente es establecer los aspectos necesarios a considerar en el contrato vinculante con el proveedor. Ambos aspectos se encuentran relacionados a lo oferente por parte de los proveedores. Dentro de los sitios web de los proveedores, se encuentran las especificaciones de los servicios de los mismos. Comúnmente, estos términos están publicados en los sitios web de dichos prestadores de servicios y se incluyen en enlaces con expresiones tales como “términos y condiciones”, “términos de uso”, “Niveles de Servicio”, “Políticas de uso aceptable”, “políticas de privacidad” y otras denominaciones como “aviso legal”, “propiedad intelectual”, “seguridad”, etcétera. Tales

documentos suelen describir los derechos y obligaciones de las partes, la forma en que será tratada la información que tratará el servicio cloud, los resguardos de seguridad que toma la compañía prestadora del servicio, etcétera (UMGD, 2014).

En base a lo establecido en el diseño de la solución, es importante revisar la locación de los datacenters, los niveles de servicio que estos ofrecen y las políticas en relación a la confidencialidad y seguridad de la información.

A continuación se abordan los principales puntos que debiese incorporar un contrato con un proveedor de servicios Cloud. Cabe destacar que por lo general, sobre todo con proveedores internacionales, no existe necesidad de establecer un vínculo mediante contrato, es la institución la que debe acoplarse a las especificaciones que estos proveedores disponen. Con los proveedores nacionales existe más flexibilidad a nivel de contrato para poder establecer y considerar las especificaciones que la institución pueda tener. Es importante mencionar que los organismos del Estado tienen completa libertad para establecer clausulas independientes a los puntos a mencionar. A continuación se establecen los principales puntos a considerar en el contrato a realizar.

5.6.1. Confidencialidad de la información

Todo contrato debe establecer la confidencialidad de la información que se almacenará en el ambiente Cloud. Es necesario revisar que propone el proveedor Cloud con respecto a esta temática, que uso se le dará a la información almacenada y quienes tienen acceso a la misma.

Bajo esta cláusula se busca asegurar que la información no sea utilizada con ningún otro fin que el de la operación del sistema por parte de la institución. También es necesario establecer que la accesibilidad a la información es exclusivamente para la institución y del prestador de servicio, ningún otro tercero debiese tener acceso a esta.

Cláusulas de confidencialidad a considerar en contrato con respecto a la confidencialidad de la información.

- **Acceso a terceros:** Se debe estipular bajo una cláusula que el acceso a la información almacenada en el sistema Cloud es de exclusividad del proveedor y del cliente.
- **Uso de la información por parte del proveedor:** Este debe hacer uso de la información exclusivamente para la ejecución de lo estipulado bajo contrato.
- **Establecer actividades del proveedor:** Se debe mantener bajo contrato las actividades específicas que el proveedor empleará con la información almacenada en el sistema.

5.6.2. Seguridad de la información

Debe establecerse en el contrato las medidas que el proveedor implementa para poder asegurar la seguridad e integridad de la información. Más allá de lo establecido en la confidencialidad de la información, se debe velar por que el proveedor posea protocolos y estándares de seguridad de la información.

- **Implementación de medidas de seguridad en base a alguna certificación:** Bajo decreto, es necesario asegurarse que el proveedor Cloud posea algún tipo de certificación de seguridad e integridad de información[4]. Si bien el decreto no es especifico, se requiere algún tipo de certificación para realizar la contratación, la cual debe estar especificada en el contrate vinculante.

- **Protección tránsito de data (canales seguros):** Es importante asegurarse que en las políticas de seguridad del proveedor se establezcan protocolos de seguridad para la transferencia de

[4] Decreto Supremo N° 83, de 2005, del Ministerio Secretaría General de la Presidencia que aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos. D.O. 12 de enero de 2005.

información. El foco de esto es evitar que algún tercero intercepte la información, ya sea para adquirir o modificar la información en tránsito. Se debe asegurar que el proveedor Cloud posea protocolos de protección y encriptación del canal. Por lo cual, el contrato debe establecer que componentes y protocolos son implementados por el proveedor. Se sugiere canales de transmisión que utilicen algoritmos asimétricos para establecer la encriptación del canal de trasmisión de información (RSA) en conjunto con encriptación simétrica para las llaves.

- **Encriptación de información almacenada:** Se sugiere niveles de encriptación superiores a DES, tales como AES (NIST) de 128, 192 o 256 (bits) para el almacenamiento de información.

Se sugiere evaluar ambas temáticas con un equipo asesor, para asegurar que los protocolos de seguridad desplegados por el proveedor son suficientes para mantener la información segura e integra, tanto en la infraestructura como en tránsito.

5.6.3. Propiedad Intelectual

Es necesario establecer una cláusula sobre la propiedad intelectual almacenada en la infraestructura Cloud. Se debe especificar que la propiedad intelectual de los documentos e información almacenados pertenecen a la institución pública y no deben ser utilizados por el prestador de servicio.

Existen 3 tipos de información que pueden ser consideradas como propiedad intelectual de la institución. Primero se tiene el sistema o software, que en el caso de ser un desarrollo especifico de la institución, el código y la propiedad intelectual del mismo es de la institución pública. La segunda es la información o documentos que pueden ser subidos o que se encuentran dentro del aplicativo o infraestructura Cloud. La tercera seria la información originada a partir del uso del sistema (bases de datos). Es importante especificar,

independiente del tipo de información, que todo debe ser considerado como propiedad intelectual de la institución.

Es importante destacar que estos 3 tipos de información pueden ser considerados propiedad intelectual de la institución, pero en muchos casos no lo son. Dado la funcionalidad de las instituciones públicas, parte de la información que estas almacenan son datos de la ciudadanía, lo que implica que ninguna propiedad intelectual debiese ser reclamada sobre esta información. Esto corre tanto para almacenamiento de información como para documentos.

