Como venimos presentando a lo largo de este curso, *Cloud Computing* y sus tecnologías asociadas, nos enfrenta a una nueva revolución. Muchos la citan como la era de la Industria 4.0. En esta predomina la innovación y el uso de la tecnología en todos los segmentos e industrias de una manera mucho más profunda y eficiente. Ahora bien, la otra cara de la moneda es que se requieren nuevos conocimientos por parte de todos los estratos de la organización, por lo que en primera instancia revisaremos a continuación los principales detalles técnicos y, seguido a esto, todo lo referido a seguridad y legalidad. Estos últimos están evolucionando mucho, pero aún se presenta mucho desconocimiento y por sobre todas las cosas falta de estandarización, lo que requiere que analicemos y hagamos todas las preguntas que nos hacen falta de acuerdo con el proyecto que deseamos llevar a la nube.

3.1 Arquitectura de la industria tecnológica

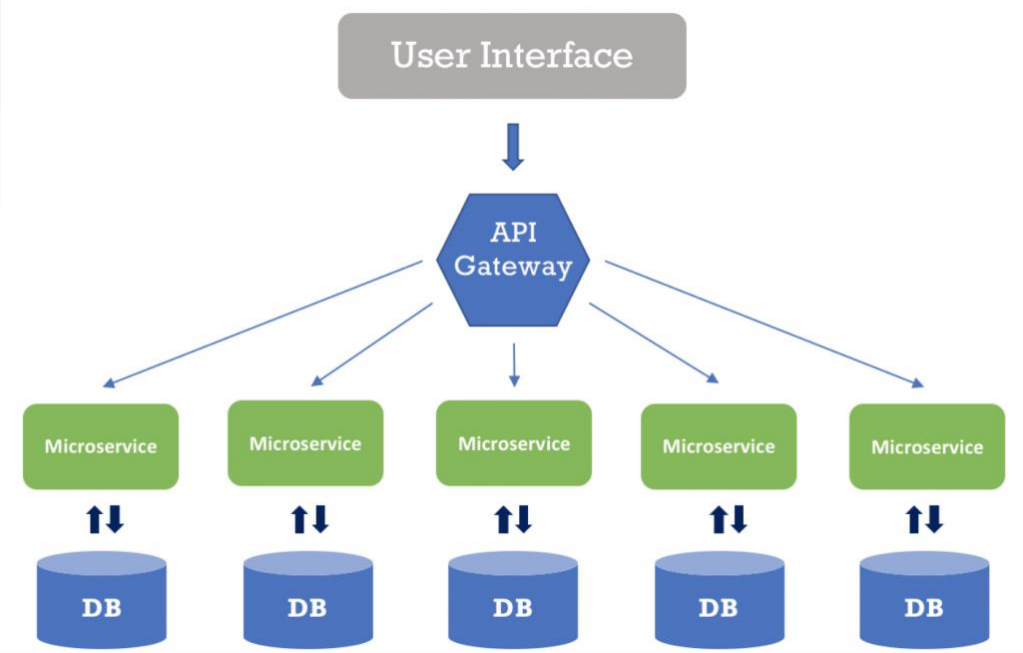
Las nuevas formas de trabajar y evolucionar los proyectos requieren de especial atención en el monitoreo, el análisis de datos, y la toma de decisiones para la mejora continua. Este *loop* iterativo es cada vez más rápido y está empujado por la vorágine de distintos segmentos y mercados.

La tecnología y todo el conjunto de aplicaciones ayuda mucho en este contexto, pero para un mayor rendimiento debe ser utilizada con el conocimiento y el criterio necesario. Si bien en *hardware* y *software* se dice que "está todo hecho", la complejidad y especialización de las soluciones lleva a que los expertos en estos temas deban dar soporte a las decisiones relacionadas a la mejor continua, ya que, en la mayoría de los casos, se presentan muchos caminos a seguir.

Para diseñar un *stack* de tecnología acorde a la empresa o proyecto, debemos arrancar de la visión global de la compañía y tener muy en claro que debemos desglosar la misma en distintos componentes de solución. En los tiempos que corren, ya que existen las grandes aplicaciones que solucionan todo, cada vez más pequeños componentes se especializan en una tarea y pueden conectarse con otros elementos de manera estándar y con poco esfuerzo técnico.

El auge actual de la arquitectura orientada a servicios (SOA) y microservicios, puso a la *web* en la mira y es muy fácil verse abrumado por toda la información disponible. Por esto, es importante analizar las categorías, siglas, y estándares, a los efectos de tener un panorama de acción más claro al momento de tomar decisiones técnicas y de negocio (Colubriale, 2017).

