
**Universidad de San Andrés**

**Escuela de Negocios**

**Maestría en Gestión de Servicios Tecnológicos y Telecomunicaciones**

# *Cumplimiento, seguridad y clasificación de la información para Cloud Computing y Cloud Storage*

**Autor: Lopez Villafañe, Rodrigo**

**Legajo : 34513032**

**Director/Mentor de Tesis: Prince, Alejandro**

**2018**


Universidad de
SanAndrés

MAESTRÍA EN GESTIÓN DE SERVICIOS TECNOLÓGICOS Y TELECOMUNICACIONES

# Cumplimiento, Seguridad y Clasificación de la información para Cloud Computing y Cloud Storage

**Alumno**: Rodrigo López Villafañe

**Director de Tesis**: Dr. Alejandro Prince

**2018**

**Buenos Aires**

**Agradecimientos**

Muchas gracias a mi tutor y a mis padres, más allá de la ayuda brindada, en la motivación para la realización de esta maestría.

**Resumen**

Identificación de amenazas para la certificación de marcos regulatorios para empresas que utilizan proveedores de nube. A partir de un análisis de los beneficios y casos existentes de empresas que contratan proveedores de Cloud Computing y Cloud Storage, se identificarán los puntos clave para lograr que las empresas clientes puedan cumplir con las regulaciones existentes.

**Palabras Clave: Cloud Computing – Seguridad en la Nube – Compliance – Regulaciones en la nube – Clasificación de la información – Amenazas en la Nube – Cloud Storage.**





**Alumno: Ing. Rodrigo Lopez Villafañe (rodrigolv123@gmail.com)**

# Contenido

## Índice de ilustraciones

**Índice de tablas**

# 1. Introducción

## 1.1 Problema de Investigación.

Hoy en día están en auge el uso de tecnologías y técnicas como Cloud Computing (CC) y Cloud Storage (CS). Permitiendo tanto a pequeñas y medianas empresas, como a grandes empresas la especialización en el almacenamiento y análisis datos (Weinhardt et al., 2009).

Si bien sus beneficios son evidentes, existen muchas amenazas relacionadas a la seguridad de la información. Estas amenazas tanto internas como externas a la empresa, pueden materializarse en riesgos generando pérdidas cuantitativas y cualitativas tanto para el proveedor de Cloud, como para el cliente.

Se debe tener en cuenta el tratamiento y seguridad de la información a lo largo de todo su ciclo de vida durante los procesos de la organización y no solo cuando se encuentra en la empresa cliente. Es necesario tener una clara definición de dichos procesos mediante informes que certifiquen el flujo de la información desde el Proveedor/Cliente hasta el Cliente/Usuario Final.

De acuerdo con el tipo de organización a evaluarse y sus procesos internos, el tratamiento y las prácticas para la seguridad y clasificación de la información deberían ser diferentes.

Los estándares y prácticas existentes solamente hacen referencia a la seguridad de la información y no a su clasificación, cuando se encuentran del lado de proveedor de la nube.

Hoy en día existen muchos criterios y documentos de clasificación de la información de acuerdo al tipo de empresa y país al que pertenezca la información. Pero en muy pocos se

menciona el tratamiento y clasificación de información por empresas terciarizadas y su relación con regulaciones, como en este caso sería un proveedor de Cloud Computing y Cloud Storage.

## 1.2 Objetivos y Alcance

Identificar puntos claves en servicios otorgados por proveedores de Cloud Computing y Cloud Storage para permitir a empresas la clasificación de información, de acuerdo a estándares y buenas prácticas en concordancia con los objetivos, misión, visión y valores de la misma.

## 1.3 Hipótesis

Estándares y buenas prácticas para el tratamiento, clasificación y seguridad de la información a ser utilizados por proveedores de Cloud Computing y Cloud Storage, pueden ser generados teniendo en consideración el tipo de empresa de que se trate, el servicio brindado y el manejo de datos que en consecuencia esta deba gestionar.

## 1.4 Preguntas de Investigación

¿Es posible la definición de puntos claves a cumplir por parte de un proveedor de Cloud Computing o Cliente para el tratamiento de la información de acuerdo con su clasificación y objetivo?

¿La utilización de servicios de Cloud Computing para el cumplimiento de normas y regulaciones globales y nacionales, genera beneficios significativos y tangibles para el usuario cliente?

QUAERERE VERUM
Universidad de
SanAndrés

# 2. Marco Teórico

## 2.1 ¿Qué es Cloud Computing?

### 2.1.1 ¿Qué consideramos Cloud Computing o Cloud Services?

El Cloud Computing consiste en la posibilidad de ofrecer servicios a través de Internet. La computación en la nube es una tecnología nueva que busca tener todos los archivos e información en Internet, sin preocuparse por poseer la capacidad suficiente para almacenar información en nuestro ordenador.

El Cloud Computing explica las nuevas posibilidades de forma de negocio, ofreciendo servicios a través de Internet, conocidos como e-business (negocios por Internet). No solo se trata de una revolución Business to Business, es decir entre empresas, sino también representa una revolución para usuarios finales, que no están conectados con el entorno de IT. Es posible, eliminar la necesidad de cómputo, por ejemplo instalando programa mediante el hosteo en la web y consulta por servicios web de documentos, solamente ante la necesidad puntual de lo que necesita el usuario (Farkas, 2017).

De acuerdo con la prestación que se provee a los usuarios (Software, Plataforma, Infraestructura) existen 3 modelos de servicios:

El primero es Infraestructura como servicio - Infraestructure as a Service (IaaS), que comprende todos los recursos computacionales necesarios para que el cliente pueda ejecutar o implementar el software que desee, en apoyo de sus funciones o necesidades específicas.

El segundo es Plataforma como servicio - Platform as a Service (PaaS) que permite la capacidad para que el cliente desarrolle en la infraestructura brindada aplicaciones (Adquiridas

o a la medida), que le permitan explotar su negocio. Permite más que IaaS, ya que el cliente puede desarrollar. A su vez, Internet como servicio - Internet as a Service (IaaS): Incluye todos los recursos de infraestructura: Instalaciones físicas, equipos de cómputo y de comunicaciones, también proporciona un conjunto de APIs que permiten al usuario la gestión e interacción con la infraestructura.

Y por último Software como servicio - Software as a Service (SaaS): El cliente solo utiliza software que ofrece el proveedor dentro de su infraestructura Cloud. (IaaS + PaaS)(Sepúlveda, Salcedo, & Vargas Gómez, 2011) .

A continuación se muestran ejemplos de los 3 tipos distintos de servicios ofrecidos desde un punto de vista de BtoB (Business to Business), ya que en esta tesis solamente se analizará el impacto de servicios ofrecidos a grandes y medianas empresas.

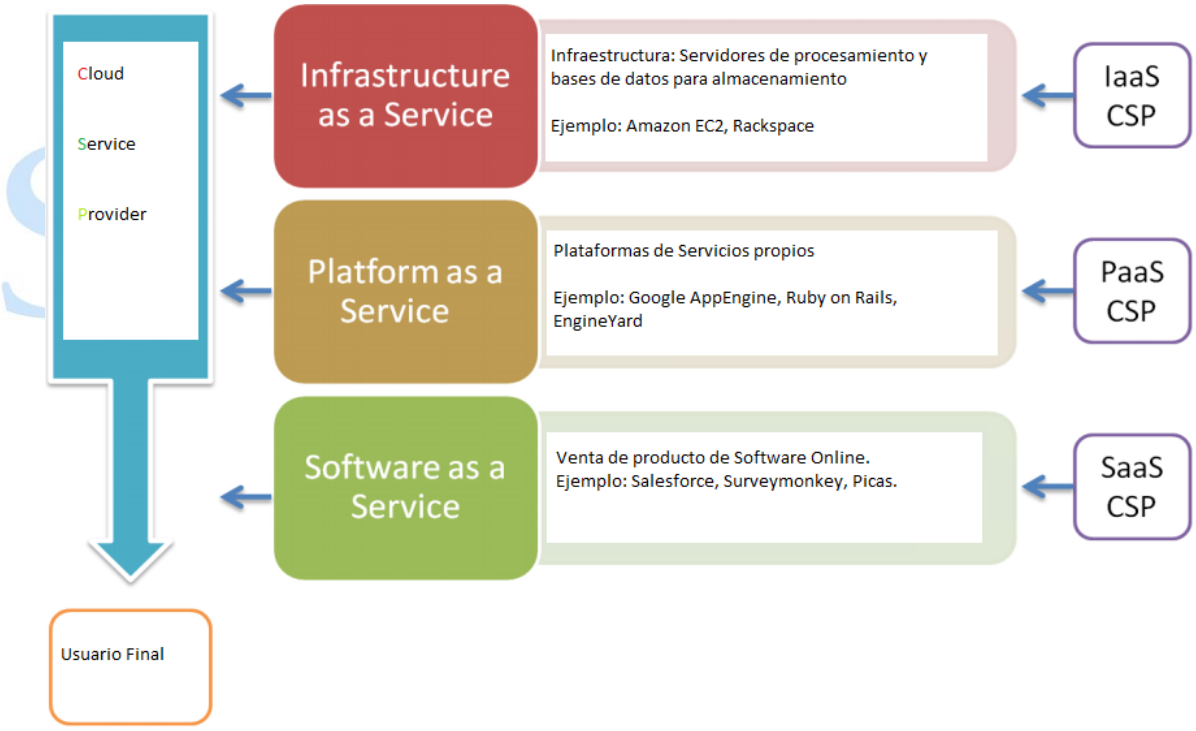

Figura 1: Modelos de Cloud Computing Services. Elaboración Propia en Base a "Manejo del riesgo y seguridad en el consumo de servicios de TI en Cloud Computing". Tesis. 20 de enero 2018.

El software como servicio es una de las modalidades más importantes de la computación en la nube. Consiste en una aplicación de software ofrecida totalmente por Internet, con todas las funcionalidades y para todos los clientes que lo soliciten (Schwartz, 2017).

### 2.1.2 Casos de pérdida derivados de la aplicación del Cloud Computing.

Caso 1:

Fecha: 01/02/2017

Conocimientos previos: AWS S3 es un servicio de almacenamiento que ofrece Amazon mediante Web Services. Los conceptos principales del S3 son los buckets y objects, consultados mediante la API de AWS. Los buckets de AWS S3 permiten guardar el versionado de objetos que se están almacenados por el cliente.

Situación: Debido a la flexibilidad de configuración de seguridad de AWS S3, por parte del cliente tanto en servidores como del lado cliente, hubo confusiones en la configuración de predefinida y exposición de información al público.

Algunas de las compañías afectadas fueron Accenture, Verizon y WWE (World Wrestling Entertainment, Inc.), que tuvieron exposición de información no debido a ataques maliciosos, sino debido a falta esfuerzos de compañías de seguridad en escaneo de

vulnerabilidades. No hay evidencia de que la información se haya copiado o robado, sin embargo es solo cuestión de tiempo, hasta que otros agentes puedan utilizar las mismas técnicas.

Uno de los elementos más atractivos de S3 es su flexibilidad, con múltiples configuraciones y conexiones a herramientas y servicios de AWS. Dicha flexibilidad permite selecciones, que a veces lidera en errores.

Solución: La encriptación es una de las elecciones para políticas de seguridad para usuarios, y aquellos que quieren encriptar todo deben rechazar objetos no encriptados. La nueva encriptación DEFAULT de S3 permite la encriptación de todos los objetos en el bucket incluyendo los nuevos, evitando problemas de configuración por falta de atención de los usuarios.

Más allá de las opciones por default en la configuración de AWS S3, se hará hincapié sobre las opciones que afectan la seguridad de los datos desde el punto de vista del usuario final, como es el caso de la visibilidad pública de un bucket S3. (Jones, 2017)

Caso 2:

Fecha: 10/11/2017

Conocimientos Previos: Equifax es una empresa que brinda información crediticia sobre consumidores. Surgen 3 conceptos de la información a partir de su uso dentro de esta empresa: Data en uso (Constante modificación de esta información), Data en movimiento (Data que está atravesando la red, o está temporalmente en una computadora, esperando a ser leída), Data en descanso (Data que está inactiva, actualmente almacenada en bases de datos, Data Warehouse, hojas de datos, etc.).

Situación: Equifax, confirma que no encripta la "Data en descanso", esto expone que la compañía tomó la decisión de no encriptar la información inactiva y fue una decisión consciente. Equifax alega que, para poder hacer una encriptación total de la información de sus clientes, la misma debe venir encriptada de sus retailers, no cumpliendo así con regulaciones como PCI, de tarjetas de crédito (PCI DSS).

Solución: Equifax enfrenta 240 tipos de demandas incluyendo consumidores, clientes y accionistas que fueron afectados por fuga de información de "data en Descanso". (Marks, 2017)

Artículo 3:

Fecha: 15/11/2107

Conocimientos Previos: Se aprobó la GDPR (General Data Protection Regulation), la cual entrará en vigencia el 25 de mayo del 2018. Es una regulación del parlamento europeo que intenta fortalecer y unificar la protección de datos para todos los individuos de la unión europea. También comprende el flujo de la información personal fuera de la unión europea.

Situación: La nueva legislación obliga a las empresas proveedoras de Cloud Computing o Cloud Storage a contratar a un Responsable de Protección de Datos Personales. La regulación afecta aquellos datos que son de carácter personal. El GDPR permite a los clientes el derecho de oponerse a que las empresas creen un perfil para su identificación.

Solución: La empresas proveedoras de CC y CS están analizando en qué grado son afectadas por esta regulación y la contratación de la posición Responsable de Protección de Datos Personales.

Creación de un decálogo donde, Las empresas españolas deberán nombrar un Responsable de Protección de Datos en seis meses.

Las empresas comienzan haciendo un análisis rápido de su situación, para pasar a preguntarse si cuentan con los procesos, recursos humanos y documentación exigida por la nueva normativa. Además, las compañías deben tener claro dónde se procesan sus datos de carácter personal y dotarse de un adecuado sistema de evaluación del impacto de protección de datos. (europapress/sociedad, 2017)

Artículo 4:

Fecha: 15/11/2017

Situación: Se dio el caso en China que Amazon debió vender parte de sus activos de infraestructura en China a Sinnet para ajustarse a legislaciones vigentes, y que Sinnet se encargara de proveer servicios de Cloud Computing. Las leyes que entraron en vigor en junio exigen que las firmas almacenen los datos a nivel local.

Artículo 5: https://www.emazzanti.net/cloud-computing-trust-but-verify/

Situación: Algunos de los riesgos al contratar un proveedor de nube son:

Dar atención al grupo de consumidores no al cliente individualmente. Los proveedores de nube trabajan a escala, y por lo general no pueden identificar problemas para cuentas

específicas. Un Hacker puede tener como objetivo los recursos de un cliente específico (Infectarlo, bajarlo, etc.) y el proveedor de nube puede decir que no es su problema ya que la mayor parte de sus servicios están disponibles.

Solución: El proveedor de nube debe tener en cuenta las necesidades específicas de cada cuenta de cliente.

Disponibilidad: El servicio de nube, es 100% dependiente de internet, hasta los mejores proveedores de nube, ocasionalmente experiencian cortes.

Solución: Service Level Agreements (SLAs), Proveedores secundarios.

Seguridad: Mantenimiento de las prácticas de seguridad actualizadas por proveedor de nube, no solo por el cliente.

Solución: SLAs.

Costos Ocultos si bien mantener la información en la nube puede ser más económico para presupuesto de IT, se deben tomar en cuenta variables como los precios de la migración, el soporte y el almacenamiento.

Solución: Presupuesto detallado. La persona que se encarga de los chequeos y políticas de seguridad no debe encontrarse ni en la organización cliente, ni en la proveedora de Cloud. (Cadell, 2017)

### 2.1.3 Casos de éxito derivados de la aplicación del Cloud Computing.

Caso 1:

Fecha: 31/12/2017

Conocimientos Previos: Bynder es una empresa que provee servicios CS exclusivamente dedicados a proyectos de marketing, incluyendo creación, aprobación y exposición de contenido.

Situación: La compañía logró un crecimiento del 200% debido al montaje de la plataforma en AWS y el uso de nuevas tecnologías propuestas como "Amazon Rekognition" (Identificación de Imágenes) y AWS Lambda (Ejecución de Código en la cual solo se cobra por tiempo de cómputo).

Bynder comenzó con servidores locales y luego a partir de un rápido crecimiento decidió tercerizar mediante productos Amazon (Amazon Elastic Compute Cloud EC2, Amazon Simple Storage Service S3 y Amazon Relational Database RDS), permitiéndole concentrarse en aplicaciones propias dedicadas a proyectos de administración de creación de marca. Esto atrajo inversiones de Venture Partners de más de 20 millones de USD. (Services, 2017)

Caso 2:

Fecha: 31/12/2017

Conocimientos Previos: Starling Bank es un banco de Inglaterra dedicado exclusivamente a Mobile, mostrando transacciones en tiempo real entre otras cosas.

Slack, es la herramienta que usan para modificar el código de las apps y les permite administrar y auditar el sistema.

Situación: La implementación de Cloud Computing para el sistema financiero obligó a la EU a crear regulaciones como PSD2 (Revised Payment Service Directive), la cual permitiría una vez implementada la exposición de información y servicios de pago para que sean utilizados por otros negocios. De esta manera negocios fuera del banco podrían usar las APIs del mismo para crear sus propios productos y servicios financieros. Esta regulación permitiría democratizar la industria de servicios financieros (2015).

Una vez cumplida la meta del desarrollo de estas APIs pasa al desarrollo de las mismas para el usuario final en dispositivos móviles (2016), Starling Bank es otorgada la primera licencia bancaria, sin sucursales físicas bancarias en el mundo (2017)

Solución: Los productos utilizados para brindar estas soluciones fueron:

Amazon EC2 (Capacidad de computo en la nube y segura de tamaña modificable)

Amazon RDS (Base de datos Relacional)

AWS Cloud Formation (Administración de Recursos y servicios de AWS)

AWS Lambda (Correr código sin necesidad de un server). (Elliot, 2015)

Caso 3:

Fecha 14/01/2017

Conocimientos Previos: Avazu es una compañía dedicada a la distribución global de marketing digital dedicado a internet fijo y móvil, mediante plataformas de soluciones de marketing, basadas en resultados y predicciones. Algunos de los problemas que Avazu tiene que enfrentar son alto tráfico, alta concurrencia, base de datos de consumidores

geográficamente dispersada y demanda de altos niveles de estabilidad, seguridad y disponibilidad.

Solución: Los servicios propuestos por AWS para la solución de estos problemas son:

Amazon S3: Almacenamiento de Objetos con alto grado de accesibilidad

Amazon Kinesis: Procesamiento y análisis de datos de Streaming en tiempo real. (Data Mining).

Amazon Dynamo DB: Almacenamiento de Bases de Datos.

AWS Pipeline: Transportar información a lo largo de diferentes regiones.