En el caso de códigos de software desarrollado a medida, usualmente se reclama como propiedad intelectual de la institución. Esta guía incentiva a la compartición de esta propiedad intelectual a través de los organismos públicos del Estado. Iniciativas como esta ayudarían a mejorar el desarrollo tecnología a nivel estatal y la reducción de costos.

Como último punto, se recomienda establecer clausulas con penalidades correspondientes a posibles violaciones de propiedad intelectual declarada por la institución pública. Estas penalidades deben ser agregadas en la sección de SLA del contrato.

5.6.4. Modificación Unilateral

Es común encontrar en términos y condiciones, que los proveedores tengan la facultad de modificar unilateralmente los términos de contratación. Lo anterior no puede ser aceptado por un organismo del Estado. De acuerdo a la jurisprudencia administrativa de Contraloría General de la República, los órganos de la Administración del Estado no pueden suscribir contratos en donde se da la facultad al prestador del servicio para modificar el contrato dando aviso a su contraparte[5] (UMGD).

[5] Véase CONTRALORÍA GENERAL DE LA REPÚBLICA, Dictamen N° 26.479 de 20 de agosto de 1996.

En caso de encontrar una cláusula de este tipo, solicitar removerla del contrato o de lo contrario no se podrá realizar una contratación con este proveedor. Lo anterior no implica que el contrato no pueda ser modificado, simplemente la modificación debe venir como un acuerdo por escrito entre ambas partes.

5.6.5. Vendor lock in

Este concepto hace referencia al uso de una tecnología, en donde el proveedor de la misma mantiene al cliente dependiente de él en base al uso de sus servicios dado que no existe la capacidad de migrar o cambiar de proveedor. Esto puede ocurrir por temas de incompatibilidad de migración dado el uso de protocolos exclusivos del proveedor, costos altos inviables de financiar.

Para evitar esta situación, lo primero al realizar una contratación es preguntarse ¿Cómo saco mi información a futuro en caso de necesitarlo? Para esto es necesario verificar en el contrato si la institución tiene la facultad de recuperar los datos almacenados en la nube de manera simple, y migrarlos a otro proveedor.

En caso de existir vendor lock in, se recomienda el análisis de la situación y buscar un proveedor de características similares que permita una migración viable a otro proveedor en caso de necesitarse.

5.6.6. Terminación del contrato

Es necesario estipular las condiciones para la terminación de servicio en caso de que la institución lo requiera, por lo cual el contrato debe la libertad de terminación de servicios y contrato por parte del cliente. A pesar de la posibilidad de migrar a otro proveedor en caso de insatisfacción del servicio, esto pone presión en los proveedores a cumplir los estándares de calidad previamente estipulados, y mantener esfuerzos en la fidelización del cliente. Por otro lado, se recomienda mantener contratos no prolongados, para así poder realizar revisiones y evaluación del proveedor en términos de la calidad de sus servicios de manera constante.

El otro aspecto que debe estar estipulado en el contrato es obligación que tiene el proveedor de eliminar de toda la data almacenada en el tiempo de operatividad que tuvo el sistema una vez que se termine el servicio. Debe existir un tiempo determinado de permanencia de la información a posterior del término de contrato, para posibles recuperaciones de información por parte de la institución. Los tiempos relacionados a la retención de información y entrega de la misma al proceso de término de contrato deben estar establecidos en los SLA correspondientes (ver punto 5.6.7).

5.6.7. SLA

Los SLA a establecer son aquellos que satisfagan de mejor manera las necesidades establecidas en el diseño de la solución. Además es necesario contemplar ciertos aspectos que no necesariamente se relacionan a la solución de por sí, más bien al servicio general que el proveedor presta. Es en esta sección donde la institución debe asegurar los estándares de calidad que está contratando y las penalizaciones correspondientes en caso que estos no se cumplan.

Para guiar esta sección se utilizan la estandarización de SLAs realizada por la Comisión Europea (European Commission, 2014). Como se mencionó en el punto 3.6, esta estandarización agrupa los SLAs en 4 grupos distintivos: desempeño, seguridad, manejo de información y protección de la información personal. Cabe destacar que esta estandarización es para guiar la identificación de SLAs relevantes, proveedores pueden tener o no estos SLAs dentro de sus términos, también pueden tener diferentes.

A continuación se abordarán los SLAs segmentados por la estandarización mencionada y como estos puntos debiesen ser abordados dependiendo de las variables comentadas anteriormente y el diseño de la solución establecido. Cabe destacar que se presentan los SLAs más relevantes para la institución, para ver lista completa referirse al documento referenciado.

5.6.7.1 Desempeño

- **Disponibilidad**

Nivel de uptime (disponibilidad): Como fue mencionado anteriormente, las instituciones tienen el deber legal de atender las necesidades públicas en forma continua y permanente, en otras palabras un porcentaje de uptime del 100%. Esto es algo difícil de alcanzar ya que los proveedores con mejor uptime de mercado (proveedores internacionales) bordean el 99,9974% de uptime (Network World, 2015). Los proveedores nacionales se encuentran por debajo de estas cifras, lo cual dificulta suplir el requerimiento base. Por lo cual es necesario entender que si se tiene como requisito utilizar servicios Cloud locales, por defecto no se estará optando al mejor uptime disponible en el mercado.

Es necesario entender que no todos los sistemas realmente necesitan un tiempo de disponibilidad máximo, sino que suficiente para obtener un correcto desempeño. En muchos casos solicitar un 100% de disponibilidad, a pesar de ser imposible, no es siquiera necesario. Es importante identificar en que momentos del servicio se desea mantener una completa disponibilidad del sistema (recordar que muchos sistemas durante la noche están completamente en desuso), lo que se relaciona al **porcentaje de solicitudes exitosas.**

Porcentaje de solicitudes exitosas: Independiente si la solución a la que se converge busca altos o suficientes niveles de uptime, es importante verificar que el porcentaje de solicitudes exitosas sobre el total de solicitudes sea alto. No sirve de nada un sistema que se encuentre siempre disponible, si al atender solicitudes tiene un alto porcentaje de error.