Figura 1. Arquitectura de microservicios



Fuente: Rodríguez, 2019, https://bit.ly/2TORk2U

Como podemos apreciar en la figura 1, la aplicación posee una interfaz de usuarios, la cual habla con una API (interfaz de aplicación de usuario) y esta se encarga de coordinar con cada microservicio el ida-vuelta de la transacción con su respectiva base de datos. Para comprender con un ejemplo, pensemos en una página web que posee:

- Clima: es un microservicio que brinda alguna empresa como https://www.accuweather.com/

- Cotización del dólar y otras monedas: es otro componente de un proveedor como http://www.dolarhoy.com/

Ambos encajan en esta estructura, poseen su base de datos particular y el *web site* los "llama" para presentarlos, pero los especialistas en cada caso son los proveedores de dichos servicios.

Estos microservicios han generado esta movida en cuanto a la especialización y, como ya ha sucedido en otras facetas de la tecnología, se han estandarizado. Los principales métodos son:

- **Llamadas a procedimientos remotos (*Remote Procedure Calls*, RPC)**: es la primera versión de los servicios web, se extendió ya que utiliza los llamados a funciones y métodos centrados en las operaciones, lo cual es muy común entre los programadores. Si bien se está dejando de usar ya que depende mucho del lenguaje de programación, aún quedan muchas aplicaciones montadas sobre estas tecnologías.

- **Arquitectura orientada a servicios (SOA, *Service-Oriented Architecture*):** se basa en mensajes, más allá de las operaciones que maneje dentro de cada mensaje. Esta fue la primera manera de encapsular una transacción dentro de un protocolo, lo que generó gran cantidad de aplicaciones y servicios.

- **Transferencia de estados (REST, *Representation State Transfer*):** es el método más popular en la actualidad, y la abstracción llega al nivel de estados. Estos concentran mensajes y operaciones. Por lo tanto, podemos construir aplicaciones preparadas para interactuar con estas *Api rest* independientemente del lenguaje y tecnología de construcción.

Y llegamos así al nivel de los **microservicios** de manera que la estrategia será reutilizar código ya desarrollado y especializado en un tema. Esto se logra a través de API´s y plataformas, que se programan en lenguajes distintos, se ejecutan, actualizan, y evolucionan de manera autónoma.

Desde ya que estas tecnologías tienen sus pros y contras, por lo que si bien son una tendencia y toda la industria se está moviendo en esta línea, es bueno conocer las ventajas y desventajas.

Ventajas de los servicios web

- Interacción entre sistemas independientes.
- Fomentan la estandarización en base a protocolos y mensajes común.
- Abre la tecnología al punto de poder construir una solución con distintas partes o bloques construidos en alguna parte del mundo.

Desventajas de los servicios web

- No son tan eficientes como los protocolos orientados a transacciones (CORBA -*Common Object Request Broker Architecture* o RMI *Remote Method Invocation*) utilizados por la industria o los bancos.

- Deben evolucionar o complementarse con elementos de seguridad que le den al protocolo de base (HTTP) un nivel más de control y seguridad.

Desde la perspectiva de negocio, si nos abstraemos y nos posicionamos en el modo arquitecto de solución, podríamos desarrollar un e-*commerce* para nuestra empresa de la siguiente manera:

1) Utilizar Wix.com para nuestra página web.
2) Conectar la página a Mercado pago como *Gateway* de pagos y transacciones.
3) Conectar las comunicaciones de formularios y seguimiento de clientes a un CRM como Hubspot.

Desde ya que necesitamos recursos técnicos para realizar esto, ¡pero ya tenemos gran parte de la solución construida!

Comprendiendo ya la lógica de construcción de soluciones actual, nos introducimos a continuación en las distintas categorías que dominan las industria en la actualidad.

3.1.1 Todo como servicio: SaaS

SaaS es la denominación de "*software* como servicio". En este caso, quien provee el servicio pone a disposición de los usuarios una aplicación o *software* para ser consumido por el cliente que no debe preocuparse por la instalación del producto, ni por cómo está *hosteado*. Aquí la solución es accedida con distintos niveles de usuarios que se pueden configurar. El proveedor es el responsable del mantenimiento, capacitación y soporte.

El cliente tiene la posibilidad de configurar la herramienta y las opciones, pero siempre dentro de un entorno de opciones cerrado. La clave aquí, es que estos sistemas están utilizados por muchos clientes. Ej.: Zendesk tiene más de 150.00, por lo que se intuye que la mayor parte de las funcionalidades y opciones están cubiertas o en Roadmap, por parte del proveedor.

Se diferencia de los modelos de IaaS o PaaS, porque aquí no se brinda alojamiento a servidores, ni se prepara una plataforma para desarrollar de aplicaciones, sino que otorga el acceso a consumir las aplicaciones directamente desde la nube.

