

COMPUTACIÓN EN LA NUBE.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.



Este estudio fue liderado por la Gerencia de Países del Cono Sur del Banco Interamericano de Desarrollo, con apoyo de las divisiones de Gestión Fiscal y Municipal e Innovación para Servir al Ciudadano.



Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

Catalogación en la fuente proporcionada por la Biblioteca Felipe Herrera del Banco Interamericano de Desarrollo.

Computación en la nube: contribución al desarrollo de ecosistemas digitales en países del Cono Sur / Agustina Schijman, Paolo Valenti, Carlos Pimenta, Aitor Cubo Contretas, Fabiano Rodrigues Bastos.

p. cm. — (Monografía del BID ; 827)

1. Cloud computing-Government policy-Southern Cone of South America. 2. Cloud computing-Security measures-Southern Cone of South America. 3. Computer security-Government policy-Southern Cone of South America. 4. Internet in public administration-Southern Cone of South America. I. Schijman, Agustina. II. Valenti, Paolo. III. Pimenta, Carlos. IV. Cubo Contretas, Aitor. V. Bastos, Fabiano Rodrigues. VI. Banco Interamericano de Desarrollo. Country Department Southern Cone. VII. Banco Interamericano de Desarrollo. División de Gestión Fiscal. VIII. Banco Interamericano de Desarrollo. División de Innovación para Servir al Ciudadano. IX. Serie. IDB-MG-827

CLASIFICACIONES JEL: 032, H70, H83

Palabras clave: Computación en la nube, gobierno digital, ciberseguridad, infraestructura como servicio, plataforma como servicio, software como servicio, nube híbrida, nube privada, nube pública

Copyright © 2020 Banco Interamericano de Desarrollo ("BID"). Esta obra se encuentra sujeta a una licencia Creative Commons IGO 3.0 Reconocimiento – No Comercial – Compartir Igual (CC-IGO 3.0 BY-NC-SA)(<http://creativecommons.org/licenses/by-nc-sa/3.0/igo/legalcode>) y puede reproducirse para cualquier fin no comercial, sea como obra original o como cualquier obra derivada, siempre que se le otorgue el reconocimiento respectivo al BID y que las obras derivadas estén sujetas a una licencia que prevea los mismos términos y condiciones que la licencia aplicable a la obra original. El BID no es

responsable de los errores contenidos en obras derivadas ni en omisiones respecto a las mismas y no garantiza que dichas obras derivadas no infrinjan derechos de terceros. Cualquier disputa relacionada con el uso de las obras del BID que no pueda resolverse amistosamente se someterá a arbitraje de conformidad con las reglas de la CNUDMI (UNCITRAL). El uso del nombre del BID para cualquier fin distinto al reconocimiento respectivo y el uso del logotipo del BID, no están autorizados por esta licencia CC-IGO y requieren de un acuerdo de licencia adicional.

Note que el enlace URL incluye términos y condiciones adicionales de esta licencia.

Las opiniones expresadas en esta publicación son de los autores y no necesariamente reflejan el punto de vista del Banco Interamericano de Desarrollo, de su Directorio Ejecutivo ni de los países que representa.

Iconos y vectores www.freepik.es

Diseño editorial, belenolivares.contacto@gmail.com



Banco Interamericano de Desarrollo

1300 New York Avenue, N.W.

Washington, D.C. 20577

www.iadb.org

AUTORES

Agustina Schijman

Economista Senior, VPC/CSC, aschijman@iadb.org

Paolo Valenti

Coordinador Digital, CSC/CAR, pablova@iadb.org

Carlos Pimenta

Especialista Principal, IFD/FMM, carloscp@iadb.org

Aitor Cubo Contretas

(anteriormente) Especialista Senior, IFD/ICS

Fabiano Rodrigues Bastos

Asesor Económico Regional, VPC/CSC, fabianob@iadb.org



Los autores agradecen a José Luis Lupo, Gerente del Departamento de Países del Cono Sur, a Emilio Pineda, jefe de la División de Gestión Fiscal y Municipal y a Lea Giménez, jefa de la División Innovación para Servir al Ciudadano, por su apoyo en el desarrollo de este producto de conocimiento.

También muestran su reconocimiento a Miguel Angel Porrua, Daniel Hernaiz, Ben Roseth y Janaina Borges de Pauda por sus valiosos comentarios y sugerencias. Los autores también quieren agradecer muy especialmente a BlueNote Management, cuyo trabajo de consultoría fue la base para esta publicación.



Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

SECCIÓN

01

**COMPUTACIÓN EN LA NUBE
Y NUEVA GENERACIÓN DE
POLÍTICAS PÚBLICAS**

PÁG. 09

SECCIÓN

03

**DESAFÍOS Y GESTIÓN
DE RIESGOS PARA LA
IMPLEMENTACIÓN**

PÁG. 23

SECCIÓN

05

**EXPERIENCIA DEL CONO
SUR EN LA MIGRACIÓN A LA
COMPUTACIÓN EN LA NUBE**

PÁG. 35

SECCIÓN

07

**LÍNEAS DE TRABAJO
EN LOS PAÍSES DEL
CONO SUR**

PÁG. 85

SECCIÓN

02

**¿DE QUÉ HABLAMOS
CUANDO HABLAMOS DE
COMPUTACIÓN EN LA NUBE?**

PÁG. 15

SECCIÓN

04

**EXPERIENCIA INTERNACIONAL
EN LA MIGRACIÓN A LA
COMPUTACIÓN EN LA NUBE**

PÁG. 29

SECCIÓN

06

**MODELOS DE COSTOS
PARA EL CONO SUR**

PÁG. 77

NOTAS

PÁG. 107

ACRÓNIMOS

AGESIC. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento

ANATEL. Agência Nacional de Telecomunicações

ANTEL. Administración Naçional de Telecomunicaciones

ANS. Acuerdos de Niveles de Servicio

ASI. Agencia de Sistemas de Información

AWS. Amazon Web Services

CaaS. Contenedor como Servicio

CAPEX. Inversiones de Capital

CERTuy. Centro Nacional de Respuesta a Incidentes de Seguridad Informática

CMF. Comisión del Mercado Financiero

CN. Computación en la Nube

DaaS. Escritorio como Servicio

DATAPREV. Empresa de Tecnologia e Informações da Previdência Social

DBaaS. Base de Datos como Servicio

EGD. Estrategia de Governança Digital

ETAP. Estándares Tecnológicos para la Administración Pública

ETICE. Empresa de Tecnologia da Informação do Ceará

FaaS. Funciones como Servicio

GDE. Gestión Documental Electrónica

GDL. Gestión de Documentos en Línea

GSI-PR. Gabinete de Segurança Institucional da Presidência da República

HCEN. Historia Clínica Electrónica Nacional

IA. Inteligencia Artificial

IaaS. Infraestructura como servicio

INE. Iniciativa de la Nube Europea

ISKE. Estandard de Sistemas de Seguridad de Tecnologías de la Información

LAI. Lei de Acesso a Informação

LEATD. Law Enforcement Access to Data

LGPD. Lei Geral de Proteção de Dados Pessoais

MITIC. Ministerio de Tecnologías de la Información y Comunicación

ONTI. Oficina Nacional de Tecnologías de la Información

OPEX. Gastos en Operaciones

PaaS. Plataforma como Servicio

SaaS. Software como Servicio

SEAF. Subsecretaría de Estado de Administración Financiera

SECaaS. Seguridad como Servicio

SENATIC. Secretaría Nacional de Tecnologías de la Información y Comunicación

SERPRO. Serviço Federal de Processamento de Dados

SGD-ME. Secretaria de Governo Digital do Ministério da Economia

STaaS. Almacenamiento como servicio

TCU. Tribunal de Contas da União

TI. Tecnologías de la Información

TIC. Tecnologías de la Información y las Comunicaciones

TOCAF. Texto Ordenado de Contabilidad y Administración Financiera

URCDP. Unidad Regulatoria y de Control de Datos Personales

VDC. Virtual Datacenter



SECCIÓN

01

COMPUTACIÓN EN LA NUBE Y NUEVA GENERACIÓN DE POLÍTICAS PÚBLICAS

LAS TECNOLOGÍAS DIGITALES

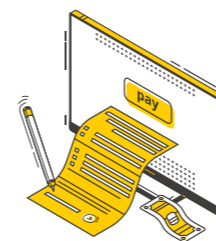
están cambiando la naturaleza
misma de las relaciones entre
CIUDADANOS, EMPRESAS Y
EL ESTADO.

Se están transformando prácticamente todos los aspectos de nuestra cotidianidad, desde cómo interactuamos con otras personas y hacemos compras, a cómo administramos nuestras finanzas y expandimos nuestros contactos laborales. La tecnología digital también está permitiendo a las empresas y las oficinas públicas ofrecer mejores servicios, hacerlo de una forma más productiva y costo-eficiente, conociendo mejor a sus usuarios, dialogando con ellos en algunos casos, habilitando nuevos espacios de participación ciudadana y transformando significativamente todos los procesos y modos de trabajo.

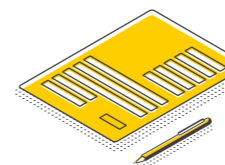
[VOLVER AL ÍNDICE](#)

La computación en la nube (CN) es mucho más que la infraestructura de almacenamiento de información; es la entrega de servicios bajo demanda, por parte de proveedores tecnológicos, de potencia de cómputo, bases de datos, almacenamiento, aplicaciones y otros

recursos de tecnologías de información (TI), a través de internet o redes privadas, con un sistema de precios basado en el consumo. que permite la posibilidad de reducción de tiempos de innovación y de contar con recursos flexibles y economías de escala.



PAGAR IMPUESTOS



APLICAR A VACANTES
ESCOLARES O DE
TRABAJO



REALIZAR TRÁMITES
DE REGISTRO CIVIL,
PUEDEN HACERSE
ON-LINE EN UN NÚMERO
CRECIENTE DE PAÍSES.

COVID - 19

Sin ir más lejos, mientras finalizamos este informe las medidas para enfrentar la crisis del COVID-19 están acelerando todavía más la transformación tecnológica y poniendo a prueba la capacidad del sector público y privado para funcionar mediados por servicios en la nube.



COVID-19

LAS MEDIDAS DE DISTANCIAMIENTO SOCIAL

para contener el riesgo de contagio del nuevo coronavirus han obligado a que interacciones LABORALES, EDUCATIVAS Y SOCIALES pasen a depender de una infraestructura digital.

La infraestructura subyacente permitió un movimiento masivo hacia el teletrabajo, la educación a distancia y el entretenimiento virtual a escala mundial, un fenómeno inimaginable una década atrás. Las herramientas para detectar contagios y dar seguimiento a su expansión también se apoyan en una infraestructura digital.

El procesamiento de imágenes médicas mediante el uso de inteligencia artificial y el análisis de big data de aplicaciones para dar seguimiento a la expansión epidemiológica, por ejemplo, descansan en una infraestructura digital. Sumado a ello, la eficiencia de muchas medidas tomadas por los gobiernos para contener el impacto económico de la crisis del COVID-19 también dependen de la tecnología digital subyacente.

En estos días, el uso de la nube en el sector salud (la telemedicina) está en el centro de la escena, ya que permite almacenar, acceder y procesar enormes volúmenes de datos en tiempo real, a distancia, y diagnosticar ciertos tipos de condiciones en pacientes que de otro modo no hubiesen recibido atención médica a tiempo. A modo más general, la experiencia de algunos países europeos y asiáticos también sugiere que la nube permite un manejo más eficiente y transparente de información pública en el manejo de la crisis, acercando gobierno y ciudadanía. Sumado a ello, a nivel agregado, la tecnología de la nube contribuye una proporción cada vez mayor al PIB de los países y permite ahorros al sector público y privado.

La aceleración de la adopción tecnológica en tiempos del COVID-19 ofrece una ventana de oportunidad para potenciar el uso de servicios en la nube y avanzar hacia una nueva generación de políticas públicas más eficientes y efectivas.

CN

La capacidad de los gobiernos para integrar múltiples bases de datos y sistemas de diferentes organismos públicos (y privados) para identificar a los potenciales beneficiarios de programas de apoyo a hogares vulnerables y empresas, y asegurar una transparente y adecuada asignación de recursos, depende en gran medida de una adecuada infraestructura digital. Específicamente, la tecnología sobre la que descansan estos ejemplos es lo que se conoce como computación en la nube.

80%

Se estima que en países desarrollados, la migración a la nube reduce los gastos de mantenimiento de infraestructura de IT en hasta un 80%. A eso hay que sumarle ahorros derivados de mejoras en procesos y de un menor uso de energía, con impactos medioambientales positivos.

En los países del Cono Sur la migración a la nube es todavía precoz y presenta diferencias entre países, entre el sector público y el privado, y entre industrias dentro del sector privado, como se indica en este reporte:

Las **BARRERAS** más comunes a la adopción de servicios en la nube en nuestros países se relacionan con:

- 1** DEFICIENCIAS DE CONECTIVIDAD E INFRAESTRUCTURA DE REDES
- 2** MARCOS REGULATORIOS
- 3** RESISTENCIA AL CAMBIO Y DÉFICIT DE CAPACITACIÓN PROFESIONAL

De cara al mundo **POST-COVID**, las discusiones sobre el futuro de:

- A** EL TELETRABAJO
- B** LOS FORMATOS EDUCATIVOS DIGITALES
- C** LA PROVISIÓN DE SERVICIOS DE SALUD A DISTANCIA
- D** LA RENDICIÓN DE CUENTAS

entre otros aspectos, pondrán sobre el centro de la escena la necesidad de profundizar la adopción tecnológica en los países del Cono Sur.



BID

En el Banco Interamericano de Desarrollo (BID) estamos observando un interés y una inversión creciente en este tipo de soluciones en la región, lo que nos motivó a realizar un estudio exhaustivo para los países del Cono Sur, es decir, Argentina, Brasil, Chile, Paraguay y Uruguay.

Este reporte sintetiza los principales hallazgos de un análisis más completo sobre el estado de avance y desarrollo de los servicios de CN en el sector público del Cono Sur, llevado a cabo por el Departamento de Países del Cono Sur y las divisiones de Gestión Fiscal y Municipal e Innovación para Servir al Ciudadano, con apoyo de la empresa consultora Blue Note.

En esta síntesis nos enfocamos en los aspectos conceptuales más relevantes de CN y los resultados principales de los estudios realizados en cada país sobre el marco regulatorio, la oferta y la demanda de servicios de CN, en base a trabajo de campo realizado a finales del 2019. El reporte ofrece información útil y novedosa tanto para los equipos del BID que trabajan en la formulación de proyectos que requieren administrar grandes cantidades de datos, como para agentes públicos y privados, tomadores de decisiones e interesados en conocer mejor el ecosistema digital y la realidad de este grupo de países en cuanto al desarrollo y oportunidades de CN.



El documento completo se puede solicitar a
Agustina Schijman al email aschijman@iadb.org



SECCIÓN

02

¿DE QUÉ HABLAMOS CUANDO HABLAMOS DE COMPUTACIÓN EN LA NUBE?

La CN permite a los clientes acceder a los servicios y recursos contratados¹, proporcionando flexibilidad de dimensionamiento y acceso. De esta forma, el cliente, sea un organismo gubernamental, una empresa o un particular, se abstrae, según el caso, de la in-

fraestructura tecnológica necesaria, la plataforma de programación y/o las capacidades de desarrollo para poder utilizar una determinada aplicación, plataforma o hardware, y requiere de un navegador web con conexión a internet para tener acceso.

LOS SERVICIOS DE COMPUTACIÓN EN LA NUBEN SE CLASIFICAN EN 3²

Cada uno de estos modelos de servicio va incorporando capas de usos y aplicaciones que permiten virtualizar funciones originalmente provistas “on-premises”^{*}.

^{*}On premises es cuando una empresa, entidad o individuo posee su propia infraestructura de TI en el establecimiento, con un centro de datos propio, por ejemplo, diferente de la contratación de servicios para utilizar la infraestructura tecnológica de terceros.



IAAS

Infraestructura como servicio, el modelo más simple



Se provee la capacidad para aprovisionar el procesamiento, almacenamiento, redes y otros recursos informáticos fundamentales. Se encuentra mayormente orientado a administradores de TI ya que provee máquinas virtuales, servidores, almacenamiento, balanceadores de carga, equipos de comunicaciones y firewalls.



PAAS

Plataforma como servicio, un modelo un poco más complejo



Provee la capacidad de implementar en la infraestructura de la nube las aplicaciones creadas o adquiridas por el cliente. El cliente no administra ni controla la infraestructura de la nube subyacente, pero tiene control sobre las aplicaciones implementadas y, posiblemente, los ajustes de configuración para el entorno de alojamiento de aplicaciones. Es principalmente utilizada para actividades de desarrollo o de despliegue de aplicaciones, como servidores web, herramientas de desarrollo, bases de datos o big data, por mencionar algunos ejemplos.



SAAS

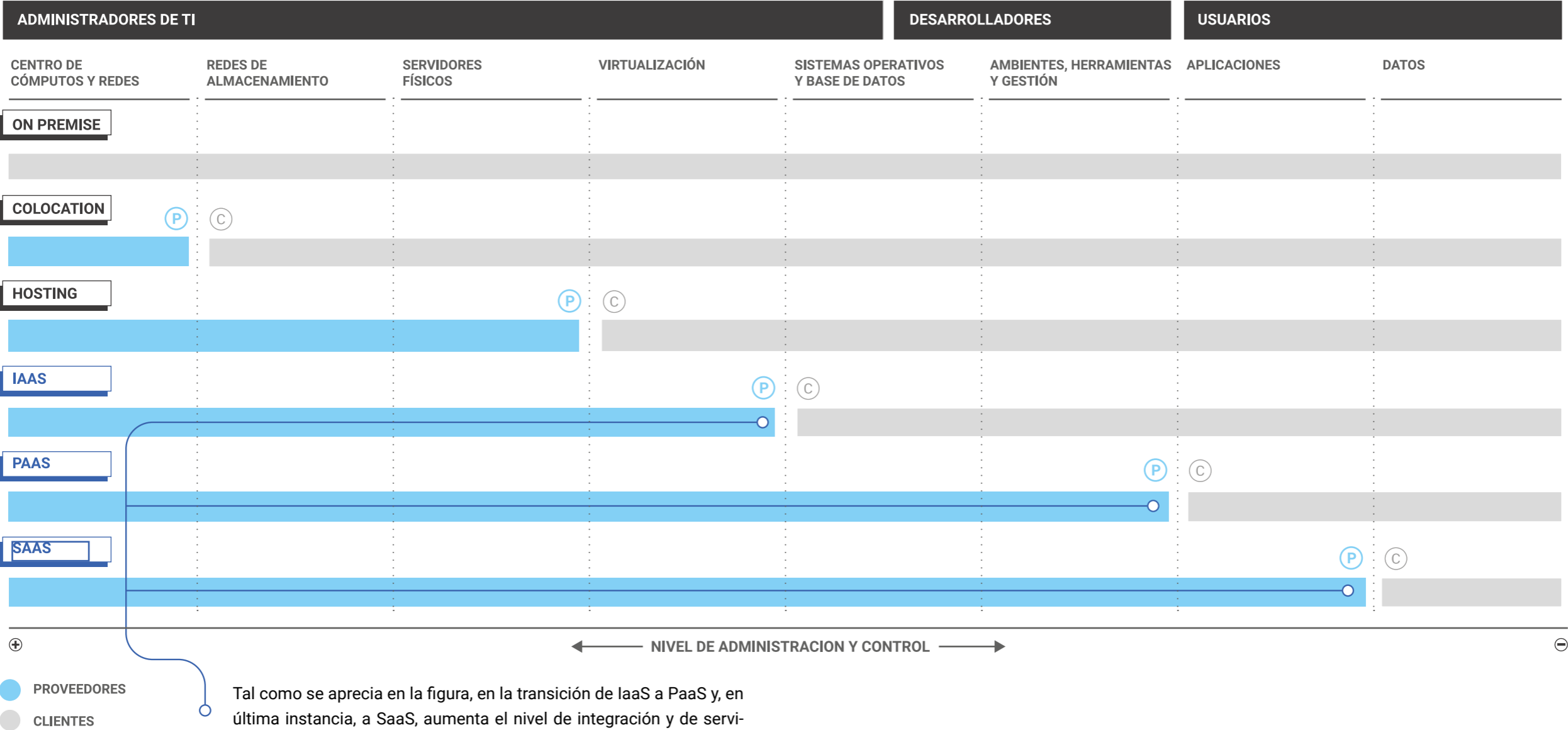
Software como servicio, el modelo más completo



Es la capacidad de uso de aplicaciones que se ejecutan en una infraestructura en la nube. Se puede acceder a las aplicaciones desde varios dispositivos a través de una interfaz de cliente liviana, como un navegador web o un interfaz de programa. El cliente no administra ni controla la infraestructura de la nube subyacente ni es responsable por el desarrollo de las aplicaciones ni por sus actualizaciones. Se encuentra mayormente orientado a usuarios finales. Algunos ejemplos pueden ser sistemas como software de manejo de la relación con el cliente, software de planificación de los recursos de la organización o correo electrónico.



Ilustración 1. Modelos de servicio de CN. Fuente: Análisis propio en base a Gartner



Tal como se aprecia en la figura, en la transición de IaaS a PaaS y, en última instancia, a SaaS, aumenta el nivel de integración y de servicios del proveedor, disminuyendo entonces el nivel de administración y control por parte del cliente.





Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

CADA UNO DE LOS 3 MODELOS DE SERVICIOS EN LA NUBE TIENE VENTAJAS Y DESVENTAJAS

Ilustración 2. Ventajas y desventajas de los modelos de servicio de CN.



IAAS

Evita inversiones de capital (CAPEX) en hardware e instalaciones, migrando hacia costos de operación (OPEX)

Reduce el riesgo del retorno de la inversión respecto a una solución on-premises

Costos de infraestructura compartidos y, por lo tanto, inferiores

Reduce erogaciones en recursos humanos

Bajas barreras de entrada

Escalamiento optimizado y automatizado

Generalmente independiente de la plataforma

Se utilizan generalmente Acuerdos de Niveles de Servicio (ANS)

Pago por uso

Auto escalable



La eficiencia y la productividad del negocio dependen en gran medida de las capacidades del proveedor

Requiere de capacidades de recursos humanos internas para su gestión y administración

Costo puede ser potencialmente mayor a largo plazo (en caso de no tener control sobre el consumo)

Se requiere un conjunto de medidas de seguridad que difieren de las tradicionales

El hecho que datos sensibles de una organización sean almacenados en hardware de un tercero puede ser percibido como una desventaja por algunas organizaciones

Riesgo de lock-in por parte del proveedor



PAAS

Consume infraestructura en la nube

Pago por uso

No se tienen que mantener, actualizar o reemplazar sistemas y software, se obtiene la última tecnología para utilización del negocio

Prueba e implementación de aplicaciones de forma más ágil

Equipos de desarrollo cuentan con la capacidad para la realización de pruebas de varias configuraciones de una aplicación en diferentes entornos, pudiendo optimizarla con mayor velocidad

No todas las aplicaciones pueden construirse para la nube, esto implica modificar aplicaciones para integrarse completamente o dejar algunas fuera de la nube

Buenos niveles de velocidad, confiabilidad y soporte son requeridos por parte del proveedor para justificar el uso de PaaS

Riesgo de lock-in por parte del proveedor



SAAS

Menor costo inicial

Reduce costos de mantenimiento de hardware y software y, consecuentemente, de recursos humanos

No necesariamente requiere recursos humanos especializados

Evita la necesidad de utilización de recursos en la infraestructura subyacente

Minimización de los retrasos en la implementación de software tradicional

Actualizaciones de hardware y software realizadas por el proveedor

Posibilidad de dar servicios digitales avanzados por parte de organizaciones que no tienen capacidades TIC, al prestarse los mismos completos desde la nube

Accesibilidad a través de navegador web y una conexión a internet o red privada

Escalabilidad a partir de las opciones de suscripción y flexibilidad para cambiar las suscripciones por parte de los proveedores

Control de la aplicación de software por parte de un tercero (sus funcionalidades, actualizaciones, etc.)

Limitación en la cantidad y diversidad de aplicaciones

Requisito de conectividad: el modelo SaaS se basa en la entrega web, ante falla del servicio de internet, perderá el acceso a su software o datos

El rendimiento de un SaaS puede ejecutarse a velocidades algo más lentas que las aplicaciones de cliente / servidor en las instalaciones propias

Riesgo de lock-in por parte del proveedor



Computación en la Nube.
Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

ESTOS SERVICIOS SE PUEDEN PRESTAR BAJO 3 MODELOS DE DESPLIEGUE³

Los modelos de despliegue se definen en función de la especificidad y el nivel de ajuste de las soluciones a las necesidades de los usuarios, y no dependen de quién es la propiedad de la nube, sino de su uso.