Amazon Route 53: Un servicio web DNS (Sistema de nombres de dominio) escalable y de alta disponibilidad en la nube. (Zhang, 2017)

Caso 4:

Fecha: 31/01/2018

Conocimientos previos: Patsnap es una plataforma para la búsqueda, mantenimiento y análisis de patentes. Utiliza Big data para poder hacer un análisis sobre las bases de datos de patentes en el mundo, traqueando no solo clientes globales sino también avances sobre las patentes.

Necesidades de Patsnap:

1. Cobertura Global: Distribución de clientes en EEUU, EU, Asia y China.

Solución: AWS Cloud Formation, permitiéndole a la empresa crear templates dentro de su plataforma para administrar y configurar sus recursos.

2. Alta seguridad: Visualización y acceso a patentes.

Solución: Virtual Private Cloud (Amazon VPC) - Creación de VPCs específicas.

AWS WAF (Web Application Firewall) - Control de tráfico malicioso

AWS Trusted Advisor - Patcheo de la plataforma.

3. Análisis de gran cantidad de datos: Se utilizaban bases de datos MONGO, para hacer un almacenamiento de todas las patentes.

Solución: Amazon Dynamo DB - Administración de bases de datos en AWS

Amazon Glacier - Archiving de datos.

AWS Data Pipeline - Mover grandes cantidad de información entre regiones de AWS. (Wu, 2017)

### 2.1.4 Amenazas actuales que afectan Cloud Computing.

Caso 1:

Fecha: 06/01/2017

Situación: Intel, compañía productora de microprocesadores encontró un fallo en el diseño de los mismos. Estos fallos pueden ser utilizados para explotar vulnerabilidades de seguridad, poniendo en riesgo ordenadores y servidores. La falla consiste en permitir al atacante acceder al Kernel de una computadora ingresando software malicioso, por ejemplo para recuperación de contraseñas, sin que el propietario lo sepa. Esto no solo afecta a usuarios particulares sino también a proveedores y clientes de Cloud Computing. (Domenech, 2018)(Clarin, 2018)

Estas dos vulnerabilidades fueron llamadas Meltdown y Spectre (PCI, 2018):

Meltdown: Le permite al atacante alquilar espacio en el Servicio Cloud que ofrece por ejemplo A.W.S. como cualquier otro cliente. Una vez que el atacante entra al servicio, mediante esta falla en el Kernel de los microprocesadores, puede acceder a aquella información como claves y contraseñas de clientes de otras cuentas de A.W.S. que se encuentren en el mismo servidor físico. (Si bien la información puede estar separada por cliente, no es anormal que varios clientes se encuentren en un mismo servidor). Amazon confirmó que ya está protegiendo a sus clientes de esta vulnerabilidad, sin embargo los mismos tienen que actualizar su software que está corriendo dentro del mismo, sin embargo se esperan bajas en los tiempos de procesamiento brindados.  Parche: Kaiser.

La vulnerabilidad consiste en evitar el aislamiento de la memoria, mediante la funcionalidad de "Out of order execution" que permite mejorar la performance de un CPU. Las Out of Order executions permiten cargar información de manera predictiva sin necesidad de autorización por parte del programa en el espacio de memoria, sin embargo se pueden modificar para ser explotadas por el atacante.(Goretsky, 2018)

Spectre: Afecta todos los microprocesadores. Rompe el aislamiento entre los procesos.

La vulnerabilidad consiste en ejecutar código malicioso mediante el uso de la funcionalidad "Speculative Execution". Esta funcionalidad consiste en ejecutar órdenes de programas sin verificar con la memoria, que esta orden, que se está ejecutando sea la siguiente, sino de una manera predictiva. De esta manera el atacante puede obtener direcciones de espacio

de memoria. Como los procesadores están siendo creados, de manera que, si la especulación es incorrecta se pueda eliminar el resultado sin problemas, se consideró que esto no era un problema de seguridad en su implementación. (Goretsky, 2018)

Solución: Si bien Intel está trabajando para eliminar la vulnerabilidad, también Windows y Linux emitieron parches para mitigar la misma.

Caso 2:

Fecha: 10/02/2018

Conocimientos Previos: Actualmente hay 2 vulnerabilidades detectadas para microprocesadores (Intel y otros), que no han podido ser mitigadas completamente por empresas como AWS.

Solución: Amazon procedió a la compra de la empresa SQRRL que es un proveedor avanzado de detección de amenazas. Dicha empresa se especializa en el análisis de enlaces, análisis de comportamiento del usuario y en ser compatible con los sistemas de seguridad y administración de eventos (SIEM). (Villatoro, 2018)

Caso 3:

Fecha: 10/02/2018

Conocimientos previos: Shellshock (Bashdoor) es una vulnerabilidad que se da en el programa Bash (Interpretación de órdenes y lenguaje de consola), sobre el shell de Unix.

Básicamente permitía ejecutar comandos cuando los comandos están concatenados al final de una definición de función guardada en los valores de las variables de ambiente. Algunas de las consecuencias, fueron ataques distribuidos de denegación de servicios (DDoS).

Heartbleed es una vulnerabilidad sobre la biblioteca de código abierto OpenSSL (Secure Socket Layer). OpenSSL es un paquete de herramientas de administración y bibliotecas que suministran funciones criptográficas a otros paquetes como OpenSSH y navegadores Web. La vulnerabilidad permitía, mediante el acceso a claves privadas de SSL de servidores, el acceso a la memoria de los mismos.

Solución: Deep security as a service fue creado por Trend Micro para asegurar procesos de carga de datos, resolviendo vulnerabilidades como Shellshock y Heartbleed, inyecciones SQL y XSS, esto permite hacer una metodología de "pago por uso". A su vez Trend Micro certifico sus servicios SaaS en PCI-DSS (Payment Card Industry), permitiendo los proyectos de clientes que utilizan los servicios proporcionados certificar más fácilmente en PCI. (Foster, 2016)

### 2.1.5 Análisis de Mercado.

De acuerdo con lo analizado se encontraron dos tipos principales de clientes, desde un punto de vista de BtoB:

Grandes Empresas: Aquellas empresas con un volumen de datos tan grande que vuelva imposible almacenar y analizar esa información en tiempo y real y de manera competitiva.

Con esto nos referimos a aquellas empresas que por ejemplo obtienen información de transacciones realizadas en su sitio web. (Ejemplo: MercadoLibre). Si bien estas empresas podrían invertir para tener la infraestructura necesaria para almacenar y procesar estos. No son el "core" (Núcleo) del negocio y el tiempo y la especialización requeridos para poder obtener dicho servicio de manera interna, no son justificables. Otro ejemplo de esto podrían ser las cadenas de McDonald's a lo largo de todo el mundo, si bien esta empresa es multinacional, no es posible analizar toda la información recabada en tiempo de sus clientes. Para potenciar el análisis y flujo de los consumidores podría ser útil contemplar el análisis de la información de transacciones recabadas por los clientes mediante el uso de Cloud Services.

Por ultimo cabe destacar aquellas empresas que trabajan con IoT (Internet of things), con un caudal tan importante de información que genera vuelve imposible mantener y analizar a una sola empresas semejante volumen de datos.

Pequeñas empresas: Aquellas empresas que solo dedican sus recursos a su "Core" (Núcleo) de servicios/productos sin la necesidad o posibilidad de análisis masivo de datos, ya sea por infraestructura, recurso o especialización.

Si bien la tecnología y los servicios de Cloud Computing/Storage se están haciendo masivos, reduciendo sus costos y permitiendo a más y más clientes acceder a los mismos, muchas veces no es posible acceder para algunas empresas a contar con estos servicios On-premise, debido a las barreras de ingreso de inversión en Infraestructura/Especialización/Recursos. De esta manera contratando el Cloud Computing/Storage mediantes terceros permite una mejora del servicio/producto a aquellos no

pueden realizarlo mediante sus propios medios. Obteniendo de esta manera no solo el servicio de manera más accesible sino también el conocimiento en el análisis de dichos datos.

Asimismo Luis Papagni, Director Provincial de Sistemas y Tecnología de la Provincia, cuando se indagó sobre el mismo tema, comentó que en empresas como ProvinciaNet les permitió implementaciones más rápidas por la alta disponibilidad y los bajos costos de implementación, solucionando inconvenientes de riesgo en la red y amenazas físicas.

Podemos observar estos dos tipos de clientes. A su vez los consumidores finales, es decir los clientes de las empresas solamente percibirán una mejora de calidad de servicio/producto pero será un proceso transparente para los mismos.

### 2.1.6 Ventajas del Cloud Computing

Bajo coste: No es necesario tener una gran cantidad de infraestructura para el almacenamiento de los datos, ya que el proveedor de servicio se encargará de almacenar la infraestructura.

Seguridad: Dependiendo de la empresa, las mismas cuentan con terceras partes que se encargan de la auditoría de sistemas de seguridad, tanto físicos como segregación de funciones y servicios.

Asimismo Alejandro Adamowicz, director de tecnología de América Latina en GSMA, cuando se indagó sobre el mismo tema, comentó que los servicios del proveedor brindados en la capa superior de servicios, beneficiaron al departamento de Seguridad informática que trabajaba On-premise anteriormente, dada la vasta experiencia del proveedor

y la preparación que tenía el mismo, para defensas contra ataques DoS, DDoS, etc. (Alejandro Adamowicz, Entrevista telefónica, 03/07/2018).

Cumplimiento de regulaciones: Las terceras partes antes mencionadas se encargan e hacer que el proveedor del servicio cumpla con las regulaciones necesitadas por el cliente. (Ejemplo SSAE16 para observar que determinado controles se cumplan para cumplir con las regulaciones que necesita el cliente).

Información a tiempo real: Para las pequeñas empresas que no poseen la infraestructura necesaria para la minería de sus propios datos, los proveedores pueden dar servicios de minería de datos, dando información en tiempo real.

Fuerte inversión en innovación: El proveedor de estos servicios siempre se encuentra en el auge de los servicios para no ser sobrepasado por competidores en calidad de servicio.

### 2.1.7 Desventajas del Cloud Computing.

Transferencia de Datos a servidor de proveedores: Si bien esto no representa problemas para clientes que tienen poca información, sí representa una gran barrera al momento de ver empresas con grandes cantidades de datos transaccionales. Es en este caso que se produce una disyuntiva de cómo se hará la puesta en producción para el uso de esta tecnología, si será mediante la metodología de "Ship it" o de "Transfer it", de acuerdo a diferentes condiciones como son las de la velocidad del ISP (Internet Service Provider), capacidad de almacenamiento de información de Hardware, urgencia de transferencia a la nube, etc. (Date, 2016). La metodología de "Ship It", hace hincapié enviar la información físicamente mediante discos duros o cintas, algo que ya se ha dado en varios casos, ya sea por la velocidad de transferencia del proveedor de internet del cliente, o por regulaciones involucradas en el país

de origen o destino, que obligan a hacer la transferencia de la información de manera física para que pueda ser analizada. La metodología de “Transfer It” hace hincapié la confiabilidad de un ISP (Internet Service Provider) y su SLA (Service Level Agreement) de velocidad de transferencia acordado.

La “Data Sovereignty” (Soberanía de datos), puede considerarse como otra desventaja de Cloud Computing. Dicho concepto entra en juego cuando la información de una organización que se encuentra dentro de un país (origen), es almacenada/analizada dentro de otro país (Destino). De esta manera está sujeto a las leyes del país (Destino) en el cual se encuentra la información. (Snipp, 2015). Esto podría generar conflictos no solo para el cliente, que no está especializado en el tratamiento de la información en el país destino; sino también para el proveedor de Cloud Computing que deberá acatar a dichas regulaciones en consentimiento con su cliente que no puede no estar de acuerdo.

# 3. Estado del Arte.

### 3.1.1 Regulaciones existentes aplicables a Cloud Computing y Cloud Storage

Hoy en día, si bien la mayoría de las empresas de Cloud Computing están localizadas en EEUU, podemos decir que la Unión Europea está teniendo cada vez más y más demanda de requerimientos Cloud de EEUU, lo cual trae consigo grandes requerimientos regulatorios para el flujo de información personal. A veces las regulaciones de la Unión Europea impiden bloques de datos de transferencia multinacional requeridos para el procesamiento de información por procesos de empresas que se encuentran en diferentes países (Schwartz, 2017).

Para estos casos, la regulación que actualmente protege la información personal de las personas en la Unión Europea es "General Data Protection Regulation" y se encuentra en constante cambio y revisión, debido al constante cambio de la información y la definición de la misma. Como ejemplo podemos observar que, en un pasado no se había concebido el traspaso de información como algo frecuente, sin embargo con la existencia del internet, y conceptos como Internet of Things (IOT) y Cloud Computing (CC), las definiciones relacionadas a esta regulación deben estar constantemente verificadas y revisadas (Victor, 2013).

En relación con lo mencionado por Víctor Jacob M., se observan 3 tipos de cambios en cuanto al procesamiento de la información personal debido al Cloud Storage y Cloud Computing:

En primer lugar la Naturaleza del procesamiento de la información en las compañías sufrió cambios debido a que las transacciones empiezan a ser cada vez de una naturaleza más internacional, volviéndose menos valiosa una regulación que haga énfasis en la protección de datos clasificada por países. Los conceptos jurisdiccionales de la Unión Europea, no encajan con la escala y naturaleza del procesamiento de este tipo de dato (Schwartz, 2017).

Es por esto que debido al Cloud Computing, se pasó de una era de transferencias internacionales de información privada, a una era de procesamiento internacional de información privada. (Transferir la información de acuerdo a la potencia de cálculo del país, sin importar donde sea). Otro ejemplo de este cambio es pasar la información a los centros de la compañía en los cuales el horario es diurno y hay gente para analizar los datos ("Follow the sun").

En segundo lugar, las leyes no están adaptadas a seguir los flujos multidireccionales de la información para las diferentes redes de procesos que tienen como objetivo un único resultado de negocios. Debido a que el significado que puede tener cada concepto de información (Información personal, procesamiento automático), puede variar de acuerdo al proceso, no hay una armonización de los conceptos, lo cual hace que las leyes no se puedan adaptar, o que haya conflicto en referencia a leyes de seguridad de la información (Schwartz, 2017).

Finalmente, en el Management de procesos, la gente ya no es dueña de la información o la tecnología, diferentes compañías almacenadas en Cloud pueden proveer diferentes datos

para un mismo proceso, o para procesos a los que la compañía no está relacionada (Schwartz, 2017).

Lo mismo ocurre con conceptos y criterios desactualizado delimitados por la Federal Comunications Comission (FCC). La Comisión Federal de Comunicaciones es una agencia estatal independiente de Estados Unidos, bajo responsabilidad directa del Congreso. El objetivo de esta es redefinir la convergencia del procesamiento en computadoras y la comunicación. Algunos de los temas principales que trata la FCC: Promover la competencia, innovación, inversión, protección del consumidor y discurso civil (Werbach, 2017).

Se puede observar una fuerte necesidad por parte de las regulaciones existentes y en proceso, a la adaptación a un cambio de paradigma, dado que las empresas comenzarán a consumir servicios y no tecnología, como hardware para la implementación de servicios internos y On-premise. (HURBEAN & FOTACHE, 2013)

Podemos tener un enfoque bi-partidario en cuanto a la implementación de regulaciones para Cloud Computing: Permitir una auto-regulación realizada por el mercado o una regulación gubernamental. Aquí se produce la disyuntiva: El gobierno no debería controlar las directivas legales en privacidad pero los usuarios proclaman que la auto-regulación en CC es complicada debido a que no hay mecanismos o políticas legales simples para implementar para la industria de CC (Sinjilawi, Al-nabhan, & Abu-shanab, 2014).

### 3.1.2 Amenazas de seguridad de Cloud Computing

Algunas de las clasificaciones que podemos encontrar sobre Cloud Computing son:

Nube Publica que se basan en hardware físico compartido perteneciente y operado por un proveedor externo. Las nubes públicas son ideales para pequeñas y medianas empresas o negocios que tienen demandas variables. Las principales ventajas de la nube pública son la velocidad con la que se pueden implementar los recursos de TI y la capacidad para pagar solo por los recursos de servidor que se utilicen. Al repartirse los costos de infraestructura entre múltiples usuarios, cada uno de ellos puede beneficiarse de un enfoque de aprovisionamiento de TI de pago por consumo con un costo bajo. Y debido al gran tamaño de las nubes públicas, es posible aumentar y reducir la potencia de cómputo según las demandas del negocio en cuestión de minutos.

Una nube privada es una infraestructura dedicada por completo a su negocio que se hospeda in situ o en el centro de datos de un proveedor de servicios. La nube privada ofrece toda la agilidad, escalabilidad y eficiencia de la nube pública, pero también proporciona mayores niveles de control y seguridad, lo que la convierte en ideal para grandes empresas o empresas con estrictas obligaciones en relación con los datos, la normativa y la gobernanza. Otra ventaja importante de la nube privada es la capacidad de personalizar los distintos componentes de cómputo, almacenamiento y red para adaptarse a sus requisitos específicos de TI, algo que no se puede lograr tan fácilmente en el ambiente de la nube pública.

La Nube Comunitaria: Es una mezcla entre nube privada y publicada. Se comparte entre varias organizaciones para tratar temas de seguridad. Generalmente es administrado internamente o por una consultora (Sinjilawi et al., 2014).

Algunos autores proponen, tipos de amenazas relacionados al tipo de nube que se está utilizando.

Tabla 1: Cuadro comparativo entre posibles amenazas más comunes entre una nube privada y una nube pública.

| Nube Privada | Nube Publica |
|---|---|
| Administración de Accesos e Identidades<br>Protección de datos.<br>Inteligencia de la seguridad.<br>Seguridad de Software, plataforma e Infraestructura | Ataque DOS<br>Ataque a la máquina Virtual<br>Código Malicioso<br>Ataque a máquina física. |
| Nube de Dominio-Específica | Nube Híbrida |
| Compliance y Auditoria.<br>Firewall y Sistemas de detección de intrusos (IDS).<br>Control de Accesos.<br>Protección de Antimalware & Antivirus | Múltiples dueños de la nube.<br>Compliance.<br>Control de Acceso y Administración de Identidades.<br>Pérdida de Información |

Tabla 1: Cuadro comparativo entre posibles amenazas más comunes entre una nube privada y una nube pública. Elaboración propia en base a "Addressing Security and Privacy Issues en Cloud Computing".(Sinjilawi et al., 2014).

Otros autores proponen amenazas basadas en la CSA (Cloud Security Alliance):

Tabla 2: Principales Amenazas identificadas por la Cloud Security Alliance (CSA).

| N° | **Nombre de Amenaza** | **Contramedida para la Amenaza** |
|---|---|---|
| 1 | Uso Maligno y Abuso de Confrontación | Monitorear listas negras públicas, registro inicial y validación de procesos. |
| 2 | Interfaces de aplicación malignas. | Control de accesos con autenticación y envío de mensajes encriptados. |
| 3 | Ingresos Internos Maliciosos | Especificar requerimientos de recursos, generación de reporte de Compliance, administración de cadena de suministros. |
| 4 | Vulnerabilidades de la tecnología | SLA, seguridad en la instalación y configuración, monitoreo de ambiente de aplicaciones. |
| 5 | Fuga/Pérdida de Datos | Usar acceso por API, proteger y encriptar la integridad de los datos, estrategias de retención. |

| | | |
|---|---|---|
| 6 | Secuestro de Tráfico | Usar credenciales de usuarios y servicios, entendimiento de SLA/Políticas de proveedores. |

Tabla 2: Principales Amenazas identificadas por la Cloud Security Alliance (CSA). Elaboración propia en base a "Security Threats and Countermeasures in Cloud Computing".(Ashktorab & Taghizadeh, 2012).