En el caso donde el diseño de solución converge a que se necesita un uptime alto, es necesario identificar que el porcentaje de solicitudes exitosa sea alto durante todo momento. En el caso que se busque un sistema que funcione en

situaciones específicas, ideal es asegurar un porcentaje de solicitudes exitosas sea alto en los tiempos donde se desea mantener el sistema disponible (ejemplo: entre 7am-6pm).

- **Tiempos de respuesta**

Tiempo de respuesta promedio: Independiente que sea un sistema de uso público o interno por la organización, cualquier sistema con tiempos de respuesta bajos impacta en la productividad de los servicios, y dado que el propósito de estos sistemas es entregar un mejor servicio, es necesario garantizar tiempos de respuesta acordes al servicio que se quiere prestar. Importante considerar que incluso garantizando que el prestador de servicios Cloud entregue buenos tiempos de respuesta, es importante considerar que la latencia y la conectividad a internet también impactarán en los tiempos a nivel global.

Tiempo máximo de respuesta: Importante también tener una métrica del máximo tiempo en que el sistema puede responder. Es importante ponerse en el caso del peor escenario posible.

- **Capacidad**

Número simultáneo de conexiones: Establecer el máximo número de conexiones simultáneas es fundamental. Este número varía dependiendo del enfoque que tenga el sistema a utilizar. De ser un sistema hecho para ser utilizado a nivel ciudadanía, las conectividades serán considerablemente mayores a las de un sistema de uso interno de la institución. A sí mismo, para poder establecer un parámetro cómodo para la institución, es necesario realizar o revisar (de ya existir) una estimación en base a la simultaneidad del sistema en cuestión.

Máxima capacidad de recursos: A pesar de los altas capacidades de almacenamiento, memoria y procesamiento que los proveedores Cloud

ofrecen, es interesante revisar los específicos que estos ofrecen en caso que no sean compatibles con lo estimable a partir del diseño de la solución.

- **Indicadores de capacidad**

Conectividad externa: Es de suma importancia verificar la capacidad de conexión entre el servicio Cloud a desplegar y algún otro servicio ya operativo. Son muchos los casos en donde el sistema o infraestructura a instanciar necesita comunicar, ya sea enviando o recibiendo, información de otros sistemas de la misma u otra institución pública. Se sugiere optar por proveedores Cloud con alta capacidad de conectividad externa.

- **Soporte**

Horas de soporte: Preferencia de soportes 24/7.

Tiempo de responsividad: Bajos tiempos de responisividad.

Tiempo de resolución: Bajos tiempos de resolución.

- **Terminación de contrato**

Periodo de recuperación de información: Es importante tener claridad en los periodos que el proveedor Cloud permiten realizar una recuperación de la información almacenada en el sistema al momento de terminar el contrato antes de que sea eliminada de sus servidores.

5.6.7.2. Seguridad

- **Confiabilidad**

Nivel de redundancia: Independiente de sistema a desplegar, la información que se está almacenando es siempre de relevancia y debe ser preservada, por lo cual en caso de fallas a servidores donde se encuentra alojado es importante contar con redundancia sobre los mismos. Existen diferentes niveles de redundancia, ya sea en número de réplicas o en locación donde se

aplica la redundancia. En caso de utilizar proveedores Cloud chilenos, es interesante como la redundancia fuera del país puede jugar un papel importante en la confiabilidad de la información. Dada la naturaleza sísmica del país, el colapso de datancenters no es algo fuera de lo normal, lo cual podría derivarse en posibles pérdidas de información. Manteniendo redundancia en locaciones con diferentes fenómenos naturales puede ser una buena manera de mitigar esta problemática.

Confiabilidad del servicio: La métrica mide el tiempo aproximado en que el sistema Cloud se mantiene operativo sin presentar ninguna falla. Lógicamente se sugieren proveedores con altos tiempos de confiabilidad de servicio.

- **Criptografía**

Verificación de seguridad

Certificaciones: Corresponde al listado completo de certificaciones que el proveedor Cloud posee con sus correspondientes fechas de expiración y periodo de renovación. Cuando se estudie la contratación del servicio *Cloud*, se sugiere poner especial atención al hecho de que el prestador del servicio cuente con alguna certificación que asegure que éste cumple con normas sobre seguridad de la información tales como, por ejemplo, la normativa ISO 27000. Se sugiere privilegiar a los prestadores de servicios que cuenten con esta clase de certificaciones puesto que, de conformidad a lo establecido en los PMG de Seguridad de la Información y en las normas técnicas de seguridad de la información (UMGD, 2014).

- **Gobernanza**

Cambios en el sistema Cloud: Establecer el periodo en que los servicios Cloud notifican sus posibles cambios es fundamental para anticiparse a alguna posible modificación que no vaya acorde con la línea de la institución. Por lo cual, cambios a nivel de SLA o del servicio como tal deben ser avisados con la suficiente anticipación para que la institución pueda ver alguna opción en

función de ser necesario realizar un cambio de proveedor. Cabe destacar que en base a lo establecido en el punto 5.6.4 sobre la modificación unilateral, la institución pública debe estar de acuerdo con cualquier tipo de modificación pre establecida en el contrato, el proveedor no debiese poder realizar modificaciones al contrato de manera autónoma.