El siguiente análisis permite tener una visión comparada de los distintos atributos de cada modelo relativo a la escalabilidad, seguridad, rendimiento, confiabilidad, costos y latencia, destacando en azul cuál es el modelo que presenta mayor fortaleza para cada atributo:

Ilustración 3. Análisis comparativo de los modelos de despliegue de CN.



NUBE PÚBLICA

Bajo este modelo de despliegue el proveedor ofrece el servicio a varios clientes desde el mismo centro de cómputo de forma que los clientes comparten recursos de almacenamiento, procesamiento, etc. Brinda una gran escalabilidad, eficiencia y ahorro de costos. Es el modelo más abierto al público, y puede ser propiedad o no de la organización, o contratada, o una combinación.

↑ ALTO → MEDIO ↓ BAJO ↻ VARIABLE

ESCALABILIDAD	↑
SEGURIDAD	↻ Seguridad del proveedor
RENDIMIENTO	→
CONFIABILIDAD	→ Depende de conectividad y proveedor
COSTO	↓ Pago por uso. Sólo costos de operación
LATENCIA	→ Ubicación geográfica del proveedor



NUBE PRIVADA

En este modelo de despliegue, más cerrado, los recursos son entregados de forma exclusiva y privada al cliente (sea un cliente del sector público o del sector privado), y este último tiene el control sobre el servicio que contrata. Los clientes siguen teniendo la flexibilidad de escalar el servicio si precisaran más recursos y el proveedor garantiza la separación de los recursos con los de otros clientes. De esta forma el cliente tendrá un mayor control sobre la seguridad y privacidad de los datos, pero el costo es mayor al del modelo de nube pública. El cliente puede ser una organización del sector público, lo que sería una nube de uso privado para una organización pública.

↓ On-premises → Instalaciones de proveedor
↻ Seguridad del proveedor o propia
→
→ Todos los equipos en instalaciones propias
↻ Costos de recursos locales humanos y de infraestructura (alta en el caso de falta de escala por parte del usuario)
↓ On-premises → Ubicación geográfica del proveedor



NUBE HÍBRIDA

Es la combinación de los modelos de nube privada y pública, pero con una administración única, es decir gestionados desde el mismo panel. También pueden integrarse servicios de centros de cómputo propios en oficinas del cliente (on-premises). Con este esquema se consigue reducción de costos sobre el modelo de nube privada, y permite disponer de nubes integradas por estándares, con portabilidad de datos y de aplicaciones, para el balanceo de carga entre ellas. Por ejemplo, mantener datos sensibles en una nube privada, conectada a una nube pública para escalabilidad y picos de demanda.

↑ Por escalabilidad de nube pública
↻ Permite añadir capas adicionales de seguridad
→ ↑
↑ Equipos en instalaciones propias, sujeto a la conectividad y disponibilidad
→ Reducción significativa de costos de recursos locales
↓ →





SECCIÓN

03

DESAFÍOS Y GESTIÓN DE RIESGOS PARA LA IMPLEMENTACIÓN

CIBERSEGURIDAD Y CLASIFICACIÓN DE DATOS

La clasificación de datos implica identificar el tipo de información, la sensibilidad para el usuario y los posibles impactos de existir una pérdida o filtración al momento de procesar y almacenar en un sistema de información propio u operado por un tercero.

Por ejemplo, los datos que se consideran “restringidos” deben tratarse con un estándar de atención más alto que los datos “sin restricciones” consumidos por el público en general. La clasificación de datos ayuda a la organización a evaluar los riesgos asociados con diferentes tipos de datos. Las organizaciones de estándares, como la Organización Internacional de Estándares y el Instituto Nacional de Estándares y Tecnología, recomiendan esquemas de clasificación de datos para que la información se pueda administrar y asegurar de manera más efectiva de acuerdo con su riesgo y criticidad relativa, desaconsejando prácticas que tratan todos los datos por igual.

El manejo de datos, su almacenamiento y flujo, a partir del uso de CN conlleva una relación de confianza entre proveedores, administradores y usuarios que enfrenta varios desafíos de ciberseguridad. Entender los riesgos, y fundamentalmente diferenciar,

segmentar y clasificar los datos, asignando responsabilidades en estas nuevas cadenas de valor transaccional, será fundamental para gestionar eficientemente las posibles soluciones a las vulnerabilidades.

Las responsabilidades de clasificación de datos variarán según el modelo de servicio en la nube, como se muestra en la siguiente ilustración.

Ilustración 4. Análisis comparativo de los modelos de despliegue de CN.

	IAAS	PAAS	SAAS
CLASIFICACIÓN DE DATOS Y RESPONSABILIDAD			
PROTECCIÓN DEL CLIENTE			
GESTIÓN DE IDENTIDAD Y ACCESO			
CONTROLES DE NIVEL DE APLICACIÓN			
CONTROLES DE RED			
SEGURIDAD DEL HOST			
SEGURIDAD FÍSICA			

PROVEEDORES CLIENTES



Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

PROTECCIÓN DE DATOS SEGÚN LOS 3 MODELOS

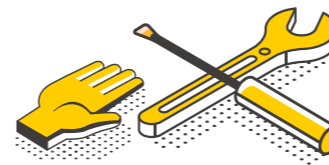
Aunque los clientes son responsables de clasificar sus datos, los proveedores de la nube deben hacer compromisos por escrito con los clientes sobre cómo protegerán y mantendrán la privacidad de los datos almacenados en su nube. Estos compromisos deben incluir información sobre prácticas de privacidad y seguridad, limitaciones de uso de datos y cumplimiento normativo. Además, los proveedores de la nube deben hacer certificaciones e informes de auditoría que demuestren el cumplimiento de estándares para que los clientes puedan verificar la efectividad de las prácticas de su proveedor de la nube. Tener esta información ayudará a los clientes a comprender si el proveedor de la nube admite los requisitos de protección de datos exigidos por su clasificación de datos.



PROVEEDORES DE IAAS



Desde una perspectiva de clasificación de datos, los requisitos del proveedor de IaaS se limitan a garantizar que el entorno virtual pueda acomodar las capacidades de clasificación de datos y los requisitos de cumplimiento del cliente. Los proveedores de IaaS tienen un papel menor en la clasificación de datos porque sólo necesitan asegurarse que los datos del cliente aborden los requisitos de cumplimiento. Sin embargo, los proveedores deben asegurarse de que sus entornos virtuales aborden los requisitos de clasificación de datos además de proteger sus centros de datos.



PROVEEDORES DE PAAS



Las responsabilidades pueden ser mixtas, porque la plataforma podría usarse en un enfoque por capas para proporcionar seguridad a una herramienta de clasificación. Los proveedores de PaaS pueden ser responsables de la autenticación y posiblemente de algunas reglas de autorización, y deben proporcionar capacidades de seguridad y clasificación de datos a su capa de aplicación. Al igual que los proveedores de IaaS, los proveedores de PaaS deben asegurarse que su plataforma cumpla con los requisitos de clasificación de datos relevantes.



PROVEEDORES DE SAAS



Con frecuencia serán considerados como parte de una cadena de autorización y deberán asegurarse de que los datos almacenados en la aplicación SaaS puedan controlarse por tipo de clasificación. Las aplicaciones SaaS se pueden usar para aplicaciones de línea de negocio y, por su propia naturaleza, deben proporcionar los medios para autenticar y autorizar los datos que se usan y almacenan.



Para una implantación y operación exitosas de CN es importante considerar una gestión de riesgos y tomar medidas preventivas antes y durante estos procesos, mitigando las posibilidades de eventuales problemas, conforme presentado en la tabla a continuación.

VENDOR LOCK-IN, INTERRUPCIÓN DE SERVICIOS, DATOS:




RIESGO	DESCRIPCIÓN	RECOMENDACIONES
<div><div>Imposibilidad de salida del servicio y cambio de proveedor (“vendor lock-in”)</div></div>	<ul style="list-style-type: none">• Se entiende por “vendor lock-in” el uso restringido o propietario de una tecnología, solución o servicio desarrollado por un proveedor. Esta situación suele tener asociados enormes costos si el cliente quiere cambiar de proveedor (ya sea por la dificultad y recursos necesarios para hacer el cambio).• Un proveedor puede intentar crear dependencia hacia sus servicios por parte de sus clientes. Lo que se consigue mediante el desarrollo de soluciones a medida que dependan de la plataforma con software, aplicaciones, hardware o equipos propietarios, o contratos únicos de servicios.	<ul style="list-style-type: none">• Fijar políticas de priorización de desarrollos basados preferentemente en código abierto. La contratación de desarrollos propietarios deberá contar con expresa autorización o justificación por falta de disponibilidad de alternativas abiertas que satisfagan los requerimientos. Adicionalmente, analizar estratégicamente la forma de contratación de servicios de CN, tratando de evitar concentrar todo en solamente un proveedor y buscando distribuir estos contratos para minimizar la dependencia de solamente una empresa o de una organización.
<div><div>Interrupción del servicio por falta o demora en los pagos</div></div>	<ul style="list-style-type: none">• Al tratarse de organismos gubernamentales, puede ocurrir que las partidas presupuestarias puedan tener atrasos de tiempos considerables y, si la falta o atraso del pago produjera una interrupción del servicio, el riesgo de contratar a dicho proveedor sería crítico.	<ul style="list-style-type: none">• Desarrollar un fondo de previsión para cubrir situaciones de indefinición presupuestaria, cambios políticos y administrativos.• Adicionalmente, el despliegue de nubes híbridas constituye un mitigante adicional.• Por último, resulta importante establecer en los contratos los plazos adecuados para tolerancia en eventuales retrasos de pago.
<div><div>Acceso no autorizado a datos sensibles</div></div>	<ul style="list-style-type: none">• El procesamiento o tratamiento de datos sensibles fuera de las instalaciones de la empresa conlleva un riesgo, ya que se tiene control limitado sobre la posibilidad que se sorteen los controles físicos, lógicos y humanos.	<ul style="list-style-type: none">• Definir una política de control de acceso. Trabajar únicamente con proveedores que garanticen al menos un mínimo nivel de protección mínimo requerido para la protección de acceso a los datos y que permitan la realización frecuente de auditorías por parte del cliente.• Incorporar ANS que establezcan penalidades al proveedor de los servicios de nube, ante accesos no autorizados a datos sensibles.

Ilustración 5: Matriz de riesgos para la implementación de servicios de CN.

RIESGO	DESCRIPCIÓN	RECOMENDACIONES
<div><div>Incumplimiento normativo</div></div>	<ul style="list-style-type: none">• Los clientes son en última instancia responsables de la seguridad e integridad de sus datos, aunque éstos se encuentren fuera de las instalaciones y gestionados por un proveedor de servicios en la nube.	<ul style="list-style-type: none">• Los proveedores de servicios de CN deben prestarse a controles y auditorías, privadas y de los entes públicos, tal como están sujetos los proveedores tradicionales del estado.
<div><div>Pérdida de control por efecto de la localización de los datos</div></div>	<ul style="list-style-type: none">• Law enforcement access to data (LEATD). Riesgo por pérdida de control de la información si la misma es transferida a otra jurisdicción legal o, incluso, si se procesa localmente, pero por un proveedor de servicios que está sujeto a jurisdicción de tribunales extranjeros. Es una preocupación de alta relevancia dado que los principales proveedores de IaaS, y muchos de los principales proveedores de PaaS y SaaS, son empresas con sede en los EE.UU.	<ul style="list-style-type: none">• Se debe consultar con los proveedores cuál es el marco regulatorio aplicable al almacenamiento y procesamiento de datos, siendo una buena práctica lograr acuerdos para que el tratamiento de los datos se subyugue al marco legal del país del suscriptor del servicio⁴.
<div><div>Acceso no autorizado a datos generales</div></div>	<ul style="list-style-type: none">• Los datos en los entornos de nube comparten infraestructura con datos de otros clientes generando riesgo de acceso no autorizado.	<ul style="list-style-type: none">• El proveedor de CN debe garantizar el aislamiento de los datos de los respectivos clientes y que los procedimientos de cifrado de la información se realizarán acordermente.
<div><div>Ausencia de protocolo de recuperación de datos</div></div>	<ul style="list-style-type: none">• La recuperación de datos es una necesidad frecuente, no siempre contemplada en todos sus niveles por los proveedores de CN.	<ul style="list-style-type: none">• Se debe exigir al proveedor que los datos sean replicados en múltiples infraestructuras para evitar que sean vulnerables a un fallo general.
<div><div>Inviabilidad a largo plazo</div></div>	<ul style="list-style-type: none">• Ante un mercado cambiante, y ante la aparición de nuevas tecnologías, se debe garantizar la sostenibilidad y evolución del abastecimiento de servicios de CN.	<ul style="list-style-type: none">• El cliente debe asegurarse la sostenibilidad y permanencia de sus datos en cualquier escenario, incluyendo la posibilidad de que los datos puedan ser migrados.





SECCIÓN

04

EXPERIENCIA INTERNACIONAL EN LA MIGRACIÓN A LA CN

LA MIGRACIÓN A LA CN SE DA TRAS VARIOS AÑOS DE TRABAJO EN LA DIRECCIÓN DE LA DIGITALIZACIÓN DEL ESTADO

Estos países han iniciado la digitalización del Estado cuando la computación en la nube no existía o se encontraba en etapas embrionarias.



En el **Cono Sur**, las políticas de digitalización ocurren con un mayor desarrollo y avance de las tecnologías y servicios de CN.

El objetivo de esta sección es aprender cuáles han sido los principales factores habilitantes para que cinco países extra-regionales, Corea del Sur, Estonia, Reino Unido, Israel y España, sean considerados casos de éxito en el ámbito de CN en el sector público. Los cinco casos ofrecen distintas trayectorias y expe-

riencias en la modernización de la gestión de la administración pública y se han apoyado en los servicios en la nube de acuerdo con las necesidades específicas de las agencias de gobierno, tamaño del mercado o la población usuaria, capacidad financiera, regulación, legado y prioridades políticas.

En el caso del Reino Unido y Corea del Sur se distingue una mayor complejidad de la formación de las políticas de migración y uso de la nube que responden a su tamaño y la necesidad de experimentación más descentralizada a través de pilotos, como experiencias acotadas, que luego se han puesto a disposición del resto de la administración.

En el caso de España, si bien no existe una política específica de uso de nube ("cloud first"), se han promulgado leyes y decretos que apuntan a ello, como establecer un esquema nacional de interoperabilidad, un esquema nacional de seguridad en el ámbito de la administración electrónica, una ley de acceso electrónico de los ciudadanos a los servicios públicos, la implementación de factura electrónica, y la instrumentación de las tecnologías de la información y las comunicaciones en la administración general del estado y sus organismos públicos.

El caso de Corea se distingue un mayor "dirigismo" centralizado, más allá de planificaciones nacionales, que han permitido que distintas agencias hagan sus propios desarrollos.

Los casos de Estonia e Israel se caracterizan por su mayor flexibilidad para adoptar soluciones nacionales que impacten de raíz y que utilicen proveedores establecidos, aunque en Israel se debe resaltar un mayor nivel de preocupación respecto a la seguridad de los datos.

La siguiente ilustración incluye el resumen del relevamiento realizado.





Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.



	1 EXISTENCIA DE UN ENCUADRE REGULATORIO ESPECIFICO	2 EXISTENCIA DE UN PLAN RECTOR NACIONAL	3 PROTECCIÓN DE DATOS Y CIBERSEGURIDAD	4 AUTORIDAD LÍDER FIJADORA DE LINEAMIENTOS Y ESTÁNDARES	5 INICIATIVAS DESCENTRALIZADAS	6 ACCESO NO AUTORIZADO A DATOS GENERALES	7 MODELOS DE DESPLIEGUE
C.S. 	 Fomento a la Computación en la Nube y la Protección de sus Usuarios (2015) ⁵	 Plan de Desarrollo de Computación en la Nube 2016-2021 ⁶	 Leyes de Protección de Información Personal (2011) ⁸ , de Promoción de uso de redes de IT y Protección de información (2015) ⁹	 Ministerio de Ciencia y TIC (MSIP); Ministerio de Seguridad y Administración Pública (MOPAS)	 No, todas las iniciativas son impulsadas por el gobierno central	 Medio. Iniciativas centralizadas, implementadas por diferentes agencias	 Nube híbrida, (privada sobre datacenter propio integrado y pública de PSN privados)
EST. 	 Sí. Definición a través de planes estratégicos y políticas específicas	 Plan e-estonia (comenzado en 1997)	 GDPR. Centro de Excelencia Cooperativo de Ciberdefensa de la OTAN 2008 (CCDCOE) por iniciativa de Estonia	 Oficina del CIO dentro del Ministerio de Asuntos Económicos y Comunicaciones, basado en normas ISKE	 Todas las iniciativas son impulsadas por el gobierno central	 Alto nivel de cooperación	 Nube Híbrida. Uso de nube pública y privada fuera de las fronteras del país
ING. 	 Sí. Definición a través de planes estratégicos y políticas específicas	 Estrategia para la Transformación del Gobierno de 2017-2020 ⁷	 GDPR. Ley de Protección de Datos (2018) ¹⁰	 Jefatura de Gabinete ¹¹	 Centralizadas en la plataforma de compra digital ¹²	 Alto. Cada agencia canaliza su requerimiento a través de la plataforma	 Presenta los tres modelos de despliegue
ISR. 	 No. Leyes relevantes: Privacidad, Libertad y Dignidad Humana	 Programa Digital Israel (Ministerio de Igualdad Social)	 Ley de Privacidad. Autoridad Nacional de Ciberseguridad (2017)	 Ministerio de Telecomunicaciones y Ministerio de Igualdad Social a través del Programa Digital Nacional	 Todas las iniciativas son impulsadas por el gobierno central	 Alto. Por ejemplo el sitio gov.il en el que participan todas las oficinas gubernamentales	 Nubes tercerizadas en territorio israelí
ESP. 	 Sí, leyes 11/2007, 25/2013, 39/2015, 40/2015 y reglamentaciones	 Plan de Transformación Digital de la Adm. Gral. del Estado y sus Org. Públicos (Estrategia TIC 2015 – 2020)	 GDPR. Centro de Excelencia Cooperativo de Ciberdefensa de la OTAN 2008 (CCDCOE) en la que España es parte	 Secretaría General de Administración Digital, dentro del Ministerio de Asuntos Económicos y Transformación	 Alta descentraliza-ción con buena interacción entre nube del estado nacional, nivel subnacional y privados.	 Alto. Existe interoperabilidad entre los distintos organismos gubernamentales entre si y con privados	 Nube híbrida.

Ilustración 6: Caracterización de experiencias en otras regiones.

UN DENOMINADOR COMÚN DE LOS 5 CASOS DE ÉXITO

es la existencia de un encuadre regulatorio específico en cuanto a la CN.

Los puntos más relevantes de dicho encuadre regulatorio son los siguientes:

- Ley de Protección de datos
- Ley de ciberseguridad
- Autoridad líder y órgano regulador en la materia
- Plan rector nacional en cuanto a la transformación digital del gobierno y política de gobierno abierto.

Este encuadre proveyó de claridad y previsibilidad a la adopción y uso de servicios en la nube para los funcionarios de los distintos organismos de gobierno que debían tomar la decisión de migrar de modelos tradicionales on-premises a modelos de nube.

Otro aspecto destacable en estos casos es la interoperabilidad, contemplándose en todos estos casos modelos de despliegue de nubes públicas y/o híbridas, no dependiendo por lo tanto de inversiones en infraestructura o de desarrollo de aplicaciones a ser realizada únicamente por el gobierno.



Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.



Corea del Sur ha demostrado que, tomando las precauciones regulatorias necesarias en términos de ciberseguridad y protección de datos, es posible impulsar los servicios de computación en la nube, tanto pública como privada, aún en escenarios de elevada sensibilidad.



Estonia es la sociedad digital más avanzada del mundo, pionera en generar iniciativas desde el año 1997 en temas como e-Gobierno, e-Impuestos, ID digital, voto electrónico, blockchain, salud y residencia electrónicas entre otras iniciativas. La gobernanza electrónica ha sido una opción estratégica para este país para mejorar la competitividad del estado y aumentar el bienestar de su gente, al tiempo que implementa una gobernanza sin problemas. Los ciudadanos pueden seleccionar soluciones electrónicas de una gama de servicios públicos en un momento y lugar conveniente para ellos, ya que el 99% de los servicios públicos ahora están disponibles para los ciudadanos como servicios electrónicos lo cual les ha dado enormes ganancias en términos de eficiencia. Estos progresos se apoyan en su pequeño tamaño de mercado, bajo nivel de complejidad y centralidad de las decisiones que permite implementar innovaciones y directrices con relativa facilidad. Gran parte de estos esfuerzos se coordinan desde la Oficina del Chief Information Officer dentro del Ministerio de Asuntos Económicos y Comunicaciones, promoviendo una aplicación transversal y homogénea a lo largo del sector público.



Por su parte, el gobierno del **Reino Unido** ha centralizado los esfuerzos respecto de selección de potenciales proveedores de servicios de CN, pero delega en cada agencia de gobierno la celebración de contratos particulares. En este esquema de descentralización de la toma de decisiones, el Reino Unido es un líder en brindar capacitación y orientar a los funcionarios en los procesos de contratación de servicios en la nube, mediante la elaboración de guías y documentos legales estandarizados que agilizan las actividades burocráticas de contratación. Aquí se puede destacar principalmente la visión de largo plazo, el establecimiento de principios guía en forma de programas de gobierno que han sido rectores e inspiradores de nuevas iniciativas que han permitido progresivos avances en la contratación y uso de CN.

En el caso de **Israel**, reconocido a nivel internacional como uno de los mejores centros de innovación en cuanto a desarrollo de software, ha establecido el sitio de gobierno abierto gov.il con el objetivo de dar acceso público a toda la información y los servicios gubernamentales. Su política cloud se encuentra comprendida dentro de un plan más amplio conocido como Programa Digital Nacional. Cabe destacar que el gobierno israelí se encuentra en proceso de migración a computación en la nube, siendo la seguridad y la protección de privacidad aún los principales desafíos y riesgos. Ello se ve reflejado en Ley de Protección de la Privacidad, la cual contempla aún mayores obligaciones que la Regulación de Protección de Datos de la Unión Europea. Es así como, con interés de los principales jugadores internacionales, actualmente Israel se encuentra en el proceso de licitación para el suministro de servicios basados en una plataforma de nube pública para la provisión de servicios a los ministerios del gobierno y otras entidades públicas, a partir de un centro de datos ubicado en territorio israelí.



Por último, **España** es un claro ejemplo de liderazgo del gobierno nacional para poder impulsar la digitalización. Focalizó algunas de sus leyes en lo que el estado español debía proveerle a sus ciudadanos, bajando directrices claras a organismos nacionales, comunidades autónomas, provincias y municipios que les permita desenvolverse descentralizadamente y generar proyectos. De este modo, han conseguido un alineamiento a principios y criterios rectores, todos tendientes hacia un mismo objetivo final: la reducción de la brecha digital y la digitalización integral del sistema administrativo gubernamental.



SECCIÓN

05

EXPERIENCIA DEL CONO SUR EN LA MIGRACIÓN A LA COMPUTACIÓN EN LA NUBE

Si bien la CN ya forma parte de la agenda pública y privada en los países del Cono Sur (Argentina, Brasil, Chile, Paraguay y Uruguay), la adopción de servicios de CN por parte del sector público es todavía incipiente y se encuentra en estados muy preliminares de estandarización y escalabilidad. A continuación se ofrece un mapeo de la situación para cada uno de los países del Cono Sur.



PAÍS

ARG.

Argentina ha avanzado significativamente en la inclusión de la CN dentro de su agenda pública en los últimos cinco años. No obstante, todavía existe un largo recorrido por delante para la implementación y puesta en práctica de políticas que permeen en todos los estamentos del Estado de manera unívoca.



En lo que hace al contexto normativo, específicamente a la protección de datos personales, el marco regulatorio permite la transferencia y procesamiento transnacional de datos desde entidades públicas y privadas y no constituye una barrera a la adopción de CN. No obstante, según el país destino sea considerado de “legislación adecuada”¹³ o no, deberán asumirse distintas prevenciones para la contratación de servicios de CN, pero en todo caso es posible con los recaudos adecuados. En este sentido, la resistencia al procesamiento transnacional de datos por el sector público es una barrera autoimpuesta, basada en gran medida en un desconocimiento de la regulación vigente.

A nivel federal, la acción de la ONTI, dentro de la Secretaría de Gobierno de Modernización, ha sido un motor en ejecución de políticas orientadas a la nube: definiendo un Decálogo TIC con orientación Cloud First¹⁴, estudiando modelos alternativos a seguir, dialogando y asesorando a las distintas reparticiones públicas para la elaboración de un plan y la fijación de estándares y mecanismos prácticos de contratación.

También ha desempeñado un papel activo la Agencia Argentina de Inversiones y Comercio Internacional, una de las promotoras de la política “Cloud First” y del objetivo que para 2027 el Gobierno Nacional esté en un 80% en la nube. Asimismo, junto al Ministerio de Modernización, esta agencia es la que impulsa el proyecto de promoción de instalación de centros de procesamiento de datos en el país.