A partir de estos ataques se proponen algunos conceptos claves para Cloud Computing que deben ser tenidos en cuenta a la hora de resguardar la seguridad, con sus correspondientes soluciones:

1. Autenticación: Sistema de administración de identidades.

2. Control de Accesos: SLAs con control de accesos.

3. Integración de políticas: Al tener varios proveedores Cloud puede haber inconsistencias en las políticas. (Solucionar inconsistencias entre políticas).

4. Administración de servicios: Cumplir con expectativas de repuesta de clientes, al ser varios proveedores Cloud.

5. Administración de Confianza: Factor de confianza de usuarios finales al proveedor Cloud.

(Sinjilawi et al., 2014).

A su vez se debe tener en cuenta el ciclo de vida de la información dentro para el cliente:

Ciclo de vida seguro de los datos:

- Crear: Clasificar y etiquetar los datos de la organización de acuerdo con la relevancia revestida. Asignación de privilegios.

- Almacenar: Establece e implementa controles de acceso. Ejecuta soluciones de cifrado en puntos vulnerables como son transporte en la red, bases de datos, y archivos almacenados. Define e implementa procesos de auditoria de acuerdo con políticas de la compañía.

- Utilizar: Establece políticas de seguimiento de Logs y controles dentro de los sistemas que manejan bases de datos.

- Compartir: Controla privilegios sobre los datos. Verifica los archivos de registro (logs). Cifra los datos en el proceso de transporte de información.

- Archivar: Encripta información en los medios donde se almacenan las copias de seguridad. Hace seguimiento al historial de resguardo.

- Destruir: Implementa técnicas de borrado seguro. Asegura la destrucción de las claves de cifrado. (Sepúlveda et al., 2011)

Métodos de preservación de privacidad de la información:

1. Método basado en la anonimidad: El algoritmo de encriptación encripta todo o parte de la información antes de enviarlo a la red.

2. Sistema de preservación de privacidad de autorizaciones: Los usuarios pueden modificar sus políticas de acceso y como acceder a la información para asegurar un acceso controlado a la información en la nube.

3. Preservación de privacidad de la arquitectura: Por arquitectura nos referimos a: Interfaz de usuario, motor de usuario, reglas de motor y bases de datos Cloud. La arquitectura Cloud es la responsable de la base de datos Cloud. A través de la interfaz de usuario, se obtiene el pedido de acceso a la base de datos y se envía este pedido a través de un pedido XML/RPC al motor de usuario, luego al motor de reglas y finalmente es enviada a la base de datos Cloud. Luego de llegar a la base de datos, se asignan identidades y encripta cada pedido. En cada paso también se hace un chequeo con el motor de mantenimiento verificando que el pedido tenga los permisos necesarios. Estas verificaciones controlan ataques tanto internos como externos para información exteriorizada.

4. Aproximación de Oruta: En esta aproximación se toman en cuenta tres entidades: Servidor Cloud, TPA (Third party auditing), y usuarios (Grupos de usuarios y usuarios). Los usuarios pueden controlar la información y su flujo en la nube, dependiendo del TPA para llevar a cabo la auditoria. (Algoritmos utilizados: Keygen, Ringsign y RingVerify). (Sinjilawi et al., 2014)

# 4. Clasificación de la Información.

### 4.1.1 Documentos de clasificación de la información en el mundo.

### 4.1.2 Política de seguridad de la información para organismos de la administración pública nacional en Argentina (Oficina nacional de tecnologías de información de Argentina)

La información debe ser mantenida y clasificada por los propietarios de la información, tanto el grado de sensibilidad, criticidad, documentación y actualización, como los permisos de acceso a la misma.

Los objetivos son garantizar un apropiado nivel de protección, lograr una clasificación de acuerdo con sensibilidad y criticidad y la definición de niveles de protección y medidas de tratamiento especial de acuerdo a la clasificación.

Existen 4 niveles de clasificación (0-3) siendo 3 el nivel más sensible y 0 el menos sensible. Está en el propietario definir la criticidad de la misma (Baja, media o alta). (Achiary, 2005).

Tabla 3: Cuadro de comparación de niveles de clasificación de la información para organismos de administración pública nacional de Argentina.

| Confidencialidad | Integridad (Modificaciones no autorizadas) | Disponibilidad (Inaccesibilidad de la información) |
|---|---|---|
| Público | Se puede reparar fácilmente | No afecta |

| | | |
|---|---|---|
| Reservado (Uso Interno) | Se puede reparar aunque puede dejar algunas pérdidas | Durante un período de tiempo no menor a una semana podría causar pérdidas significativas |
| Reservado (Confidencial) | Es difícil su reparación y puede dejar pérdidas significativas | Durante un período no menor a un día podría causar pérdidas significativas |
| Reservado (Secreto) | No puede repararse ocasionando pérdidas grandes | Durante un período de tiempo no menor a una hora podría causar pérdidas significativas |

Tabla 3: Cuadro de comparación de niveles de clasificación de la información para organismos de administración pública nacional de Argentina.

Elaboración propia en base a Tesis “Clasificación de la Información” de J. Sosa.

Una vez asignado un valor por cada una de las categorías anteriores se clasifican según estos criterios:

Criticidad baja: Valores de clasificación son menores o iguales a 1

Criticidad Media: Algún valor de clasificación es 2

Criticidad Alta: Algún valor de clasificación es 3.

### 4.1.3 Actualización Clasificación de la información para efectos de aseguramiento de la información Banco de la República de Colombia.

Para Colombia se proponen cinco niveles de clasificación de la información, que son, Información Clasificada, Información reservada, Información privada, información de uso interno e información pública. (Sosa, 2012)

Para cada una de estas clasificaciones se tienen atributos internos.

Tabla 4: Atributos Internos para clasificación de información dentro del banco de la República de Colombia.

| | Clasificada | Reservada | Privada | De Uso Interno | Pública |
|---|---|---|---|---|---|
| Confidencialidad | X | X | X | | |
| Integridad | X | X | | | X |
| Disponibilidad | X | | | | X |
| Autenticación | X | X | X | | |
| Control de Acceso | X | X | X | | |

| | | | | | |
|---|---|---|---|---|---|
| No repudiación | X | | | | X*(Opcional) |
| Observancia | X | X | X | | |

Tabla 4: Atributos Internos para clasificación de información dentro del banco de la República de Colombia.

Elaboración propia en base a Tesis “Clasificación de la Información” por J. Sosa.

A su vez, vale la pena mencionar que en Colombia existen Niveles de clasificación de Información – Unidad administrativa Especial Aeronáutica Civil – que no están alineados con las unidades financieras, ya que sus objetivos y riesgos son completamente diferentes.

La información se clasifica de la siguiente manera:

Altamente Confidencial (AC): Solo puede ser accedida por quienes ejerzan las funciones de: Director General, Subdirector General, Secretario de Sistemas Operacionales, , Secretario General y Secretario de Seguridad Aérea, Directores de Área, Jefes de Grupo y Jefes de Oficina. El mal uso de la misma puede ir en detrimento de los intereses de la UAEAC.

Confidencial (C): Es información crítica y solamente podrá ser conocida al interior de la Entidad ya que el conocimiento externo de la misma podrá ocasionar efectos negativos sobre la Entidad.

Restringida (R): Solo podrá ser accedida por grupos específicos de usuarios que requieren del conocimiento de esta información para estricto cumplimiento de sus funciones

Pública (P): Podrá ser utilizada por todos los empleados directos de la UAEAC y por empleados temporales, contratistas y/o terceros a la UAEAC

Los criterios para tener en cuenta esta clasificación son: Costo de reemplazo, interrupción del negocio, Pérdida de clientes, Violación de la propiedad, requerimientos Legales y pérdidas económicas. La clasificación interna de estos puede ser.

Tabla 5: Cuadro de clasificación de información para clasificación de criterios dentro de la Unidad administrativa Especial Aeronáutica Civil de Colombia.

| | Confidencialidad | Integridad |
|---|---|---|
| Alto | Fuga de información por accesos y/o revelaciones de información no autorizada afectaría seriamente las operaciones del negocio, generando alta pérdida monetaria y/o de imagen | Datos inexactos, incompletos o modificados sin autorización, causaría fallas en la operación, pérdidas económicas, pérdida en la productividad, pérdida de imagen ante el cliente. |
| Medio | Fuga de información por accesos y/o revelaciones de información no afectaría seriamente las operaciones del negocio y no dan lugar a alta pérdida monetaria. | Datos inexactos, incompletos o modificados sin autorización, no impactaran seriamente la operación del negocio o pérdida de imagen; daría lugar a soluciones prontas. |

| | | |
|---|---|---|
| Bajo | El uso y/o revelación de información por usuarios no autorizados no afecta la operación del negocio. | Contar con alternativas de información permitiría hacer posible la continuidad de la operación del negocio. |

Tabla 5: Cuadro de clasificación de información para clasificación de criterios dentro de la Unidad administrativa Especial Aeronáutica Civil de Colombia.

Cuadro de elaboración propia en base a Tesis "Clasificación de la Información" J. Sosa, 2012.

Otra clasificación que podemos encontrar en Colombia es la del ministerio de comunicaciones. Lo primero que se tiene en cuenta para la clasificación de la información es separarla entre la impersonal y la personal. Lo segundo es clasificar la información desde un punto de vista cualitativo en función de su publicidad y la posibilidad legal de obtener acceso a la misma.

Tabla 6: Cuadro de Clasificación de la Información por Ministerio de Colombia en función de su publicidad y posibilidad de acceso.

| Información Pública | Información semi-privada | Información privada | Información reservada |
|---|---|---|---|
| | | | |

| | | | |
|---|---|---|---|
| Puede ser obtenida y ofrecida sin reserva alguna y sin importar si la misma sea información general, privada o personal. Por vía de ejemplo, pueden contarse los actos normativos de carácter general, los documentos públicos en los términos del artículo 74 de la Constitución, y las providencias judiciales debidamente ejecutoriadas. | Será aquella que por versar sobre información personal o impersonal y no estar comprendida por la regla general anterior, presenta para su acceso y conocimiento un grado mínimo de limitación, de tal forma que la misma sólo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Es el caso de los datos relativos a las relaciones con las entidades de la seguridad social. | Aquella que por versar sobre información personal o no, y que por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio. | Por versar igualmente sobre información personal y sobre todo por su estrecha relación con los derechos fundamentales del titular - dignidad, intimidad y libertad- se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones. Cabría mencionar aquí la información genética, y los llamados "datos sensibles" o relacionados con la ideología, la inclinación sexual, los hábitos de la persona, etc.”. |

| | | | |
|---|---|---|---|
| | | | |

Tabla 6: Cuadro de Clasificación de la Información por Ministerio de Colombia en función de su publicidad y posibilidad de acceso.

Elaboración propia en base a Tesis “Clasificación de la Información” J. Sosa, 2012.

### 4.1.4 COBIT 4.1 en USA.

COBIT es un marco de trabajo y un conjunto de herramientas de gobierno de Tecnología de información (TI) que permite a la gerencia cerrar la brecha entre los requerimientos de control, aspectos técnicos y riesgos de negocios.

En la sección de Planear y Organizar, donde el segundo paso es definir la arquitectura de la información, se definen las siguientes características (IT Governance Institute, 2007).

Tabla 7: Características para la definición de la Arquitectura de la información según COBIT 4.1 en USA.

| | |
|---|---|
| Modelo Arquitectura de información Empresarial | Establecer y mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI. El modelo debe facilitar la creación, uso y el compartir en forma óptima la información por parte del negocio de tal manera que se mantenga |

| | |
|---|---|
| | su integridad, sea flexible, funcional, rentable, oportuna, segura y tolerante a fallos |
| Diccionario corporativo de datos y Reglas de sintaxis de los datos de la organización | Facilita compartir elementos de datos entre las aplicaciones y los sistemas, fomenta un entendimiento común de datos entre los usuarios de TI y del negocio, y previene la creación de elementos de datos incompatibles |
| Esquema de clasificación de datos y los niveles de seguridad | Basados en que tan crítica y sensible es la información se establece un esquema de clasificación que aplique a toda la empresa (pública, confidencial y secreta). Para este esquema se debe incluir la siguiente información pertinente:<br>o Detalles acerca de la propiedad de datos<br>o Definición de niveles apropiados de seguridad y de controles de protección<br>o Descripción de los requerimientos de retención y destrucción de datos, incluyendo información de que tan críticos y sensibles son.<br>Se usa como base para aplicar controles como el control de acceso, archivo o cifrado. Este |

| | |
|---|---|
| | proceso mejora la calidad de la toma de decisiones gerenciales asegurándose que se proporciona información confiable y segura, y permite racionalizar los recursos de los sistemas de información para igualarse con las estrategias del negocio. Este proceso de TI también es necesario para incrementar la responsabilidad sobre la integridad y seguridad de los datos y para mejorar la efectividad y control de la información compartida a lo largo de las aplicaciones y de las entidades. |
| Administración de Integridad | Definir e Implementar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos |

Tabla 7: Características para la definición de la Arquitectura de la información según COBIT 4.1 en USA.

Elaboración propia en base a "Marco de Trabajo Objetivos de Control Directrices Gerenciales Modelos de Madurez", COBIT, 2007.

### 4.1.5 TCSEC ("Trusted Computer Security Evaluation Criteria") Orange Book

Creado por el departamento de Defensa de Estados Unidos. Este libro suministra especificaciones de seguridad. Se definen siete conjuntos de criterios de evaluación denominados clases (D, C1, C2, B1, B2, B3 y A1). Cada clase de criterios cubre cuatro aspectos de evaluación: política de seguridad, imputabilidad, aseguramiento y documentación. Los criterios correspondientes a estas cuatro áreas van ganando en detalle de una clase a otra, constituyendo una jerarquía en la que D es el nivel más bajo y A1 es el más elevado. Luego de un tiempo estos estándares fueron aplicados internacionalmente mediante (ISO/IEC).

Tabla 8.A: Clasificación de la información de acuerdo con el Departamento de defensa de Estados Unidos.

| | | | | | |
|---|---|---|---|---|---|
| **Confidencialidad** | Súper Secreto | Secreto | Confidencial | No clasificado | |
| | | | | Sensible pero No clasificada | Solo para uso oficial |

Tabla 8.A: Clasificación de la información de acuerdo con el Departamento de defensa de Estados Unidos.

Elaboración Propia en base a Tesis "Clasificación de la Información", J. Sosa, 2012.

Para el caso de los niveles, cada nivel requiere que todos los niveles anteriores sean cumplidos.

Tabla 8.B: Criterios para clasificación de Información de acuerdos a Aspectos de evaluación (Política de seguridad, imputabilidad, aseguramiento y documentación).

| Nivel | Descripción |
|---|---|
| Nivel D: Protección Mínima | Sin seguridad, está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. Podemos observar como ejemplo: MS-DOS y System 7.0 Macintosh |
| Nivel C1: Protección Discrecional | Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.<br>Requisitos necesarios para este nivel:<br>Acceso de control discrecional: Definición de grupos de usuarios y recursos.<br>Identificación y Autenticación. |
| Nivel C2: Protección de Acceso Controlado | Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos. Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a |

| | |
|---|---|
| | usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.<br>Requiere que se audite el sistema. Esta auditoria es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios.<br>La auditoría requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.<br>Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores. |
| Nivel B1: Seguridad Etiquetada | Soporta seguridad multinivel, como la secreta y ultra secreta. Se establece que el dueño del archivo no puede modificar los |

| | |
|---|---|
| | permisos de un objeto que está bajo control de acceso obligatorio.<br>A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.).<br>Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados.<br>También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos. |
| Nivel B2 (Protección Estructurada) | Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior.<br>El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son |

| | |
|---|---|
| | modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios. |
| Nivel B3 (Dominios de seguridad) | Este nivel requiere que la Terminal del usuario se conecte al sistema por medio de una conexión segura. Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.<br>Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido.<br>Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y pruebas ante posibles violaciones. |

| | |
|---|---|
| Nivel A1 (Protección verificada) | Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.<br>Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento. |

Tabla 8.B: Criterios para clasificación de Información de acuerdos a Aspectos de evaluación (Política de seguridad, imputabilidad, aseguramiento y documentación).

Elaboración Propia en base a "TCSEC". Web http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/TCSEC.php . 23 marzo 2018.

### 4.1.6 GIAC Security Essentials Certification (GSEC) en USA.

Se trata de una certificación relacionada a seguridad de la información, llamada Global Information Assurance Certification para la seguridad de la información del gobierno (Government Security – GSEC). Se hace hincapié sobre clasificación de la información en el módulo de "políticas de Seguridad" (Security Policy).

Antes de la clasificación la información se debe: Identificar los recursos de información que necesitan ser protegidos (Localización, como, propietario, custodio de los datos, formato de la información), identificar las medidas de protección de la información (Autenticación, Acceso basado en roles, Cifrado, Controles administrativos, Controles tecnológicos, Garantía), y por último identificar la clases de información (Confidencialidad, Disponibilidad, Integridad, Propiedad, Altamente Sensible, Función Sensible, Restringida de negocio, Restringida de propietario, uso de la compañía, uso interno, uso público, negocio crítico, negocio, No esencial).

Tabla 9.A: Criterios de protección de sensibilidad y confidencialidad en clasificación con clases de información de acuerdo con GIAC - GSEC.

| Criterio de protección | Altamente Sensible | Función Sensible | Propietario Discreto | Uso del a compañía | Uso Público |
|---|---|---|---|---|---|
| Autenticación | Id, contraseña, ingreso encriptado | Id, contraseña, ingreso encriptado | Id y contraseña | Id y contraseña | No hace falta autenticación |

| | | | | | |
|---|---|---|---|---|---|
| Aprovisionamiento | Alta adm. O autorización del propietario de los datos y acceso individual | Administración de autorización basado en roles | Autorización y administración delegada al creador o propietario | Acceso automático para empleados | Acceso automático para todos los empleados. |

Tabla 9.A: Criterios de protección de sensibilidad y confidencialidad en clasificación con clases de información de acuerdo con GIAC - GSEC.

Elaboración Propia Tesis "Clasificación de la Información", J. Sosa, 2012.