5.6.7.3. Manejo de información

- **Clasificación de data**

Uso de data de la institución por proveedor Cloud: En este SLA se establece el grado de uso de la información que la institución está almacenando en los sistemas Cloud. Se debe buscar proveedores que se remitan a lo establecido en el punto 5.6.1 y punto 5.6.4 en base a la propiedad intelectual y la confidencialidad de la información.

Uso de data derivada del uso del sistema por el proveedor Cloud: Remitirse a los puntos 5.6.1 y 5.6.4 en base a la propiedad intelectual y la confidencialidad de la información.

- **Replica, respaldo y restauración de información**

Latencia de replicación: Se recomiendan mínimos tiempos de latencia en replicación para mantener que en caso de haber una caída de sistema principal, la réplica se encuentre con data actual minimizando el error por inconsistencias de información.

Frecuencia de respaldo: Alusión a la frecuencia en que se hacen respaldos completos de información. Para establecer un parámetro acorde, es necesario establecer que tan dinámica es la información a tratar en el sistema que la institución pública pretende desplegar.

Tiempo de retención de respaldo: Idealmente tiempos suficientes o mayores en función de la frecuencia de respaldo.

Números de Respaldos: Número de respaldos de acceso simultaneo de diferentes generaciones de información. A mayor cantidad de respaldo, mejor integridad de la información o restauración de posible información perdida por error de sistema o humano.

5.6.7.4. Protección de data personal

Listado de códigos de protección, estándares y certificaciones: Importante revisar este listado con apoyado de un organismo educado en temáticas de estándares de protección para asegurar el resguardo de la información.

- **Limitaciones de Uso, retención y filtración de datos:**

Uso de data de clientes por medio del uso de la ley: Este punto requiere énfasis en casos donde el proveedor sea internacional. Dado las diferentes leyes de países, es posible que entidades de gobierno de dichos países tengan acceso a información almacenada por entidades privadas. Importante revisar las leyes de dichos países en donde se desea utilizar servicios Cloud.

- **Transparencia y notificaciones**

Lista de proveedores subcontratados: Se debe incluir un listado con todas las entidades las subcontratadas que tengan relación con el procesamiento de información de la institución. Referirse al punto 5.1.1, donde se presentan los aspectos legales a considerar en subcontratación y resellers.

Categoría de data especial: Es de suma importancia revisar este apartado en caso de existir en los SLAs del proveedor revisado. Es acá donde se establece tipificaciones de datos que el proveedor esta adecuado a procesar

de acuerdo a estándares y regulaciones. Estas tipificaciones pueden ser: datos de salud, financieros, educacionales, etc.

- **Responsabilidad del proveedor**

Políticas de violación de datos personales: En este aparto se describe las políticas del proveedor con respecto a la violación de datos personales de la institución, además de la documentación necesaria que respalde dichas políticas.

- **Locación geográfica de la información:**

Lista de locaciones geográficas: Esta lista incluye las locaciones en donde la data puede ser procesada o almacenada. De vital importancia en relación al punto 5.6.1 sobre la confidencialidad de la información.

5.7. Resumen: Guía Metodológica para el uso de Cloud Computing para instituciones públicas chilenas

- **5.1. Aclaraciones Legales**

Se establece como el punto de partida de esta guía dado la necesidad de aclarar los aspectos legales que deben ser tomados en consideración para la implementación de servicios Cloud. Sin esta temática en consideración, cualquier decisión tomada a posterior puede verse en conflicto con algún aspecto legal que deba ser cumplido para una correcta implementación de la tecnología. Se vela por establecer sistemas que estén acordes a las normativas establecidas, sobre todo si se trata de una institución pública.

- **5.2. Estrategia Cloud**

Dado que el objetivo a largo plazo es aprovechar los múltiples beneficios que la tecnología Cloud ofrece a las instituciones públicas, es necesario establecer una estrategia que vele por lograr este objetivo. La estrategia presentada se

origina en base a la visión propia establecida en esta guía en complemento con los esfuerzos de la unidad de modernización y gobierno digital de difundir el uso de sistemas Cloud a nivel público. Esta estrategia puede ser o no seguida, de no ser seguida, se recomienda establecer algún tipo de plan que contenga actividades al corto, mediano y largo plazo.

- **5.3. Equipo Asesor**

Una vez dimensionado las legalidades y estrategia, es momento de incorporar algún tipo de proveedor que pueda ser de ayuda a la hora de establecer los futuros puntos en cuestión. En base a la estrategia presentada en esta guía, se promueve el uso de expertos en temáticas Cloud para poder construir o implementar un sistema acorde a la necesidad planteada, tomando todas las precauciones necesarias para su correcta operación y mantención. “Pastelero a tus pasteles”.

- **5.4. Evaluación económica Cloud (TCO)**

Sin presupuesto para poder implementar un sistema Cloud, se hace imposible realizar la tarea. Es necesario realizar un análisis financiero para poder evidenciar la factibilidad de implementar algún sistema Cloud. En caso de no contar con el presupuesto necesario para implementar el sistema, las opciones son descartar la implementación o revisar la posibilidad de realizar un reajuste de presupuestos en servicios de TI. Es importante realizar este análisis antes de pasar a fases que requieran más compromiso y tiempo a invertir dado que si no existe presupuesto, no es posible la implementación.

- **5.5. Diseño de Solución**

Con ayuda de un proveedor asesor, es momento de establecer el diseño de la solución a la cual se quiere converger. En base a los requerimientos de la institución, es necesario analizar las diversas variables que los ambientes Cloud ofrecen para así lograr una posible solución que satisfaga las necesidades de la institución.

- **5.6. Contratación Cloud**

Con los puntos anteriores cubiertos, la institución se encuentra en posición de analizar las posibles ofertas disponibles en el mercado y realizar la contratación pertinente en caso de encontrar un proveedor que satisfaga la solución establecida. Muchas veces el mismo equipo asesor debiese ser capaz de ofrecer, ya sea como reseller o dueño de la infraestructura, los servicios a los que se quiere optar.