En el plano de generación de incentivos, la Ley de Economía del Conocimiento, reglamentada a fines de 2019, define incentivos fiscales para la promoción del establecimiento e inversión en CN dentro del país.

Desde 2017, además, se avanzó en atender la ciberseguridad, estableciendo un comité tripartito por representantes del Ministerio de Defensa, Seguridad y Modernización que definió una Estrategia Nacional de Ciberseguridad que establece principios y siete áreas de trabajo donde se destaca el fortalecimiento de capacidades de prevención, detección y respuesta; la protección y recuperación de los sistemas de información del Sector Público; y el fomento de la industria de la ciberseguridad. Argentina adhiere al convenio de Budapest, el que busca homogeneizar la regulación de los delitos informáticos a nivel internacional.

**ENTRE
20% Y 30%
ANUAL**

TASA APROXIMADA EN QUE
CRECE EL MERCADO DE CN

**80% EN
LA NUBE**

DEL GOBIERNO NACIONAL
COMO OBJETIVO 2027

Hacia fines de 2019, el mercado de CN, contemplando los distintos modelos de servicios de IaaS, PaaS y SaaS, se estima en aproximadamente US\$ 400 a 500 millones¹⁵

El mercado de CN en Argentina está compuesto [atentado] por compañías internacionales (i.e., Amazon Web Services, Google Cloud, Microsoft Azure, IBM, Oracle, SAP, Salesforce, Red Hat), proveedores alternativos (i.e., Huawei/Telefónica, Telecom y Fibertel) y un proveedor público de servicios de centro de datos (i.e., ARSAT - Empresa Argentina Soluciones Satelitales SA). El mercado de CN crece a una tasa aproximada de entre el 20% y 30% anual¹⁶. Los proveedores internacionales mencionados, hasta el momento de la generación del presente informe, no poseen infraestructura local en Argentina. Sin embargo, en algunos casos han manifestado que tienen intención de realizar inversiones para desarrollar dicha infraestructura localmente.

PROTECCIÓN DE DATOS PERSONALES

NORMATIVA VIGENTE

- Ley N° 25.326¹⁷
- Decreto 1558/2001¹⁸
- Disposición 07/2008
- Disposición 60-E/2016
- Resolución 40/2018.
- Proyecto de Ley de Protección de Datos Personales¹⁹ (238/18)

INSTITUCIONES REGULADORAS

- Agencia de Acceso a la Información Pública (AAIP)

PRINCIPALES PROVISIONES

- Marco general de protección de datos aplicable en la República Argentina.
- Establece el tipo contractual (contrato de prestación de servicios de tratamiento de datos personales).
- Establece lineamientos orientativos relativos a reglas de privacidad y confidencialidad en el tratamiento de datos personales en la órbita pública.
- Establece las cláusulas contractuales tipo de transferencia internacional para la cesión y prestación de servicios de datos personales.
- Genera la política modelo de protección

CIBERSEGURIDAD

NORMATIVA VIGENTE

- Decreto 577/2017²⁰
- Resolución 829/2019²¹

INSTITUCIONES REGULADORAS

- Comité de Ciberseguridad

PRINCIPALES PROVISIONES

- Crea y otorga competencias al Comité de Ciberseguridad, el cual elaborará la Estrategia Nacional de Ciberseguridad.
- Aprueba la Estrategia Nacional de Ciberseguridad, fijando los objetivos claves a ser alcanzados.

REQUERIMIENTOS DE CONTRATACIÓN

NORMATIVA VIGENTE

- Disposición 1 - E/2017 (ONTI) y Anexo Disposición 1 - E/ 2017 – ETAPs
- BCRA Comunicación A 6354²² y 6375/2017²³

INSTITUCIONES REGULADORAS

- Oficina de Tecnologías de la Información (ONTI)
- Banco Central de la República Argentina (BCRA)

PRINCIPALES PROVISIONES

- Establecimientos de los “Estándares Tecnológicos para la Administración Pública Nacional” por parte de la ONTI
- Desarrollo de condiciones técnicas para contratación de IaaS por parte del Estado
- Permitir a las entidades financieras tercerizar en instalaciones de terceros con recursos técnicos y/o humanos propios o de terceros aquellas actividades de administración, archivo e imprenta que no consistan en atención de clientes o público general.

PROMOCIÓN ESTABLECIMIENTO DE DATACENTERS

NORMATIVA VIGENTE

- Decreto 117/2017
- Ley 27.506 “Economía del conocimiento”

INSTITUCIONES REGULADORAS

- Agencia Nacional de Inversiones y Comercio Internacional

PRINCIPALES PROVISIONES

- Eliminación de ciertos impuestos aduaneros para el ingreso de equipamiento clave
- La ley ofrece formalizar incentivos fiscales adicionales en la reglamentación



Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

La agenda pública de CN, direccionada desde el área de modernización, ha permitido tener algunos casos de éxito, como ha sido el caso de la iniciativa Gestión Documental Electrónica (GDE)²⁴. Esta iniciativa es un ejemplo de cómo una administración gubernamental pone a disposición de administraciones pequeñas un SaaS, brindándoles acceso a funcionalidades a las que de otra forma no podrían acceder por motivos presupuestarios. Estas iniciativas fomentan la reducción de la brecha digital y el desarrollo de un ecosistema al cual se puede sumar a empresas privadas para el desarrollo de soluciones SaaS que interactúen con los servicios y soluciones provistas por el gobierno.

No obstante, aun cuando el país presenta importantes avances en la promoción de la adopción de servicios de CN, su alcance en el sector público es aún limitado: menos de un 15% de las agencias nacionales se encuentra utilizando algún servicio de CN.

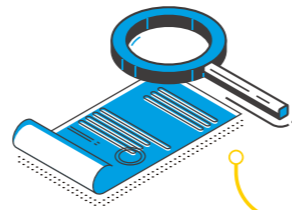
MENOS DEL 15% DE LAS AGENCIAS NACIONALES

EN EL SECTOR PÚBLICO SE ENCUENTRA UTILIZANDO ALGÚN SERVICIO DE CN

A nivel subnacional el avance es más incipiente y dispar. Algunas provincias han avanzado mediante el establecimiento de datacenters propios y otras mediante el apalancamiento en el datacenter de ARSAT (caso de Provincia Buenos Aires). Algunas iniciativas han encontrado, no obstante, buena acogida entre las provincias: el sistema de compras en línea (originalmente adoptado por la ciudad de Buenos Aires y luego llevado a la Nación) ya se ha implementado en 11 provincias²⁵.

A nivel municipal, el ritmo de adopción es más lento por barreras tales como la conectividad, capacidad técnica, inercia de la propia operación. En todo caso, lo primero en la digitalización de los municipios es el desarrollo de una página web, con hosting en el proveedor público ARSAT²⁶ sobre la cual, todavía muy incipientemente, desarrollan algunos servicios en línea.

Cabe destacar el caso de la Ciudad Autónoma de Buenos Aires que ha tomado la iniciativa en la adopción de CN, inclusive con mayor avance que la administración nacional, apalancada por la Agencia de Sistemas de Información (ASI), la cual lidera las implementaciones de servicios PaaS y SaaS integrando soluciones de distintos proveedores junto con desarrollos propios.



GESTIÓN DOCUMENTAL ELECTRÓNICA

La GDE fue uno de los primeros cambios introducidos por la política de modernización; permite simplificar trámites, mejorar los procesos, reducir los tiempos administrativos y brindar la posibilidad de acceder a la información generada por la administración pública. Se trata un sistema informático integrado por distintos módulos, a los cuales se puede acceder desde el “escritorio único” y que contiene y administra todas las reglas para generar y almacenar digitalmente documentos oficiales electrónicos, garantizando la disponibilidad, inviolabilidad y protección de la docu-

mentación oficial, evitando así la manipulación física y el traslado de expedientes. Desde su puesta en funcionamiento, regulada mediante el decreto 561/2016, el papel dejó de ser el soporte de la organización administrativa en Argentina. La tramitación digital, sin papeles, se inició en mayo de 2016 y, sólo dos años después, el decreto 733/2018 ordenó la eliminación del papel de forma total en toda la Administración Pública Nacional para agosto de 2018 y, en todo el sector público, para enero de 2019.

AGENCIA DE SISTEMAS DE INFORMACIÓN

Agencia de Sistemas de Información (ASI) es el órgano rector en materia de tecnologías de la información y las comunicaciones en el ámbito del Poder Ejecutivo del Gobierno de la Ciudad Autónoma de Buenos Aires. Es la agencia que provee de infraestructura y conectividad a todos los organismos gubernamentales de la ciudad y posee dos centros de cómputo en edificios diferentes dentro de la misma. Realizan desarrollo y mantenimiento de aplicaciones, tanto en la nube como en centros de cómputos propios. La ASI ha declarado el “Cloud first” para el Gobierno de la Ciudad. Como órgano rector, administra todos los contratos con los proveedores de nube y lanza continuamente licitaciones integrando soluciones de varias empresas. Esto le permite tener alta interac-

ción con el ciudadano y hasta medir su nivel de satisfacción con los servicios públicos, el pago de tasas y recibir retroalimentación de los servicios provistos en línea. En el año 2016, operando al límite de capacidad y con la infraestructura descentralizada, se definió centralizar los centros de cómputo. La visión de la ASI es migrar 100% a la nube, mediante la siguiente agenda: migración 100% en la nube en 2023, modelo de gobernanza para administrar nubes con diferentes proveedores, continuidad de ejecución de los programas de capacitación de perfiles tecnológicos, modificación de estructura interna y creación del área “Cloud”, implementación de firma Cloud del ciudadano y generación de la oficina de datos abiertos de la ciudad.



Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

Las principales barreras a la adopción de CN en Argentina se vinculan con la necesidad de coordinación, infraestructura y proceso, las cuales a su vez generan posibles líneas de acción en el corto plazo que llaman a estimular el desarrollo de capacidades, eliminar incertidumbres del marco regulatorio, empoderar transversalmente a las agencias que lideran la fijación de políticas, eliminar barreras y promover inversiones.

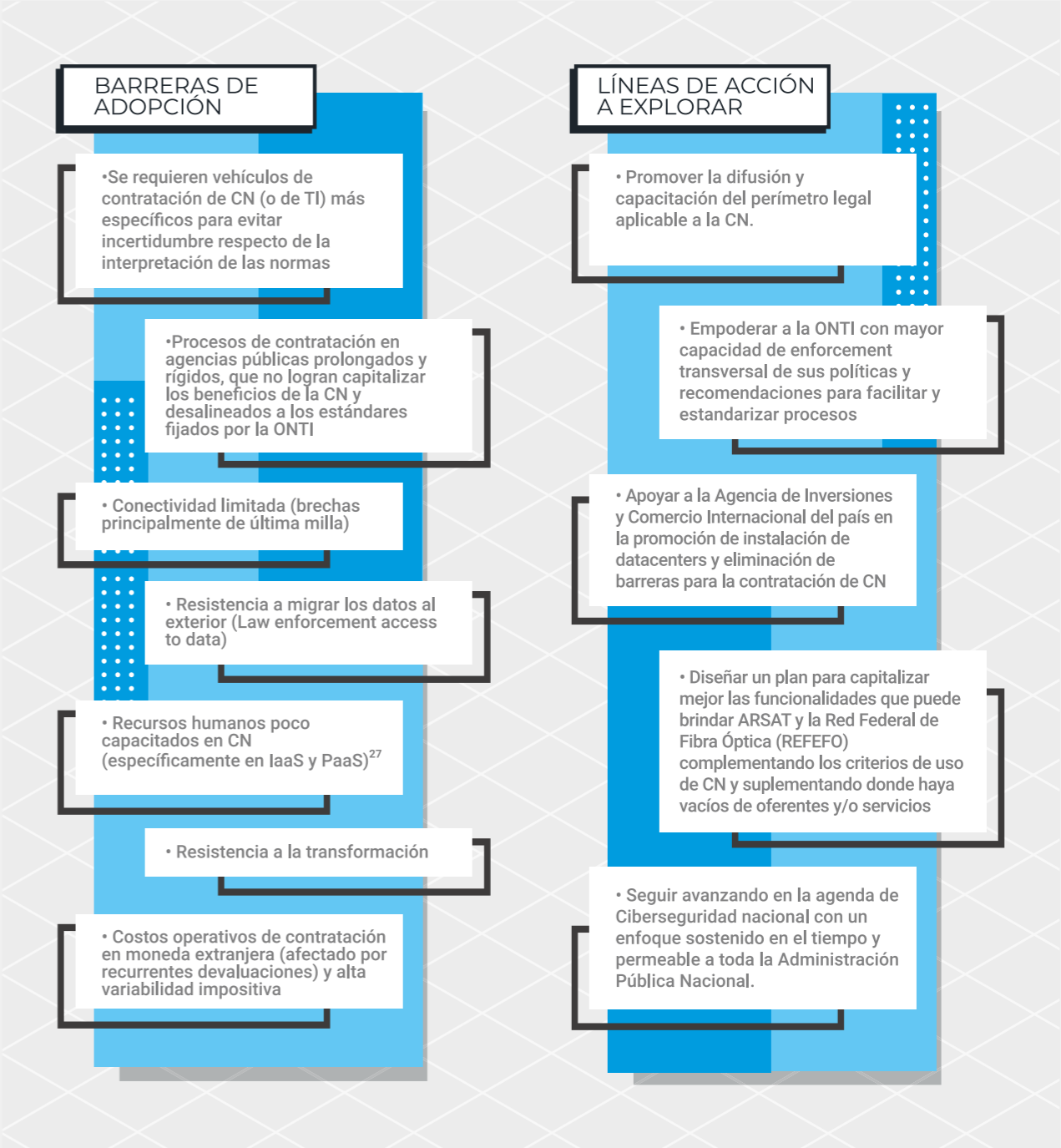


Ilustración 8. Argentina: Barreras a la adopción y líneas de acción de corto plazo a explorar.



PAÍS

BRA.

Brasil ha venido avanzando en forma constante en la adopción de servicios en la nube por parte del sector público. Más allá de algunas iniciativas dispersas a nivel de los principales estados, como São Paulo y Río de Janeiro, el Gobierno Federal es el que ha desarrollado y coordinado las principales acciones en relación con CN y la promoción e instalación de datacenters (aunque muchos de ellos no están integrados en una solución común).



Dado su considerable mercado, existen grandes proveedores estatales de TI, tales como Serviço Federal de Processamento de Dados (SERPRO), Empresa de Tecnologia e Informações da Previdência Social (DATAPREV), Telecomunicações Brasileiras S/A, empresas públicas de procesamiento de datos de los estados, entre otros, que mayormente operan nubes privadas. Brasil es el país en la región con mayor presencia de los grandes proveedores privados, tales como Microsoft Azure, Amazon Web Services (AWS), Google Cloud e IBM, varios de ellos operando centros de datos.

La estrategia brasileña para la transformación digital (E-Digital), publicada a fines del año 2018, definió acciones estratégicas colocando al gobierno como facilitador de esta transformación digital en el sector productivo del país, la capacitación en las nuevas tecnologías y el rol del estado como prestador de servicios y garante de derechos. Cabe destacarse que esta “Estrategia de Governança Digital 2016-2019 (EGD)” data de enero de 2016 y fue revisada en 2018, sin embargo, no menciona específicamente objetivos de uso de CN.

Sin embargo, el marco regulatorio habilitante presenta algunos desafíos como la localización forzada de los datos en el territorio nacional y las severas sanciones aplicables previstas en la Lei Geral de Proteção de Dados Pessoais (LGPD). La LGPD aprobada en mayo de 2019, es una ley general con alcance horizontal y extraterritorial muy alineada con el Reglamento General de Protección de Datos europeo, que creó la Autoridad Nacional de Protección de Datos, y que se aplicará a cualquier operación de tratamiento de datos que (i) se realice en Brasil; (ii) involucre una oferta de productos y/o servicios a usuarios ubicados en Brasil; o (iii) recopile datos personales dentro del territorio brasileño.

La Secretaría de Gobierno Digital vinculada al Ministerio de Economía (SGD-ME) desempeña un papel muy importante en la coordinación de iniciativas de modernización del estado, en un proceso que persigue la transformación digital de acciones estatales para satisfacer las demandas de los ciudadanos. Recientemente se han publicado estándares que permiten facilitar la contratación de servicios de TI, priorizando las soluciones basadas en la nube.

El SGD-ME ha estandarizado y licitado los servicios en la nube a través de precios abiertos, lo que permite a las agencias federales adherirse a los ganadores de subastas electrónicas, acelerando y facilitando el proceso de contratación para las agencias, aún para aquellas con menor capacidad técnica en la CN.

El Tribunal Federal de Auditoría (TCU), organismo de control externo del gobierno federal que tiene la misión de monitorear la ejecución presupuestaria y financiera del país y contribuir a la mejora de la administración pública en beneficio de la sociedad, llevó a cabo una licitación hacia fines de 2018 para la contratación de servicios en la nube (aun habiendo anteriormente señalado una serie de riesgos para el empleo de CN en la administración pública federal). Del mismo modo, la Oficina de Seguridad Institucional Presidencial (GSI-PR) ha buscado coordinar y disciplinar los problemas de seguridad de la información, brindando mayores garantías y estabilidad al uso de soluciones basadas en la nube por parte de los sectores público y privado.

Iniciativas para la capacitación y formación de personal de organismos públicos, aunque aún incipientes, han contribuido a calmar los temores y a destacar los beneficios de adoptar nuevas tecnologías que permiten a las agencias centrarse en las aplicaciones y servicios ofrecidos a los ciudadanos (dejando para empresas especializadas las cuestiones relacionadas con infraestructura, equipamiento de TI, conectividad, plataformas de desarrollo y desarrollo y operación de aplicaciones).



Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

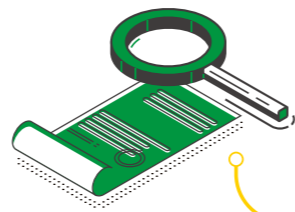
La Política Nacional de Seguridad de la Información, elaborada por el GSI-PR y publicado a finales de 2018 por medio de un decreto, definió cuestiones relacionadas con la ciberseguridad, la defensa cibernética, la seguridad física, la protección de datos organizacionales y estableció acciones para garantizar la disponibilidad, integridad, confidencialidad y autenticidad de la información. Tras expresar su intención de adherirse en julio de 2019, a fines del mismo año, el Comité de Ministros del Consejo de Europa invitó a Brasil a adherirse a la Convención sobre Ciberseguridad, también conocida como la Convención de Budapest, celebrada en 2001. Una vez que se concluya su adhesión, Brasil se unirá a un grupo internacional que incluye países como Argentina, Australia, Canadá, Chile, Costa Rica, Estados Unidos, Japón, Paraguay, República Dominicana y miembros de la Unión Europea, entre otros.

**5% SECTOR
PRIVADO
1% SECTOR
PÚBLICO**

EL PORCENTAJE DE LOS
PRESUPUESTOS DE TI
DESTINADOS A CN

Se estima que el mercado de CN en Brasil alcanzará los US\$ 2.600 millones en 2019, creciendo a una tasa anual del 35% para alcanzar los US\$ 6.500 millones en 2022, lo que indicaría que el mercado brasileño todavía tiene un gran espacio para expansión en los próximos años

El país sigue ocupando solamente la 13ª posición en el mercado de CN a nivel mundial. Según el relevamiento realizado, se estima que el porcentaje de los presupuestos de TI destinados a CN no llega al 5% en el sector privado y es inferior al 1% en el sector público. El crecimiento anual estimado, superior al 30%, debería ser impulsado en gran medida por el mercado de CN para las empresas privadas, mientras que en el gobierno el proceso de migración se espera sea algo más lento debido al gran legado y las restricciones presupuestarias impuestas a las agencias públicas.



TRIBUNAL FEDERAL DE AUDITORIA (TCU)

El proceso de licitación adoptado por el TCU, que contó con soluciones creativas para abordar la diversidad de demandas y la diversidad de servicios y productos sujetos a contratación, es considerado una referencia nacional en la adopción de la CN en proyectos de los gobiernos federal, estatales y municipales de Brasil. Recursos limitados y la búsqueda de la modernidad y escalabilidad de sus servicios, llevaron a TCU a evaluar alternativas para expandir su centro de datos, el cual se encontraba en operación desde 2010, iniciando un proceso gradual de migración hacia servicios de infraestructura y servicios en la nube. Para la licitación se adoptó un mo-

delo de especificación y fijación de precios del objeto de la licitación de servicios de CN que aportó flexibilidad y dinamismo a la definición de los productos y servicios que se contrataron efectivamente. El hecho de que el organismo de control haya superado las incertidumbres jurídicas y técnicas inicialmente expresadas, y que haya contratado efectivamente servicios de CN, representa un avance importante y ha servido como referencia en la adopción de estos servicios por parte de otras agencias del sector público en Brasil como Petrobras, SGD-ME y ETICE, entre otros que utilizaron modelos similares a los adoptados por TCU.

NÃO ME PERTURBE

Lanzado en julio de 2019, desarrollado y migrado en apenas 30 días, Não Me Perturbe es una plataforma para el registro de las solicitudes de bloqueo de los consumidores que ya no desean recibir llamadas de telemarketing. Con un volumen superior a los 200.000 accesos simultáneos en el primer día y más de 3 millones de bloqueos ya realizados (a noviembre de 2019), esta iniciativa, coordinada entre el regulador del sector y las compañías privadas de telecomunicaciones, representa una de las grandes historias de éxito del empleo en CN en una asociación público-privada en Brasil. Además de reducir significativamente la cantidad de quejas en el regula-

dor de la industria de las telecomunicaciones (Anatel), la iniciativa demostró la viabilidad de establecer mecanismos eficaces de autorregulación y la posibilidad de contratación rápida de capacidad de almacenamiento y servicios de CN, en forma dinámica, y sin generar riesgos y costos excesivos para los contratantes de estos servicios. Esta iniciativa, que únicamente fue posible debido a las características intrínsecas de la CN, está siendo ampliada a varias cuestiones relacionadas con la mejora del servicio al cliente, especialmente con respecto a la transparencia de las ofertas y la cobranza correcta de los servicios prestados.