Tabla 9.B: de Clasificación de los criterios: Integridad y uso apropiado, Disponibilidad, Conformidad.

| | Integridad y uso Apropiado | Disponibilidad | Conformidad |
|---|---|---|---|
| Alto | Actualización de acuerdo a las especificaciones del propietario de los datos. | No hay tolerancia para la interrupción del servicio durante las horas de negocio. Formación de la Cruz de las | Capacidad de supervisión regulares Monitoreo regular de violación Operación regular de control de registro |

| | | | |
|---|---|---|---|
| | Separación de funciones para las operaciones financieras.<br>Todas las copias de la información se tienen en cuenta y se destruyen antes de la eliminación<br>Sujeto a cambios de control<br>Tutoriales de código requerido<br>Cifrar todas las transacciones de información<br>Cifrar la información en reposo | operaciones comerciales de personal requerido<br>La protección antivirus necesaria | de las funciones sensibles<br>Reunión periódica revisión del registro de<br>La red y detección de intrusión en el sistema |
| Medio | Actualización de acuerdo a las | | |

| | | | |
|---|---|---|---|
| | especificaciones del propietario de los datos.<br>Sujeto a cambios de control<br>Tutoriales de código requerido<br>Cifrar las transacciones por Internet. | Debe ser recuperado dentro de las 8 horas de trabajo<br>Formación de la Cruz de las operaciones comerciales de personal requerido<br>La protección antivirus necesaria | Violación registros disponibles para su revisión.<br>Registros de transacciones disponibles para su revisión.<br>Capacidad de supervisión por petición.<br>Registros de eventos disponibles para su revisión.<br>La red y detección de intrusión en el sistema |
| Bajo | Sin integridad o uso de controles apropiados | La protección antivirus necesaria | La auditoría no está habilitado; revisar el registro no está disponible. |

| | | | |
|---|---|---|---|
| | | | no hay control |

Tabla 9.B: de Clasificación de los criterios: Integridad y uso apropiado, Disponibilidad, Conformidad.

Elaboración Propia Tesis “Clasificación de la Información”, J. Sosa, 2012.

La clasificación de criterios de Continuidad de Negocio puede ser “Recuperado” o “No recuperado”. (Sosa, 2012)

### 4.1.7 Normas para la clasificación de la información en Sistema Federales en USA.

Los impactos para las normas de sistemas federales de EEUU se definen bajo el impacto de los tres conceptos principales de seguridad de la información: Confidencialidad, Integridad y Disponibilidad. (Mell & Grance, 2011)

Impacto potencial Bajo: La pérdida de la confidencialidad, integridad o disponibilidad tiene efectos adversos limitados en las operaciones de la organización, los activos de la organización, o individuos.

Impacto potencial Moderado: La pérdida de la confidencialidad, integridad o disponibilidad tiene efectos adversos serios en las operaciones de la organización, los activos de la organización, o individuos.

Impacto potencial Alto: La pérdida de la confidencialidad, integridad o disponibilidad tiene efectos adversos severos o catastróficos en las operaciones de la organización, los activos de la organización, o individuos.

Definición de Categorías de seguridad (SC):

SC tipo de información = {(confidencialidad, impacto), (integridad, impacto), (disponibilidad, impacto)}

 Información Pública

SC de información pública = {(confidencialidad, NA), (integridad, moderado), (disponibilidad, moderado)}.

 Información investigativa

SC información sobre las investigaciones = {(confidencialidad, alto), (integridad, moderado), (disponibilidad, moderado)}.

 Información administrativa

SC = {información administrativa (confidencialidad, bajo), (integridad, bajo), (disponibilidad, bajo)}.

### 4.1.8 Política de Seguridad del Reino Unido.

El gobierno del reino unido posee 3 niveles de seguridad relacionados a clasificación de la información: Oficial, Secreto y top secreto.

HMG opera una política de clasificación que permite identificar y valorar la información de acuerdo con su sensibilidad y conducir las protecciones correctas. Esto comprende tres niveles: OFICIAL, SECRETO y SECRETO TOP para los que existen diferentes disposiciones de seguridad. OFICIAL abarca la mayoría de las actividades diarias del gobierno, la prestación de servicios, la actividad comercial y el desarrollo de políticas.

La información SECRETA y TOP SECRET generalmente requerirá protección soberana a medida, pero la información OFICIAL se puede gestionar con buenas soluciones comerciales que mitiguen los riesgos que enfrenta cualquier gran organización corporativa. De esta forma, el gobierno puede ofrecer de manera segura y eficiente, y dar forma a sus servicios para satisfacer las necesidades del usuario. (Gov, United Kingdom, 2017)

### 4.1.9 Marco de seguridad de Clasificación de la información de acuerdo con el gobierno de Queensland (Australia)

La clasificación de la información de acuerdo con el Gobierno de Queensland Australia se divide en 2 grandes categorías, Publica y No pública.

Tabla 10: Categorías de Clasificación de la Información de Australia.

<table>
<tr><td colspan="4">Toda la información utilizada por el gobierno de Queensland</td></tr>
<tr><td rowspan="3">Información Pública</td><td colspan="3">Información No Pública</td></tr>
<tr><td rowspan="2">Información No Clasificada</td><td colspan="2">Información de Seguridad Clasificada</td></tr>
<tr><td>Información de seguridad No Nacional</td><td>Información de Seguridad Nacional</td></tr>
</table>

| | | | |
|---|---|---|---|
| | | Altamente protegida | Top secreto |
| | | Protegida | Secreto |
| | | X-In-Confidence | Confidencial |
| | | | Restringido |

Tabla 10: Categorías de Clasificación de la Información de Australia.

Elaboración Propia en base a Tesis "Clasificación de la Información", J. Sosa, 2012.

Como se puede observar en la figura para la información oficial no pública se divide en dos categorías: la no clasificada y de seguridad clasificada. La información que no puede ser pública pero que no necesita un control especial en cuanto a seguridad se deja en la categoría no clasificada para tener en cuenta que ya se le realizó una evaluación a esa información.

Las diferencias entre X-In-Confidence y Protegida de Información de seguridad No Nacional y las categorías de Seguridad Nacional, se da debido a diferencias en la norma de Seguridad de clasificación de la información de Queensland y el gobierno australiano, para que sean compatibles entre sí. (Gobierno de Queensland, 2009)

### 4.1.10 Seguridad de la Información en Canadá

El gobierno de Alberta, Canadá identificó 4 niveles para esta clasificación:

Sin restricción: Información que es poco probable que cause daño. Está disponible para el público, empleados y contratistas, sub contratistas y agentes que trabajan para el gobierno. Esta también es llamada a veces como pública.

Protegida: Información sensible para el gobierno y que puede impactar algunos servicios del mismo. Incluye información personal, financiera. Está disponible para empleados y para empleados no autorizados que necesiten conocer la información para propósitos relacionados con los negocios. A su vez esta se subdivide en 3 categorías: Protegida A, B y C. Estas categorías dependen de cuánto daño le causen a la organización dependiendo de la información tratada. (Gov Alberta Canada, 2014)

Confidencial: Información sensible para el gobierno que puede causar pérdidas graves de privacidad, ventaja competitiva, perdida de confidencialidad en los programas del gobierno y puede causar hasta daños en las asociaciones, relaciones y reputación. Solo está disponible para una función, grupo o rol específico.

Restringida: Información que es extremadamente sensible y puede causar grandes daños en la integridad y la imagen (pérdida de la vida, riesgos para la seguridad pública, pérdidas sustanciales financieras, dificultades sociales, y un gran impacto económico). Está disponible sólo para las personas nombradas o posiciones específicas.

A su vez se puede ver que en Alberta se posee un ciclo de vida de la información para el gobierno, consistente de los siguientes pasos crear/recolectar, organizar, usar, almacenar, archivar y destruir.

### 4.1.11 Cuadro Comparación de Clasificación de la Información de acuerdo con los estándares vistos

Tabla 11: Cuadro Comparativo de categorías de Clasificación de la Información de acuerdo a los países / Buenas prácticas analizadas.

| **Norma/Estándar País** | **Clasificación Básica 1** | **Clasificación Básica 2** | **Clasificación Básica 3** | **Clasificación Básica 4** |
|---|---|---|---|---|
| Administración Pública / Argentina | Público | Reservado (Uso Interno) | Reservado (Confidencial) | Reservado (Secreto) |
| Banco / Colombia | Pública | Restringida | Confidencial | Altamente Confidencial |
| TCSEC /USA | No clasificado (D) | Confidencia (C1,C2) | Secreto (B1, B2, B3) | Súper Secreto (A2) |
| GIAC-GSEC/USA | - | Bajo | Medio | Alto |
| Sistemas Federales/USA | - | Impacto Potencial Bajo | Impacto Potencial Medio | Impacto Potencial Alto |
| UK | - | Moderada | Secreto | Top Secreto |
| Queensland/Australia | Información/ No Clasificada - Publica | Restringido | Confidencial(Secreto | Secreto/ Seguridad Nacional |
| Canadá | | Protegida (A, B y C) (Pequeños | Confidencial (Daños moderados) | Restringida (Grandes Daños) |

| | | | | |
|---|---|---|---|---|
| | | daños a servicios). | | |

Tabla 11: Cuadro Comparativo de categorías de Clasificación de la Información de acuerdo a los países / Buenas prácticas analizadas.

Elaboración propia Tesis "Cumplimiento, Seguridad y clasificación de la información para Cloud Computing y Cloud Storage", Rodrigo Lopez Villafañe, 2018.

### 4.1.12 Cloud Computing como RegTech

Las Regulation Technologies (RegTechs), incluyen el uso de tecnologías, en particular tecnología de la información (TI), en el contexto del monitoreo, la presentación de informes y el cumplimiento normativas. Para los reguladores, RegTech proporciona los medios para avanzar hacia un enfoque basado en el riesgo, donde el acceso y la gestión de los datos son más detallada y efectiva.

Debido a las Finntech (Financial Technologies) la industria de servicios financieros se vuelve cada vez más digital y la brecha entre los costos y los costos de cumplimiento y monitoreo manual y automático se está ampliando (Regulaciones). Combinado con los avances recientes en ciencia de datos y análisis, el crecimiento de RegTech se puede entender como automatización de procesos para reduccion de acciones regulatorias y multas.(Arner, Barberis, & Buckley, 2016).

Hoy en día, empresas que brindan servicios de CC, están implementando Regulation Technologies para lograr que no solo clientes, puedan cumplir sus requisitos regulatorios sino también el mismo proveedor.

Como ejemplo podemos observar AWS “re:Invent”, un socio/partner de AWS que se encarga de implementar tecnologías de GRC (Gobierno, Riesgo y Cumplimiento) para el beneficio de los clientes de AWS y que cumplan con los requisitos regulatorios.

Beneficios:

Desde una perspectiva regulatoria, RegTech permite la posibilidad de un monitoreo continuo que mejoraría el desempeño general de una infracción regulatoria. Además ofrece la capacidad de monitoreo continuo, brindando información cercana a tiempo real, a través del aprendizaje profundo y filtros de inteligencia artificial (IA), en el funcionamiento de los mercados a nivel nacional y mundial. Esto permitiría a los reguladores tomar acción proactivamente en vez de esperar a que ocurre el acto o catástrofe.

### 4.1.13 Conclusión del estado del Arte

A partir de la identificación y revisión de textos de autores relacionados a Seguridad en Cloud Computing y regulaciones de protección de datos, podemos observar que existen diferentes regulaciones que tratan de contener la protección de datos CC. Sin embargo las mismas se encuentran desactualizadas o no pueden seguir los pasos y velocidad de evolución de la tecnología.

Por otro lado, podemos observar que existen varios papeles de trabajo, estudios y tecnologías (RegTechs), que analizan los riesgos/amenazas que afectan tanto a proveedores de CC, como a sus empresas clientes y usuarios finales, sin embargo estas tecnologías están a disposición de la empresas, no así la manera de utilizarlas.

Por último, podemos observar que se hacen varias referencias por dichos autores a una clasificación de la información y segregación de la misma, para mantener la privacidad de la información, en relación con el usuario. Si bien considero esto acertado, es necesario hacer una segregación y clasificación de la información más detallada, no solo en relación a la información del usuario, sino a la clasificación de la misma en cuanto al tipo de empresa y de procesos que involucran al CC de la misma.

# 5. Cloud Computing y Cloud Storage en la Argentina.

## 5.1 Estadísticas referentes a la adopción de regulaciones y estándares de Cloud Computing y Cloud Storage en la Argentina.

Los mercados emergentes continúan rezagados en la adopción de políticas favorables a la nube.

La Software Alliance mostró mediante un estudio que evalúa las políticas informáticas en la nube en todo el mundo, que la Argentina se encuentra en la posición 17/24 en las economías de TI. Cayendo un lugar desde el año anterior, demostrando que el entorno legal y regulatorio para la computación en la nube está estancada en la innovación.(Itsitio, 2018)

El reporte BSA Global Cloud Computing Scorecard 2018, presenta la metodología que refleja las políticas que ayudan al crecimiento exponencial de la computación en la nube en los últimos 5 años, poniendo énfasis en las leyes nacionales de privacidad y seguridad, y en la infraestructura de banda ancha.

Tabla 12: Criterios de Scorecard BSA Global Cloud Computing 2018 para Argentina y clasificación en posición 17 de escala de países.

| Orientación al desarrollo de acuerdo con BSA Global Cloud Computing | |
|---|---|
| Privacidad de datos | |
| ¿Hay alguna ley de protección de datos o regulación existente? | Si |
| ¿Que alcance tiene la ley de protección de datos o regulación? | Comprehensivo |
| ¿Hay alguna autoridad de protección de datos? | Si (Dirección de datos personales) |

| | |
|---|---|
| ¿Cuál es la naturaleza de la autorizada de protección de datos? | Comisionado de venta |
| ¿La autoridad de datos, esta aplicando la ley de datos o regulación de una manera efectiva? | Si |
| ¿Es la ley o regulación de protección de datos compatible con marcos reconocidos a nivel mundial que facilitan transferencias de datos internacionales? | Si, con el marco de trabajo de la EU |
| ¿Los controladores de datos están libres de requisitos de registro? | No |
| ¿Existen requisitos de transferencia de datos transfronterizos? | Requerimientos detallados |
| ¿Las transferencias de datos transfronterizas están libres de restricciones arbitrarias, injustificables o desproporcionadas, como requisitos de localización de servidores o datos nacionales o sectoriales específicos? | Parcialmente |
| ¿Hay una ley o reglamento de notificación de violación de datos personales? | No |
| ¿Los requisitos de notificación de violación de datos personales son transparentes, basados en el riesgo y no demasiado preceptivos? | No aplica debido a la pregunta anterior |
| 82/5000<br>¿Existe un derecho de acción privado e independiente disponible por incumplimiento de la privacidad de los datos? | Si |
| Seguridad | |
| ¿Existe una estrategia nacional de ciberseguridad? | Si, pero está en borrador |
| ¿La estrategia nacional de ciberseguridad es actual, completa e inclusiva? | No aplica |

| | |
|---|---|
| ¿Existen leyes o directrices apropiadas que contengan requisitos de seguridad generales para los proveedores de servicios en la nube? | Parcialmente |
| ¿Las leyes o la orientación sobre los requisitos de seguridad son transparentes, están basadas en el riesgo y no son excesivamente preceptivas? | Parcialmente |
| ¿Existen leyes o directrices apropiadas que contengan requisitos específicos de auditoría de seguridad para los proveedores de servicios en la nube que tengan en cuenta la práctica internacional? | Parcialmente |
| ¿Los estándares de seguridad internacional, la certificación y las pruebas se reconocen como requisitos locales? | No |
| Cibercrimen | |
| ¿Existen leyes o regulaciones de cibercrimen? | Si |
| ¿Son consistentes las leyes o regulaciones de cibercrimen con la Convención de Budapest sobre cibercrimen? | Si |
| ¿Las leyes y políticas locales sobre el acceso de las fuerzas del orden a los datos evitan los mandatos específicos de la tecnología u otras barreras al suministro de productos y servicios de seguridad? | Si |
| ¿Existen acuerdos para el intercambio transfronterizo de datos con fines policiales transparentes y justos? | Si |
| Derechos de propiedad intelectual | |
| ¿Existen leyes o regulaciones de derechos de autor compatibles con las normas internacionales para proteger a los proveedores de servicios en la nube? | Parcialmente |

| | |
|---|---|
| ¿Las leyes o regulaciones de derechos de autor se aplican e implementan efectivamente? | No |
| ¿Existe una protección legal clara contra la apropiación indebida de secretos comerciales? | Si |
| ¿Se aplica efectivamente la ley o regulación sobre secretos comerciales? | No |
| ¿Existe una protección legal clara contra la elusión de las Medidas de Protección Tecnológica? | Si |
| ¿Se aplican efectivamente las leyes o reglamentos sobre la elusión de las Medidas de Protección Tecnológica? | No |
| ¿Existen protecciones legales claras para las invenciones implementadas por software? | Si |
| ¿Se aplican efectivamente las leyes o reglamentos sobre la protección de las invenciones implementadas por software? | Parcialmente |
| Estándares y Armonización internacional | |
| ¿Existe un organismo regulador responsable del desarrollo de normas para el país? | Si |
| ¿Están los estándares internacionales favorecidos sobre estándares domésticos? | Parcialmente |
| ¿El gobierno participa en el proceso de establecimiento de normas internacionales? | Si |
| ¿Existen leyes o regulaciones de comercio electrónico? | No |
| ¿En qué instrumentos internacionales se basan las leyes o reglamentos de comercio electrónico? | No aplica |
| ¿Existe alguna ley o reglamento que otorgue a las firmas electrónicas un peso legal claro? | Si |
| ¿Los proveedores de servicios en la nube están libres de filtrado obligatorio o censura? | Si |

| Promoción de libre intercambio | |
|---|---|
| ¿Existe una estrategia o plataforma nacional para promover el desarrollo de servicios y productos en la nube? | No |
| ¿Existen leyes o políticas vigentes que implementen la neutralidad tecnológica en el gobierno? | No |
| ¿Los servicios de computación en nube pueden operar libres de leyes o políticas que imponen o dan preferencia al uso de ciertos servicios, estándares o tecnologías de productos? | Si |
| ¿Los servicios de computación en nube pueden operar libres de leyes, políticas de adquisición o reglas de licencia que discriminen según la nacionalidad del proveedor, desarrollador o proveedor de servicios? | Parcialmente |
| ¿Ha firmado e implementado el país acuerdos internacionales que aseguren que la adquisición de servicios en la nube esté libre de discriminación? | No |
| ¿Los servicios ofrecidos por proveedores de la nube están libres de aranceles y otras barreras comerciales? | No |
| ¿Los servicios de computación en nube pueden operar libres de leyes o políticas que imponen requisitos de localización de datos? | Si |
| Preparación IT, Despliegue de banda ancha | |
| ¿Hay un plan nacional de banda ancha? | El plan Argentina Conectada 2010 promovió la inclusión digital, pero no incluyó objetivos nacionales específicos. No existe una estrategia nacional de banda ancha. |
| ¿El Plan Nacional de Banda Ancha se está implementando efectivamente? | Parcialmente |
| ¿Existen leyes o políticas que regulan la "neutralidad de la red"? | Regulaciones extensivas |

Tabla 12: Criterios de Scorecard BSA Global Cloud Computing 2018 para Argentina y clasificación en posición 17 de escala de países.

Elaboración propia en base a BSA Global Cloud Computing Scorecard 2018, (BSA, 2018).

Que es el Scorecard:

Al examinar el marco legal y regulatorio de 24 países, el Scorecard busca ofrecer una plataforma para el debate entre los responsables de la formulación de políticas y los proveedores de servicios en la nube. Este diálogo puede ayudar a desarrollar un régimen internacional armonizado de leyes y regulaciones que faciliten la computación en la nube.