6. Conclusiones

En esta memoria se propone una guía Metodológica para el uso de tecnologías Cloud en el sector público chileno. El aporte es un paso a paso de recomendaciones para una posible implementación y/o evaluación de la tecnología Cloud en las instituciones públicas chilenas.

En una primera instancia, se establecieron aspectos relevantes sobre la tecnología Cloud para ilustrar al lector sobre la temática a abordar.

A posterior, para poder desarrollar la guía, fue necesario establecer los aspectos relevantes que una institución pública debiese tener presente para implementar y/o evaluar la tecnología. Para esto, entrevistas fueron realizadas a proveedores Cloud con experiencia trabajando con instituciones públicas. También entrevistas a coordinadores de TI de instituciones públicas fueron realizadas. Con ambos espectros de la situación, y su visión única de la situación, conclusiones fueron establecidas. Paralelamente, se realizó investigación en función de recolectar antecedentes para poder construir esta guía. Como último punto a considerar en el desarrollo de la guía, se encuesto a los entrevistados en función de la relevancia de los puntos establecidos en la guía Practical guide for Cloud Computing. Se les solicito calificar del 1 al 5 cada uno de los puntos establecidos en dicha guía, en función de la relevancia que estos puntos tienen en relación al contexto nacional.

En base a la información recopilada y las conclusiones establecidas de la misma, se establecieron los puntos que la guía aborda.

Para validar los puntos establecidos en la guía, se retomó el contacto con los entrevistados en la etapa de recolección de antecedentes (Capítulo 4). Se les envió un resumen de la guía, detallando los puntos abordados con una descripción de estos, solicitando su input en el trabajo realizado.

Juan Pablo Reyes de la empresa LINETS define la guía como corta y precisa. “Creo que la verdad es que no es necesario explicar más allá de lo realizado”.

También destaca el enfoque a tercerizar la implementación, mantención y soporte a proveedores especializados en la temática, destacando que el foco de los organismos del Estado no es ser experto en tecnologías Cloud.

Una segunda entrevista fue realizada con Mario Araneda de la empresa Intesis, para analizar el trabajo realizado. Mario establece: “Estarían todos los puntos necesarios, a mi parecer se encuentran estructurados de manera secuencial con respecto al proceso en cuestión”. También destaca: “La guía toca temáticas específicas que hoy en día no se les da la suficiente importancia y no se abordan con la debida profundidad, temas como el TCO y la estrategia Cloud”. Como recomendación, Mario postula armar un equipo asesor el cual realice una reunión introductoria a la guía para encaminar a las instituciones públicas en la temática. También le parece interesante realizar un complemento a la guía donde se ayude a la institución en cómo proceder a posterior de la contratación e implementación del sistema.

En base al feedback recolectado se puede concluir que se logró identificar los principales aspectos de la tecnología Cloud que conciernen a los organismos del Estado en una estructura lógica referente al proceso de implementación Cloud. Por otro lado, dado la falta de documentos guías sobre la tecnología Cloud referente a instituciones públicas chilenas, se establece que este documento será un complemento para los encargados de evaluar y/o levantar proyectos Cloud al momento de realizar estas tareas ya que en la actualidad la bibliografía referente al contexto Cloud e institución pública chilena es escaza.

Aplicaciones futuras

Se propone una re-enfoque de esta guía enfocada a la astronomía, en donde la aplicación de tecnologías Cloud beneficiaria de sobremanera los diferentes aplicativos que se utilizan en el sector. Actualmente la astronomía es un sector de amplio desarrollo en Chile, donde diversas instituciones desarrollan

constante investigación sobre la temática. La idea sería orientar los puntos establecidos en esta guía en función de las necesidades de dichas instituciones para fomentar el uso de tecnologías Cloud en el sector astrónomo.

Bibliografía

Agencia Europea de seguridad de las redes y de la información. (2011). Seguridad y resistencia en las nubes de la Administración Pública. Informe para la toma de decisiones.

Amazon. (2016). AWS TCO calculator. Obtenido de https://awstcocalculator.com/

Asicom Data Center. (2016). Datacenter en chile: no todo lo que brilla es tier. Obtenido de http://www.asicomdatacenter.com/datacenter-en-chile-no-todo-lo-que-brilla-es-tier/

Centro de Gobierno Electrónico, U. (2015). Modelo de Madurez de Gobierno Digital.

CISCO. (2011). Cloud Computing Concerns in the Public Sector.

Cloud Standards Customer Council. (2014). Practical Guide to Cloud Computing.

Cloud Tech. (2015). Federal agencies like the cloud – but aren't ready to commit yet. Obtenido de cloudcomputing-news: http://www.cloudcomputing-news.net/news/2015/jan/27/federal-agencies-cloud-arent-ready-commit-yet/

Datacenter Dynamics. (2015). CHILECOMPRA FACILITA LA ADQUISICIÓN DE SERVICIOS EN LA NUBE. Obtenido de Datacenter Dynamics: http://www.datacenterdynamics.es/focus/archive/2015/02/chilecompra-facilita-la-adquisici%C3%B3n-de-servicios-en-la-nube

DE, A. E. (2001). Seguridad y resistencia en las nubes de la Administración Pública. Informe para la toma de decisiones.

Departamento de informática UTFSM. (2012). A Methodology to Evaluate ICT Platforms in the Implementation of e-Government.