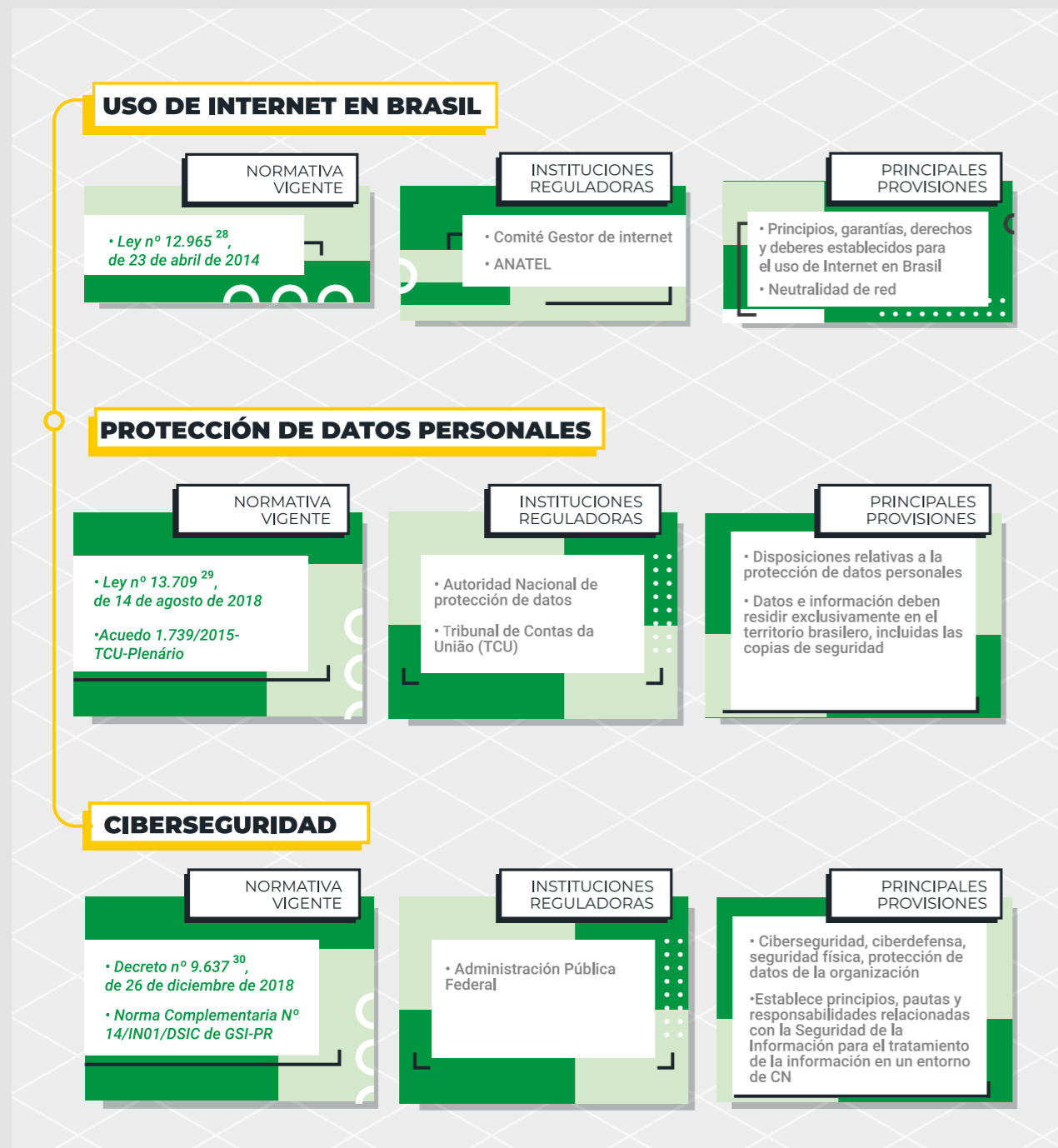
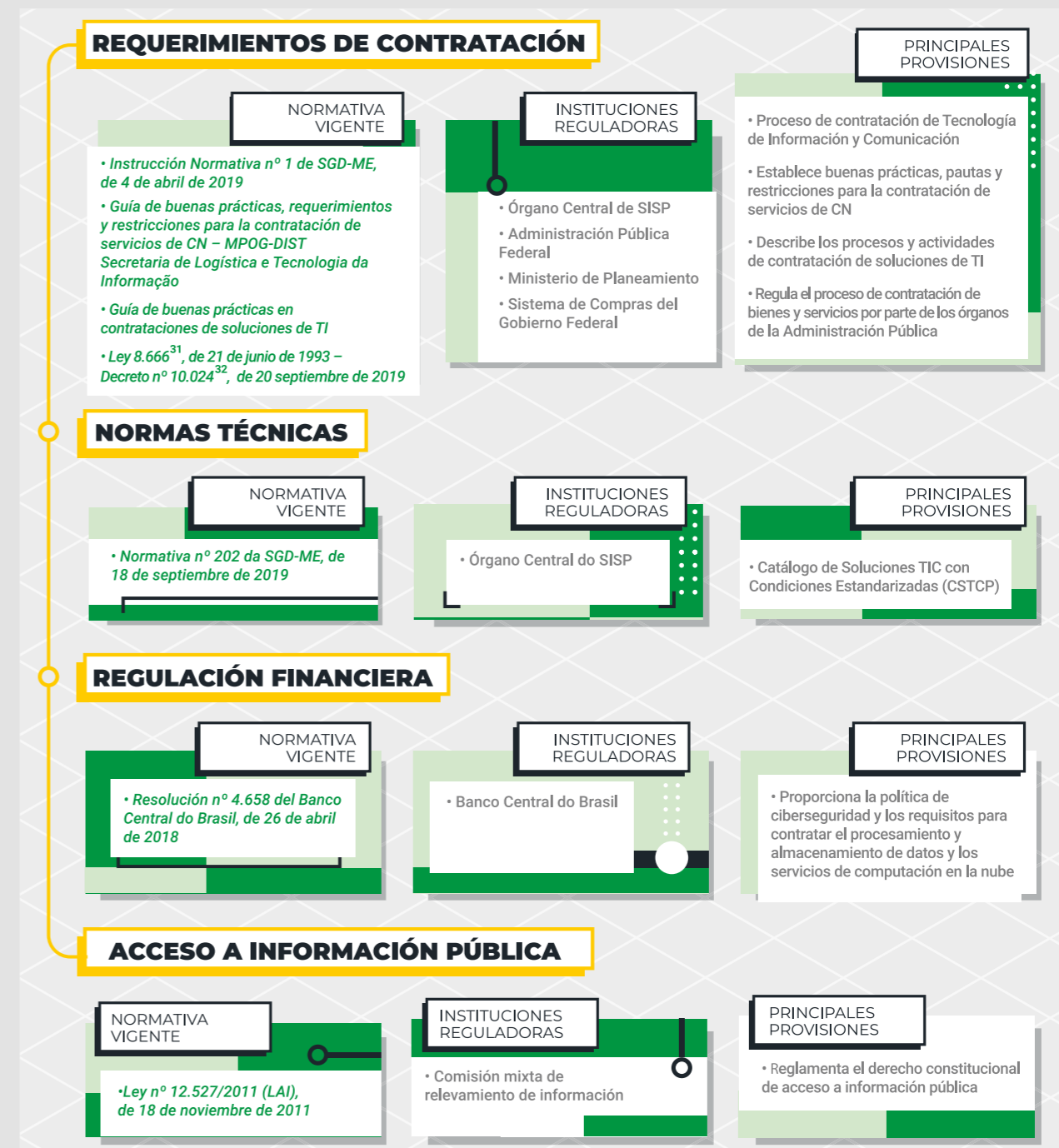


Ilustración 9. Brasil: marco regulatorio de los servicios en la nube.



La oferta de servicios de CN en el mercado brasileño tiene un número grande y creciente de jugadores. Entre ellos se encuentran las grandes empresas internacionales (Amazon AWS, Microsoft Azure, Google Cloud e IBM) que prestan servicios en la nube pública en todas sus modalidades (IaaS, PaaS y SaaS), contando éstas con grandes centros de procesamiento de datos, instalados tanto en el exterior como en territorio brasileiro para cumplir con las restricciones de ubicación de datos del sector público. También están presentes en el mercado proveedores alternativos que actúan como integradores de soluciones proporcionados por las principales compañías internacionales, como ser Locaweb, Mandic, Primesys, Algar, vivo, Hola, Tivit, Alog y Level 3. Por último, se tiene a los proveedores estatales, los que también actúan como integradores de soluciones aportadas por grandes empresas internacionales para agencias gubernamentales como SERPRO, DATAPREV, Telebrás, Empresa de informática do Governo do Estado de São Paulo y Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro. El uso, por parte del sector público de las grandes empresas internacionales, permanece aún en una escala menor³³.

80% GRANDES PROVEEDORES

40% PARA MICROSOFT,
20% PARA AMAZON Y
20% PARA GOOGLE.

Incluso con estos integradores públicos y privados que actúan como intermediarios y soporte de los clientes, el mercado brasileño se concentra con más del 80% en unos pocos grandes proveedores de servicios de nube, divididos entre el 40% para Microsoft, 20% para Amazon y 20% para Google. Ello ocurre como consecuencia de la fuerte adopción de software de oficina (Office 365), inclusive en el sector público, y ERP (SAP), principalmente en el sector privado. El 20% restante se encuentra atomizado en otras compañías con menor participación de mercado.

La mayor parte de las contrataciones de servicios en la nube se centran aún en IaaS (para copias de seguridad y conectividad). Por su parte, la provisión de SaaS ya representa más del 60% del crecimiento del mercado de CN.



Ilustración 10. Brasil: Barreras a la adopción y líneas de acción de corto plazo a explorar.

PAÍS

CHI.

Chile desde hace varios años viene promoviendo iniciativas de modernización para lograr un estado más simple y eficiente. Uno de los pilares de este proceso de modernización ha sido el desarrollo de un Gobierno Electrónico y la vocación de convertirse en un “Hub digital” para la provisión de servicios de CN en la región.



En 2019 renovaron su estrategia de gobierno digital y adoptaron políticas y estándares para la interoperabilidad, ciberseguridad, identidad digital (con el objetivo de que el 100% de los servicios provistos sean accesibles por medio de clave única para fines de 2020), política de compras tecnológicas, política “open source first” y política de incentivo al uso de la nube.

La División de Gobierno Digital, desde la Presidencia, es la encargada de liderar y apoyar a las instituciones públicas en la implementación de la estrategia de transformación digital, con un rol de generador de políticas, facilitador, consultor y normativo. Desde allí se está promoviendo la implementación de CN, modificando leyes y regulaciones para favorecer la adopción.

El Gobierno de Chile se encuentra implementando y modificando leyes y normas para favorecer la adopción de servicios de CN y para fortalecer los derechos de los usuarios, por ejemplo en lo que hace a datos personales. Más allá de esto, existen actualmente normas y disposiciones que encuadran jurídicamente la contratación por parte del estado de este tipo de servicios en sus distintas modalidades y que le proporcionan un marco favorable para su desarrollo, tales como protección de datos personales,

firma electrónica, requerimientos de contratación, legislación bancaria y financiera, por mencionar algunos. La administración pública ha declarado tener el enfoque “Cloud First”, y se encuentra avanzando en la actualización de la ley, vigente desde 1999, sobre protección de la vida privada, para adaptarla en 2020 en la creación de un organismo de control, regulación del consentimiento y obligaciones de los responsables de los datos. No obstante ello, existen, en algunos organismos del sector público, barreras culturales autoimpuestas al momento de tomar decisiones referentes a la migración de datos a la nube. En cuanto a la posibilidad de transferencia y procesamiento transnacional de datos, la Comisión del Mercado Financiero (CMF) es el único organismo que ha definido regulación específica, impidiendo la localización de datos fuera del territorio chileno.

En cuanto a ciberseguridad, se encuentra en el Senado, a consideración, un proyecto de ley que implica actualizar la legislación actual en base al Convenio de Budapest. Se dictó la ley que regula la firma electrónica y los servicios de certificación de firma, estableciendo los distintos tipos de firma electrónica, los aspectos tecnológicos, los documentos electrónicos, su presentación y valor probatorio y el uso de este tipo de firma por los órganos del Estado.

**ENTRE
20% Y 30%
ANUAL**

TASA APROXIMADA EN QUE
CRECE EL MERCADO DE CN

**Se estima que el mercado
de CN en Chile se encuentra
entre los US\$170 y los
US\$200 millones.**

En línea con las tendencias internacionales, y específicamente en América Latina, se estima que este mercado crece a una tasa aproximada de entre el 20% y 30% anual³⁵. Realizando un análisis del gasto en IaaS, PaaS y SaaS en el sector público, desde el año 2014 a julio de 2019, las contrataciones en SaaS se han multiplicado por 6, con un incremento considerable desde 2016 a la fecha, lo que marca una tendencia al crecimiento en la inversión en dichos servicios. A nivel ministerial, el Ministerio de Salud ha realizado el principal gasto en tecnología dentro del periodo 2014 a 2019, seguido por las municipalidades y el Ministerio de Trabajo y Previsión Social.

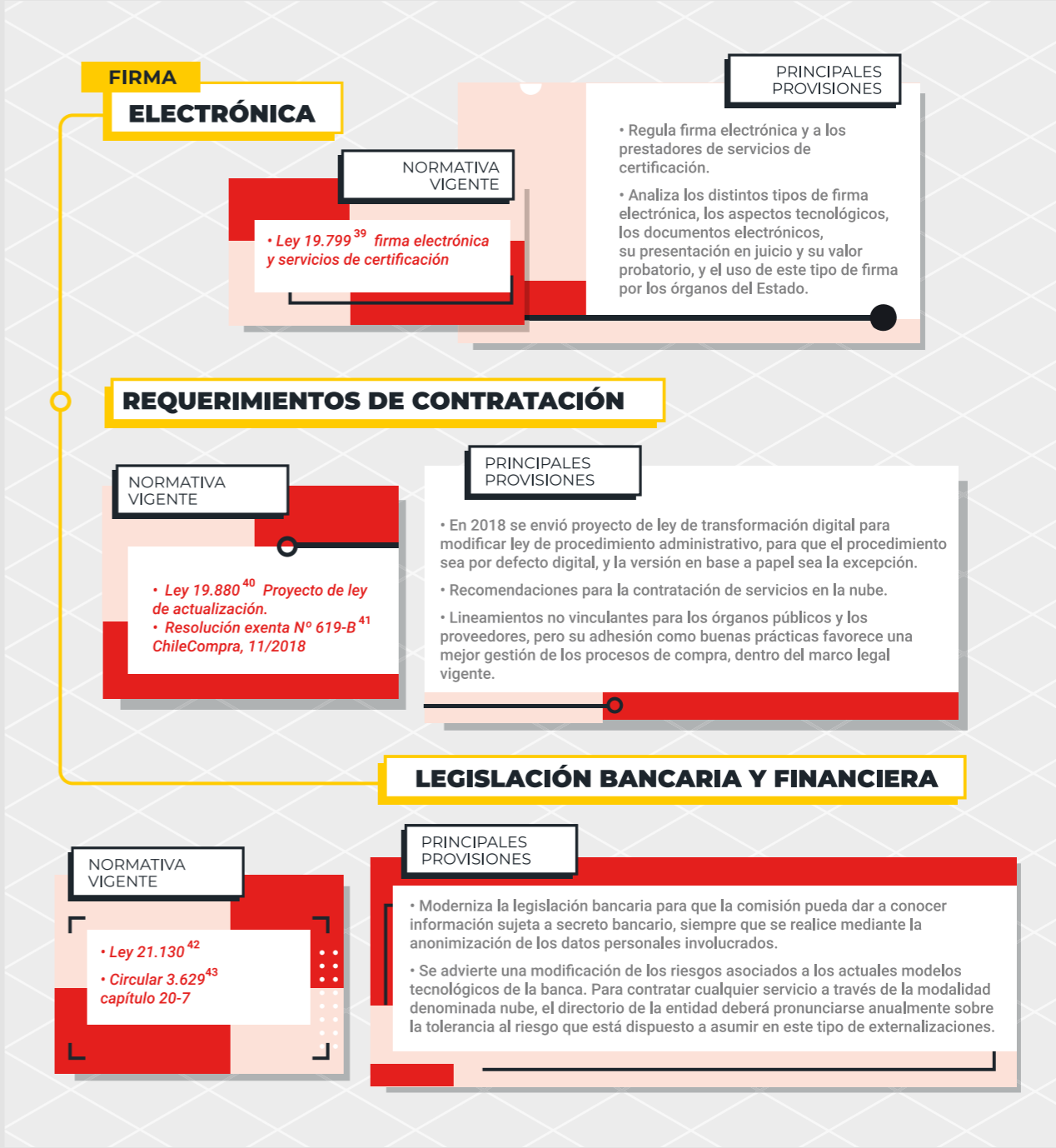


Ilustración 11. Chile: marco regulatorio de los servicios en la nube.



Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

La utilización de CN por parte de los organismos tributarios en Chile se encuentra en desarrollo como parte de la estrategia de transformación digital del Estado. El Ministerio de Hacienda tiene como objetivo, mediante la utilización de la nube, integrar digitalmente los sistemas de todas las instituciones, tanto públicas como privadas. En este sentido, el Servicio de Impuestos Internos de Chile ha sido pionero en impulsar la transformación digital.

La oferta de CN muestra proveedores de IaaS, PaaS y SaaS que se están apoyando en una creciente conectividad dada por la promoción e instalación de cables submarinos, política que ha tenido continuidad en las administraciones de los últimos años. Sin embargo, todavía persisten algunas brechas de conectividad al interior del país, dada su vasta geografía y zonas remotas con baja densidad poblacional que cuentan con relativamente menores recursos que la media del país.

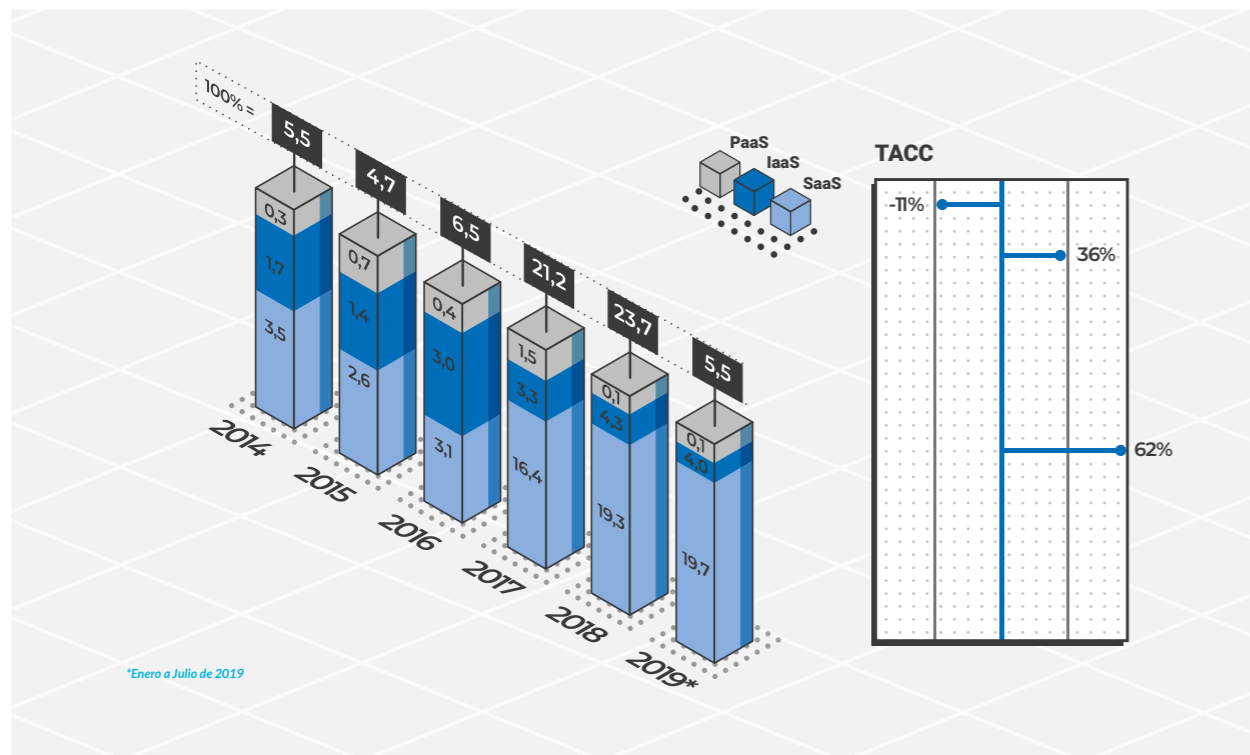
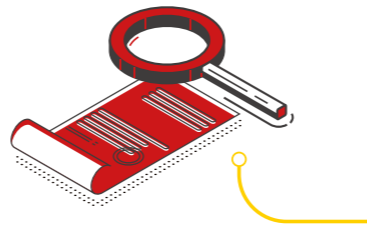


Ilustración 12. Chile: Gasto en IaaS, PaaS y SaaS en sector público (millones US\$)

CHILECOMPRA

Chile Compra es un ejemplo de plataforma web organizada y centralizadora en iniciativas de migración a la nube y de todas las compras públicas. En el año 2014 comenzó el proceso de migración de sus sistemas a la nube. Dicha migración comenzó con la configuración de máquinas virtuales en Azure para almacenamiento de información y generación de servidores virtuales. Actualmente utilizan la ofimática provista por Office 365 de Microsoft y la interface de administración de Microsoft Azure para proveer los servicios que ChileCompra brinda a sus proveedores. Para el proyecto de la nueva tienda para convenios marco y licitaciones, en formato SaaS, ChileCompra se encuentra utilizando el producto “Magento Commerce Cloud” en servidores sitios en San Pablo, Brasil. Este producto, al ser un e-commerce ya desarrollado, ofrece como ventajas la velocidad en la gestión de los cambios y adaptación del sistema. ChileCompra se encuentra avanzando hacia un nuevo esquema de arquitectura de microservicios y contenedores, por lo que ha adquirido nodos de OpenShift de RedHat para generar

una nube privada, utilizando el SSO (single sign-on).

Las entidades del sector público pueden utilizar los servicios de ChileCompra para la adquisición de servicios de TI y CN. ChileCompra emitió en noviembre de 2018 la directiva de contratación pública número 32, en la cual establece recomendaciones, no vinculantes, para la contratación de servicios en la nube. A partir del 25 de febrero de 2020 se implementará la nueva tienda Cloud en el portal [mercadopublico.cl](https://www.mercadopublico.cl), tienda con servicios tecnológicos en la nube por la cual compran 850 organismos de gobierno.

Entre 2014 y 2019 el gasto en servicios de CN, según relevado por ChileCompra, pasó de 5,5 millones de US\$ a 23,7 millones US\$ en 2018 (y 23,8 millones en los primeros siete meses de 2019). Los principales organismos públicos consumidores de SaaS, IaaS y PaaS han sido el sector de salud, el gobierno central y las municipalidades, habiendo consumido, en el periodo mencionado, cerca del 50% del gasto de tecnología en sector público.

COMISIÓN DEL MERCADO FINANCIERO DE CHILE

En junio de 2019 la CMF adjudicó a la empresa Entel Chile la provisión de una plataforma de procesamiento de CN. El alcance de la solución abarcó la provisión de servicios de procesamiento, almacenamiento, redes internas, seguridad, licenciamiento y soporte a aplicaciones de productividad y negocios, como parte de una solución integral contratada en modalidad de servicio. Se implementó en dos centros de cómputo, con conectividad que permite alta disponibilidad, ubicados dentro del territorio de Chile, de manera que la CMF pudiera alternar y/o trasladar sus servicios a cualquiera de ellos de acuerdo a una periodicidad establecida, cambiando el rol de prima-

rio y secundario. La plataforma de virtualización implementada provee una nube pública dentro de los centros de cómputo en el territorio de Chile, sin limitaciones de cantidad de servidores ni de licenciamiento, y permite la administración centralizada de las máquinas virtuales a través de un portal web, que permite la autogestión por la CMF y proporciona acceso a un amplio catálogo de recursos de cómputo, almacenamiento, redes y seguridad. Esta plataforma interactúa, en un esquema de nube híbrida, con el centro de cómputo que la CMF poseía con anterioridad a la migración y que conservó para algunos sistemas internos.

Dentro de los jugadores internacionales de mayor relevancia que proveen servicios de IaaS, PaaS y SaaS son, los que cuentan con infraestructura en territorio chileno son los siguientes:

GOOGLE

fue la primera empresa internacional en instalar, en el año 2015, con una inversión de **US\$ 150 millones**, un centro de cómputo en Chile. Recientemente anunció la intención de construir un segundo centro de cómputo a principios de 2020 con una inversión proyectada de US\$ 200 millones⁴⁴.

HUAWEI

en agosto de 2019, inauguró un centro de cómputo TIER 3 en la región metropolitana de Santiago con una inversión de más de **US\$ 100 millones**⁴⁵.

MICROSOFT

posee un **“collocation datacenter”**, donde el hardware y software son propiedad de Microsoft pero la infraestructura donde se encuentran los mismos es propiedad de la empresa local Sonda.

ORACLE

anunció que instalará un **centro de cómputo** en Chile en 2020⁴⁶.

ENTEL CHILE

cuenta con **dos centros de cómputo**.

En cuanto a la oferta de SaaS, a modo de ejemplo, se puede destacar el caso de Claveúnica, la cual funciona como una contraseña única para acceder a todos los servicios del Estado chileno. La misma es provista en la nube a todas las administraciones. Hacia fines de 2019 la misma contaba con cerca de 6,5 millones de ciudadanos activos.

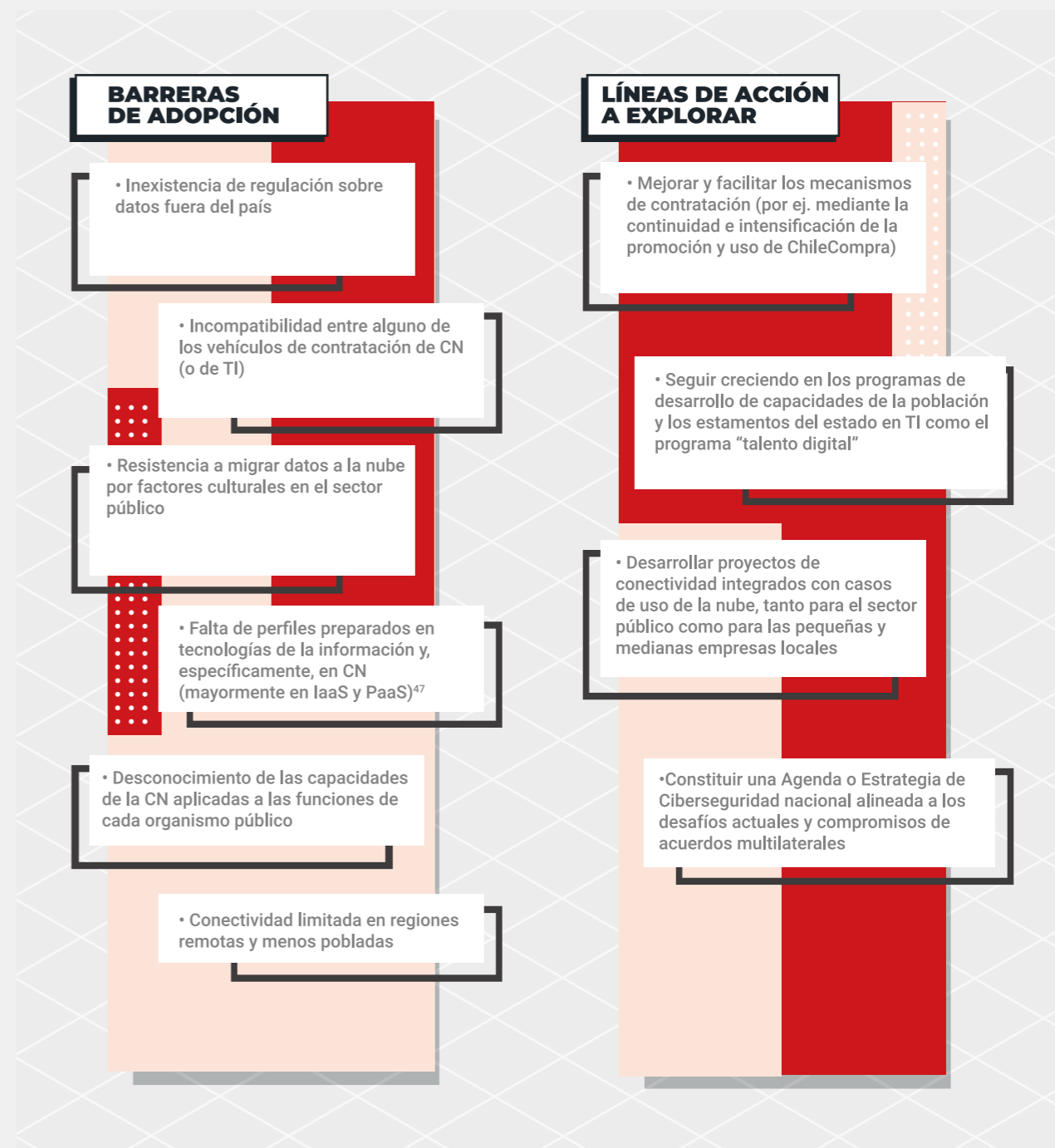


Ilustración 13. Chile: Barreras a la adopción y líneas de acción de corto plazo a explorar.



Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

PAÍS

PAR.

Paraguay se encuentra en proceso de transformación del contexto de la contratación y utilización de servicios de CN.

En octubre de 2018 se sancionó la Ley 6.207⁴⁸, mediante la cual se creó el Ministerio de Tecnologías de la Información y Comunicación (MITIC).



Allí se erige al MITIC como el regulador especializado en términos de protección de información personal y gubernamental, ciberseguridad, de infraestructura tecnológica pública, de los procesos públicos de adquisición de herramientas tecnológicas, despliegue de redes de conectividad nacionales.

Producto de esta reconfiguración, el marco normativo y regulatorio se encuentra en evolución y se ha buscado dotar de carácter obligatorio a resoluciones previas, así como también actualizar su contenido y elaborar lineamientos de acuerdo con las nuevas atribuciones del MITIC. Respecto de la división política, el MITIC tiene injerencia sobre las decisiones de infraestructura tecnológica de los departamentos; pero en el caso de los municipios, éstos tendrán autonomía para el manejo de su presupuesto. Si bien no se ha relevado normativa específica sobre los servicios de CN existen algunas normas y disposiciones que encuadran jurídicamente su utilización en forma indirecta desde diferentes ángulos y modalidades.

El encuadre normativo respecto de los servicios de CN no presenta avances considerables. Aún no se han desarrollado estándares técnicos ni políticas de cloud first para favorecer la adopción de estos servicios. A pesar de este vacío legal, hay organismos y entidades del Estado como la Administración Nacional de Electricidad o el Ministerio de Desarrollo Social⁴⁹, que ya han adquirido este tipo de servicios por iniciativas propias de sus equipos de TI. Es importante destacar que el MITIC cuenta con un servicio para los organismos y entidades del Estado denominado Nube-PY⁵⁰ que, siguiendo un modelo de despliegue de nube privada, tiene como finalidad ofrecer infraestructura y software como servicios a los organismos que lo soliciten.

El factor común identificado en el sector público es la tendencia hacia la inversión en infraestructura on-premises, bajo el argumento de operar información crítica del Estado de manera soberana e independiente.

Por ello se destacan los centros de procesamiento de datos de la Subsecretaría de Administración Financiera, la Subsecretaría de Tributación, Banco Central, e incluso del MITIC, entre otras entidades. Cabe destacar que el Banco Central se encuentra trabajando en la confección de una regulación que permita la utilización de los servicios de CN, no solamente en las entidades privadas, sino también al interior del propio organismo. Esta administración y adquisición de tecnología en forma independiente resulta en ineficiencias tanto económicas como en el uso de la capacidad adquirida.



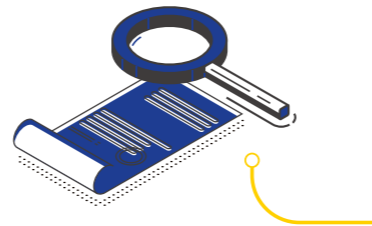
Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

Uno de los objetivos del MITIC es centralizar la infraestructura disponible de todas las entidades de gobierno bajo un esquema de nube híbrida, que incorpore aplicaciones de los proveedores de servicios de CN más reconocidos a nivel internacional. El fin es potenciar los recursos de la Nube-PY, incorporando funcionalidades de nube pública que economicen tiempos de desarrollo, escalen los beneficios más rápidamente, sin comprometer información crítica del Estado.

Los grandes proveedores de servicios en la nube a nivel internacional ofrecen su abanico de ofertas en el país. Sin embargo, el único con presencia comercial y oficina local es Microsoft.

Adicionalmente Microsoft ha firmado un memorándum de entendimiento para acompañar al MITIC en sus esfuerzos por llevar a cabo los proyectos asociados al Programa de Agenda Digital⁵⁷.



La oferta de proveedores locales de servicios en la nube presenta un desarrollo incipiente. Se han detectado tres proveedores de IaaS con capacidad de procesamiento local (Tigo, Excelsis y Teisa), además cabe mencionar a empresas como COPACO, Bancard y Rieder, que ofrecen servicios de web hosting y correo electrónico. Adicionalmente, existen empresas que ofrecen diferentes tipos de software como servicio (Softshop, Todosoft, UniTi, Konecta, OLAM, Keeper, Codium); éstas también funcionan como fábricas de software personalizados, presentando alianzas con proveedores internacionales de IaaS, PaaS y DBaaS para sus desarrollos. No se han identificado proveedores locales de PaaS y DBaaS.

NUBE-PY

El proyecto Nube-PY ofrece infraestructura y software como servicio a las agencias del estado paraguayo. Los servicios de Nube-PY se montan sobre un datacenter con servidores de alto rendimiento y redundantes, con recursos de cómputo y almacenamiento, infraestructura de redes de 10 GB y networking conectado a la Red Metropolitana e internet de alta velocidad. En lo que respecta a IaaS, los clientes se auto provisionan máquinas virtuales por catálogo interno personalizado por institución o por catálogo interno estandarizado. A esto se le suma la autogestión de hosting virtual de servidores (físico-a-virtual o despliegue de nuevos servidores); visualización y control de alertas, monitoreo y prevención sobre riesgos y eficiencia del VDC; acceso a servidores

mediante las herramientas brindadas por MITIC. Están incluidas capacitaciones al personal de la institución por parte del equipo de TI de MITIC sobre la utilización y administración de la nube, que será de carácter obligatorio para obtener el acceso al servicio. En términos de SaaS, Nube-PY ofrece una gama de aplicaciones ciudadanas, una plataforma de firma digital según lo definido en la Ley 4.017 de 2010, un sistema de GDL, una plataforma de interoperabilidad para el intercambio de información entre organismos, un software para la implementación de trámites administrativos en línea, además de los servicios de hosting web, correo institucional y plantillas estandarizadas para sitios institucionales y de datos abiertos.

CENTRALIZACIÓN DE CENTRO DE DATOS

Como parte del proceso de relevamiento de la situación actual en el marco del Proyecto de Agenda Digital, el equipo de infraestructura del MITIC ha realizado un inventario de la infraestructura tecnológica de los organismos que se encuentra bajo su ámbito de aplicación. Con un nivel de respuesta del 60% de los consultados, se han detectado alrededor de 160 racks de servidores, estimando un nivel de utilización inferior al 30%. Basado en estos datos y en la autoridad que le concede la Ley 6.207 de 2019 como administrador de la infraestructura tecnológica de todas las entidades que dependan del gobierno nacional, los especialistas del MITIC han ideado un proyecto de optimización de la infraestructura, mediante la centralización de estos bajo la administración del Ministerio. El objetivo perseguido es la implementación de una nube core de gobierno mediante

una plataforma basada en el software de virtualización OpenStack. Esto permitiría unificar el poder de cómputo y almacenamiento de todos los recursos del estado y, a través de un orquestador, administrar centralizadamente máquinas virtuales que abastezcan la demanda de las agencias de gobierno. Comprende un cambio de paradigma en el desarrollo de aplicaciones, yendo hacia un modelo de contenedores. Esta solución contempla la alternativa de migrar hacia una nube híbrida, incorporando aplicaciones de la nube pública para ganar escalabilidad y velocidad de implementación, pero sin comprometer la soberanía y control de los datos. De acuerdo con el ritmo de actualización de equipamiento proyectado por el Ministerio, centralizar estos recursos podría significar un ahorro en costos de aproximadamente US\$ 60 millones.

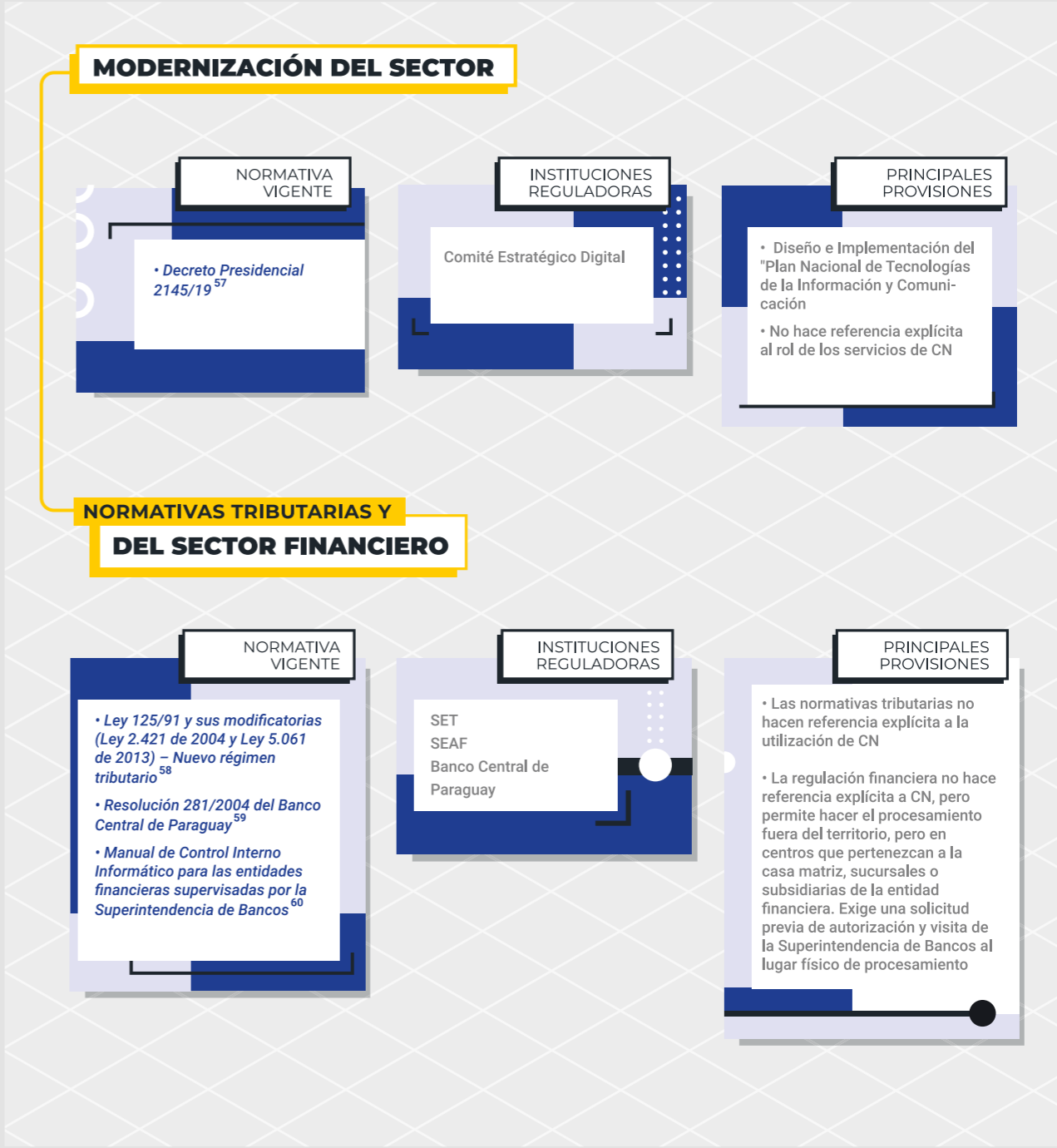


Ilustración 14. Paraguay: marco regulatorio de los servicios en la nube.



Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

Es relevante mencionar el rol del MITIC como proveedor de IaaS y SaaS a través de la Nube-PY, que además de su servicio de infraestructura, incluye aplicaciones orientadas a los ciudadanos, gestión de documentos en línea (GDL), portal de datos abiertos, hosting web y correo electrónico, entre otros.



Ilustración 15. Paraguay: Barreras a la adopción y líneas de acción de corto plazo a explorar.





Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

PAÍS

URU.

Uruguay se ha colocado a la vanguardia como referente regional y mundial en gobierno digital y preside el D9⁶², el grupo de países digitalmente más avanzados a nivel global.



Con su inclusión en el D7 (en 2017, ahora D9 por la cantidad de países que lo integran), Uruguay ha sido el primer país latinoamericano en ocupar un espacio de decisión global respecto al desarrollo de las sociedades digitales.

Uruguay cuenta, a nivel nacional, con un único organismo responsable por las cuestiones relativas al uso y desarrollo de CN: AGESIC. La AGESIC es el órgano responsable por temas de vital importancia para el uso y desarrollo de CN, como ser la protección de datos personales, ciberseguridad y adquisiciones por parte del Estado. La AGESIC es una unidad ejecutora con autonomía técnica dependiente de Presidencia. Fue creada por el art. 72 de la Ley N° 17.930 de diciembre de 2005.

AGESIC procura innovar y hacer más eficiente la forma en que la ciudadanía se relaciona con el Estado, siendo el caso de “Usuario gub.uy” un claro ejemplo de ello.

Respecto a la conectividad y despliegue de fibra en el país, el 75% de las conexiones de los hogares ya cuenta con instalación, mientras que el 82% de los hogares está conectado a Internet por banda ancha⁶³, esperando llegar al 100% de los hogares en el primer trimestre de 2020 (según anunciado por el Ministro de Industria, Energía y Minería del Uruguay en junio de 2019), habiendo, en 2010, Antel iniciado el proyecto de fibra al hogar.

El marco regulatorio de Uruguay establece límites claros respecto a la adopción de CN por parte de los distintos organismos del sector público.

100% DE HOGARES EN LA NUBE

CONECTADOS POR BANDA ANCHA COMO OBJETIVO 2020

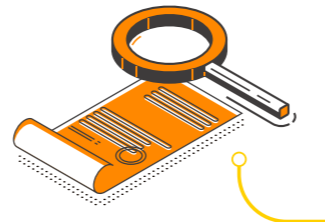
Se destaca la regulación en cuanto al control de los datos personales, la cual permite la transferencia de datos personales hacia países u organismos internacionales o supranacionales que cumplan con una legislación adecuada. Sin embargo, en lo que respecta a datos de la administración central, por ser todos ellos considerados activos estratégicos o información crítica del Estado, los mismos no pueden ser transferidos hacia otras jurisdicciones, sino que deben quedar alojados en territorio nacional uruguayo, en datacenters debidamente certificados para tal fin. Otro aspecto para destacar a nivel regulatorio en Uruguay es la política de software de código libre⁶⁴, por la cual se determina la obligatoriedad de uso de software libre, salvo que se fundamente la razón para no hacerlo.



Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

Para la provisión de servicios SaaS del tipo de inteligencia artificial (IA) o machine learning, atento a una limitación en la oferta local, la AGESIC ha autorizado excepciones para la contratación de este tipo de servicios a empresas internacionales (permitiendo en dichos casos la transferencia internacional de datos y el uso de software que no sea open source). Algunos ejemplos de ello son escucha o análisis de sentimientos en redes sociales y la identificación de evasión impositiva. Aun siendo excepciones que deben superar un proceso de aprobaciones, las mismas permitirían ver una vocación del gobierno uruguayo por no verse relegado en el uso de tecnologías de avanzada a nivel internacional que no cuentan con un desarrollo comparable a nivel local.



En cuanto a la demanda, se estima que el mercado de computación en la nube en Uruguay se encuentra en torno a los US\$ 40 a US\$60 millones, con un crecimiento anual en torno al 30%.

Por su parte, en cuanto a la oferta, tal como se indicara anteriormente, y en lo que respecta a los organismos del Estado, la misma se encuentra limitada por cuestiones regulatorias (obligatoriedad de alojar en territorio uruguayo los datos de la administración central. La empresa de telefonía Antel cuenta con los dos centros de cómputos más grandes del país (uno es el situado en Pando y otro más pequeño es el que se encuentra en Pocitos), el centro de procesamiento de Pando es el único que cuenta con la certificación de AGESIC. El gobierno uruguayo cuenta también con un datacenter propio ubicado en el mismo edificio de presidencia (sobre el mismo está montada la nube de presidencia, generada como forma de consolidar distintos datacenters).

USUARIO GUB.UY

“Usuario gub.uy” (anteriormente llamado ID Uruguay) es un sistema que permite, mediante una única cuenta, acceder a todos los trámites y servicios digitales del estado sin necesidad de nuevos registros ni contraseñas adicionales. Con el “Usuario gub.uy” los ciudadanos cuentan con una única cuenta para poder ingresar de manera cómoda, fácil y segura a servicios digitales del estado uruguayo. Los siguientes son algunos de los organismos más importantes que ya han adoptado el sistema:

- Dirección General Impositiva
- Intendencia de Montevideo
- Ministerio de Ganadería, Agricultura y Pesca
- Ministerio del Interior
- Ministerio de Salud Pública
- Ministerio de Transporte y Obras Públicas
- Ministerio de Trabajo y Seguridad Social
- Ministerio de Vivienda, Ordenamiento Territorial y Medio Ambiente
- Unidad Reguladora y de Control de Datos Personales: Registro de Base de Datos
- Unidad Reguladora de Servicios de Comunicaciones

RED SALUD

La Historia Clínica Electrónica Nacional (HCEN) se basa en el intercambio de información clínica entre prestadores de salud para dar sustento a la continuidad asistencial y al rol de rectoría del Ministerio de Salud Pública. El Programa Salud.uy posibilita el intercambio de información clínica de forma segura. Dicho intercambio es realizado a través de la Red Salud. La Red Salud es una red privada para la conexión de instituciones, públicas y privadas, con competencias legales en materia de salud que permite que se realice el intercambio seguro de información de los usuarios de salud a través de la plataforma Salud.uy. La Red Salud es una red de alta velocidad, que cuenta con velocidades que van de 10 a 100Mbps.

Es una red de alta disponibilidad, escalable, segura, auditada por CERTuy y monitoreada 24/7. La conexión se realiza mediante contrato directo de las organizaciones con Antel. Mediante el proyecto Accesos Salud.uy se busca empoderar al usuario respecto a quien o quienes pueden acceder a su información clínica electrónica en el marco de la HCEN. Cada usuario tendrá la posibilidad de configurar las políticas de acceso a la información por parte del equipo de salud en el marco de la reglamentación vigente. Cuenta con el objetivo de alcanzar un 100% de adopción para el año 2020. La adopción de la HCEN es mandatoria para todos los prestadores, tanto públicos como privados del país.

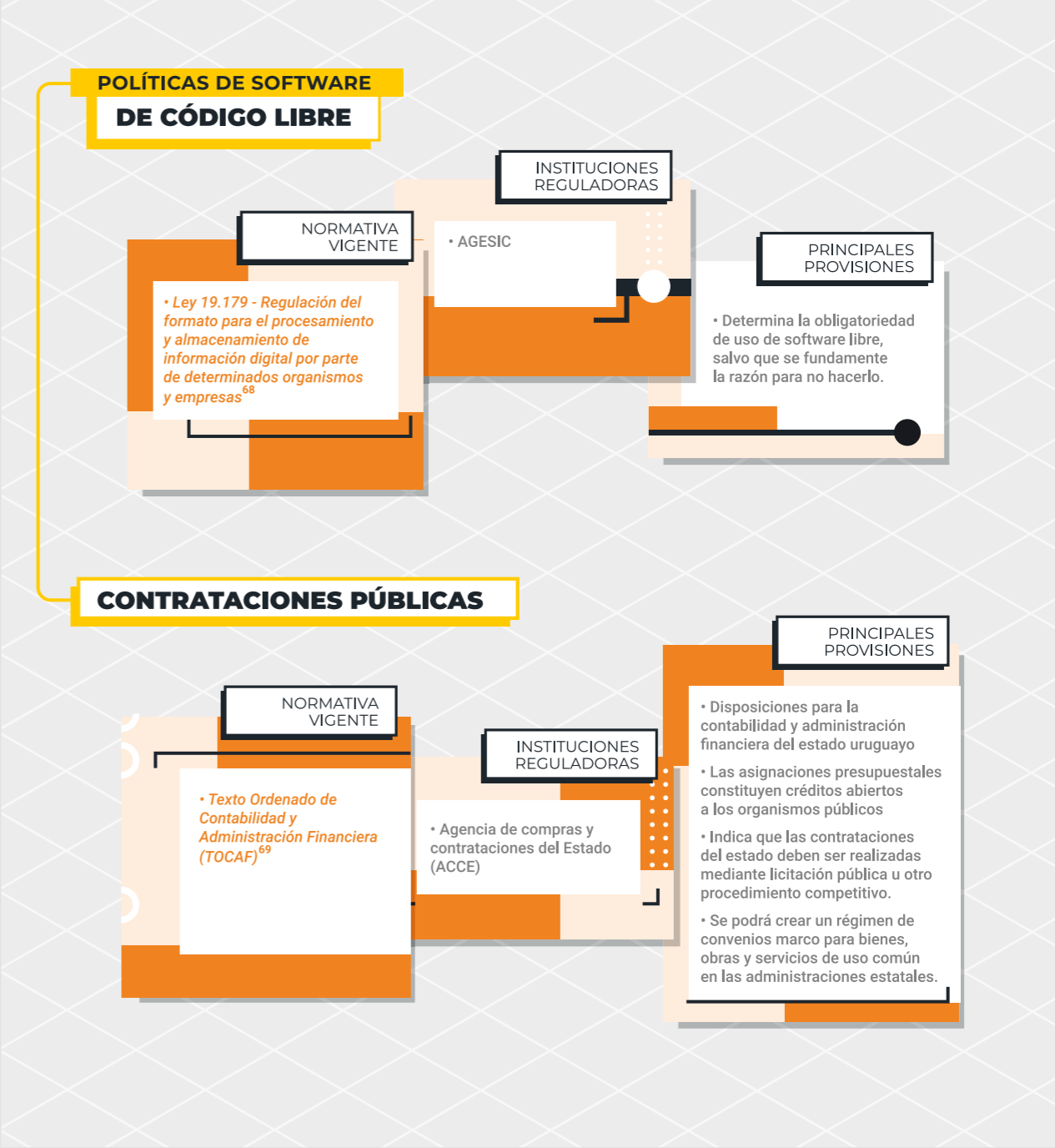


Ilustración 16. Uruguay: marco regulatorio de los servicios en la nube.

Desde Pando, Antel brinda los distintos modelos de servicios de CN. Los mismos son clasificados en cuatro familias de servicios: alojamiento, MiNube (infraestructura, aplicaciones y servicios), servicios complementarios y de internet y conectividad privada. La nube de Presidencia ofrece tanto servicios de IaaS, como de PaaS y SaaS. Los servicios de la Nube de Presidencia se ofrecen en dos centros de datos: el de Torre Ejecutiva y el de Antel Pando, esto permite mejorar la resiliencia, asegurando la continuidad del negocio y protegiendo los datos alojados en la Nube.

La HCEN es uno de los servicios que la nube de Presidencia presta a los organismos del Estado.

En cuanto a los principales proveedores de servicio de CN internacionales (Google, Microsoft Azure, Amazon Web Services), proveedores de servicios de IaaS, PaaS y SaaS, ninguno de ellos posee capacidad de procesamiento en territorio uruguayo (Microsoft, en sociedad con Sonda, posee un módulo de Azure Stack en datacenter de Antel), proveyendo estos sus servicios de IaaS, PaaS y SaaS de manera internacional. En octubre de 2019 Google anunció⁷⁰ la instalación de un datacenter en zona franca en el departamento de Canelones, siendo entonces el segundo datacenter de la firma en Sudamérica.

En cuanto a la oferta de datacenters locales privados, el uso de los mismos por parte de entes de gobierno se encuentra desalentado por no contar con la certificación de la AGESIC y por no poder contratar los mismos mediante modelos de contratación directa, como si ocurre con Antel por ser un organismo del Estado.