Conclusiones obtenidas a partir de Scorecard (BSA, 2018).

1. Al no adoptar leyes de privacidad adecuadas algunos países impiden el crecimiento del mercado en la nube. Esto podrían evitarlo logrando políticas de privacidad y seguridad avanzadas, perfeccionando regímenes de protección de datos personales, permitiendo el flujo entre fronteras de datos.

2. En los mercados emergentes se observa la falta de adopción de políticas favorables en la nube, que dificultan su crecimiento. Entre otros algunos ejemplos son, la falta de seguridad de datos, requisitos de localización y regulaciones.

3. Falta de alineación entre los estándares locales y las prácticas recomendadas internacionalmente. Es decir los estándares, certificaciones y pruebas aceptadas

internacionalmente ayudan a mejorar la seguridad Cloud, sin embargo los estándares locales no están alineados con las mismas. Entre estos casos se puede observar Argentina, India, México y Sudáfrica).

4. Las políticas de localización de datos se consideran una barrera para el Cloud Computing, lo que genera impactos financieros negativos para los mercados locales.

5. A partir de la utilización de Cloud Computing surge la necesidad de una red potente. El éxito en iniciativas de mejora de banda ancha es variado, pero necesario para la adopción de Cloud Computing.

6. Argentina Mexico y Vietnam no han implementado estrategias nacionales de ciberseguridad, promoviendo la administración unificada entre público y privada de la ciberseguridad.

7. Si bien las tarifas y barreras para el intercambio de software y aplicaciones son raras, dificultan nuevos productos tecnológicos usados para acceder a servicios Cloud en algunos países. Argentina, Brasil y Rusia son aquellos países que más dificultan el intercambio de software.

## 5.2 Regulaciones de protección de datos como desarrolladores de competitividad nacional en latino-américa.

La adopción de la nube se encuentra en una etapa inicial en Latino-América y se esperan crecimientos de un 70% anual en este mercado. Las decisiones que son tomadas hoy por los que hacen las políticas y las partes interesadas van a definir cuanto se pueden beneficiar los ciudadanos de determinadas naciones y en la región, de esta tecnología en el corto y mediano plazo. Dichas políticas no solo definirán como se utilizará los beneficios brindados por el Cloud Computing, sino que también afectará la competitividad a nivel nacional, afectando productividad y eficiencia (Gutiérrez & Korn, 2017).

Por otro lado Martin Wessel, Technology Evolution Manager en Telecom, comentó que si bien se pretende que el regulador, haga análisis "Ex post" y "Ex ante" o detectivos y preventivos, debemos tener en cuenta que CC y CS se encuentran en una etapa de adopción en la Argentina, y muchas veces la aplicación de regulaciones reduce o frena la innovación como es en este caso la aplicación de nuevas tecnologías para empresas nacionales. (Martin Wessel, entrevista telefónica, 10/07/2018).

### 5.2.1 El interés de reglas de protección de datos en la nube.

En América Latina, el interés en la protección de datos también está en aumento. Desde la década de 1980, muchos gobiernos en América Latina han proporcionado un derecho constitucional para que las personas tengan acceso a corregir sus datos personales. También conocido como "habeas data", esta protección está destinada a "salvaguardar la libertad

individual del abuso en la era de la información. "Habeas asegura" un control real sobre datos personales sensibles, deteniendo el abuso de dicha información, lo cual será perjudicial para el individuo. Debido a que estas disposiciones de Habeas Data están típicamente en constituciones nacionales, reciben "el mayor nivel de protección posible, más rápidos procedimientos y los mejores tribunales usualmente lo acompañan. " Por ejemplo, la Sección 43 (3) de la Constitución de Argentina proporciona un fuerte Habeas fuerte:

"Cualquier persona deberá presentar esta acción para obtener información sobre datos sobre sí mismo y su propósito, registrados en registros públicos/privados o bases de datos, y en caso de datos falsos o discriminación, esta acción puede presentarse para solicitar la supresión, rectificación, confidencialidad o actualización de dichos datos. La naturaleza secreta de las fuentes de información periodística no deberán ser perjudicadas"

Desde el 2000, los países de América Latina están pasando leyes de protección de datos intensivas que se modelan según la directiva de protección de datos de Europa de 1995. Estas leyes varían ampliamente, pero generalmente contienen restricciones a la nube sobre el uso y la transferencia de datos, requieren consentimiento expreso del interesado antes del proceso, permiten a las personas acceder y corregir cada interacción posible de sus datos personales.

Un caso ilustrativo de es Colón la compañía de seguros de Argentina:

Si bien Colón Seguros fue la primera empresa de seguros en aplicar su infraestructura en la nube (E-colon y Colon asistencias), lo más relevante de este caso es el marco legal. Debido

a que no existía el conocimiento, no estaban alineados y no estaba íntegramente definido en las leyes Argentinas la protección de datos personales para proveedores de nube. Se le presentó (En conjunto con AWS) a la Dirección de datos personales, como se cumplía con la GDPR (Global Data Protection Regulation) perteneciente a la Unión Europea. Dado que el marco legal está basado en la EU, la compañía Colon no encontró problemas a la hora de cumplir con las regulaciones nacionales para el manejo de datos personales (Frias, 2018).

En el 2000, Argentina lanzó la primera ley de protección de datos exhaustiva, que compartía muchas de las directivas Europeas pre-Cloud.

Adoptando leyes del estilo EU en el 2000, para el 2003 la comunidad Europea aceptó su determinación y adecuación. Como cuestión general, las transferencias de datos internacionales desde Argentina son prohibidas a menos que el interesado otorgue un consentimiento expreso previo si el país de destino no tiene lo que el regulador argentino considera que son leyes "adecuadas". No se ha establecido un "puerto seguro" para facilitar los flujos de datos a países que no se consideran "Adecuados".

Por otro lado empresas como Forrester Wave analizan proveedores de administradores de nube Hibrida entre otros, con diferentes reportes y aplican diferentes criterios de evaluación para su análisis. Entre ellos los clientes se analizan por su compliance hacia diferentes regulaciones y políticas de seguridad tanto nacionales como internacionales (Bartoletti, O'Donnell, E. Nelson, & Caputo, 2018).

En Argentina, la Dirección Nacional de Protección de Datos Personales estableció los criterios de utilización de computación en la nube por parte de cualquier organización, pública

o privada en el caso de contratar a una empresa del exterior. El contratante debe asegurarse de cumplir con la Ley Argentina de Protección de Datos (25.326) y de la disposición 60 del 18 de noviembre de 2016 de la misma DPDP que exige firmar con el proveedor un Acuerdo de transferencia Internacional de Datos (comúnmente llamado DTA). Este Acuerdo garantiza entre otros puntos la aplicación de la ley y jurisdicción argentina para la transferencia de datos, el reconocimiento por ambas partes de la supervisión de la dirección Nacional de Datos Personales y que, ambos son eventuales responsables por los incumplimientos contractuales frente a los titulares de los datos (Prince, 2017).

### 5.2.2 Beneficios de Cloud Computing en Latino América

1. Creación de trabajos a través de la innovación: La implementación de Cloud Computing genera nuevos trabajos a través de la innovación local. Esto es debido a que los costos de inversión inicial en infraestructura se reducen en gran manera. Millones de estos trabajos son los que el mercado latino intenta atraer.

Por ejemplo, en un estudio publicado por la Comisión Económica para América Latina y el Caribe (CEPAL o CEPAL), el análisis de los economistas Andrea Colciago y Federico Etro encontró que la adopción de computación en la nube por parte de las empresas en Brasil podría generar de 900,000 nuevos empleos. Del mismo modo, el Instituto Mexicano para la Competitividad (IMCO) descubrió recientemente que con la tecnología de la nube, México puede crear 1.800 nuevas pequeñas y medianas empresas, empleando en total unos 63.400 empleados. Esto se basa en una estimación conservadora de los ahorros de solo el uno por ciento de los costos fijos de las empresas debido a los beneficios de la nube.

2. Ahorro de Costos: Debido a los ahorros en los costos de infraestructura se estima que los países en el rubro de IT ahorrarán en costos estimativamente en un 20% a 30%, debido a la mínima inversión inicial en una conexión de internet para acceder a estos servicios.

Desde el punto de vista del proveedor también se pueden observar ahorros en electricidad, ya que los data center a gran escala requieren menos electricidad para operar mayor cantidad de servidores, resultando en menores emisiones de carbono.

3. Democratización del cómputo e inclusión social: Al ser tan accesible por parte de los clientes, permite que pequeñas y medianas empresas tengan acceso a tecnologías a las cuales no era posible sin grandes inversiones de capital iniciales. Se prevee en Argentina grandes crecimientos de clientes en la nube para los cuidados medicos.

4. Aumento de Agilidad: La flexibilidad en cuanto a los requisitos del cliente, es un fuerte para Cloud Computing debido a que le permitió achicar o aumentar la demanda de servicios a voluntad a cliente, sin necesidad de inversiones fuertes iniciales.

5. Seguridad: Si bien, se puede interpretar que al usar la nube la información puede ser más vulnerable, se ha comprobado, mediante estadísticas de ataques que esto no es real. Pequeñas y medianas y medianas empresas ahora tienen acceso a técnicas de seguridad superiores debido a que las compañías proveedoras de Cloud Computing, poseen y se especializan en la seguridad en la nube. Esto permite una mejora en todo el ambiente de

seguridad relacionado para el cliente que pasó a tener sus servidores en la nube (Gutiérrez & Korn, 2017).

### 5.3 Principios básicos para una regulación general balanceada de protección de datos en la nube.

Tabla 13: Principios básicos para una regulación general balanceada a ser tenidos en cuenta por agentes regulatorios.

| Protección de Datos | Mayor transparencia | Transferencia de datos entre fronteras | Armonización de reglas de protección de datos e Interoperabilidad | Reforzar las fuerzas contra el cibercrimen |
|---|---|---|---|---|
| Los reguladores deben asegurarse que los clientes tengan visibilidad sobre la manera en que se están | Las regulaciones de privacidad y seguridad de datos deben brindar información sobre los programas de seguridad y salvaguardas, | La transmisión de datos entre países es una ventaja que ofrece la nube. Las regulaciones impiden a veces la transmisión de datos entre países debido a falta de adecuación de regulaciones de otros países a las | Las reglas de protección de datos varían país a país. Solo a través de la colaboración de gobierno a gobierno se pueden hacer reglas accesibles. Los gobiernos podrían comenzar | El objetivo de atacar estos 3 puntos es reforzar la credibilidad del cliente en la nube: 1) crímenes contra ciudadanos |

| | | | | |
|---|---|---|---|---|
| protegiendo los datos del cliente. Teniendo como metas: Asegurar la seguridad de los datos, proteger la privacidad del consumidor y crear confianza en la nube. | brindar resúmenes de esos programas a los clientes y divulgar sus prácticas de privacidad a cualquier cliente. | propias (Ej.: EU con otros países que no son Argentina o Uruguay). Si bien, las compañías de nube pueden crear datacenters locales, a largo plazo estos países se verán afectados. | trabajando para desarrollar reglas que faciliten el flujo de datos a través de las fronteras nacionales y regionales. O juntos para desarrollar y acordar principios compartidos en una nube. | individuales, tales como ataques a niños, 2) crímenes contra naciones como el terrorismo, Y 3) delitos económicos como el fraude con tarjetas de crédito. |

Tabla 13: Principios básicos para una regulación general balanceada a ser tenidos en cuenta por agentes regulatorios.

Elaboración Propia en base a BSA Scorecard 2018.

# 6. Casos de Estudio.

## 6.1 Amazon Web Services y Compliance.

Capa de Virtualización en Cloud Computing: Es la capa que permite correr varios servidores virtuales, aplicaciones o servicios en un mismo servidor físico. Amazon lo usa para poder compartir servidores entre clientes.

Si bien Amazon no se hace responsable por la configuración que tienen sus clientes en la infraestructura proporcionado por AWS, esta comunica su seguridad de la siguiente manera:

1. Obteniendo certificaciones específicas de industria, y aprobaciones de empresas que brindan soporte (Terceras partes).

2. Publicando información sobre la seguridad de AWS y prácticas de controles en el sitio web.

3. Dando reportes, certificados y otra documentación requerida por los clientes de AWS bajo NDAs (Non disclosure Agreements).



### 6.1.1 Responsabilidad Compartida

Mover la infraestructura IT de una empresa a AWS crea un modelo de responsabilidad compartida. En este modelo de responsabilidad compartida, AWS se encarga de administrar, operar y controlar los componentes desde el sistema operativo principal y la

capa de virtualización hasta la seguridad física de las facilidades en las cuales opera el servicio. Esta división permite al cliente cumplir con requerimientos específicos de industria.

### 6.1.2 Modelo de Seguridad Compartida de Amazon

En la figura 2, se observa el modelo de responsabilidad compartida para la información de clientes en AWS.

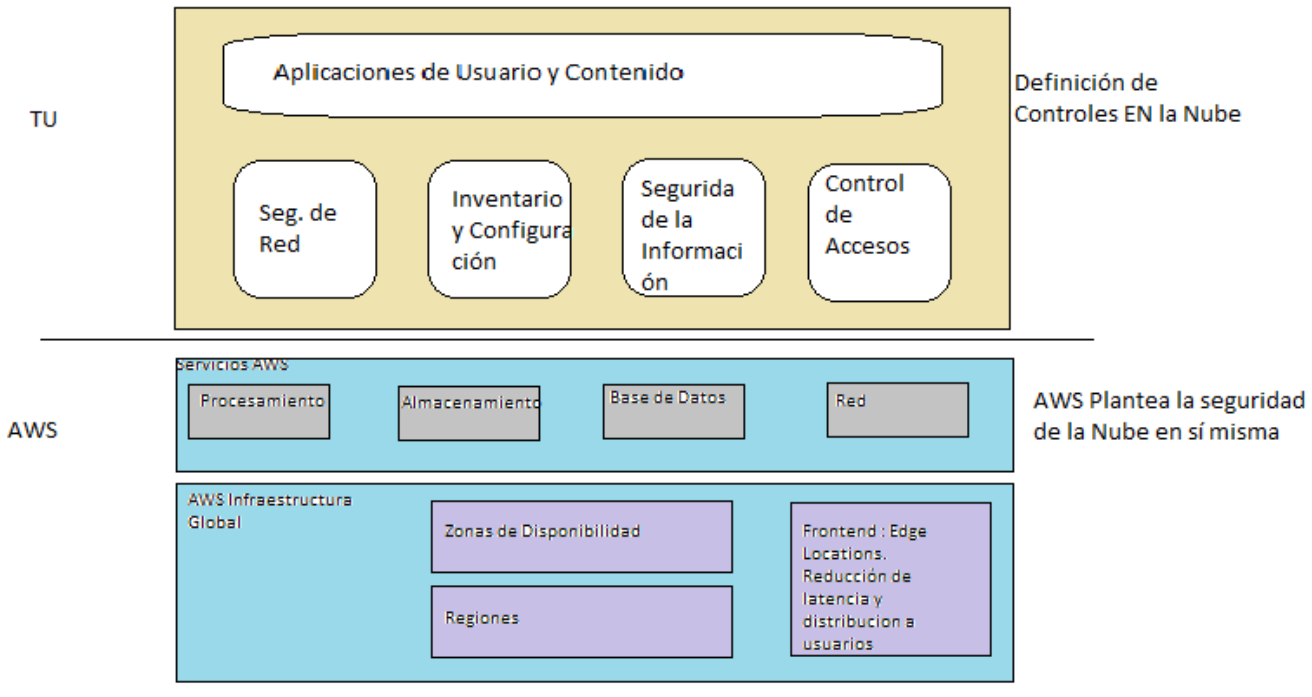


Figura 2: Modelo de Responsabilidad Compartida para la información de clientes en AWS.

Elaboración propia en base a documento "Amazon Web Services: Risk and Compliance", 2017.

Básicamente, se acuerda que AWS se hará cargo de la seguridad de la infraestructura del Cloud, sin

embargo no se responsabilizará por la información que se esté utilizando en los servidores AWS. Los controles internos de las cargas de trabajo serán llevados a cabo por el cliente. Esto no solo se debe, a querer brindar una mayor flexibilidad al cliente, sino también porque la información de todos los clientes es diferente y debe ser tratada de acuerdo a los objetivos de cada compañía.

Asimismo Julio César Fuoco, Asesor de Empresas en Management, Tecnología y Procesos, cuando se indagó sobre el mismo tema, comentó que en los proveedores de nube observaba dos tipos de servicios: Housing (Administración de servidores por parte del cliente) y Hosting (Administración de servidores y alarmas por parte del proveedor). Si bien estas diferencias pueden ser poco significativas, a la hora absorber la responsabilidad regulatoria, son un gran factor. En Axton, empresa de tecnología de procesos, decidió utilizar Housing, para poder hacer frente a regulaciones que no eran concernientes al proveedor. (Julo Cesar Fuoco, entrevista telefónica, 24/05/2018).

A su vez AWS ofrece herramientas de seguridad desde diferentes aspectos:

- Seguridad de la red: Aumentan la privacidad y control del acceso a la red:

- Firewalls, para crear redes privadas dentro de AWS.

- Encriptación en la capa de transporte.

- Opciones de conectividad para crear conexiones privadas o dedicadas con sistemas On Premise.

- Tecnologías para mitigación de taques DDOS.

- Inventario y gestión de la configuración: Permite la rápida respuesta ante estándares y mejores prácticas.

- Empleo de herramientas para administración de recursos dentro AWS de acuerdo con estándares de la organización.

- Utilización de herramientas para el trackeo de cambios.

- Creación de templates estándar pre-configurados para las máquinas virtuales de EC2

- Encriptación de Datos: La Data en descanso (Data at Rest) puede ser encriptada de manera eficiente y escalable en la nube.

- Capacidad de encriptación de datos en AWS storage y bases de datos como EBS, S3, Glacier, Oracle RDS, SQL Server RDS y Redshift

- Gestión de claves para encriptación flexibles.

- Para el cumplimiento con regulaciones, almacenamiento de claves criptográficas con equipos dedicados.



- Control de Accesos: Creación de políticas de acceso en los servicios de AWS.

- Identificación de acceso en todos los recursos de AWS.

- Identificación multifactor.

- Integración con directorios corporativos para reducir al máximo el trabajo administrativo.

- Monitoreo y registro de actividades:

- Visibilidad en las APIs para ver desde donde se hacen las llamadas al WS.

- Opciones de creación de logs.

- Opciones de alerta ante eventos o límites.

A su vez AWS permite mediante "AWS Professional Services and AWS Partner Network" asesoría para lograr compliance con diferentes regulaciones en todo el mundo.

Cumplimiento con regulaciones: Actualmente la infraestructura AWS cumple las siguientes regulaciones:

- ISO 27001
- FedRAMP
- DoD CSM
- PCI DSS

A su vez AWS cumple con las leyes de protección de datos de la EU. Permitiendo a sus clientes saber que la data personal está siendo tratada con el mismo grado de protección de la EA.