Digital Market Place. (2015). Digital Market guidance: G-Cloud framework. Obtenido de Digital Market guidance: G-Cloud framework: https://www.digitalmarketplace.service.gov.uk/g-cloud/framework

Emol. (2015). Obtenido de http://www.emol.com/noticias/Tecnologia/2015/12/17/764328/Confirman-que-falla-en-WhatsApp-en-Chile-se-debio-al-bloqueo-en-Brasil.html

Empresa de transporte de pasajeros metro SA. (2015). SERVICIO DE RESPALDO EN LA NUBE. Obtenido de MercadoPúblico: https://www.mercadopublico.cl/Procurement/Modules/RFB/DetailsAcquisition.aspx?qs=5mnWZWPZk7gUim5fxOzWrsC1PX6pToKrx80vWSsEihkohWqH12ULdvwUVkjI4Ecy

ENISA. (2011). Seguridad y resistencia en las nubes de la Administración Pública.

European Comission. (2014). European Cloud Partnership. Obtenido de https://ec.europa.eu/digital-agenda/en/european-cloud-partnership

European Commission. (2014). Cloud Service Level Agreement Standardisation Guidelines. brussels.

European Comssion. (2012). Unleashing the Potential of Cloud Computing in Europe. Obtenido de http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

Gsoedl, J. (2011). Techtarget. Obtenido de Hybrid cloud storage: http://searchstorage.techtarget.com/magazineContent/Hybrid-cloud-storage

INTECO . (2011). Resumen ejecutivo del Estudio sobre cloud computing en el sector público en España.

Leviathan Security Group. (2015). Value of Cloud Security: Vulnerability.

Ley 19.628. (18 de 8 de 1999). SOBRE PROTECCION DE LA VIDA PRIVADA. Obtenido de http://www.leychile.cl/Navegar?idNorma=141599

Ley 19.866. (30 de 7 de 2003). LEY DE BASES SOBRE CONTRATOS ADMINISTRATIVOS DE SUMINISTRO Y PRESTACION DE SERVICIOS. Obtenido de https://www.leychile.cl/Navegar?idNorma=213004

Ley 20.285. (11 de 8 de 2008). SOBRE ACCESO A LA INFORMACIÓN PÚBLICA. Obtenido de http://www.leychile.cl/Navegar?idNorma=276363

Mercado Público . (2015). Chile se convierte en el primer país de Latinoamérica donde el Estado podrá contratar servicios en la nube (cloudstore) y de Datacenter. Obtenido de Mercado Público: https://www.mercadopublico.cl/portal/CloudDataCenter/que_es.html

National Institute of Standards and Technology. (2011). The NIST Definition of Cloud Computing.

Network World. (2015). http://www.networkworld.com/. Obtenido de http://www.networkworld.com/article/2866950/cloud-computing/which-cloud-providers-had-the-best-uptime-last-year.html

Network World. (2015). Which cloud providers had the best uptime last year? Obtenido de Network World: http://www.networkworld.com/article/2866950/cloud-computing/which-cloud-providers-had-the-best-uptime-last-year.html

Seguridad de la Información. (2015). Obtenido de Web Ministerio de educación: http://web.minsal.cl/seguridad_de_la_informacion/

TechTarget. (2011). cloud services reseller. Obtenido de techtarget: http://searchcloudprovider.techtarget.com/definition/cloud-services-reseller

UMGD. (2014). Buenas prácticas en materia de contratación de Servicios de Computación en la Nube (Cloud Computing) al interior de la Administración del Estado.

Uptime Institute. (1990). Tier Classification System. Obtenido de https://uptimeinstitute.com/tiers

Wikipedia. (2015). Wikipedia. Obtenido de Service level agreement: https://en.wikipedia.org/wiki/Service-level_agreement

Anexos

Anexo 1: Tabla de instituciones públicas según nivel de madurez y segmento de inversión TI.

Institución	Nombre Institución	Nivel de Madurez	Segmento
DIRGEOOPP	Dirección General de Obras Públicas	2	1
UAF	Unidad de Análisis Financiero	2	1
CHILECOMPRA	Dirección de Compras y Contratación Pública	3	1
SCJ	Superintendencia de Casinos de Juego	2	1
SubEdu	Subsecretaría de Educación	2	1
INH	Instituto Nacional de Hidráulica	2	1
SSFFAA	Subsecretaría para las Fuerzas Armadas	2	1
SRA	Subsecretaría de Redes Asistenciales	2	1
SUPERDESALUD	Superintendencia de Salud	3	1
SMA	Superintendencia del Medio Ambiente	2	1
SRCel	Servicio de Registro Civil e Identificación	2	1
SAG	Servicio Agrícola y Ganadero	2	1
SII	Servicio de Impuestos Internos	3	1
SVS	Superintendencia de Valores y Seguros	3	1
Tesorería	Servicio de Tesorerías	3	1
SSBN	Subsecretaría de Bienes Nacionales	2	1
MTT	Secretaría y Administración General de Transportes	2	1
CENABAST	Central de Abastecimiento del Sistema Nacional de	2	1
SEC	Superintendencia de Electricidad y Combustibles	3	1
INAPI	Instituto Nacional de Propiedad Industrial	2	1
CNE	Comisión Nacional de Energía	2	1
ODEPA	Oficina de Estudios y Políticas Agrarias	2	1
SERNAC	Servicio Nacional del Consumidor	2	1
DPP	Defensoría Penal Pública	3	1
MINTRAB	Subsecretaría del Trabajo	2	2
SERNAGEOMIN	Servicio Nacional de Geología y Minería	2	2
SBIF	Superintendencia de Bancos e Instituciones Financi	3	2
SERVICIO CIVIL	Dirección Nacional del Servicio Civil	2	2
SP	Superintendencia de Pensiones	2	2
SML	Servicio Médico Legal	2	2
JAC	Junta de Aeronáutica Civil	3	2
ONEMI	Oficina Nacional de Emergencia	2	2
CDE	Consejo de Defensa del Estado	2	2
CONAF	Corporación Nacional Forestal	2	2
SubSecretaría de Hacienda	Secretaría y Administración General	2	2
SISS	Superintendencia de Servicios Sanitarios	2	2
SUPEREDUC	Superintendencia de Educación	2	2
DIRECON	Dirección General de Relaciones Económicas Interna	2	2
FNE	Fiscalía Nacional Económica	2	2