Ilustración 17. Uruguay: Barreras a la adopción y líneas de acción de corto plazo a explorar.



SECCIÓN

06

MODELOS DE COSTOS PARA EL CONO SUR

PROCESO DE MIGRACIÓN A LA NUBE



MIGRACIÓN HACIA SERVICIOS DE IAAS

Se reemplazarán gastos de infraestructura por nuevos gastos corrientes (el abono IaaS del proveedor) y esos gastos corrientes se tornarán variables en función de las necesidades de procesamiento, almacenamiento, transferencia de datos y soporte.

También podría mutar la estructura del equipo de TI, ya que podrán reconfigurarse aquellos recursos específicamente asignados a la gestión de la infraestructura. En esta instancia se mantendrán los gastos asociados al software, entre los que se encuentran el sistema operativo, motores de base de datos y entornos de desarrollo de aplicaciones. Aquí podrían entrar en consideración las soluciones de código abierto, que dotan de mayor flexibilidad e interoperabilidad a la arquitectura diseñada.

Si bien su implementación es libre, al igual que las soluciones propietarias, se necesita un equipo que lo administre, por lo que su operación requerirá de un equipo in-house o el pago de una tarifa anual para garantizar soporte técnico y actualización de las versiones instaladas.



MIGRACIÓN HACIA SERVICIOS DE PAAS

En la migración hacia un modelo de servicios PaaS, el cliente no administra la infraestructura. En este caso tendrá el control sobre el entorno de desarrollo, que le permitirá crear sus propias aplicaciones.

En este modelo los gastos corrientes se asocian al costo de la licencia del entorno de desarrollo y las horas de trabajo necesarias para diseñar las aplicaciones propias. Además, se agregan cargos por exceso de almacenamiento, procesamiento y transferencias de datos respecto de las condiciones del plan contratado. En este punto también podría reconfigurarse el equipo de TI con mayor foco en el entendimiento de la operación y el desarrollo de aplicaciones.



MIGRACIÓN HACIA SERVICIOS DE SAAS

El modelo de SaaS es el que presenta una mayor integración en la adopción de servicios en la nube. En esta etapa la clave radica en identificar el software que mejor responda a las necesidades de la organización. En esta instancia, los gastos corrientes provienen, únicamente, de la licencia del software (SaaS), los salarios del equipo de TI y de soporte técnico interno.

Las soluciones on-premises obligan a los organismos a considerar una inversión inicial asociada a servidores, racks, firewall, almacenamiento, sistemas operativos, motor de base de datos, software de virtualización y desarrollo de aplicaciones. Adicionalmente,

se requiere una estimación en el mediano plazo de los requerimientos de espacio físico, servicios públicos, conectividad, así como también la conformación de un equipo de TI capacitado para operar la arquitectura de red apropiada.



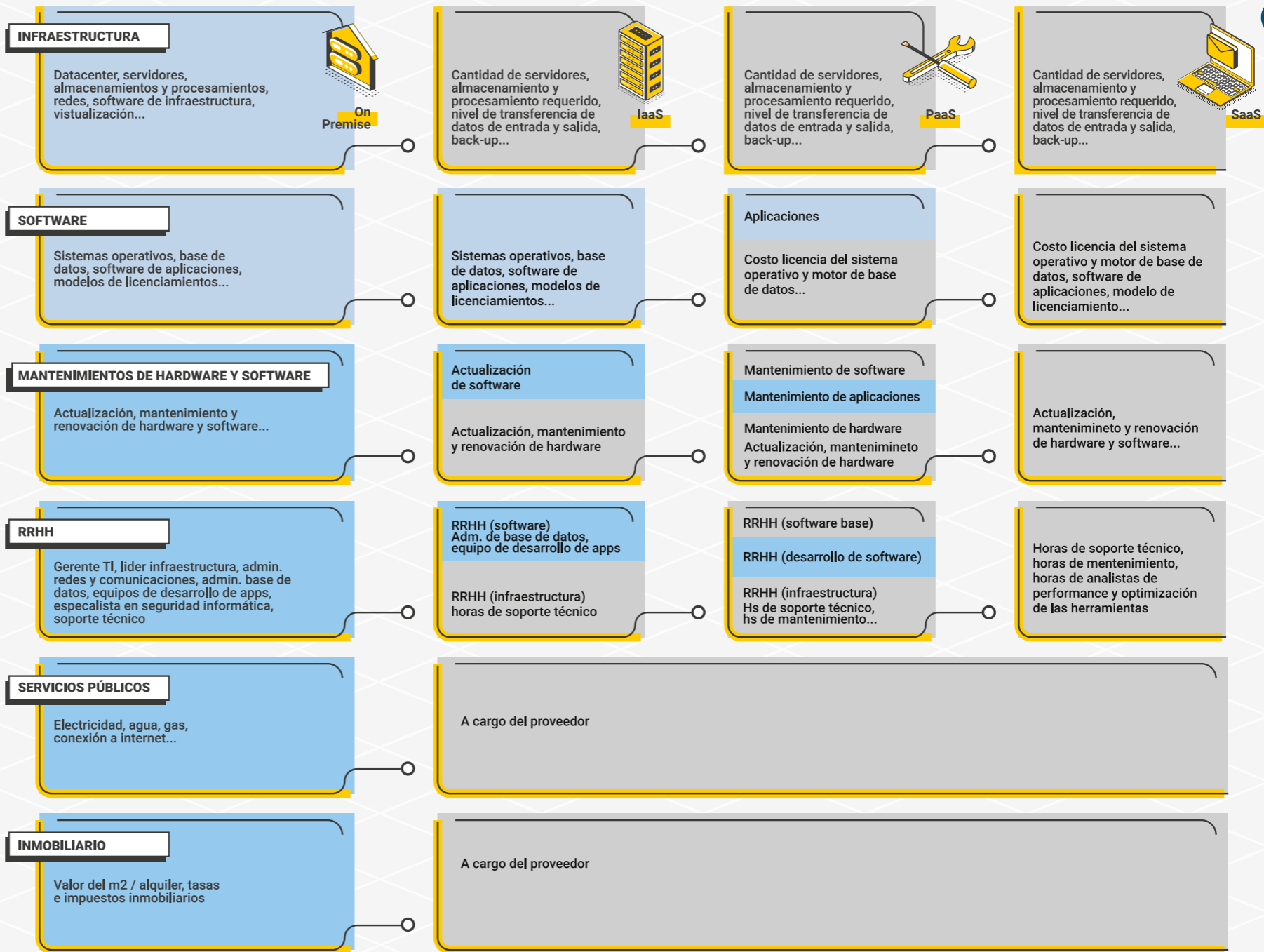
ELEMENTOS DE COSTOS GENÉRICOS

Los elementos de costos van migrando y pasando de erogaciones de capital a costos corrientes al pasar de soluciones on-premises a modelos de servicio de CN. Los elementos de costos a ser considerados son:

- la infraestructura y su depreciación.
- el software.
- el mantenimiento del software y hardware.
- el personal.
- servicios públicos (principalmente electricidad).
- y el costo inmobiliario del espacio físico para alojar la infraestructura.

Los niveles de adopción de servicios en la nube provocan una reconfiguración de los elementos genéricos de la estructura de costos. Esta transformación también se genera al interior de los equipos de TI, que mutan desde funciones de administración y operación de infraestructura, hacia funciones de control y seguimiento de los servicios de CN, para asegurar el uso eficiente y apropiado de los mismos y para evitar incrementos inesperados en los gastos corrientes.

Ilustración 18. Conversión para el usuario de gastos de capital a costos de operación.





Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

RESULTADOS DEL EJERCICIO DE MODELACIÓN DE COSTOS

El ejercicio de valoración estima el costo presente neto de un aplicativo de gestión de relacionamiento con los clientes⁷² para atención ciudadana (aplicativo considerado a modo ilustrativo para los fines del ejercicio) en los cinco países del estudio para dos perfiles de intensidad de uso (uno mayor, de alcance nacional, y uno menor, de alcance municipal). La valoración contempla la posibilidad de uso de los modelos de servicio on-premises, IaaS, PaaS y SaaS; tres modelos de despliegue (nube pública, híbrida y privada); dos alternativas de localización geográfica del datacenter del proveedor (Estados Unidos y Brasil); y, finalmente, la posibilidad de contar con un centro de procesamiento de datos de gobierno que ofrezca sus servicios.

Cada uno de los modelos de servicios y desplie-

que contemplados en el modelo de costos presenta un esquema de facturación diverso de CN, el que depende de factores tales como la intensidad de uso, las características de la infraestructura y el software, la localización del centro de datos que proveerá el servicio, el esquema de pago que seleccione el cliente, entre otros elementos. La complejidad del modelo de costos realizado radica en reflejar estos diferentes esquemas, a fin de ajustar la estimación a los casos reales identificados como escenarios principales de análisis.

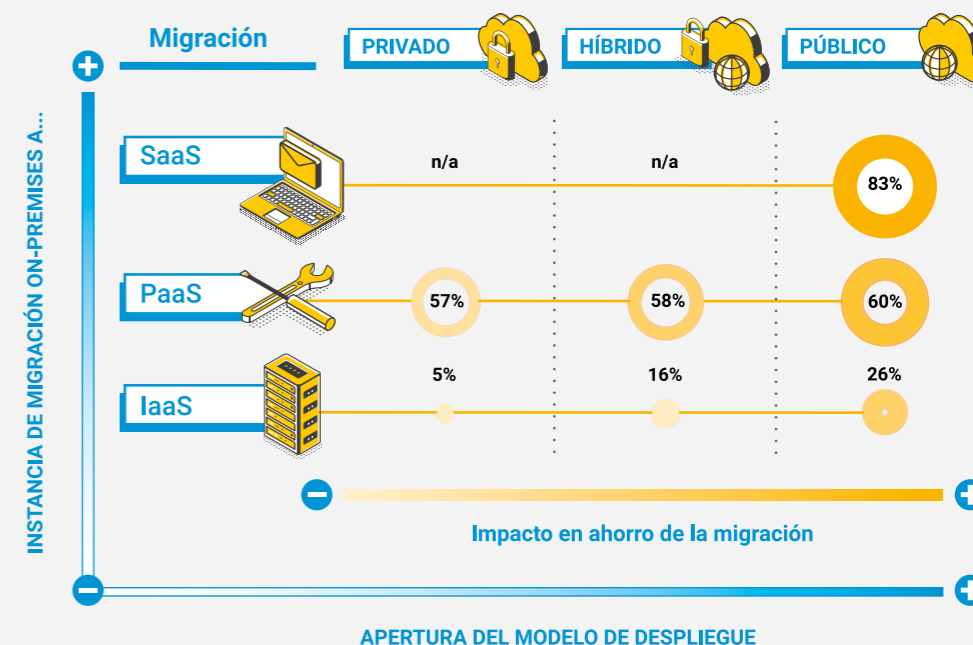
El modelo supone en todos los casos la implementación de soluciones de código abierto, tanto para los sistemas operativos, motores de base de datos, software de virtualización y entornos de desarrollo de aplicaciones.

En términos estructurales, el resultado se compondrá de una valoración por flujo de fondos incrementales a cinco años, con periodicidad mensual, que serán descontados en base a las tasas de descuento de referencia del mercado para cada país. El resultado del modelo de costos genérico permitirá analizar valores relativos entre distintos grados de los modelos de servicio en la nube, remarcando el beneficio incremental versus la situación on-premises.



A modo ilustrativo, los resultados presentados a continuación reflejan el escenario con un perfil de demanda elevado (nacional), con infraestructura localizada en Estados Unidos brindada por un proveedor de carácter privado. Como se observa, existe eficiencia de costos en la medida en que se integran servicios de CN (de on-premises a SaaS) y en la medida en que se migra a un modelo de despliegue de nube pública.

Ilustración 19. Resultado económico de la migración a la nube. Cuadro de resultados por país: perfil nacional, localizado en EEUU, proveedor privado (Ahorro máximo estimado)



El ejercicio concluye que los modelos de despliegue en nube pública son aquellos que presentan mayores niveles de ahorro frente a la situación on-premises. Sin embargo, a lo largo de las entrevistas realizadas, se ha identificado cierta reticencia a la migración a la nube pública. Ante ese

escenario, las soluciones híbridas podrían combinar los beneficios del ahorro que otorgan los servicios en la nube con los requerimientos de soberanía y control de información presentes tanto en las legislaciones de protección de datos personales como en las preferencias de los funcionarios de gobierno.



Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

Aun cuando queda claro la reducción de costo por el uso de los servicios de CN, resulta importante destacar que el costo no es el único factor al definir una estrategia de CN.

Se deben también considerar **ASPECTOS ESTRATÉGICOS** tales como:

- 1 NIVEL DE DEPENDENCIA DE PROVEEDORES, SEAN PÚBLICOS O PRIVADOS (VENDOR LOCK-IN)
- 2 LA PORTABILIDAD DE DATOS Y SISTEMAS
- 3 LA CIBERSEGURIDAD
- 4 LA FACILIDAD PARA INTEGRAR SERVICIOS
- 5 EL RENDIMIENTO DE LOS APLICATIVOS
- 6 LOS EFECTOS EN EL MERCADO DE PROVEEDORES, ENTRE OTROS



CONCLUSIONES:

Teniendo en cuenta dicha aclaración, y en lo referido al análisis económico estrictamente, a partir del modelo de costos se concluye que:

El informe completo sobre el que se respalda este reporte contempla un análisis en mayor detalle sobre costos por país ante diferentes escenarios.



El documento completo se puede solicitar a Agustina Schijman al email aschijman@iadb.org

1

El impacto de los servicios en la nube es mayor allí donde la masa crítica de usuarios no es la suficiente para justificar las mínimas inversiones de infraestructura tecnológica necesarias para operar este tipo de aplicativos, por ejemplo, a nivel de gobiernos subnacionales o locales. Allí donde las economías de escala no justifican el nivel de inversión para adquirir equipos, la utilización de los servicios de CN dota de flexibilidad y rapidez a la implementación, lo que permite una puesta en funcionamiento ágil, efectiva y menos costosa, reduciendo los tiempos de capacitación y el requerimiento de recursos humanos. Por lo tanto, cuando no se alcanza la masa crítica de usuarios, la CN es la única alternativa para dichos organismos para digitalizar su operación y así poder ofrecer a ciudadanos y funcionarios propios los beneficios que las nuevas tecnologías de la información permiten (inclusive, para algunas municipalidades u organismos pequeños la CN puede ser la única alternativa para prestar ciertos servicios).

El ahorro en costos es mayor conforme los usuarios integran servicios de CN, avanzando en el sendero de migración de servicios desde un esquema on-premises, pasando a IaaS hasta llegar finalmente al modelo SaaS; ese impacto se potencia en la medida que se acompaña con una migración desde un modelo de despliegue privado hacia la opción de nube pública

3

En lo referido a modelos de nube privada, en Brasil el ahorro por la migración a IaaS se encontraría alrededor del 5%. En los restantes países, esta opción sería más costosa que el despliegue on-premises (ello se da debido al impacto impositivo de estos servicios en el mercado brasileiro). La localización del datacenter en Brasil reduce los beneficios, en términos económicos, de la migración a la nube producto de los mayores costos impositivos. No obstante, presenta menor latencia que soluciones localizadas en EEUU

4

Los beneficios de migración a la nube resultan mayores cuando son provistos por soluciones de gobierno que cuando el servicio es provisto por una empresa privada. Cabe destacar que, en algunos casos, este tipo de modelo de servicio se encuentra subsidiado por la entidad de gobierno que lo administra. Si bien esto significa un ahorro en costos para la agencia que adquiere el servicio, debe evaluarse el costo global para el gobierno de dicha alternativa. Adicionalmente, deben evaluarse los niveles de calidad de servicio brindados por estas soluciones de gobierno, comparándolas con los servicios y propuestas ofrecidos por los jugadores privados de clase mundial.



SECCIÓN

07

LÍNEAS DE TRABAJO EN LOS PAÍSES DEL CONO SUR

BARRERAS A LA ADOPCIÓN POR PARTE DEL SECTOR PÚBLICO



BARRERAS ORGANIZACIONALES

MODELOS DE CONTRATACIÓN

Esquemas de contratación obsoletos y enfocados en la adquisición de equipamiento e infraestructura



PROCEDIMIENTOS

Presupuestos asignados a los organismos de gobierno en forma anual, lo que no da certeza sobre la factibilidad de afrontar el gasto operativo en años siguientes.
Obligación explícita o implícita a utilizar un proveedor del estado



RECURSOS HUMANOS

Falta de personal capacitado para la contratación y posterior administración de servicios de IaaS y de PaaS de CN (no sería limitante para SaaS)



CULTURALES

Preocupaciones vinculadas a la ciberseguridad y al desconocimiento de la regulación



FALTA DE DISPARADORES

La obsolescencia tecnológica y/o necesidad de adquisición de nueva infraestructura (y su alta necesidad de inversión) resultan en muchos casos los disparadores de migración a la nube



BARRERAS POLÍTICAS

COORDINACIÓN Y PREVISIBILIDAD

Diferencias políticas entre líderes de agencias, e incertidumbre ante cambios de gobierno (pérdida de la memoria institucional)



LAW ENFORCEMENT ACCESS TO DATA

Potencial pérdida de control de la información en caso de ser transferida a otras jurisdicciones



BARRERAS DE INFRAESTRUCTURA Y RECURSOS

CONECTIVIDAD

La transferencia y procesamiento de datos requiere de buena conectividad y baja latencia



73

RECURSOS ECONÓMICOS

Continuidad de presupuesto para solventar los gastos de servicios de CN



BARRERAS INSTITUCIONALES Y REGULATORIAS

REGULACIÓN AUSENTE

La ausencia de regulación conlleva a desconcierto respecto a la posibilidad normativa de adoptar la CN



LIMITANTES NORMATIVAS

Condicionamientos a la transferencia internacional de datos y requisitos de geolocalización
Falta de neutralidad tecnológica, por ejemplo obligatoriedad de uso exclusivamente de código abierto



Ilustración 20. Algunos ejemplos de barreras para la adopción de CN por parte del sector público en países del Cono Sur.

VOLVER AL ÍNDICE



Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.



BARRERAS ORGANIZACIONALES

PROCEDIMIENTOS Y MODELOS DE CONTRATACIÓN

Los modelos de contratación aún no responden, totalmente, a los modelos de pago-por-uso de los servicios de contratación en la nube y, en muchos casos, los organismos de gobierno, cuando contratan dichos servicios, lo hacen de una manera “tradicional”, como ser pre-comprando crédito o reservando una determinada capacidad fija de recursos. Ello responde, mayormente, a que las partidas presupuestarias aún responden a una lógica de inversión de costo fijo y por ciclos anuales. Por el contrario, la contratación de servicios de CN requiere de capacidad técnica de dimensionamiento y de estimación de los gastos anuales y, en segundo lugar, requieren de un compromiso de erogación de un gasto fijo creciente a lo largo de los años. Adicionalmente, para el caso de contratación de servicios de CN de los referentes de clase mundial (Amazon AWS, Microsoft Azure, Google Cloud e IBM), éstos suelen facturar en dólares, lo que agrega una variable adicional a la dificultad de previsión del nivel de gastos. Por último, la contratación internacional de servicios de CN reviste un riesgo de interrupción de servicio ante falta o demora

en el pago (por ejemplo por problemas con controles de capitales, tarjeta de crédito utilizadas para los pagos, etc.). Estas barreras relacionadas a los modelos de contratación para los servicios de CN han sido identificadas en los cinco países contemplados en el presente informe. En el caso de Chile se puede destacar que, mediante ChileCompra, se cuenta con vehículos de contratación específicos para los servicios de CN pero aún existe falta de conocimiento al respecto por parte de los organismos públicos y permanece vigente, al igual que en los otros mercados, la cuestión relativa a las partidas presupuestarias anuales. Teniendo en cuenta las leyes de contratación y licitación en estos países, la selección de un proveedor privado para un contrato significativo puede llegar a demorar más de un año o dos y, en muchas ocasiones, es usual que al final sea declarado desierto o el proceso cancelado. Una opción a ser estudiada sería la implantación de plataformas de adquisición de TI y CN como el Marketplace de Reino Unido (<https://www.digitalmarketplace.service.gov.uk/>).

RECURSOS HUMANOS

En todos los países de la región se ha identificado una falta de recursos humanos calificados en la CN, específicamente para IaaS y PaaS. Esta falta de recursos se ha evidenciado no solamente en lo referido a recursos técnicos para la implementación y administración de los servicios de CN sino también en los recursos de compras, por ejemplo, para comprender los modelos de negocio y beneficios en potenciales ahorros de costos. Estos últimos recursos son aquellos que deben contar con las capacidades para identificar y valorar los beneficios que la implementación de servicios de CN podría representar para su organismo. En el caso de Uruguay se han relevado también situaciones en las que los procesos de contratación de personal técnico

serían obsoletos y no se encontrarían en línea con las nuevas tendencias en cuanto a formación de perfiles técnicos de sistemas (no necesariamente enfocados en carreras de grado, sino que con foco en la realización de cursos específicos y autoaprendizaje). No obstante, cabe resaltar que para el caso de SaaS se da la situación inversa ya que, al tercerizar el servicio completo, el requerimiento de personal capacitado es significativamente inferior, o prácticamente nulo. La barrera de recursos humanos, en cuanto a SaaS, aplicaría únicamente para el caso de requerir, por cuestiones regulatorias, o de otra índole, desarrollos nacionales (tal como ocurre en Uruguay o en Chile por su vocación de convertirse en un “Hub digital”).

RECURSOS CULTURALES

Fuertemente vinculadas a las anteriores, tienen que ver con la falta de conocimiento de los beneficios de los servicios de CN y con los temores y consideraciones, no fundamentados, sobre los riesgos relacionados a la ciberseguridad. Una segunda cuestión que preocupa a la hora de evaluar la migración a la nube es el vendor lock-in, por el cual, una vez migrados a una plataforma de CN, la flexibilidad para migrar a una nueva plataforma en el futuro, sea pública o privada, aun cuando sea posible, se presenta siempre como un interrogante

sobre su factibilidad y facilidad a la hora de querer implementarla. Dicha situación se observa en los casos de Argentina, Brasil, Chile y Paraguay en que, aun estando permitido a nivel regulatorio, los distintos organismos de gobierno optan por seguir operando en sus centros de procesamiento on-premises en lugar de migrar a servicios en la nube, o realizan una migración lenta y/o limitada (únicamente migrando cierto tipo de información de menor relevancia).

FALTA DE DISPARADOR PARA LA MIGRACIÓN A LOS SERVICIOS DE CN

En muchas situaciones los organismos públicos cuentan con infraestructura legacy, on-premises, con capacidad de uso, sobre la cual pueden realizar el procesamiento de los datos de su entidad. En dichos casos la inversión ya ha sido realizada y, por lo tanto, el procesamiento de los datos no representa un costo adicional más allá del costo, hundido, de mantenimiento de dicho centro de procesamiento de cómputos.

A modo de ejemplo de esta situación se puede mencionar el caso de la ASI en la Ciudad de Buenos Aires en que, como primera medida, se optó por una concentración de diversos centros de cómputos remotos y descentralizados y, luego, ante la necesidad de erogaciones significativas por falta de capacidad o mantenimiento, se optó por migrar hacia la nube bajo modelos híbridos.



BARRERAS INSTITUCIONALES Y REGULATORIAS

REGULACIÓN AUSENTE

La ausencia de regulación genera incertidumbre respecto a la posibilidad de adopción de los servicios de CN, bajo qué modalidad hacerlo, con qué recaudos, cuáles son sus riesgos, etc. Ante esto, la posición de los entes de gobierno suele ser la de no adopción de servicios de CN frente a la falta de claridad sobre las posibilidades de uso. En cuanto a la ausencia de lineamientos nor-

mativos, aun cuando en otros países objeto del presente informe, tal como se indicara previamente, se considera que la regulación en términos de los servicios de CN es aún incompleta, el caso más claro es el de Paraguay, en que la regulación aún se encuentra en etapa temprana y no hace referencia específica a los servicios de CN.

LIMITACIONES NORMATIVAS

Las limitaciones normativas son aquellas que establecen condiciones de borde a la adopción de los servicios de CN y resultan en el no uso de dichos servicios, o en un uso no eficiente de éstos. Como ejemplo de esta situación, se puede mencionar el caso del sector gobierno de Uruguay, en que la limitación de transferencia internacional de datos de la administración central obliga al uso exclusivo de datacenters locales. En este caso se podría presentar el riesgo de pérdida de competitividad o de posicionamiento como gobierno a la vanguardia de las cuestiones digitales en el caso que los datacenters locales no adopten las mejores prácticas (sea como resultado de no poder seguir el ritmo

de inversiones y de investigación y desarrollo de los proveedores de este servicio de clase mundial o por otros motivos no económicos). Se presenta una situación similar en cuanto a la obligatoriedad de utilización de aplicaciones de código abierto, lo cual podría indicar que no hay un tratamiento neutral a la tecnologías y o distintas empresas oferentes de servicios. Si bien, esto puede ser algo que va en línea de evitar el citado "vendor lock-in" puede ser un limitante para adoptar otros desarrollos propietarios que ofrezcan soluciones a un problema específico, algo que no necesariamente encierra al gobierno en una contratación en tanto esos desarrollos sean interoperables.