De esta manera AWS, logra que las compañías cumplan con las regulaciones existentes a un costo menor. (Amazon, 2015)

### 6.1.3 Controles IT AWS

AWS provee información sobre sus controles IT de las siguientes 2 maneras:

1. Definición específica de controles: AWS publica una gran cantidad de controles IT en sus reportes de SOC1 (Service Organization Controls 1 (SOC 1) Type II report), para auditorias anuales financieras. El SOC1 es un estándar mundialmente reconocido por el AICPA (American Institute of Certified Public Accountants).

Este reporte es una auditoria tanto de efectividad de diseño y operatividad de los objetivos y actividades de control definidos por AWS (Esto incluye la definición de objetivos y actividades de control sobre la infraestructura que maneja AWS). Que el reporte SOC1 sea de tipo II indica también que la efectividad y el diseño hayan sido auditados por auditores externos. (Entre otras regulaciones SOX (Ley Sarbanes Oxley) e ISO 27001 pueden pedir este reporte).

2. Compliance estándar de controles generales: Debido a su certificación sobre ISO 27001, AWS cumple con los estándares y mejores prácticas de seguridad en sus ambientes.

A su vez debido al cumplimiento de la regulación PCI (Payment Card Industry) cumple con un conjunto de controles necesarios para compañías que manejan pagos con tarjetas de crédito.

Por último, Debido a su cumplimiento con los estándares FISMA (Federal Information Security Management Act - legislación para proteger información de gobierno y operaciones y activos), puede cumplir con los requisitos de agencias de gobierno.

### 6.1.4 Administración de Riesgos

AWS ayuda a identificar a sus clientes en su plan de negocios, los riesgos existentes y las áreas responsables para tratar dichos riesgos.

Además de dicho ambiente de control, se crea un ambiente de seguridad y políticas basadas en COBIT (Control Objectives for Information and related Technology), integrado con ISO 27001, AICPA (American Institute of Certified Public Accountants), PCI DSS v3.2 (Payment Card Industry) y NIST (National Institute of Standards and Technology).

AWS hace escaneos de vulnerabilidades en sus sistemas y los del cliente, para poder certificar la seguridad de la infraestructura en servicio, sin embargo esto no reemplaza la necesidad de un escaneo de vulnerabilidades desde el lado del cliente (Vulnerability Tests/ Penetration Tests).



Ambiente de control

El ambiente de control está compuesto de los siguientes conceptos:

1. Políticas
2. Procesos
3. Actividades de control.

### 6.1.5 Certificaciones AWS, Programas, Reportes, Confirmación de Proveedores

AWS se certifica con terceras partes y auditores independientes para proveer a sus clientes información relevante respecto a las políticas, procesos y controles establecidos. Algunos de las terceras partes son:

1. CJIS (FBI's Criminal Justice Information Services): Revisión de clientes mediante los estándares de CIJS. Algunas de las funcionalidades que permiten cumplir con estos estándares de seguridad son: AWS CloudTrail - Registro de actividades, S3 Server-Side Encryption - encriptación, IAM federated identity management - Identificación multifactor en la nube).

2. CSA (Cloud Security Alliance): STAR es una iniciativa de la CSA para hacer transparente los controles de seguridad propuestos por proveedores en la nube, para que los clientes puedan tomar decisiones sobre proveedores basados los controles de seguridad que brindan los mismos.

3. Cyber Essential Plus: Es una certificación del gobierno de Inglaterra, que ayuda a las organizaciones a demostrar seguridad operacional con cyber-ataques comunes. Se establecen los controles técnicos necesarios y el ambiente de trabajo necesario, mediante una certificación anual externa acreditada por un asesor. El alcance de la certificación abarca solamente la EU.

4. DoD (Department of Defense): El modelo de seguridad Cloud (SRG) provee un testeo formalizado y proceso de autorización para proveedores de nube, para así obtener una

autorización provisional del DoD. Esto provee una certificación reusable que atestigua el cumplimiento de los estándares del DoD.

5. FedRAMP (Federal Risk and Authorization Management Program). Requerido por agencias del gobierno en la transmisión de cargas de trabajo en un ambiente Cloud.

6. FERPA (Familiy Educational Rights and Privacy Act): Es una ley federal que protege la privacidad de registros estudiantiles. Esta ley aplica a escuelas que están bajo inversiones de departamento de educación de estados unidos.

7. FIPS (Estándar de procesamiento de información federal): Estándar del gobierno de EEUUU que detalla los requerimientos de seguridad para módulos criptográficos que protegen información sensible. (Para evitar problemas se usan

8. GxP: Lineamientos y guías de trabajo aplicado para organizaciones de ciencias que hacen comida y productos como drogas, dispositivos y aplicaciones médicas.

9. HIPAA (Health Insurance Portability and Accountability Act): Este acto permite a AWS manejar información protegida relacionada con salud

10. IRAP (Information Security Registered Assessors Programa) permite al gobierno australiano, validar para los clientes, que realizan los controles apropiados y

determinados para un modelo de responsabilidad de acuerdo con el ASD-ISM (Australian Signal Directorate Information Security Manual).

11. ISO 9001: Esta certificación provee soporte a clientes que desarrollan, migran y operan sus sistemas de calidad controlados por IT en la nube. Se pueden utilizar los reportes de certificación ISO 90001 para apalancar otras certificaciones como son GxP (Ciencias de la vida), ISO 13485 en dispositivos medicos, AS9100 en Aero espacio e ISO /TS 16949 en automóviles.

ISO 90001:2008 es un estándar para la administración de productos y servicios. Los principios de este estándar son:

A- Foco en el consumidor

B- Liderazgo

C- Involucramiento de la gente

D- Procedimientos

E- Administración de sistemas

F- Mejora Continua

G- Aproximación fáctica a la toma de decisiones

H- Relación mutuamente benéfica con proveedores

12. ISO 27001/27002: Certificación para administración de sistemas de información, que cubre la infraestructura de AWS, los data centers y los servicios. Se trata de un estándar que establece los requerimientos y mejores prácticas para la administración de compañías e información de clientes basado en análisis de riesgos periódicos de cambios de

escenarios de amenazas. Para poder certificar una compañía debe demostrar que tiene una aproximación sistemática para el tratado de riesgos de seguridad que afectan la confidencialidad, integridad y disponibilidad de información de la compañía y/o cliente.

13. ISO 27017: Guía de implementación para controles de seguridad de la información que se relaciona específicamente a servicios Cloud. AWS se encuentra certificado.

14. ISO 27008: Es el primer estándar internacional que hace foco en la protección de datos personales en la nube. Está basado en ISO 27002 y provee una guía de implementación sobre controles aplicables Información Identificable Personal pública en la nube (PII). AWS se encuentra certificado, mediante el ISMS (Information security management system), cubriendo la infraestructura, data centers y servicios.

15. ITAR (US International Traffic in Arms Regulations Compliance): Las compañías sujetas a la regulación ITAR de exportación deben controlar exportaciones no intencionadas restringiendo el acceso a personas de USA y restringiendo la información física a USA. AWS GovCloud (US) provee un ambiente físicamente localizado en USA cumpliendo con ITAR.

16. MPAA (Motion Picture Association) mejores prácticas para guardar procesar y entregar contenido de media. Mayormente utilizado por contenidos de media.

17. MTCS (Multi-Tier Cloud Security) Tier 3 Certification: Estándar de administración de seguridad operacional, basado en los estándares de Information Security Mangement Systems (ISMS) de ISO 270001/02. Obligando a AWS a:

1. Evaluar Sistemáticamente riesgos de seguridad, teniendo en cuenta amenazas y vulnerabilidades de la compañía.

2. Designar e implementar una suite de controles de seguridad de la información para mitigar los riesgos de seguridad.

3. Hacer de la designación e implementación de procesos un proceso continuo para que se adapte los cambios de la compañía.

18. NIST (National Institute of Standards and Techonology): Se presentaron las guías de trabajo 800-171 "Guía de trabajo finales, para la protección de información sensible del Gobierno por terceras partes" (Para sistemas no federales). AWS ya cumple con esta guía de trabajo, y fácilmente los clientes de AWS pueden cumplir con dichas guías.

19. PCI DSS Level 1: (PCI) Payment Card Industry Data Security Standar (DSS). AWS afirma que su infraestructura cumple con los estándares de PCI para el almacenamiento, procesamiento y transmisión información de tarjetas de crédito en la nube.

20. SOC1 (Service Organization Controls reporte de tipo II). Este reporte esta realizado en acuerdo con el AICPA (American Institute of Certified Public Accountants) en conjunto con 801 (Anteriormente conocido como el SSAE16 - Reporte de cumplimiento de controles físicos para datacenters) y la ISAE (International Standards for Assurance

Engagements). Estos dos reportes permiten cumplir con un conjunto de requerimientos de auditoria financieros (SOX) para EEUU y cuerpos de auditoria internacionales.

Objetivos de Controles SOC1 (El reporte en sí mismo muestra los objetivos y los procedimientos de la aplicación de los controles por un auditor independiente):

1. Seguridad de la Organización: Controles que aseguran que las políticas de seguridad han alcanzado toda la organización

2. Acceso de Usuario Empleado: Controles que asegurada que las cuentas de usuarios de empleados de Amazon fueron creadas, modificadas y borradas de una manera periódica y con revisión.

3. Seguridad Lógica: Controles que aseguran que la información está apropiadamente resguardada, debido a una correcta segregación de funciones para accesos internos y externos.

4. Manejo de información Seguro: Controles que aseguran que la información está segura en el mapeo entre el cliente y los servidores de AWS.

5. Seguridad Física y Protección del ambiente: Controles que aseguran que el acceso físico está restringido a personal autorizado y que los mecanismos para malfuncionamiento y desastres físicos funcionan correctamente.

6. Administración de Cambios: Controles que aseguran (De emergencia/ y no rutinarios) que los cambios a los recursos IT están autorizados, testeados aprobados y documentados.

7. Integridad, disponibilidad y redundancia de la información: Controles que aseguran que la seguridad de los datos es mantenida a los largo de todas las fases de transmisión, almacenamiento y procesamiento.

8. Manejo de Incidentes: Controles que aseguran que los incidentes sean analizados, resueltos y registrados.

Estos controles están dedicados a auditorías financieras. Vale aclarar que este reporte es un reporte confidencial.

21. SOC2 (Service Organization Controles Reporte tipo 2): Cubre los mismos servicios que el reporte SOC1, sin embargo también trata los siguientes principios de manejo de la información para organizaciones de servicio: Seguridad, disponibilidad, integridad en el procesamiento, confidencialidad y privacidad. Vale aclarar que este reporte es un reporte confidencial.

22. SOC3 (Service Organization Controls reporte tipo 3): Es un reporte público en resumen del reporte SOC2. El reporte incluye una opinión de un consultor externo y su evaluación en cuanto a la efectividad de los controles realizados por AWS, su evaluación general e infraestructura y servicios.

### 6.1.6 Aplicación de casos de compliance AWS en respuestas a Clientes.

1. ¿Quién es el responsable de que controles? AWS se hará cargo los controles referentes al a infraestructura. Todos los demás son responsabilidad de sus clientes, incluyendo conexiones.

2. ¿Cómo se puede auditar a un proveedor de nube? Debido a que todos los controles por encima de la capa de infraestructura se encuentra fuera de la responsabilidad de AWS, los controles físicos se encuentra en el reporte SOC1 tipo 2 y es un reporte disponibles para revisión de auditoria y equipos de compliance.

3. ¿Cómo se obtiene SOX compliance, si hay sistemas abarcadas que se encuentren el ambiente de la nube del proveedor? Si el cliente procesa información financiera en la nube, entonces los auditores del cliente pueden definir que algunos equipos de AWS pueden tener en cuenta para la certificación SOX. Debido a que la mayoría de los accesos lógicos están determinados por el consumidor, es el consumidor entonces quién está mejor posicionado para definir si las actividades de controles cumplen con los estándares requeridos.

4. ¿Es posible cumplir con los requerimientos HIPAA utilizando un proveedor de nube? Los clientes pueden utilizar servicios de seguridad de AWS que mantienen y superan los estándares requeridos para proteger datos de salud electrónicos.

5. ¿GLBA (Gramm Leach Bliely Act o Acto de modernización de servicios financieros), es posible cumplir con esta regulación y un cliente de servicios en la nube? La mayoría de los requerimientos de GLBA están administrados por el cliente, de necesitar soporte sobre los controles físicos, el cliente puede utilizar el reporte SOC1 tipo 2.

6. ¿Dónde reside la información del cliente? AWS define en que región física estarán ubicados los servidores. La replicación de datos de los objetos de datos del S3, se hacen

en clúster regionales y no en otra región. Los clientes deciden en que región estarán aplicados su servers. AWS se compromete a no mover la información de sus clientes, salvo que sea en contra de pedidos de entidades gubernamentales.

7. ¿Los requerimientos de E-Discovery son cumplidos? Los clientes son responsables por procedimientos que involucran la identificación, recolección, procesamiento, análisis y producción de documentos electrónicos.

8. Están permitidos los tours en los datacenters? No. No se permite acceso a terceras partes a los datacenters debido a que contienen información de diferentes usuarios. Para hacer las validaciones de los Data Centers, se usan los reportes SOC Type 1 y Type 2 para las validaciones de los controles físicos.

9. ¿Acciones con privilegio, son monitoreadas y controladas? La información de los consumidores está aisladas lógicamente por instancias.

10. ¿Accesos internos controlados? Los controles del reporte SOC1 certifican la seguridad de los controles que impiden accesos no autorizados o indebidos de internos.

11. ¿La segregación de clientes esta implementada correctamente? Se utilizan softwares específicos de virtualización de software. Esta arquitectura fue validada por consultar PCI (PCI Qualified Security Assessor) y cumplir con los requerimientos PCI DSS. Es de remarcar que AWS tiene opciones de única tenencia, sin embargo se debe seleccionar esta opción. Instancias dedicadas son Amazon EC2 lanzadas dentro de las Amazon Virtual Private Cloud (Amazon VPC) que corren un hardware dedicado a un solo consumidor.

12. ¿El Cloud trata vulnerabilidades de Hypervisor? (Hypervisor es el software que se encarga de distribuir recursos entre las instancias de máquinas y el hardware disponible). Actualmente EC2 utilizar una versión customizada del Xen Hypervisor. Este Hypervisor está

customizada a medido y constantemente testeado contra vulnerabilidades y ataques tanto interno como penetración de equipos externas. A su vez también permite aislamiento entre máquinas de varios clientes.

13. ¿Administración de vulnerabilidades realizadas correctamente? ¿Se patchean los sistemas correctamente? Tanto del Hypervisor como de los servicios de red es responsable AWS en su patcheo. Sin embargo de acuerdo con ISO 27001, NIST, y los requerimientos de PCI, los clientes son responsables de los sistemas operativos montados en dichas máquinas, por ende de patchear sus propios sistemas.

14. Proveen soporte sobre los servicios de encriptación? Si, AWS permite al cliente utilizar sus propios servicios de encriptación para todos los servicios (S3, EBS, SimpleDB y EC2). Los túneles de IPSec a VPC también están encriptados. (También se puede tercerizar la encriptación).

15. ¿Cuáles son los derechos del proveedor de nube (AWS) sobre la información del cliente? Los clientes mantienen la propiedad sobre la información. AWS erra a favor de la privacidad de la información del cliente, salvo que las leyes que entren en conflicto de tenga una base sólida.

16. ¿La información del cliente está correctamente aislada? Toda la información de los clientes tiene la posibilidad de ser correctamente asegurada e aislada. Amazon S3 provee controles avanzados de acceso a datos.

17. ¿Utiliza AWS terceras parte para la prestación de servicios? No, AWS no permite acceso a tercera partes.

18. ¿El proveedor de nube le permite al cliente la administración de la seguridad de acceso a archivos, desde PC y dispositivos móviles? Si, AWS le permite a los consumidores administrar aplicaciones clientes y móviles de acuerdo a sus propios requerimientos.

19. ¿El proveedor de nube le permite al cliente asegurar sus servidores virtuales? Si, AWS le permite al cliente implemente la arquitectura de seguridad deseada.

20. El servicio incluyes capacidades de IAM (Identity Accesss Management)? AWS provee unos servicios de IAM para identificar, obtener credenciales y organizar por grupos permisos de una manera centralizada.

21. ¿Se específica cuando van a ser bajados los equipos para mantenimiento? NO se bajan los equipos para su mantenimiento o parches. El patcheo de los equipos no afecta al os clientes. El mantenimiento de las instancias es supervisado por los clientes.

22. ¿El proveedor le permite al cliente escalar su arquitectura más allá de su contrato original? Se puede escalar hacia arriba o hacia abajo, y el cliente solo paga por el uso.

23. ¿El proveedor se compromete a un alto grado de disponibilidad? Existen SLAs en el cual se acuerdan los niveles de SLA. (Ejemplo EC2 se compromete a un tiempo arriba de servidores de 99.95% a lo largo del servicio anual. Amazon S3 se compromete a un 99.9% de tiempo arriba de servidores por mes. Créditos de servicio son proveídos en caso de que no se cumplan con estos requerimientos.

24. Como se protege el proveedor contra ataques de DDoS? La red de AWS provee una protección significativa contra amenazas tradicionales de red, y está en criterio del cliente implementar servicios adicionales.

25. ¿Se puede exportar la información almacenada? El servicio de AWS para Importación/Exportación para S3 acelera mover grandes cantidades de información afuera de AWS usando dispositivos portables de almacenamiento para transporte.

26. ¿AWS le permite al cliente tener planes de continuidad de negocio? Si, además permite la utilización de instancias de servidor backup redundantes, planes de replicación de datos, y arquitecturas de disponibilidad multiregión.

27. ¿Se específica la durabilidad de los datos en el servicio? Una vez almacenados Amazon S3 además de almacenar los datos repara y detecta redundancias entre los datos.

28. Backup a cintas es algo que no provee AWS, sin embargo el usuario es libre de contratar un proveedor para que haga el backup en cintas.

## 6.2 Azure (Microsoft Company).

Microsoft tiene la siguiente ideología: La transferencia de responsabilidad sobre datos y aplicaciones sensibles de los clientes a los proveedores de la nube requiere la formación de un nuevo marco para establecer y mantener la confianza entre las partes contratantes.

Azure y Office 365 son las primeras herramientas en el mercado que fueron capaces de cumplir con políticas de seguridad del FBI's Criminal Justice Information Services (CJIS). Los requisitos del FBI especifican que si los empleados de las organizaciones que brindan servicios a las fuerzas del orden público tienen acceso a datos protegidos, deben pasar rigurosos

controles de antecedentes penales. Someter al personal de centros de datos a dichos controles CJIS de manera rutinaria e institucionalizada es un proceso costoso.

### 6.2.1 Ley de protección de datos y la adaptación de Microsoft a través del tiempo para continuar brindando sus servicios.