SSDEFENSA	Subsecretaría de Defensa	2	2
SEA	Servicio de Evaluación Ambiental	3	2
SBMA	Subsecretaría del Medio Ambiente	2	2
MINMINERIA	Secretaría y Administración General	2	2
SUBSECRETARIA DE OP	Secretaría y Administración General	2	2
SUSESO	Superintendencia de Seguridad Social	2	2
PREVISIÓN SOCIAL	Subsecretaría de Previsión Social	2	2
SBES	Subsecretaría de Evaluación Social	2	2
SERNATUR	Servicio Nacional de Turismo	2	2
DIPRES	Dirección de Presupuestos	2	2
DGAC	Dirección General de Aeronáutica Civil	2	2
SubEcoPYMe	Subsecretaría de Economía y Empresas de Menor Tama	2	2
SUBTEL	Subsecretaría de Telecomunicaciones	2	2
AGENCIA EDUCACIÓN	Agencia de Calidad de la Educación	1	2
MINREL	Secretaría y Administración General y Servicio Ext	3	2
DIBAM	Dirección de Bibliotecas, Archivos y Museos	2	2
AGCI	Agencia de Cooperación Internacional de Chile	2	2
MINVU	Subsecretaría de Vivienda y Urbanismo	3	2
CNTV	Consejo Nacional de Televisión	2	2
INE	Instituto Nacional de Estadísticas	2	3
CCHEN	Comisión Chilena de Energía Nuclear	3	3
DICREP	Dirección General de Crédito Prendario	2	3
ISL	Instituto de Seguridad Laboral	2	3
SERCOTEC	Servicio de Cooperación Técnica	2	3
CIECHILE	Comité de Inversiones Extranjeras	2	3
SSP	Subsecretaría de Salud Pública	2	3
CNCA	Consejo Nacional de la Cultura y las Artes	2	3
SubSe	Subsecretaría del Interior	2	3
SubPreDel	Subsecretaría de Prevención del Delito	2	3
INACH	Instituto Antártico Chileno	2	3
SSOHIGGINS	Servicio de Salud Libertador General Bernardo O'Hi	1	3
SSTALCAHUANO	Servicio de Salud Talcahuano	2	3
SSARAUCO	Servicio de Salud Arauco	2	3
CNR	Comisión Nacional de Riego	2	3
SSBIOBIO	Servicio de Salud Bio-Bio	2	3
SSMetropolitanoC	Servicio de Salud Metropolitano Central	2	3
SSCONCEPCION	Servicio de Salud Concepción	1	3
SSVIÑA	Servicio de Salud Viña del Mar - Quillota	2	3
GENDARMERIA	Gendarmeria de Chile	2	3
DIRECTEMAR	Dirección General del Territorio Marítimo	2	3
SSMO	Servicio de Salud Metropolitano Oriente	2	3
MINAGRI	Subsecretaría de Agricultura	2	3

SUBPESCA	Subsecretaría de Pesca y Acuicultura	2	3
SSOSORNO	Servicio de Salud Osorno	2	3
DIFRON	Dirección de Fronteras y Límites del Estado	2	3
SSÑUBLE	Servicio de Salud Ñuble	2	3
SSMN	Servicio de Salud Metropolitano Norte	2	3
SSMAULE	Servicio de Salud Maule	2	3
SSVALPO	Servicio de Salud Valparaíso - San Antonio	1	3
SSMetropolitanoO	Servicio de Salud Metropolitano Occidente	2	3
SSRELONCAVI	Servicio de Salud del Reloncaví	1	3
SENCE	Servicio Nacional de Capacitación y Empleo	2	3
INDAP	Instituto de Desarrollo Agropecuario	2	3
FOSIS	Fondo de Solidaridad e Inversión Social	3	3
SSMS	Servicio de Salud Metropolitano Sur	2	4
SSMSO	Servicio de Salud Metropolitano Sur-Oriente	2	4
SENDA	Servicio Nacional de Prevención y Rehabilitación	2	4
PARQUEMET	Parque Metropolitano	2	4
CORFO	Corporación de Fomento de la Producción	3	4
JUNJI	Junta Nacional de Jardines Infantiles	2	4
SSARAUCANIAN	Servicio de Salud Araucanía Norte	2	4
DIPRECA	Dirección de Previsión de Carabineros de Chile	2	4
IND	Instituto Nacional de Deportes	2	4
CONICYT	Comisión Nacional de Investigación Científica y Te	2	4
SENAME	Servicio Nacional de Menores	2	4
CAPREDENA	Caja de Previsión de la Defensa Nacional	3	4
SENAMA	Servicio Nacional del Adulto Mayor	2	4
SBSS	Subsecretaría de Servicios Sociales	2	4
IPS	Instituto de Previsión Social	2	4
INJUV	Instituto Nacional de la Juventud	2	4
CONADI	Corporación Nacional de Desarrollo Indígena	2	4
FONASA	Fondo Nacional de Salud	2	4
MINDEP	Subsecretaría del Deporte	2	4
DARQ	Dirección de Arquitectura	2	4
DOPOR	Dirección de Obras Portuarias	2	4
DIPLAN	Dirección de Planeamiento	2	4
SENADI	Servicio Nacional de la Discapacidad	2	4
SERNAPESCA	Servicio Nacional de Pesca y Agricultura	2	4
MINJUSTICIA	Subsecretaría de Justicia	2	4
SUPERIR	Superintendencia de Insolvencia y Reemprendimiento	2	4
DCONyFIN	Dirección de Contabilidad y finanzas	1	4
DOH	Dirección de Obras Hidraúlicas	1	4

Anexo 2: Tablas de comparación de costos para Cloud v/s Local para mediana y gran organización.