BARREAS DE INFRAESTRUCTURA Y RECURSOS

CONECTIVIDAD

La transferencia y procesamiento de datos requiere una buena conectividad y baja latencia. Por su parte, un impacto esperado de la CN es la reducción de la brecha digital entre las ciudades importantes y los poblados más remotos con menor cantidad de recursos; en la medida que dichos poblados no cuenten con buena conectividad, no podrán acceder a los servicios de CN

RECURSOS

La migración a los servicios de CN requiere de recursos en dos sentidos: recursos humanos para su implementación y administración eficiente (en el caso de IaaS y de PaaS, no así para el caso de SaaS, tal como

se aclaró al detallar las barreras organizacionales) y recursos económicos para su mantenimiento en el tiempo, aún frente al crecimiento de su necesidad de fondos año a año.

que los gobiernos centrales puedan disponibilizar para los municipios de un país. En los países del Cono Sur se ha visto que, mientras en Uruguay y Chile la conectividad no se presenta como una barrera significativa para el desarrollo de CN, sí podría serlo para los casos de Brasil, Argentina y, principalmente, de Paraguay.

COORDINACIÓN Y PREVISIBILIDAD

Sea por recelo de la información, por diferencias políticas, desconocimiento u otros motivos, algunos organismos o entidades territoriales no utilizan recursos disponibles por parte de la administración central principalmente de tipo IaaS o PaaS, aun cuando ésta cuente con una plataforma que ofrezca significativas facilidades de implementación. Como ejemplo, podemos citar el caso de Argentina en que no todos los organismos hacen uso de ARSAT y, aun contando con dicha infraestructura y sus servicios a disposición, optan por hacer uso de infraestructura propia on-premises o, hasta incluso, de servicios

LAW ENFORCEMENT ACCES TO DATA (LEATD)

Aun cuando la regulación lo permita, la cuestión vinculada al law enforcement access to data y la transferencia de datos a jurisdicciones transfronterizas ha surgido como una preocupación por los funcionarios de distintos entes de los gobiernos de la región.

No obstante, en Brasil y Uruguay, dicha situación no se ha manifestado ya que, por restricciones normativas, la información de los entes de gobierno no puede ser transferida ni alojada fuera de territorio nacional.

BARRERAS POLÍTICAS

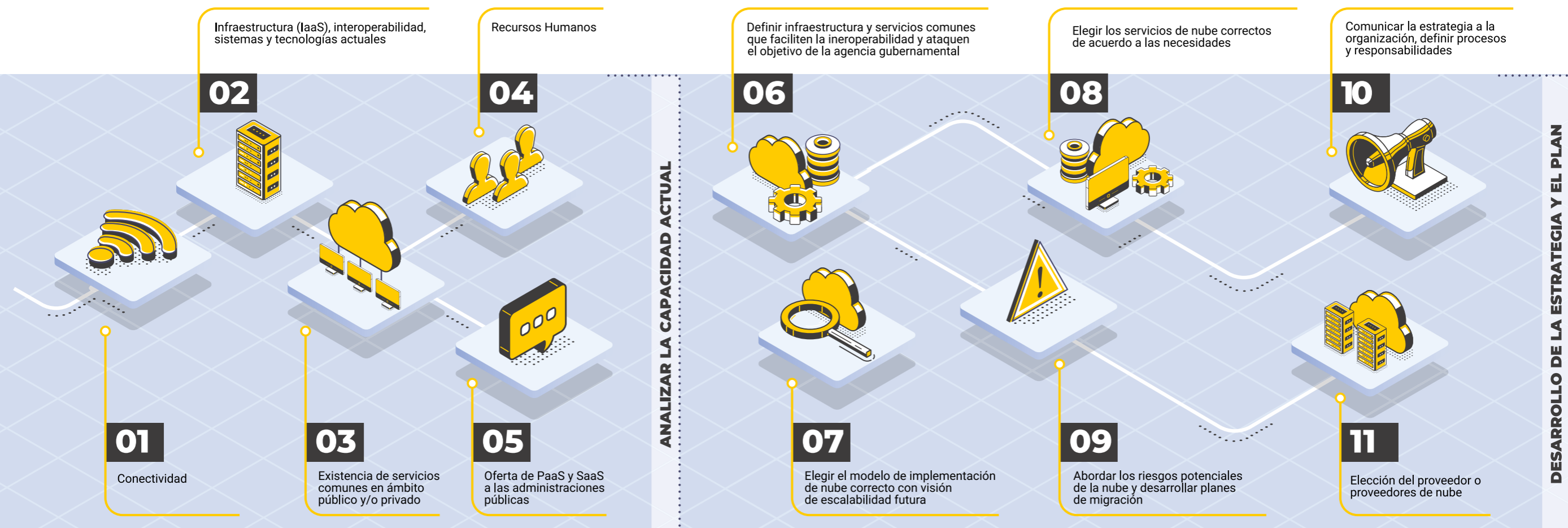


de nube pública. Otro ejemplo es el caso de Uruguay, donde no todos los organismos de gobierno hacen uso de la nube provista por Antel o del servicio de Usuario gub.uy a pesar de la recomendación provistas por AGESIC. Por su parte, en Paraguay la autonomía de municipios no favorece la adopción de sistemas en la nube provistos por MITIC por temor a la implementación de mecanismos de rendición de cuentas. En el caso de Brasil, el federalismo se hace muy evidente en tanto el enfoque puede ser muy distinto Estado por Estado.



Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.



HOJA DE RUTA TECNOLÓGICA

Ilustración 21: Hoja de ruta tecnológica.

La importancia de confeccionar una estrategia de utilización de CN y plasmarla en una hoja de ruta tecnológica es un hito que debe estar presente en las agendas de los gobiernos tanto nacionales, regionales, provinciales y municipales. El crecimiento en el uso de CN implica una transición de experiencias desde las de tipo IaaS a PaaS y SaaS que conlleva un camino de sofisticación en tratar de recabar y entender mejor los datos provenientes de los servicios contratados y de la interacción con los ciudadanos.

El salto tecnológico va a estar dado principalmente por poder hacer inteligencia de datos y considerar a éstos como un activo principal para la gestión de gobierno. Para esto, es necesario invertir en tecnologías emergentes con mayor contracción hacia los estándares abiertos que permitan integrar diferentes soluciones.

Esta estrategia y su consecuente hoja de ruta tecnológica, variará de acuerdo con las características particulares de cada país y de cada una de las organizaciones gubernamentales dentro de los mismos pero, independientemente de lo mencionado, contará con puntos en común que se deberán tener en cuenta. Se recomiendan dos fases para la confección de la hoja de ruta: la primera, un análisis de la capacidad actual y, la segunda, el desarrollo de la estrategia y el plan.



LOS SERVICIOS EN LA NUBE EN LA AGENDA PÚBLICA

Los cinco países estudiados incluyen el uso de la nube en sus agendas públicas y han avanzado con resultados mixtos en la definición de políticas de contratación y estándares internos. Sin embargo, podría decirse que la política de tipo “cloud first” tiene mayor historia y trabajo institucional en Uruguay y Chile, ha sido más contemporáneo en Argentina y Brasil y es todavía muy preliminar en Paraguay, que ha comenzado a definir políticas específicas muy recientemente.

El caso de éxito de **Uruguay** se vincula, muy probablemente, al liderazgo que ha mantenido la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC), la cual ha centralizado la formación de las políticas públicas de Gobierno Digital, Gobierno Abierto y seguridad y privacidad, ha fijado estándares para la utilización de la nube en el gobierno y ha difundido a las entidades del sector público las soluciones que proveen. También, la Agenda Uruguay Digital 2020 se ha actualizado de manera corriente y está sujeta a periódicas consultas públicas. El liderazgo, centralización y claro rol de AGESIC, apoyado en el soporte de la empresa estatal ANTEL, particularmente con el hosting de datos, ha permitido tener una política unívoca con una visión y metas claras⁷⁴.



Argentina, al igual que Uruguay, tiene una repartición gubernamental creada ad hoc para llevar adelante la transformación digital y las políticas de la nube. En Argentina, la Secretaria de Gestión e Innovación Pública, dentro del Ministerio de Modernización, ha hecho avances interesantes en la definición de estándares gracias al trabajo de la Oficina Nacional de Tecnologías de Información (ONTI) y la promulgación de la Agenda Digital 2030 en noviembre de 2018, con metas y líneas de acción de gobierno digital⁷⁵. Sin embargo, estos progresos han sido todavía muy incipientes y no han podido ser escalados para tener mayor impacto. Los cambios de categoría institucional de ese ministerio en los años recientes, al igual que los vaivenes económico-políticos en los que frecuentemente se halla inmerso este país resultan en un facultativo para la continuidad en el tiempo de lo avanzado en estas materias.



En el caso de **Chile** y Brasil, se observan algunas situaciones similares, por cuanto han definido las políticas públicas de gobierno y desarrollo digital con un rol preminente de los Ministerios de Economía, ambos también tienen respectivas agendas digitales relanzadas más recientemente. En Chile, la División de Gobierno Digital de la Secretaría General de la Presidencia de Chile oficia el rol de ser la “consultora de transformación digital del Estado” que asesora y brinda apoyo a las instituciones públicas en el diseño de servicios y en la transformación digital, con el objetivo de implementar servicios al ciudadano⁷⁶. Esta Secretaria General de la Presidencia, junto con el Ministerio de Economía, Fomento y Turismo y el Ministerio de Transporte y Telecomunicaciones, son los que elaboraron la Agenda Digital vigente. El elemento quizás más relevante es que la agenda cuenta con una Secretaría Ejecutiva que tiene como función la coordinación interministerial y hacer el seguimiento de los respectivos planes⁷⁷.

En **Brasil**, si bien la “Estrategia de Governança Digital 2016-2019 (EGD)” data de enero de 2016 y fue revisada en 2018, no menciona específicamente objetivos de uso de CN. Se espera que la Secretaria de Gobierno Digital del Ministerio de Economía de Brasil comience a definir nuevos parámetros más específicos de contratación de servicios en la nube siguiendo en la línea de la reciente Instrucción Normativa nro.1, del 4 de abril de 2019, en la que se deja claro una política “cloud-first” para los organismos y entidades que necesiten crear, ampliar o renovar su infraestructura y centros de datos. La revisión de la EGD de Brasil se encuentra en curso.



Por último, **Paraguay** tiene menos historial y más trabajo pendiente en la definición de estándares técnicos, planes, metas y políticas “cloud first”. No obstante, se destaca que el MITIC cuenta con un servicio para los organismos del Estado denominado Nube-PY que, siguiendo un modelo de despliegue de nube privada, tiene como finalidad ofrecer IaaS y SaaS a los organismos que lo soliciten. Al mismo tiempo, desde noviembre de 2018, Paraguay se encuentra trabajando con apoyo del BID en su proyecto agenda digital, donde se contempla el desarrollo del gobierno digital que permita al gobierno mayor eficiencia en la atención al ciudadano⁷⁸.



Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

LOS PILARES DE TRABAJO EN LAS AGENDAS FUTURAS DE LOS PAÍSES

El futuro de la gestión de servicios de TI y CN en los gobiernos va a requerir contar con liderazgo institucional y agencias más proactivas, con visión de futuro, que re-imaginen continuamente el modo en que sirven a sus ciudadanos. Para esto la CN va a ser un activo fundamental en tanto permitirán desarrollar una “cultura centrada en aprovechar el uso de los datos” para tomar mejores y más informadas decisiones.

En el crecimiento de las ciudades inteligentes, sería de esperarse que “el ciudadano esté al centro” de las decisiones y que por tanto no se les requiera continuamente proveer los mismos datos y que los mismos se guarden de manera segura de modo que estos nunca duden que ellos mismos son los propietarios de sus datos. La confianza en esa gestión de los datos va a ser crítica para la gestión de gobierno, para lo cual habrá que pensar en soluciones de CN con autenticación de dos vías, encriptación y uso de blockchain para que estos aprueben el uso o re-uso de sus datos. En el futuro, también se espera que haya una proliferación de sistemas SaaS predictivos de las demandas ciudadanas y del humor social, que se apoyen en soluciones de inteligencia artificial y en el machine learning, por ejemplo, para predecir y proyectar el nivel de deuda impositiva o predecir malestar social respecto algún servicio.

Atentos a esa prospección, se considera que los aspectos claves para trabajar en las agendas públicas se organizan en cuatro pilares.



RECTORÍA Y COORDINACIÓN

Resulta crítico la existencia de entes empoderados a nivel nacional y subnacional que ejerzan un liderazgo y de alguna manera sea el evangelizador de las políticas, buenas prácticas y se imponga transversalmente por sobre organismos pares, haciendo frente a la resistencia cultural al cambio, y que defina estándares que permitan lograr escalabilidad. El rol de la comunicación y “bajada” de los principios rectores de estas agencias será fundamental. Por esto, es importante que dichos organismos posean mediciones de logro o avance en la ejecución de proyectos de CN mediante la utilización de indicadores de performance sumariados en tableros de control, que faciliten la gestión, toma de decisiones y la inspección y supervisión por parte de otras agencias y el público en general. En efecto, las estrategias digitales de transformación del Estado requieren liderazgo, comunicación, roles definidos, y escrutinio

En un Estado moderno, donde haya toda una gama de servicios SaaS, la gestión de los datos tiene que ser considerada como el “activo principal”. Es por ello que la seguridad será el aspecto fundamental para lograr mantener la confianza de los ciudadanos. Es así como el foco debe estar puesto en la prevención de riesgos y la protección de los datos que permita asegurar la continuidad operativa de los servicios en todo momento. El monitoreo de las actividades “maliciosas” y la contracción a la mejora de los sistemas de gobernanza y ciberseguridad debe ser continuo. Cuando haya contrataciones privadas o asociaciones público-privadas para la provisión de servicios, deben fijarse protocolos de trabajo e intercambio de datos interno/externo, con uso de terminales encriptados y sistemas modernos de identidad, acreditación y manejo de accesos. Si bien aquí se observan avances en los países estudiados, fijando estándares y nuevas regulaciones de protecciones de datos y agencias específicas ad hoc, hace

con transparencia. Hasta el momento, la información disponible de los proyectos ejecutados en los países es de variada índole y dispar, lo que no hace posible establecer indicadores, benchmarks de logro, y suele estar sujeta a las políticas de difusión o manejo web del gobierno. Es así que se requiere tener un compromiso más estricto con los objetivos de las agendas, los planes y metas trazados para que sean de cumplimiento e impacto efectivo. Estas buenas prácticas van a permitir incluso hacer una presupuestación, dimensionamiento y financiamiento de los proyectos más preciso. Se observa, también, que muchas veces la capacidad de imponer estándares desde el Ejecutivo Nacional es limitada a nivel subnacional, algo que se exagera aún más en los países federales como Brasil o Argentina.

SEGURIDAD



falta más camino por recorrer en lo que hace a su capacidad transversal de imponer políticas. Es por esto que resulta fundamental mejorar la difusión de las buenas prácticas y asegurar su cumplimiento en todos los ámbitos. Dentro del estado, por ejemplo, no es totalmente frecuente la disponibilidad de los acuerdos de Términos y Condiciones de Seguridad en las contrataciones con terceros; en ocasiones, la excusa de la seguridad se erige como una barrera a la adopción de CN. Finalmente, en materia de ciberseguridad, todo parece ser muy incipiente y preliminar, y seguramente habrá mucho más que hacer en término de “prueba y error” hasta encontrar protocolos y arreglos institucionales que sean funcionalmente eficientes. Lo desarrollado por los países estudiados ha sido principalmente mediante la cooperación inter e intra-gubernamental. Es claro entonces que las estrategias nacionales de ciberseguridad requerirán muy probablemente en el futuro agencias específicas ad hoc.

La brecha de capacidades es hoy, quizá, la barrera más significativa que enfrentan los países en tanto transitan la llamada “4ta Revolución Industrial”; los Estados son los articuladores claves para mediar entre las necesidades de transformación digital y las capacidades de sus funcionarios para una migración de servicios a la nube. Por esto, resulta clave que, dentro de las Agendas Digitales, el desarrollo de capacidades ocupe un rol central; las agencias líderes deben determinar los roles que se requieren actualmente y en el futuro. Deben desarrollarse estándares de capacitación, organizar distintos programas que alcancen transversalmente al estado y las agencias subnacionales, con un sistema de acreditaciones que permita categorizar funcionarios y personal de TI en la implementación, mantenimiento y toma de decisiones. Dadas las limitaciones

CONTRATACIÓN

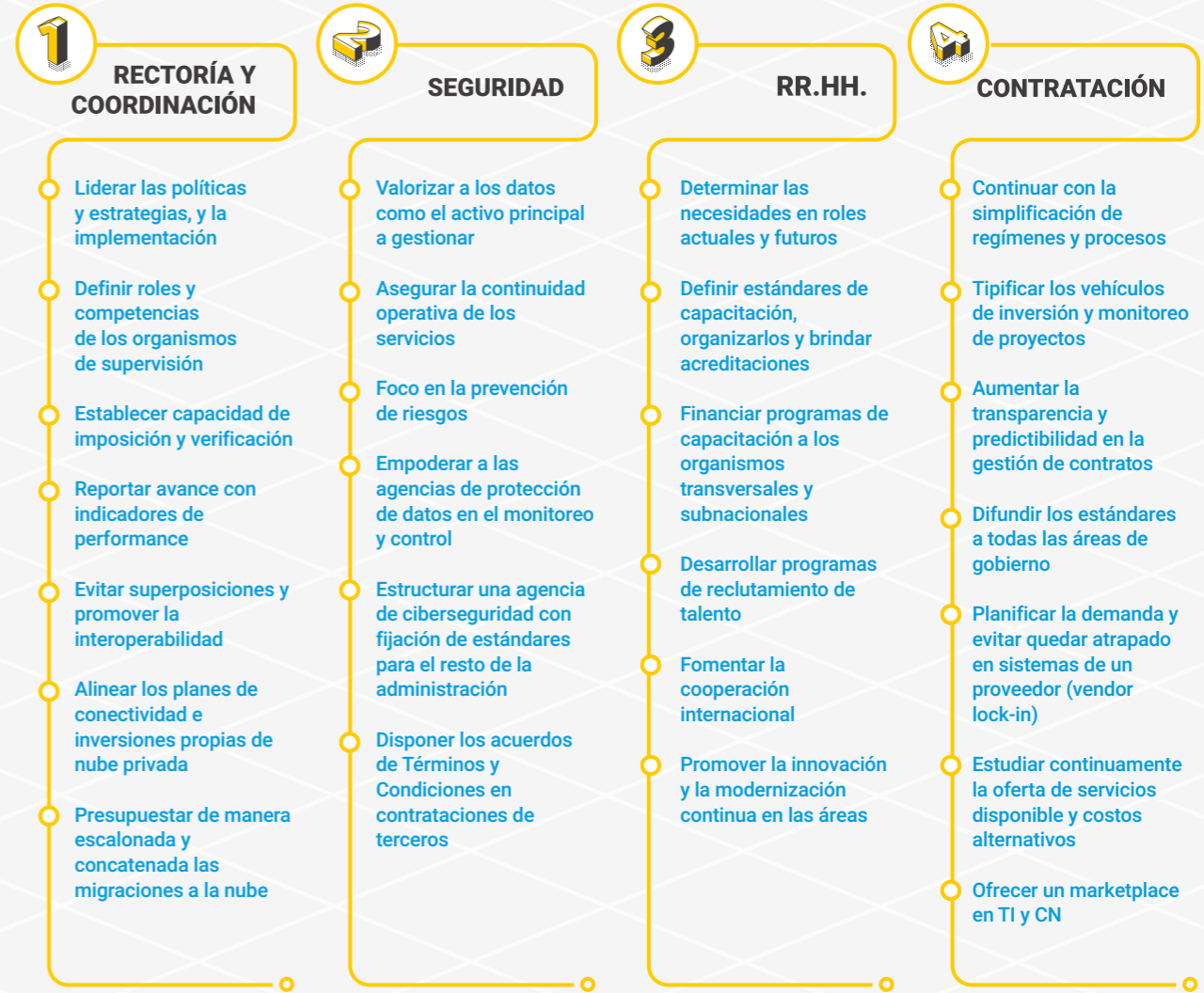
Los oferentes de soluciones de CN para el sector público han sido consistentes en señalar que hace falta trabajar mucho más en la simplificación de regímenes y procesos a los modelos de contratación pública para eliminar ambigüedades y reducir la incertidumbre que a veces los aqueja. Por un lado, debe haber flexibilidad para poder encontrar el modelo de nube que cada agencia necesita, por otro, es necesario que las contrataciones puedan ser escalables a fin de poder hacer negociaciones conjuntas y promover soluciones colaborativas. Un claro ejemplo de esto es el Digital Marketplace del Reino Unido⁷⁹ donde hay un punto común de todo el gobierno donde se encuentran los compradores y oferentes de servicios de CN y conexos, se guía y se sortean las instancias de contratación e incluso se provee datos e investigación. Los países estu-

tradicionales para la asignación presupuestaria en este campo, será crítico entonces estimular la cooperación internacional. Adicional a la formación de sus funcionarios, y más específicamente en el caso de SaaS, los estados deberán también promocionar la capacitación de perfiles para la creciente demanda que verán las empresas proveedoras de servicios de CN. Finalmente, el desarrollo futuro de servicios en la nube en el estado dependerá de que exista un enfoque a promover la innovación y la modernización continua en las áreas para incorporar nuevas tecnologías apoyadas en el big data, el uso de inteligencia artificial que estimulen desarrollos propios de cada uno de los países en vez de que estos compren soluciones de tipo “llave en mano”.

diados necesitan una mejor y más clara tipificación de los vehículos de inversión y un monitoreo centralizado de los proyectos en ejecución. Para esto es necesario trabajar en difusión de los estándares a todas las áreas de gobierno con el foco de que se construya una memoria institucional que permita capitalizar en lo aprendido y por ejemplo evitar quedar atrapado en sistemas de un solo proveedor (vendor lock-in). En paralelo, también resulta crítico aumentar la transparencia y predictibilidad en la gestión de contratos. Finalmente, es fundamental que las agencias líderes de la transformación a la nube realicen una planeación de la demanda del gobierno en tanto se acerque a la obsolescencia o momentos de reemplazo de equipamiento on-premises.



Ilustración 22. Pilares de trabajo en las agendas futuras de los países.



MÁS ALLÁ DEL “CLOUD FIRST”: HACIA UN ENFOQUE DE CONVIVENCIA INTELIGENTE DE SOLUCIONES (“CLOUD SMART”)

Del análisis de los casos y sus barreras surge que uno de los desafíos principales para los distintos organismos es pasar a una concepción de uso y contratación de CN como un ecosistema o plataforma digital de soluciones del Estado⁸⁰.

Esto permitirá que progresivamente los gobiernos vayan introduciendo el análisis de datos y la inteligencia en sus procesos como una prioridad estratégica para crecer en brindar mejores servicios a sus ciudadanos.

La tendencia más reciente de los países líderes en el uso de la nube parece ir más hacia los enfoques híbridos, con ambientes multi-cloud heterogéneos, distribuidos y federados, estos pueden ser efectivos para manejar las distintas cargas de trabajo. Es importante que las agencias de gobierno diseñen su estrategia de CN como una caja de herramientas que ofrece distintas opciones y capacidades para ser más efectivo en el servicio público y en la atención al ciudadano; no hay “un saco que le quepa a todos” para la transformación del gobierno.

Cada agencia gubernamental debería estar equipada para evaluar sus opciones basada en su misión, necesidades de servicios, requerimientos técnicos y sus limitaciones regulatorias. Las decisiones respecto de modelos de cómputo y tecnología deben balancearse considerando los costos, por un lado, y el riesgo de ciberataques, por otro.

Como referencia, la nueva estrategia “Cloud Smart” del gobierno federal de Estados Unidos lanzada en 2019⁸¹, actualiza la estrategia de la década anterior con un enfoque que va más allá del tradicional “cloud first” que está presente, y aún se aplica incipientemente, en los países estudiados. Esta “estrategia inteligente” se funda en tres pilares clave para hacer más eficientes las inversiones, mejorar la seguridad y para brindar servicios de calidad a los ciudadanos: seguridad, contratación y recursos humanos.

Aquí, se sugiere que las medidas de adopción de CN no deben ser tomadas en función de quién tiene la propiedad de los recursos, o en la estimación de ahorros, sino que las agencias deben evaluar sus necesidades y buscar marcos de trabajo y soluciones, de la nube u otros, que mejor les permitan cumplir con su misión. Este enfoque podría caracterizarse como “teleológico” por cuanto privilegia el foco en la finalidad⁸². En este caso, la función de la agencia rectora nacional debería ser la de asegurar la convivencia del ecosistema de soluciones de la nube contratadas por todo el estado buscando promover la estandarización, interoperabilidad y la colaboración de recursos contratados.