En octubre de 2015, el Tribunal de Justicia de la UE ("TJUE") invalidó abruptamente a EE. UU. el marco de la UE Safe Harbor, que se basó en un acuerdo de 15 años entre USA y la Comisión Europea que había permitido a miles de empresas para mover información personal a través del Atlántico mientras permanecen en cumplimiento de las normas de protección de datos de la UE. El TJUE puso en duda la legalidad de las transferencias transatlánticas de datos.

En Microsoft, hacía tiempo que habían reconocido que un colapso repentino de Safe Harbor era una posibilidad y ya había tomado medidas para prepararse para ello. A partir de 2010, se tuvo la tarea de crear un nuevo contrato en la nube basado en las cláusulas contractuales estándar.

Tal contrato mejorado no era algo que estaban obligados por ley a ofrecer, pero sabían que permitiría a sus clientes permanecer en el cumplimiento de la legislación de la UE, al menos provisionalmente, incluso sin Safe Harbor.

Durante un período de varios años, el equipo de cumplimiento se reunió en numerosas ocasiones con funcionarios de la Comisión Europea y los 28 Estados miembros de la UE y las Autoridades de Protección de datos (DPA) para elaborar una solución. En abril de 2014, las

DPA determinaron que las cláusulas modelo en el nuevo contrato de nube empresarial reunían los requisitos para un marco legal válido que rija los flujos de datos internacionales.

Estas cláusulas, que ahora ofrece Azure de forma predeterminada a todos los clientes en la nube, garantizan que incluso sin Safe Harbor, toda la información de identificación personal almacenada en la nube de Microsoft sigue cumpliendo los rigurosos estándares de privacidad de Europa sin importar donde está ubicado. (Sauer, 2016).

### 6.2.2 Herramienta de Compliance nativa de Microsoft.

El proveedor de la nube ofrece las herramientas de compliance, pero el cliente de la nube es quien debe usarlas para operar un entorno de nube compatible. (Miller, 2017)

La Herramienta que provee Azure es el "Compliance Manager" para satisfacer las necesidades de seguridad, cumplimiento y privacidad:

1. Ayuda a realizar evaluaciones continuas de riesgos mediante calificaciones de cumplimiento

2. Ofrece información procesable, desde una vista de certificación / regulación

3. Simplifica actividades de cumplimiento, con la capacidad de crear evaluaciones múltiples para cada estándar y regulación.

Tabla 14: Compliance con regulaciones existentes por parte de Azure.

| Global | US Government | Industry | Regional |
|---|---|---|---|

| | | | |
|---|---|---|---|
| CSA-STAR-Attestation | CJIS | 23 NYCRR Part 500 | BIR 2012 (Netherlands) |
| CSA-Star-Certification | DoD DISA L2, L4, L5 | APRA (Australia) | C5 (Germany) |
| CSA-STAR-Self-Assessment | DoE 10 CFR Part 810 | CDSA | CCSL/IRAP (Australia) |
| DFARS | EAR (US Export Administration Regulations) | CFTC 1.31 | CS Gold Mark (Japan) |
| ISO 20000-1:2011 | FDA CFR Title 21 Part 11 | DPP (UK) | Cyber Essentials Plus (UK) |
| ISO 22301 | FedRAMP | FACT (UK) | DJCP (China) |
| ISO 27001 | FERPA | FCA (UK) | EN 301 549 (EU) |
| ISO 27017 | FIPS 140-2 | FFIEC | ENISA IAF (EU) |
| ISO 27018 | IRS 1075 | FINRA 4511 | ENS (Spain) |
| ISO 9001 | ITAR | FISC (Japan) | EU-Model-Clauses |
| SOC 1, 2 and 3 | NIST 800-171 | GLBA | EU-U.S. Privacy Shield |

| | | | |
|---|---|---|---|
| WCAG 2.0 | NIST Cybersecurity Framework (CSF) | GxP | GB 18030 (China) |
| | Section 508 VPATS | HIPAA/HITECH | GDPR (EU) |
| | | HITRUST | IDW PS 951 (Germany) |
| | | MARS-E | |
| | | MAS + ABS (Singapore) | |
| | | MPAA | |
| | | NEN-7510 (Netherlands) | |
| | | NHS IG Toolkit (UK) | |
| | | OSFI (Canadá) | |
| | | PCI DSS | |
| | | SEC 17a-4 | |
| | | Shared Assessments | |
| | | SOX | |

Tabla 14: Compliance con regulaciones existentes por parte de Azure.

Cuadro de elaboración propia en base a https://azure.microsoft.com/en-us/, Web, consulta 2018.

### 6.2.3 Casos de Éxito de Azure.

Collector Bank: El banco utiliza las tecnologías de nube de Microsoft para crecer y diversificarse sin una inversión costosa en infraestructura de TI. Además, el sector europeo de servicios financieros está muy regulado, y las regulaciones anteriores no se escribieron teniendo en cuenta los avances de la tecnología de la nube. Collector ha decidido enfrentar el desafío regulatorio de frente, trabajando con los reguladores y Microsoft para operar dentro de un marco que promueve la seguridad, la privacidad y las prácticas innovadoras.

Para Collector, asegurar el cumplimiento con GDPR (Global Data Protection Regulation), debe tomar decisiones tecnológicas basadas no solo en el asesoramiento y la experiencia de su personal de TI, sino también en sus equipos legales y de cumplimiento. Dice Svensson (Jefe de Cumplimiento en el banco): "Queremos seguir creciendo, por lo que debemos ser ágiles. Eso incluye tener un fuerte concepto interno de cumplimiento que valora la tecnología. "Collector Bank también considera a Microsoft un participante activo y valioso en el proceso regulatorio europeo. "Vemos a Microsoft haciendo esfuerzos claros para comprender las necesidades de las compañías de servicios financieros como Collector y el entorno en el que operamos", dice Svensson. (Microsoft, 2018b)

A partir de estas palabras podemos observar que Microsoft toma una posición más activa en cuanto al cumplimiento que AWS. (Microsoft, 2018a)

Sberbank Leasing (SBL): SBL eligió Microsoft Azure como su plataforma en la nube y Microsoft Operations Management Suite para administrar su entorno en la nube. Desde el traslado de datos a la nube, SBL procesa conjuntos de datos aún más grandes de manera más rápida, promoviendo la eficiencia, la innovación y un mejor servicio al cliente. Y, aprovechando la sólida seguridad, SBL cumple con los requisitos normativos para mantener los datos seguros y privados.

## 6.3 Azure vs AWS.

Si bien se presentarán las diferencias que observamos entre AWS y AZURE desde un punto de vista de cumplimiento para regulaciones y adaptación a necesidades del cliente, es notable remarcar que no es la única característica (Soporte, flexibilidad de contratos, herramientas de explotación de datos, etc.) a tener en cuenta al momento de elegir un proveedor.

Esto se ve reflejado cuando Diego Cohen, Supervisor de Tecnología del área de Sistemas Administrativos de MercadoLibre, comentó “De todo el abanico de servicios que brindan los proveedores de nube fue difícil escoger los servicios y elegir el más adecuado para adaptar la tecnología actual a los servicios brindados por la nube. Un ejemplo fue la resolución de DNS (Servicio de DNS, "route 53" - Resolución de nombres dentro de la nube de Amazon) que puedo alocar en Amazon o dejar en MercadoLibre. Para dejarla en Amazon, necesito tener todos mis equipos en Amazon. Entre las ventajas veo que es más amigable y de rápida implementación desde Amazon, para todas las instancias de Amazon. Y entre las desventajas

observo que en esquema multicloud, no funciona, ya que no se puede consumir desde otro Cloud". (Diego Cohen, Entrevista personal, 30/06/2018).

Diferencias:

1. A diferencia de Amazon se encarga casi completamente en asesorar al cliente de cumplir con las regulaciones que tiene en Scope Microsoft.

2. Podemos observar que Azure tiene menor flexibilidad en cuanto las características de configuración de sus ambientes Cloud, sin embargo, esto es porque toma mayor responsabilidad sobre los datos y cumplimientos del cliente. Es un ejemplo de esto el caso de claves de encriptación, a las cuales el cliente no tiene acceso.

3. Al igual que Amazon, Azure no entregará información del cliente sin una orden judicial expresa con declaraciones validas, parándose del lado de protección de datos del cliente.

4. Al igual que AWS, Azure posee un equipo dedicado a la revisión y cumplimiento de regulaciones.

5. Ambas empresas hacen hincapié a que en todo momento el cliente es el dueño de la información en movimiento o en descanso.

### 6.3.1 CSA: Cloud Security Alliance

Esta organización sin fines de lucro, provee una serie de preguntas de seguridad, control y procesos que pueden ser utilizadas para la selección del proveedor de nube.

Seguridad de aplicación e interfaces (Seguridad de Aplicaciones):

1. ¿Usa estándares de la industria, para hacer seguro el ciclo de vida de sus desarrollos?

2. ¿Utiliza alguna herramienta de análisis de código fuente para detectar errores previos a producción?

3. ¿Utiliza análisis manual de código fuente para detectar errores previos a producción?

4. ¿Verifica que sus proveedores se adhieran a los estándares de industria para la seguridad en el ciclo de vida de desarrollo?

5. (SaaS) ¿Revisa sus aplicaciones para vulnerabilidades de seguridad y verifica errores previos a producción?

En el ciclo de vida de AWS se incorporan las mejores prácticas de industria. Cumpliendo con estándares como ISO 27001, certificado por auditores externos.

Seguridad de aplicación e interfaces (Requerimientos de Acceso de clientes):

1. Todos los requerimientos para regulaciones son cumplidos antes de dar acceso a los clientes a los ambientes de AWS?

2. ¿Todos los requerimientos y niveles de confianza están documentados?

AWS provee la documentación y certificación sobre sus controles de seguridad de IT reportando directamente a sus clientes.

Seguridad de aplicación e interfaces (Integridad de Datos):

1. Se corren rutinas de integridad de datos sobre ingresos manuales de datos, para evitar problemas de datos corruptos:

Mediante los reportes SOC se pueden observar los controles de integridad de datos, en todas las fases incluyendo transmisión almacenamiento y procesamiento.

Auditoria y compliance (Auditorias independientes):

1. Permiten a terceras partes analizar sus reportes SOC2 e ISO 27001?

2. ¿Realizan regularmente Tests de penetración sobre red y aplicaciones, recomendados por buenas prácticas? ¿Están sus resultados disponibles para sus clientes en cualquier momento?

3. ¿Realizan auditorías internas y externas, recomendadas por las buenas prácticas? ¿Están sus resultados disponibles para sus clientes en cualquier momento?

AWS tiene disponibles online y públicamente los resultados de sus reportes SOC3 e ISO27001. También hace un escaneo regular servicios finales de direcciones IP para vulnerabilidades (No se incluyen instancias de clientes). De detectarse vulnerabilidades se notifica a las partes involucradas para remediarlas. A su vez se hacen escaneos de vulnerabilidades externas por compañías de seguridad independientes.

A su vez, se realizan auditorías internas y externas y análisis de riesgos, en conjunto auditores independientes.

Auditoria y compliance (Mapeo regulatorio de sistemas de información):

1. ¿Existe la posibilidad de encriptar y segmentar lógicamente la información, de manera tal que solo se pueda acceder a la información de un cliente, sin poder acceder a la información de otros?

2. ¿Existe la posibilidad de recuperar la información en caso de pérdida de datos?

En AWS los clientes tienen responsabilidad de su información por la tanto la encriptación de su información corre por cuenta de ellas en las instancias aisladas. Es posible usar cualquier método de encriptación para los servicios prestados por AWS. A su vez para la recuperación de información AWS permite la utilización de proveedores de almacenamiento en cintas sin embargo no se responsable debido a que no es parte de los servicios brindados.

3. ¿Tiene la posibilidad de restringir los datos de acuerdo a locaciones específicas?

Si, AWS posee regiones de servidores, de las cuales no puede mover la información designada por el cliente, salvo que no cumpla con leyes explicitas que entren en conflicto con AWS.

4. ¿Tiene algún programa que permita la identificación de modificaciones a requerimientos regulatorios y asegura el cumplimiento con regulaciones nuevas?

AWS monitorea todos los requerimientos legales y regulatorios. AWS está validada por auditores independientes para certificar cumplimiento regulatorios ISO.

Administración de continuidad de negocio:

1. ¿Provee al cliente de opciones de hosteo geográficamente resilientes?

2. ¿Provee al cliente con infraestructura de fallos a otros proveedores?

Los datacenters están construidos en clusters en varias regiones globales, proveyendo al cliente la flexibilidad en instancias y almacenamientos de datos en diferentes regiones globales, y dentro de países regiones de disponibilidad.

A su vez los planes de continuidad de negocio están testeados y aprobados con estándares ISO 270001.

Administración y continuidad de negocio (Conectividad/Telecomunicaciones):

1. ¿Provee a los clientes con las rutas de transporte de la información entre los sistemas AWS?

2. ¿Pueden los clientes definir como es transportada su información y a través de que jurisdicciones legales?

Los clientes de AWS pueden definir en qué regiones físicas su información y servidores estarán localizados. AWS no va a mover la información del cliente de entidades físicas sin notificarle al cliente y de no entrar en situaciones legales con entidades gubernamentales. A su vez el cliente puede controlar las rutas de tráfico.

Los data centers de AWS tienen protecciones contra riesgos ambientales, certificadas por las mejores prácticas de ISO 27002.

Administración y continuidad de negocio (Mantenimiento de Equipo):

1. ¿Se posee equipo de recuperación de máquinas virtuales?

2. ¿Se pueden exportar imágenes de máquinas virtuales a otro proveedor de nube?

3. Se pueden replicar las imágenes de las máquinas virtuales en servidores On premise?

La funcionalidad EBS (Elastic Block Store, almacenamiento de volúmenes para instancias AWS EC2) Snapshot le permite al cliente recuperar y exportar imágenes virtuales en cualquier momento. De esta manera los usuarios pueden exportar su AMIs (Amazon Machine Image) y trabajarlas On Premise.

A su vez lo reportes SOC2 certifican que AWS puede proveer energía en caso de fallos de proveedor de energía (Mediante equipos UPS).

Administración y continuidad de negocio (Análisis de impacto):

1. Se posee un seguimiento de SLA?

AWS Cloudwatch provee un monitoreo de los recursos Cloud y las aplicaciones que corren los consumidores en AWS. A su vez AWS publica minuto a minuto toda la información de disponibilidad de servicio en el Service Health Dashboard.

Administración y continuidad de negocio (Política de retención):

1. ¿Tiene AWS controles técnicos que puedan realizar la retención de la información?

2. ¿Tienen procedimientos documentados que puedan responder pedidos de terceras partes o gobiernos sobre información de clientes?

AWS le permite al cliente el borrado de su información. Sin embargo, el cliente de AWS mantiene la propiedad sobre su información, por eso es cuestión del cliente la administración de políticas de retención.

AWS erra a favor de la protección de información del cliente y su privacidad, determinando que leyes debe responder. AWS no duda en discutir órdenes legales si no se encuentran bien justificadas.

Control de cambios y administración de configuración (Nuevos desarrollos/Adquisiciones):

1. ¿Hay políticas y procedimientos establecidos para la adquisición y desarrollo de nuevos sistemas, bases de datos, infraestructuras, servicios, operaciones y facilidades?

2. ¿Hay documentación para la configuración, utilización e instalación de productos?

El marco de trabajo de AWS estableció políticas y procedimientos basados en NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 y los requerimientos PCI DSS.

Control de cambios y administración de configuración (Desarrollos de terceras partes):

1. ¿Tienen controles para asegurar estándares de calidad para nuevos desarrollos?

2. Tienen controles para detectar fallas de seguridad en actividades de desarrollo terciarizadas?

Por lo general AWS no terciariza desarrollos. AWS incorpora estándares de calidad SDLC (System Development Lifecycle Mangement) a sus procesos.

Control de cambios y administración de configuración (Administración de calidad de pruebas):

1. ¿Hay mecanismos para identificar vulnerabilidades a través de debugging y de testeo de código, y a su vez aplicarlo a versiones de software ya en uso?

Los boletines de seguridad de AWS notifican a los clientes sobre eventos de seguridad y privados. (AWS Security Bulletin RSS). También se publica la información de servicios en el Service Health Dashboard.

Control de cambios y administración de configuración (Instalaciones inhabilitadas de software):

1. Se controlan las instalaciones no autorizadas de software en servidores AWS?

AWS contiene programas, procedimientos y procesos para verificar software malicioso, alineado con los estándares ISO 27001.

Control de cambios y administración de configuración (Cambios de producto):

1. ¿Cuándo se hace un lanzamiento de nuevo producto o servicio, se capacita y provee documentación a los usuarios con los nuevos roles, derechos y responsabilidades sobre estos nuevos servicios/productos?

Los reportes SOC permiten hace un control de cambios sobre productos.

Seguridad de datos y administración del ciclo de vida de la información (Clasificación):

1. ¿Proveen la capacidad de identificar máquinas virtuales?

Las máquinas virtuales son asignadas mediante el servicio EC2. Los clientes pueden retener el control sobre donde se almacena la información.

2. ¿Se puede identificar hardware a través de etiquetas de políticas/metadata, etc.?

AWS EC2 permite la habilidad de etiquetar recursos. En una forma de metadata, los usuarios pueden usar las etiquetas EC2 para crear nombres de instancias amistosas, mejorar las búsquedas, y mejorar la coordinación entre múltiples usuarios.

3. ¿Tienen la capacidad de usar la localización física como autenticación?

AWS tiene la capacidad de accesos basados en direcciones IP. Algunas de las condiciones a utilizarse son horarios, dirección IP originaria y certificados SSL.

4. ¿Utilizan el etiquetado de información según estándares? (Ejemplo Oasis XML).

El cliente mantiene el control sobre la información por ende es el encargado de hacer el etiquetado de la información si desea cumplir con requerimientos de estándares.

Seguridad de datos y administración del ciclo de vida de la información (Inventario de información/Flujos):

1. ¿Se mantiene un inventario y documentan la información para los servicios de aplicación y la red de infraestructura y sistemas?

2. ¿Se puede asegurar que AWS no va a mover la información de regiones sin permiso del cliente?

AWS no tiene el permiso para la modificación del uso de regiones seleccionado por el cliente.

Seguridad de datos y administración del ciclo de vida de la información (Comercio electrónico y transacciones):

1. ¿Se proveen metodologías de encriptación para que puedan proteger sus datos, si se requiere el transporte a través de redes públicas?

Todas las APIs AWS están disponibles mediante endpoints protegidos por SSH que proveen autenticación de servidor. AWS alienta a los clientes a usar sus métodos propios de encriptación para todos los clientes incluyendo S3, EBS, SimpleDB y EC2. Los túneles IPsec hacia la VPC también están encriptados. A su vez el cliente puede utilizar AWS Key Management System (KMS) para crear claves de encriptación.

Seguridad de datos y administración del ciclo de vida de la información (Data no productiva):

1. ¿Tienen procedimientos para asegurar que la información productiva no está siendo utilizada en ambientes no productivos?

Como el cliente es dueño de la información en los ambientes de AWS es el cliente quién se debe encargar que su data no sea reproducida en sus otros ambientes dentro de AWS.