Tabla 0.1: Comparación costo de implementación entre ambiente Local y Cloud para un organización mediana.

		Local		Cloud	
Item	Price ($)	Quantity	Cost ($)	Quantity	Cost ($)
Installation Costs (per server / per hour)	125	32	4,000	8	1,000
Workstation Configuration (per system / per hour)	125	500	62,500	500	62,500
Total Implementation Costs			66,500		63,500

Tabla 0.2: Comparación costos de mantenimiento entre ambiente Local y Cloud para una organización mediana.

		Local		Cloud	
Item	Price ($)	Quantity	Cost ($)	Quantity	Cost ($)
Power & Cooling - 45 Drive NAS[15]	415	2	830	0	0
Power & Cooling - PowerEdge R520	329	2	658	1	329
Power & Cooling - Backup Hardware	110	2	220	0	0
Patching (per event / per server)	149	48	7,152	12	1,788
Maintenance Agreement - NAS Hardware	3,213	2	6,426	0	0
Maintenance Agreement - Servers	7,864	2	15,730	1	7,864
Yearly Cloud Subscription - see Table 15	83,390	0	0	1	83,390
Total Operations Costs			31,016		93,371

Tabla 0.3: Comparación Costo Hardware/Software entre ambiente Local y Cloud para una organización mediana.

Item	Price ($)	Local Quantity	Local Cost ($)	Cloud Quantity	Cloud Cost ($)
45 Drive NAS[12] Intel Dual-core i3-3240 8GB RAM Gigabit Network Card	7,437	2	14,875	0	0
Disks - Seagate 4TB STBD4000400[13]	180	90	16,200	0	0
Backup Hardware - Server Hardware (PowerEdge R520)	4,037	1	4,037	0	0
Backup Hardware - Tandberg Data T160 Tape Library[14]	21,420	2	42,840	0	0
Backup Media (Tapes LTO-6)	47	83	3,943	0	0
Anti-Virus Software - Server Hardware (PowerEdge R520)	4,037	1	4,037	1	4,037
Anti-Virus Software - Client Licenses (including year 2 & 3 maintenance)	29,106	1	29,106	1	29,106
Windows 2012 R2 Server (backup and AV Servers)	882	2	1,764	1	882
Total Hardware & Software			116,802		34,025

Tabla 0.4: Comparación costo de implementación entre ambiente Local y Cloud para una organización grande.

Item	Price ($)	Local Quantity	Local Cost ($)	Cloud Quantity	Cloud Cost ($)
Installation Costs (per server / per hour)	125	40	5,000	16	2,000
Workstation Configuration (per system / per hour)	125	2500	312,500	2500	312,500
Total Implementation Costs			317,500		314,500

Tabla 0.5: Comparación costos de mantenimiento entre ambiente Local y Cloud para una organización grande.

		Local		Cloud	
Item	Price ($)	Quantity	Cost ($)	Quantity	Cost ($)
Power & Cooling - SAN[18]	701	2	1,402	0	0
Power & Cooling - Backup Library	110	5	550	0	0
Power & Cooling - AV/Backup Servers	329	3	987	3	987
Patching (per event / per server)	149	60	8,940	24	3,576
Maintenance Agreement - NAS Hardware	71,716	1	71,716	0	0
Maintenance Agreement - Backup Hardware	3,213	5	16,065	2	6,426
Yearly Cloud Subscription - see Table 15	449,750	0	0	1	449,750
Total Operations Costs			99,660		460,739

Tabla 0.6: Comparación Costo Hardware/Software entre ambiente Local y Cloud para una organización grande.

		Local		Cloud	
Item	Price ($)	Quantity	Cost ($)	Quantity	Cost ($)
Storage Area Network - Petarack Hardware[16] 2 - Intel Xeon E5 Sandy-Bridge Processors 512GB of memory Dual head units Dual network cards Dual network cards	375,000	2	750,000	0	0
Disks - Western Digital WD4001FYYG 4TB[17]	360	252	90,881	0	0
Backup Server Hardware (PowerEdge R720xd)	8,712	1	8,712	0	0
Backup Hardware (Tandberg Data T160 Tape Library)	21,420	5	107,100	0	0
Backup Media (Tapes LTO-6)	47	203	9,643		0
Anti-Virus Software - Server Hardware (PowerEdge R720xd)	8,712	2	17,424	2	17,424
Anti-Virus Software - Client Licenses (including year 2 & 3 maintenance)	145,530	1	145,530	1	145,530
Windows 2012 R2 Server	882	3	2,646	2	1,764
Total Hardware & Software			1,131,936		164,718

Anexo 3: Resultado encuesta sobre la relevancia de los 10 puntos de la guía Practical Guide to Cloud Computing a los entrevistados.

Tabla 0.7: Resultados de la encuesta con respecto a la importancia de los puntos planteados en la guía Practical Guide To Cloud Computing

	Jonny Heiss (Intesis)	ManuelSuarez (Synaptic)	Juan Pablo Reyes	Flavia Gomez (HospitalR.D.R)
Preparación de un equipo:	1	5	4	4
Desarrollar una estrategia Cloud:	4	5	4	4
Tipo de Arquitectura Cloud	2	1	1	1
Tipo de servicio Cloud	2	1	1	1
Encargado de desarrollar,	4	4	2	3
Acuerdos de servicio	5	4	3	4
Resolución de problemas de	5	4	5	4
Integración de servicios Cloud con	5	3	2	3
Realizar una prueba de concepto	1	5	1	1
Administración del ambiente Cloud	4	2	4	3