SEGURIDAD CONTRATACIÓN RR.HH.

TRES PILARES CLAVES DE LA
ESTRATEGIA CLOUD SMART

Actuar inteligentemente también permitirá evitar los riesgos descritos en este documento al momento de definir una hoja de ruta, agregando análisis de cómo mejorar la capacidad de contratar y administrar contratos de TI y de CN; permitiendo la portabilidad de datos y aplicaciones (evitando el “vendor lock-in”); asegurando estándares comunes de clasificación de datos y ciberseguridad; con protocolos de recuperación de datos; análisis e investigaciones de datos en otras jurisdicciones; gestión del cambio, y fundamentalmente, que existan los recursos presupuestarios suficientes para toda la duración del proyecto y su mantenimiento operativo.



En el caso de los **países del Cono Sur** analizados en este informe, por la insipiente por parte de los entes de gobierno en el uso de CN, se entiende que la lógica evolutiva es:

- 1 CLOUD FIRST
- 2 CLOUD SMART



LA IMPORTANCIA DE LA COOPERACIÓN INTERNACIONAL

La CN se está desarrollando en todo el mundo y será fundamental para que los países puedan desarrollarse en la “nueva economía de datos”.

Sin embargo, como se señaló anteriormente, la provisión de servicios eficientes por parte del estado dependerá de la interoperabilidad y las economías de escala que éste pueda generar en sus proyectos. De este modo, se abaratan costos y se podrá construir sobre el camino recorrido, de aprendizaje de otros, cada vez que una agencia particular decida migrar a la nube o comenzar una nueva implementación. La institucionalización de las prácticas y metodologías de uso y contratación son fundamentales para poder nutrir la oferta de servicios, ya que les otorga predictibilidad a los proveedores.

En esta línea, la cooperación y el diálogo internacional también serán un elemento crítico para el intercambio de buenas prácticas y el desarrollo de proyectos de investigación conjuntos. Por ejemplo, Brasil es un socio clave para la Unión Europea, al igual que Japón, Estados Unidos y Corea del Sur, para llevar adelante su plan del Mercado Digital Regional y la Estrategia de CN de 2012⁸³. El foco es tratar de tener un nivel mínimo de interoperabilidad y portabilidad que deberían resultar en promover más competencia en el mercado de servicios CN.

El plan europeo, conocido como Horizonte 2020, destaca la importancia de la colaboración para minimizar las barreras a la adopción de estos servicios, principalmente la complejidad del marco legal (derechos de usuarios, localización y protección de datos y privacidad), la seguridad y la falta de estándares comunes. De la cooperación UE-Brasil se espera poder avanzar en aplicaciones de big data centralizadas en la nube y en la coordinación de políticas públicas.

La cooperación internacional es también un prerrequisito para el financiamiento internacional de proyectos por cuanto conlleva el trabajo mediante estándares reconocidos pasibles a ser calificados y certificados. Los modelos de “Financiación Combinada”, basados en la cooperación con organismos multilaterales, pueden ayudar a movilizar el capital público en sectores de innovación en la gestión gubernamental y a los países a pegar saltos cualitativos en su transformación digital.

Para esto, los países deben contar con una lista jerarquizada de proyectos de transformación digital del estado alineados con sus Agendas Digitales, planes de Desarrollo Nacional y los Objetivos de Desarrollo Sostenible.

Las agencias de gobierno deben realizar evaluaciones regulares de la experiencia de sus usuarios y sus necesidades para asegurarse que primen la eficiencia, la accesibilidad y la privacidad. Es fundamental tener diagnósticos continuos para decidir dónde es crítico invertir para acompañar el crecimiento de la demanda y prevenir cuellos de botella o simplemente para mejorar la performance, reducir fallos a larga escala y que nunca se comprometan los datos de los ciudadanos. La modernización del estado en esta materia, cuidando los recursos de todos, implicará cada vez más también apoyarse en soluciones de diagnóstico automatizadas basadas en inteligencia artificial y en machine learning.

Por ejemplo, la Iniciativa de la Nube Europea (INE)⁸⁴ parte de su estrategia del Mercado Digital Regional, tiene algunos elementos que pueden ser interesantes para los países estudiados, en particular a lo que hace a la visión de futuro a insertarse en las agendas digitales.

El objetivo de los europeos es el de crear una economía basada en el uso de datos y de conocimiento que fortalezca competitivamente a los países, posicionándolos en la innovación.

La idea es que estos sectores de la economía puedan maximizar los beneficios del Big Data mediante el movimiento, la compartición y la reutilización de datos entre los mercados y fronteras y entre las instituciones y disciplinas de investigación⁸⁵.

La disponibilidad de datos dista de lo necesario para que surjan nuevas empresas o servicios o se realicen investigaciones útiles, que se nutran con información compartida en tiempo real de sitios públicos; claramente puede ser un vector de fomento de la competitividad para las empresas y para las decisiones del sector público. El avance de los usos e implementaciones de inteligencia artificial, tanto en el sector público como privado, va a depender mucho de la disponibilidad de datos, conectividad y de capacidad de cómputo. La CN será un facilitador fundamental para que esto suceda.

INE busca proveer a la comunidad científica, a la industria y a los hacedores de políticas públicas con:

- 1** UNA INFRAESTRUCTURA DE CLASE MUNDIAL PARA GUARDAR Y MANEJAR DATOS,
- 2** CONECTIVIDAD DE ALTA VELOCIDAD PARA EL FLUJO DE DATOS
- 3** CADA VEZ MÁS PODEROSA CAPACIDAD DE CÓMPUTO UTILIZANDO COMPUTADORAS DE ALTO RENDIMIENTO PARA PROCESAR LOS DATOS.



EJES DE TRABAJO Y COOPERACIÓN EN EL MEDIANO Y LARGO PLAZO

Con excepción de Uruguay, la adopción de servicios en la nube por parte de las administraciones públicas de los países del Cono Sur se encuentra en una fase inicial.

Su consolidación como un servicio provisto recurrentemente requiere de un proceso de transición y transformación al interno del estado que puede extenderse en el tiempo. Como tal, existen numerosos desafíos y áreas de trabajo donde la cooperación y el apoyo multilateral pudiera tener un rol de soporte y guía a las iniciativas en curso, como así también en el establecimiento de programas específicos de apoyo con una mirada más orientada al mediano y largo plazo. A continuación se destacan dos ejes y subáreas a trabajar en los países analizados: el institucional y organizacional, y el relativo a financiamiento.

Si bien aparecen señalados los países y áreas prioritarias de actuación, prácticamente todas las áreas listadas tienen acciones todavía a complementarse en todos los países del Cono Sur.

INSTITUCIONAL Y ORGANIZACIONAL

Políticas de CN, marco normativo, protección de datos personales y ciberseguridad



Lineamientos y Guía de CN ("cloud first" o "cloud smart")



Normar los vehículos de contratación pública y revisión de procesos existentes



Divulgación y desarrollo de capacidades sobre alcance de normas, mecanismos de contratación y modelos de adopción



Centralización de la coordinación y promoción de CN



FINANCIAMIENTO

Recursos de capital para inversión en modelos de despliegue híbridos



Recursos de capital para apoyar la conectividad



Capacitación técnica a recursos TI y compras



Reestructuración organizacional: modificación de perfiles, cambio de organigrama modelos de adopción





Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.



APOYO INSTITUCIONAL Y ORGANIZACIONAL

Desde el punto de vista de la gestión organizacional, un aspecto imperioso para zanjar barreras al crecimiento es mejorar la comunicación y divulgación del alcance efectivo de normas de protección de datos, estándares y mecanismos de contratación, ello con el fin de desarrollar consensos y conocimientos acerca de la legislación imperante y de las funcionalidades de los servicios de CN (para facilitar así su incorporación al interior del sector público). Una guía práctica de implementación con pasos delimitados y con impacto comunicacional para facilitar su comprensión debería ser una herramienta a considerarse para alcanzar este objetivo. En Argentina, por ejemplo, se requieren delimitar las acepciones alternativas al marco normativo, para eliminar incertidumbre de qué se puede o no hacer. En Brasil es necesario trabajar en el mismo aspecto pero más enfocado en entender los alcances, riesgos y cuidados relativos a la ciberseguridad. En Chile, para difundir el alcance efectivo de normas de protección de datos, modelos de contratación y mecanismos de adopción; y en Paraguay para establecer un consenso en los actores del sector público y privado que favorezca el cambio de paradigma que implica la implementación de estos servicios.

La necesidad de crear vehículos de contratación pública específicos y revisión de procesos de contratación que favorezcan la adopción de los servicios en la nube es otro eje crítico. Aquí aplican países como Brasil, donde es necesario implementar los mecanismos de contratación empleados recientemente en la esfera federal a nivel estatal y municipal, para favorecer su adopción en otras esferas de gobierno; en Chile será necesario apoyar la creación de vehículos de contratación específicos dotados de mayor agilidad para que permitan tratar la contratación de servicios en la nube como utilities, incorporándolos en la asignación presupuestaria de las agencias; y finalmente en Uruguay donde se requiere apoyar los modelos de contratación que se encuentren alineados con el formato de pago-por-uso que son la esencia de este tipo de servicios.

Apuntalar la centralización de la coordinación y promoción de CN para favorecer la armonización a nivel federal e interregional resulta crítico. En este punto se destacan Argentina, cuyo principal desafío es diseñar un marco guía de trabajo más armonizado y coordinado entre la administración federal, las provincias y los municipios; y Brasil, que requiere de la elaboración de un programa de gobierno específico que coordine y consolide las iniciativas reguladoras de las agencias actualmente dispersas en las esferas federal, estatal y municipales.

Finalmente, consideramos de utilidad el acompañamiento para la definición de normativas asociadas a la estructuración de estándares técnicos, protección de datos personales y su clasificación, ciberseguridad. Además sería

importante considerar la posibilidad de promover una renovación de las leyes de contratación para TI y, específicamente, para CN con el fin de reducir y adecuar los tiempos de contratación de proveedores privados y de evitar procesos de licitación desiertos. Asimismo, sería importante contar con un manifiesto de CN (“cloud first” o “cloud smart”) para acelerar la adopción de estas soluciones. Iniciativa con notable impacto en Paraguay, con mucho campo para el desarrollo normativo e institucional.



FINANCIAMIENTO

En lo que respecta a financiamiento, se observa mayor homogeneidad respecto de los desafíos comunes y las iniciativas que pueden ser acompañadas y fortalecidas.

Las necesidades de recursos de capital para inversión en modelos de despliegue híbridos pareciera ser un elemento primordial al cual apoyar. En este punto, Argentina podría dar un impulso de implementación a nivel provincial y municipal apoyándose en una estrategia más clara con su empresa estatal ARSAT. En Chile podrían potenciarse las redes públicas con las soluciones de proveedores internacionales que han desplegado localmente promoviendo soluciones de complementariedad. En Paraguay se podrían ampliar la oferta los servicios de la Nube-PY mediante la incorporación de soluciones públicas reconocidas a nivel global.

La capilaridad de los servicios en la nube se encuentra asociada a las condiciones de conectividad que presenta cada país. En la región, la conectividad presenta cierto déficit que incrementa la brecha digital, por ello se convierte un elemento fundamental que debe contemplarse al momento de apoyar iniciativas de este aspecto. En Argentina, podría acompañarse la amplificación de la Red Federal de Fibra Óptica a nivel municipal y rural; en Chile continuar apoyando las inversiones en cables submarinos y el tendido de fibra regionalmente; y en Paraguay apoyar los esfuerzos por mejorar la conectividad tanto internacional como a nivel municipal.

Uno de los elementos que han destacado los funcionarios en los países relevados ha sido la necesidad de potenciar la capacitación técnica de sus recursos humanos tanto del sector TI como en el área de compras y contrataciones. Este esfuerzo podría acompañarse con la difusión de los beneficios y los modelos de la implementación de los servicios en la nube, principalmente para aquellos profesionales formados con los estándares tecnológicos tradicionales, destacando sus características en términos de ciberseguridad y protección de datos y en términos de sus beneficios económicos, flexibilidad y escalabilidad. En esta órbita se destacan iniciativas a lo largo de los cinco países analizados.

Por último, Argentina y Brasil han destacado la necesidad de acompañar las políticas de adopción con una reestructuración organizacional que implique modificación de perfiles y cambios en el organigrama de los organismos a fin de que haya una visión más colaborativa y compartida de los recursos, evitar duplicidades y ahorrar recursos.





Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

NOTAS

Nota 1.

Contratados de empresas privadas o proveídos directamente por entidades del sector público. **Volver**

Nota 2.

Si bien existen otros modelos de servicios como DBaaS (base de datos como servicio), DaaS (escritorio como servicio), CaaS (contenedores como servicio), FaaS (funciones como servicio), SECaaS (seguridad como servicio), STaaS (almacenamiento como servicio), el presente estudio hace foco en los tres modelos más comúnmente utilizados (IaaS, PaaS y SaaS). **Volver**

Nota 3.

El NIST define un cuarto modelo de despliegue denominado “Comunitario” en el que varias organizaciones comparten recursos, el mismo es contemplado en el presente estudio ya que su consideración general es de menor uso y ya que podría ser contemplado como parte de los tres modelos de despliegue principales. **Volver**

Nota 4.

Este riesgo podría exacerbarse en la medida que, en ocasiones, puede desconocerse la localización efectiva de los datos. Se pueden establecer contratos con adenda especificando taxativamente los países donde los datos deben alojarse. Se recomienda, por parte del ente contratante, un conocimiento del entorno jurídico de las jurisdicciones en que se encuentren sus datos, prefiriendo jurisdicciones con legislación adecuada (o mediante adendas que repliquen dichas condiciones) **Volver**

Nota 5.

Ver [Ley de Fomento a la Computación en la Nube y la Protección de sus Usuarios](#). **Volver**

Nota 6.

Ver [Plan de Desarrollo de Computación en la Nube 2016-2021](#). **Volver**

Nota 7.

Ver [Estrategia para la Transformación del Gobierno de 2017-2020](#). **Volver**

Nota 8.

Ver [Ley de Protección de Información Personal \(PIPA\)](#). **Volver**

Nota 9.

Ver [Ley de Promoción de uso de redes de IT y Protección de información](#). **Volver**

Nota 10.

Ver [GDPR. Ley de Protección de Datos](#). **Volver**

Nota 11.

Ver plataforma web de la [Jefatura de Gabinete de Reino Unido](#). **Volver**

Nota 12.

Ver Gov.uk Digital [Marketplace](#). **Volver**

Nota 13.

Ver N° 25.326, [Disposición 60-E/2016](#). **Volver**

Nota 14.

Especificados en el [decálogo TIC](#) instrumentado por la ONTI. **Volver**

Nota 15.

La estimación del tamaño de mercado de computación en la nube reviste la dificultad de la indefinición de su base por parte de los distintos informes publicados y los modelos de servicio de CN (IaaS, PaaS y SaaS). Dicho rango de valores se basa en el supuesto que Latino América representa un 2% del mercado mundial de CN y Argentina el 8% de este último. Se tomaron informes de 451 Reaserch, Frost & Sullivan, Gartner para arribar a dichas estimaciones. **Volver**

Nota 16.

Según informes de 451 Research, Allied Market Research, Frost & Sullivan, Gartner. **Volver**

Nota 17.

Ver [Ley 25.326](#) sobre protección de datos personales. **Volver**

Nota 18.

Ver [Decreto 1558/2001](#) sobre la protección de los datos personales. **Volver**

Nota 19.

Ver [proyecto de ley de protección de datos personales](#). **Volver**

Nota 20.

Ver [Decreto 577/2017](#) sobre ciberseguridad. **Volver**

Nota 21.

Ver [Resolución 829/2019](#) sobre ciberseguridad. **Volver**

Nota 22.

Ver [comunicación 6354/2017](#) del BCRA. **Volver**

Nota 23.

Ver [comunicación 6375/2017](#) del BCRA. **Volver**

Nota 24.

Ver [Decreto 561/2016 – Sistema de Gestión Documental Electrónica \(GDE\)](#). **Volver**

Nota 25.

Si bien representa una importante ventaja el hecho que, en un país federal, se adopte un mismo sistema en distintas provincias, en la actual implementación todavía deben incorporarse sinergias de relevancia, entre ellas la compartición de un mismo registro de proveedores, hoy diferente para cada provincia. **Volver**

Nota 26.

Actualmente con más de 1.200 páginas de municipios. **Volver**

Nota 27.

En el caso de los servicios SaaS, la ausencia o escasez de recursos no constituye una barrera o desventaja ya que en este modelo de servicio la necesidad de capital humano queda del lado del proveedor del servicio SaaS. **Volver**





Nota 28.

Ver [Lei nº 12.965](#), de 23 abril de 2014 - Marco Civil da Internet. **Ver**

Nota 29.

Ver [Lei 13709](#). Lei Geral de Proteção de Dados Pessoais. **Ver**

Nota 30.

Ver [Decreto 9.637](#) sobre ciberseguridad. **Ver**

Nota 31.

Ver [Lei 8.666](#) sobre licitaciones y contratos administrativos. **Ver**

Nota 32.

Ver [Decreto 10.024](#) sobre licitaciones y contratos administrativos. **Ver**

Nota 33.

A inicios de 2020, se encuentra en curso una migración por parte del gobierno al uso de ofimática. **Ver**

Nota 34.

En el caso de los servicios SaaS, la ausencia o escasez de recursos no constituye una barrera o desventaja ya que en este modelo de servicio la necesidad de capital humano queda del lado del proveedor del servicio SaaS. **Ver**

Nota 35.

Según informes de 451 Research, Allied Market Research, Frost & Sullivan, Gartner. **Ver**

Nota 36.

Ver [Ley 19.628](#) sobre protección de la vida privada. **Ver**

Nota 37.

Ver [Ley 19.223](#) sobre tipificación de figuras penales relativas a la informática. **Ver**

Nota 38.

Ver [PNCS](#). **Ver**

Nota 39.

Ver [Ley 19.799](#) sobre firma electrónica y servicios de certificación. **Ver**

Nota 40.

Ver [Ley 19.880](#) sobre los actos administrativos que rigen los actos de los órganos de la administración del estado. **Ver**

Nota 41.

Ver [Resolución exenta N° 619-B ChileCompra](#). **Ver**

Nota 42.

Ver [Ley 21.130](#) sobre la modernización de la legislación bancaria. **Ver**

Nota 43.

Ver [Circular 3.629 capítulo 20-7](#). **Ver**

Nota 44.

Ver Inversión centro de cómputo Google en Chile: [“Google sees Chile as favorable for investment”](#) y [“Google is proud to call Chile home to one of our data centers”](#). **Ver**

Nota 45.

Ver [Inversión centro de cómputo Huawei en Chile](#). **Ver**

Nota 46.

Ver [Inversión centro de cómputo Oracle en Chile](#). **Ver**

Nota 47.

En el caso de los servicios SaaS, la ausencia o escasez de recursos no constituye una barrera o desventaja ya que en este modelo de servicio la necesidad de capital humano queda del lado del proveedor del servicio SaaS. **Ver**

Nota 48.

Ver [Ley 6.207 de 2019](#), creación del MITIC **Ver**

Nota 49.

Ver [Portal de Contrataciones Públicas de la República del Paraguay](#). **Ver**

Nota 50.

Ver Portal [Nube-PY](#). **Ver**

Nota 51.

Ver [Microsoft apoyará a Paraguay en la implementación de la Agenda Digital](#). **Ver**

Nota 52.

Ley N° 6.207 - Creación del MITIC. **Ver**

Nota 53.

Ver [Decreto Presidencial N° 2.274](#), que reglamenta la Ley 6.207 de 2019. **Ver**

Nota 54.

Ley N° 1682/2001 de información de carácter privado. **Ver**

Nota 55.

Ley N° 1969, de 3 de septiembre de 2002. **Ver**

Nota 56.

Ver [Proyecto De Ley “De Protección De Datos Personales”](#). **Ver**

Nota 57.

Ver Decreto Presidencial 2145/19 **Ver**

Nota 58.

Ver [Ley 125/91 y sus modificatorias \(Ley 2.421 de 2004 y Ley 5.061 de 2013\)](#). **Ver**

Nota 59.

Ver [Resolución 281/2004 del Banco Central de Paraguay](#). **Ver**

Nota 60.

Ver Manual de Control Interno Informático para las entidades financieras supervisadas por la Superintendencia de Bancos. **Ver**





Computación en la Nube.

Contribución al desarrollo de ecosistemas digitales en países del Cono Sur.

Nota 61. ○

En el caso de los servicios SaaS, la ausencia o escasez de recursos no constituye una barrera o desventaja ya que en este modelo de servicio la necesidad de capital humano queda del lado del proveedor del servicio SaaS. **Volver**

Nota 62. ○

Ver [D9 Leading Digital Governments](#). **Volver**

Nota 63. ○

Ver nota de Presidencia del 31 de mayo de 2019: [Uruguay alcanzará el 100 % de cobertura en tecnología de fibra óptica](#). **Volver**

Nota 64. ○

Ver [Ley 19.179. Regulación del formato para el procesamiento y almacenamiento de información digital por parte de determinados organismos y empresas](#). **Volver**

Nota 65. ○

Ver [Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data](#). **Volver**

Nota 66. ○

Ver [Decreto 92/014. Marco Normativo de Ciberseguridad](#). **Volver**

Nota 67. ○

Ver [Ley N 18.381. Acceso a la Información Pública](#). **Volver**

Nota 68. ○

Ver [Ley 19.179. Regulación del formato para el procesamiento y almacenamiento de información digital por parte de determinados organismos y empresas](#). **Volver**

Nota 69. ○

Ver [Texto Ordenado de Contabilidad y Administración Financiera \(TOCAF\)](#). **Volver**

Nota 70. ○

Ver nota del Diario El País de octubre de 2019: ["Google instalará un centro de datos en el Parque de las Ciencias en Canelones"](#). **Volver**

Nota 71. ○

En el caso de los servicios SaaS, la ausencia o escasez de recursos no constituye una barrera o desventaja ya que en este modelo de servicio la necesidad de capital humano queda del lado del proveedor del servicio SaaS. **Volver**

Nota 72. ○

CRM: Customer Relationship Management. **Volver**

Nota 73. ○

La conectividad de la APN en Brasil y la mayoría de los estados es buena, la barrera de conectividad se da principalmente a nivel de municipios. **Volver**

Nota 74. ○

Ver [Agenda Uruguay Digital 2020](#) y sus actualizaciones. **Volver**

Nota 75. ○

Ver [Agenda Digital Argentina](#). **Volver**

Nota 76. ○

Ver [Gobierno Digital en Chile](#). **Volver**

Nota 77. ○

Esta Secretaria Ejecutiva está integrada por los subsecretarios de Hacienda, General de la Presidencia, quien la presidirá, Economía y Empresas de Menor Tamaño, y de Telecomunicaciones. **Volver**

Nota 78. ○

Ver [Proyecto de Agenda Digital paraguay](#) y [Programa de Apoyo del BID](#). **Volver**

Nota 79. ○

Véase [GOV.UK Digital Marketplace](#) donde existen guías, formatos y modelos de contratos, todo tipo de proveedores, investigaciones. **Volver**

Nota 80. ○

Véase concepto desarrollado por Gustavo Giorgetti: [Estonia: cómo el modelo de la sociedad más digital del mundo se aplica en Neuquén, Red/Acción, 18 de febrero de 2019](#). **Volver**

Nota 81. ○

Ver ["2019 Federal Cloud Computing Strategy – Cloud Smart"](#). **Volver**

Nota 82. ○

La teleología (discurso, tratado o ciencia según la Real Academia Española) es la rama de la metafísica que se refiere al estudio de los fines o propósitos de algún objeto o algún ser, o bien literalmente, a la doctrina filosófica de las causas finales. Usos más recientes lo definen simplemente como la atribución de una finalidad, u objetivo, a procesos concretos. **Volver**

Nota 83. ○

Ver [European Commission, Digital Single Market](#). **Volver**

Nota 84. ○

Ver [European Cloud Initiative](#) para mayor detalle de sus componentes **Volver**

Nota 85. ○

La iniciativa europea incluye la [European Open Science Cloud](#) (EOSC) que se va a apoyar en la [European Data Infrastructure](#) (EDI) y en el uso de computación cuántica y de constituir un ecosistema de computación de alta performance [High Performance Computing](#) (HPC). Para dar una idea de las magnitudes de inversión que una estrategia digital de este tipo conlleva: las inversiones públicas y privadas necesarias para implementar la Iniciativa de la Nube Europea se las estiman en €6.7 mil millones, de acuerdo con la Comisión Europea. De éstos, se estima que alrededor de €2 mil millones del financiamiento del plan Horizonte 2020 van a estar asignados a la INE, y que los restantes €4.7 mil millones van a ser necesarios ser desembolsados tanto por el sector público como el privado a lo largo de al menos 5 años. **Volver**