Seguridad de datos y administración del ciclo de vida de la información (Deshecho seguro):

1. ¿Soporta el borrado seguro de archivos y backups de acuerdo con los criterios del cliente?

2. Pueden proveer un procedimiento público para salir del contrato de servicio, incluyendo seguridad que toda la información del cliente sea borrada una vez que este deje de ser cliente de AWS.

Cuando un dispositivo de almacenamiento llega al fin de su vida útil, AWS comienza un proceso de desmantelamiento que evita que personal no autorizado acceda a la información de dicho consumidor. Las técnicas de desmantelamiento se detallan en NIST 800-88.

Los volúmenes EBS de Amazon son presentados al cliente como bloques crudos no formateados previamente a ser borrados. La eliminación de los datos se produce antes de la reutilización, para asegurar al cliente que la información ha sido borrada. El cliente también puede elegir sus propios métodos de borrado como por ejemplo NIST 800-88.

Seguridad del Datacenter (Administración de Activos):

1. ¿Mantiene un inventario de los activos críticos y su propiedad?

2. ¿Tiene un inventario de todas sus relaciones con proveedores críticos?

De acuerdo con los estándares ISO 27001, los activos son asignados un propietario, traqueados y monitoreados por el personal de AWS. Existe un equipo de mantenimiento de relaciones con todos sus proveedores

Seguridad del Datacenter (Autorización fuera del sitio):

1. ¿Provee a los clientes documentación de los escenarios en los cuales puede mover la información de un lugar físico a otro?

En principio, AWS no tiene ningún escenario en el cual no deba mover la información de región.

Cumplimiento y administración de Riesgos:

1. ¿Permite a sus clientes proveer su propia imagen de máquina virtual para certificar cumplimiento de determinados estándares?

Los clientes pueden proveer su propia imagen de máquina virtual. Importar máquinas virtuales permite a los clientes importar desde sus servidores on premise a ambientes de instancias Amazon EC2

Cumplimiento y administración de Riesgos:

1. ¿Realizan un testeo de riesgos asociados al cumplimiento de información al menos una vez al año?

Alineado con el estándar ISO 27001, AWS mantiene un programa de administración de riesgos para mitigar y administrar riesgos. Además también mantiene la certificación ISO 27018, demostrando que AWS mantiene un sistema de controles para cumplir con la protección privada del contenido.

Recursos Humanos (Análisis de Historial):

1. ¿De acuerdo con las leyes locales, regulaciones, éticas y frenos contractuales, todos los empleados, contractuales y terceras partes están sujetas a una verificación de historial?

AWS hace un análisis de historial criminal, permitido por la ley aplicable, como parte de un análisis para identificar acceso a facilidades y posiciones de AWS

Recursos Humanos (Fin de contrato):

1. ¿Las políticas, procedimientos y guías documentadas hacen referencia a cambios de sector o despido de gente? ¿Cómo se tratan dichos permisos?

Certificado por reportes SOC, AWS al terminar un contrato con un empleado revoca todos los permisos al mismo. A su vez si se realiza un cambio de sector se envía una autorización al superior pidiendo permiso para mantener los permisos anteriores.

Administración de identidad y Accesos (IAM) (Credenciales e ID de usuarios):

1. ¿Se provee a los usuarios integraciones con soluciones de Single Sign On (SSO) para los servicios brindados?

El servicio IAM provee identificación para la administración de consolas de AWS. La autenticación multifactor es opcional.

IAM soporta el acceso delegado para la administración de consolas de AWS y APIs AWS. Con la identidad en federación, entidades externas pueden, mediante identificador corporativo o web, como Amazon Cognito, Login con Amazon, Facebook, Google o cualquier OPENID CONNECT (OIDC) compatible.

Seguridad Móvil (Políticas BYOD):

1. ¿AWS permite a los clientes crear políticas de seguridad sobre los dispositivos móviles ya sean BYOD (Bring your own Device) o corporativos?

Los clientes mantienen la responsabilidad y control de la información y los dispositivos multimedia asociados. Es responsabilidad de cliente la administración de seguridad de dispositivos móviles y el acceso de los clientes al contenido.

# 7. Conclusiones

## 7.1 Puntos Clave para la clasificación de la información y compliance en la nube al corto plazo.

Para poder hacer una identificación de los puntos clave necesarios para la clasificación de la información dentro de los servidores de un proveedor Cloud para un cliente, necesitamos en primera instancia analizar los casos de éxito y fracaso vistos en el capítulo "Que es Cloud Computing" de esta tesis.

A partir de este capítulo podemos deducir que los casos de fracaso se dieron debido a los siguientes motivos:

1. Errores de configuración por desconocimiento de la tecnología, por parte de la empresa cliente (Ejemplo: Verizon en la configuración sus servidores de AWS).

2. Falta de conocimiento de la empresa cliente en cuanto a los requisitos regulatorios (Ejemplo: Equifax, desconocimiento de encriptación de data en descanso).

3. Generación de Nuevas regulaciones (Ejemplo: GDPR)

4. Inflexibilidad del país en cuanto a la herramienta (Ejemplo: Venta de Servidores AWS a China por decisión del gobierno).

A su vez en relación a los casos de éxito podemos decir que además de lograr aprovechar la ventajas que brinda CC explicadas a lo largo de dicho capítulo, pudieron adaptarse a nuevos requisitos regulatorios, dado su conocimiento sobre la materia, y amenazas existentes (Ejemplo: Meltdown y Spectre son las 2 amenazas con mayor impacto del 2018 que

afectaros todos aquellos que tenían servidores Cloud. Dichos casos fueron solucionados con parches a los procesadores correspondientes).

A su vez como hemos identificado en el capítulo de "Regulaciones existentes a aplicables a Cloud Computing y Cloud Storage", podemos observar casos que afectan en gran medida a los proveedores y sus clientes como la GDPR (Global Data Protection Regulation), y regulaciones como SOX, PCI, BACEN, etc., que afectan indirectamente dicho proveedor y clientes, precisando los reportes como son SOC1, SOC2, etc. También podemos observar de este lado que no solo es el cliente quién debe estar actualizado en cuantos los nuevos requerimientos regulatorios, sino que los mismos también deben ser cumplidos y analizados por el proveedor de CC, requiriendo así un esfuerzo de ambas partes.

A partir de lo visto en el capítulo de "Clasificación de la información", podemos identificar que si bien los países/rubros pueden poseer criterios de clasificación de la información similares entre sí, y hasta a veces los mismos se pueden repetir como son las cosas de información "Pública, Reservada, Restringida, Confidencial y Top Secret"; las regulaciones y sus certificaciones no son compatibles entre sí completamente, lo cual genera un doble esfuerzo para una compañía que precise cumplir con ambas regulaciones y también para su proveedor Cloud. En este caso podemos observar el Concepto de Regtech identificado en este capítulo que permite en asociación con CC y conocimiento del cliente, facilitar el cumplimiento de cualquier tipo de requerimientos. Es un caso de ejemplo, la herramienta SAP GRC, que permite a la compañía generar requerimientos y políticas a cumplir sin importar a que regulación nos referimos.

Por otro lado, mencionando el capítulo de "Estadísticas referentes a la adopción de regulaciones y estándares de Cloud Computing y Cloud Storage en la Argentina" podemos decir que la Argentina tiene empresas de primer nivel y se encuentra en proceso de captar empresas IT para la creación de empleos que hagan propensa la adopción de tecnologías como son Cloud Computing y Cloud Storage. Sin embargo desde un punto de vista regulatorio, no hay un desarrollo tan significativo para controlar el flujo de datos cuando los mismos se encuentran en servidores de terceros, como no así en la GDPR de la EU.

Por último, analizando los casos mostrados en el capítulo "Casos de Estudio" de Amazon Web Services y Azure (Microsoft), podemos decir que el proveedor de nube seleccionado puede hacer una gran diferencia no solo a la hora de la migración de nuestros servidores On-Premise a la nube, sino también en materias regulatorias y buenas prácticas. Es el ejemplo de AWS, un caso en el cual podemos observar cómo se "alienta" una gran variedad de regulaciones, sin embargo a partir de la capa de infraestructura la responsabilidad recae sobre el cliente. En contraposición en Microsoft esa capa puede ser un poco más flexible abarcando más y capacitando al cliente en la regulación para que pueda cumplir con sus requisitos, estando Microsoft al tanto de los últimos avances regulatorios y legales en el país donde residen los datos.

En resumen los puntos clave identificados para la clasificación de la información y compliance en la nube al corto plazo, son:

1. Hoy en día los proveedores de CC y CS ofrecen a los clientes sus servicios y limitan sus responsabilidades en referencia a las regulaciones hasta la capa de infraestructura (AWS, Azure, etc.). Dado que el dueño de la información continúa siendo el cliente, y los proveedores de nube solo toman responsabilidad por una capa y no de una manera holística, entran en juego los socios/partners de nuestro proveedor de nube. Es un ejemplo para Amazon Web Services o Azure los siguientes partners:

Dedalus: Consultoría integración, transformación digital y servicios administrados.

Escala24*7: Auditoría, cumplimiento y soportes de servicios de migración a nube. Migración aplicaciones e infraestructura. Optimización de arquitecturas. Administración y monitoreo 24*7

Edrans: Orientado a software Development y Deployment.

Nubelu (Logicalis): Administración de servicios en la nube.

BMC: Empresa que tiene por objetivo principal el control de costos en la nube.

Rackspace: Administración y soporte en AWS.

Si bien algunos pueden estar dedicados a la administración de recursos de nubes, la mayoría también se especializa en auditorias y cumplimiento de regulaciones. Estos casos pueden ser de gran ayuda para pequeñas y medianas empresas que no reconocen aún los requisitos de las regulaciones con las cuales deben cumplir en base al país o región en el que operan.

2. El marco regulatorio está entre otras cosas basado en la clasificación de la información. En general todos los países/regiones/industrias poseen grados de clasificación similares. Lo cual hace que las bases de los marcos regulatorios puedan ser similares, sin embargo, como observamos cumplir con una regulación no es aplicable a certificaciones que tengan bases similares. La certificación se debe hacer por cada regulación y estas varían a lo largo del tiempo. Es necesario tener un equipo de auditoria interna centrado en el cumplimiento de las regulaciones con completa visibilidad de las herramientas disponibles para la administración de la información en CC y la generación de políticas que puedan permitir las certificaciones revisadas por auditorías externas.

3. Asesoramiento y notificación de las regulaciones que deben ser cumplidas al proveedor de CC. Si bien la responsabilidad y propiedad de los datos recae en el cliente, es necesaria una identificación de los requisitos por parte del cliente para el cumplimiento de las regulaciones para evitar errores solucionables, por casos como configuraciones erróneas.

4. Implementación de Regtech (Regulation Technologies) como GRC (Governance Risk and Compliance) y Compliance Manager que faciliten la documentación de procesos, revisión de logs, manejo de incidentes y certificaciones en la nube. Dado que es una nueva tecnología algunas herramientas todavía no están adaptadas a revisar herramientas como IAM (Identity Access Management - Herramienta para manejo de autorizaciones en servidores de proveedores externos).

## 7.2 Visión para los próximos 5 a 10 años en referencia a compliance en la nube.

Dada la gran cantidad de marcos regulatorios existentes y el gran parecido en cuanto a sus objetivos y clasificaciones visto a lo largo de la tesis "Cumplimiento, Seguridad y Clasificación de la información para Cloud Computing y Cloud Storage", podemos decir que a lo largo del tiempo habrá una convergencia entre marcos regulatorios, la cual permitirá a diferentes países cumplir con diferentes regulaciones simultáneamente.

Es trabajo de las autoridades encargadas del desarrollo regulatorio en cada país, dicha convergencia y aceptación de marcos regulatorios externos para empresas operadoras.

Puede que esto no afecte a pequeñas y medianas empresas que están desarrollándose todavía y no poseen una burocratización, en el buen sentido de la palabra, de sus procesos, sin embargo para grandes empresas multinacionales o incluso "Born Global", esto termina volviéndose un punto crítico a lo largo del tiempo, debido a que los esfuerzos deberían estar completamente dedicados al servicio brindado y no a certificaciones en teoría transparentes para el usuario final.

## 8. Bibliografía


Achiary, C. Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional (2005).

Amazon. (2015). *Introduction to AWS Security by Design*.

Arner, D. W., Barberis, J., & Buckley, R. P. (2016). FinTech, RegTech and the Reconceptualization of Financial Regulation. *Forthcoming: Northwestern Journal of International Law and Business*, *2*(October), 1–51. https://doi.org/10.1177/0027950111411368

Ashktorab, V., & Taghizadeh, S. R. (2012). Security Threats and Countermeasures in Cloud Computing.

Bartoletti, D., O'Donnell, G., E. Nelson, L., & Caputo, M. (2018). *The Forrester Wave™: Hybrid Cloud Management, Q2 2018*.

BSA. (2018). *2018 BSA GLOBAL CLOUD COMPUTING SCORECARD*. *BSA, Software Alliance*.

Cadell, C. (2017). Amazon vende activos de la nube en China presionado por nuevas reglas más duras. Retrieved from https://lta.reuters.com/article/internetNews/idLTAKBN1DE266-OUSLI

Clarin. (2018). Detectan importante falla de seguridad en procesadores Intel: cómo afecta a los equipos. *Clarin/Tecnología*. Retrieved from https://www.clarin.com/tecnologia/detectan-importante-fallo-seguridad-procesadores-intel-afecta-equipos_0_ry9DUJsQM.html

Date, S. (2016). Should You Upload or Ship Big Data to the Cloud ?

Domenech, J. (2018). Encuentran un fallo en el diseño de algunos procesadores de Intel. Retrieved from Encuentran un fallo en el diseño de algunos procesadores de Intel

Elliot, D. (2015). Breaking the Banking Mould. Retrieved from https://aws.amazon.com/es/solutions/case-studies/starling/

europapress/sociedad. (2017). Las empresas españolas deberán nombrar un Responsable de Protección de Datos en seis meses. *Europapress/sociedad*. Retrieved from http://www.europapress.es/sociedad/noticia-empresas-espanolas-deberan-nombrar-responsable-proteccion-datos-seis-meses-20171115143746.html

Farkas, M. (2017). From Desktop to Cloud Top (Vol. 40, pp. 9–10).

Foster, J. (2016). Securing your cloud workloads just got easier: Deep Security as a Service is now on AWS Marketplace! Retrieved from https://blog.trendmicro.com/securing-cloud-workloads-just-got-easier-deep-security-service-now-aws-marketplace/

Frias, R. (2018). AWS experience ARG. In *AWS experience Cases Argentina*. Buenos Aires.

Gobierno de Queensland, A. (2009). *Queensland Government Information Security Policy Framework. Framework.*

Goretsky, A. (2018). Vulnerabilidades Spectre y Meltdown: todo lo que necesitas saber. *Welivesecurity.com*. Retrieved from https://www.welivesecurity.com/la-es/2018/01/05/vulnerabilidades-spectre-meltdown-todo-lo-que-necesitas-saber/

Gov, United Kingdom, G. (2017). *Security Policy Framework.*

Gov Alberta Canada, G. (2014). *Data and Information Security Classification Standard*.

Gutiérrez, H. E., & Korn, D. (2017). *Facilitando the Cloud : Data Protection Regulation as a Driver of National Competitiveness in Latin America*. *The University of Miami Inter-American Law Review* (Vol. 45).

HURBEAN, L., & FOTACHE, D. (2013). Mobile Technology: Binding Social and Cloud into a New Enterprise Applications Platform, *17*(2), 73–84. https://doi.org/10.12948/issn14531305/17.2.2013.06

IT Governance Institute. Marco de Trabajo Objetivos de Control Directrices Gerenciales Modelos de Madurez, 4.1 Cobit § (2007). Retrieved from www.isaca.org/cobitfeedback

Itsitio. (2018). Cómo se posiciona Argentina en la adopción de políticas cloud. Retrieved from https://www.itsitio.com/ar/como-se-posiciona-argentina-en-la-adopcion-de-politicas-cloud/

Jones, T. (2017). Default AWS S3 encryption walls off vulnerable customer data. Retrieved from http://searchaws.techtarget.com/news/450429898/Default-S3-encryption-walls-off-vulnerable-customer-data?utm_content=control&utm_medium=EM&asrc=EM_ERU_85357879&utm_campaign=20171114_ERU Transmission for 11/14/2017 (UserUniverse: 2468071)&utm_source=ERU&src

Marks, G. (2017). How the Equifax breach could hurt Google, Amazon ... and my small firm. Retrieved from https://www.foxbusiness.com/features/how-the-equifax-breach-could-hurt-google-amazon-and-my-small-firm

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. *National Institute of Standards and Technology, Information Technology Laboratory*, *145*, 7. https://doi.org/10.1136/emj.2010.096966

Microsoft. Subsidiary of largest Russian state- owned bank chooses the cloud to promote growth and strong security times (2018).

Microsoft. Swedish bank overcomes regulatory hurdles and embraces the cloud to foster innovation (2018).

Miller, D. (2017). An Introduction to Cloud Computing for Legal and Compliance Professionals.

PCI, S. B. (2018). Microprocessor flaw shows vulnerability in cloud computing. *Smart*. Retrieved from http://www.smartbrief.com/branded/F984E648-8A5C-4D46-AD5A-0509307CFD77/AE543AD5-924F-48B1-B83A-98DE1C2117DB

Prince, A. (2017). *Computación en la nube en el Estado*.

Sauer, R. (2016). Achieving Trust and Compliance in the Cloud. *Journal, International In-House Counsel*, *9*(36), 1–12.

Schwartz, P. M. INFORMATION PRIVACY IN THE CLOUD, 161 § (2017).

Sepúlveda, E., Salcedo, O., & Vargas Gómez, E. (2011). *SECURITY AND RISK MANAGEMENT WHEN USING CLOUD*.

Services, A. W. (2017). Bynder Case study. Retrieved from https://aws.amazon.com/es/solutions/case-studies/bynder/

Sinjilawi, Y. K., Al-nabhan, M. Q., & Abu-shanab, E. A. (2014). Addressing Security and Privacy Issues in Cloud Computing, *6*(2), 192–200. https://doi.org/10.4304/jetwi.6.2.192-199

Snipp, C. M. (2015). What does data sovereignty imply: what does it look like? (Vol. 15, pp. 83–91).

Sosa, J. (2012). *Clasificación de la información*.

Victor, J. M. (2013). The EU general data protection regulation: Toward a property regime for protecting data privacy. *Yale Law Journal*, *123*(2), 513–528.

Villatoro, G. (2018). Amazon adquiere plataforma de detección de amenazas Sqrrl.

Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., Meinl, T., Michalk, W., & Stößer, J. (2009). Cloud Computing – A Classification, Business Models, and Research Directions. In *Business & Information Systems Engineering* (Vol. 1, pp. 391–399). https://doi.org/10.1007/s12599-009-0071-2

Werbach, K. (2017). *The Network Utility* (Vol. 60).

Wu, R. (2017). PatSnap Case Study. Retrieved from https://aws.amazon.com/es/solutions/case-studies/patsnap/

Zhang, Z. (2017). Avazu Case Study. Retrieved from https://aws.amazon.com/es/solutions/case-studies/avazu/