Office 365, Zendesk, Hubspot, Google Docs, y muchas más, son ejemplos de aplicaciones SaaS. En cada caso el acceso se da por algún tipo de pago por uso, que puede estar regulado por usuarios, transacciones, cantidades de datos, tiempo, etc., pero que en definitiva siempre es una renta de una aplicación en la nube que no requiere desarrollo de ningún tipo. En general, se accede desde la web vía navegador o muchos de ellos poseen *apps* en los *stores* (tiendas) de IOs o Android.

En cuanto al hosting y seguridad, como es el proveedor quien gestiona toda la infraestructura, es quien se encarga se administrar todo. Como veremos más adelante, los clientes deben leer y aceptar las políticas de seguridad del proveedor y los contratos de adhesión, y utilizar el servicio bajo esas consideraciones, siendo conscientes de cuáles son las responsabilidades de cada uno en la prestación del servicio.

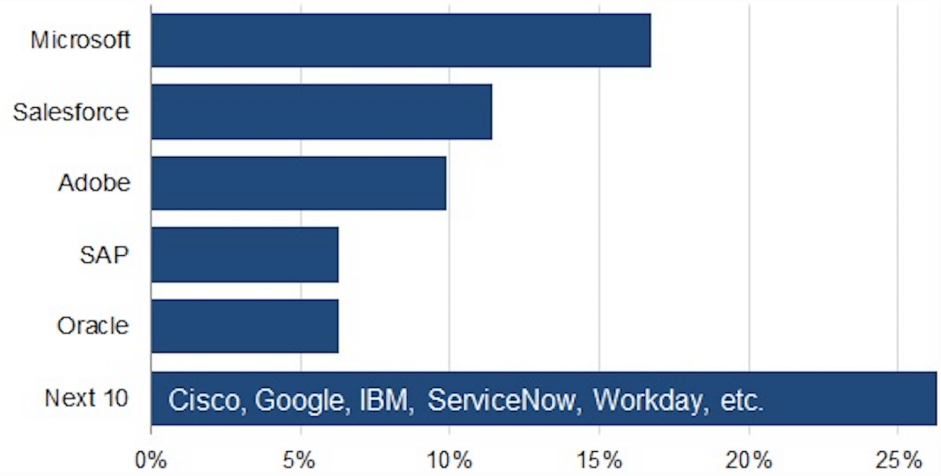
Analizamos a continuación los pros y contras de este tipo de soluciones.

Tabla 1: Pros y contras de los servicios del tipo Saas

+	-
Minimización de costos fijos, esto se acomodan en base a demanda de las operaciones	Integración con aplicaciones Legacy o nativas de la organización
Escalabilidad y redimensionamiento	Alta dependencia del proveedor
Tiempos mínimos de implementación	Incertidumbre respecto al futuro del proveedor y sus avances
Facilidad de uso y orientación a usuarios finales	

Fuente. Elaboración propia.

Figura 2. *Market Share* de proveedores SaaS 2019



Fuente: Kinsta, 2019, https://bit.ly/37Iy0OH

Como cierre, podemos inferir en la figura 2, que los grandes vendores de *software* están presentes en la modalidad SaaS y siguen liderando. Ahora bien, es importante considerar que existen miles de aplicaciones en esta categoría y que debemos analizar de manera detallada las alternativas para lo cual existen muchos *sites* de comparación de funciones y precios como los siguientes:

- https://www.comparasoftware.com/
- https://www.appvizer.es/
- https://www.capterra.com/
- https://www.g2.com/

Como conclusión de este punto, podemos asegurar que hay aplicaciones en la nube para casi todas las situaciones, pero que tendremos que bucear bastante para comprar *features*, precios y prestaciones, antes de tomar una decisión.

3.1.2 Todo como servicio: IaaS

IaaS es la denominación del modelo de infraestructura como servicio. En esta forma de servicio, el proveedor brinda el hosting u hospedaje a los datos y asigna un grupo de computadoras de diferentes capacidades para la gestión de estos, durante un tiempo, y en un espacio determinado.

Estos espacios pueden ser físicos, es decir que cuando contratamos un servidor, este coincida con una maquina real; o bien virtuales, siendo estos últimos una manera de "simular" un equipo real. Como analizamos anteriormente, el esquema de virtualización provee muchas eficiencias a los proveedores y aporta economía a los clientes.

En cualquiera de las dos modalidades, el proveedor le asigna esa capacidad al cliente y esta la puede gestionar a través de una aplicación o consola. Es muy importante comprender que los clientes no tendrán nunca acceso físico a las instalaciones, ni podrán administrar la infraestructura de base. Esto siempre queda del lado del proveedor. De esta manera, una empresa de cualquier dimensión puede armar su infraestructura tecnológica en la nube. La estrategia del proveedor está en equiparse y actualizarse de manera adecuada con el *hardware* y *software* de administración necesario, para poder amortizar los costos entre varios clientes y a partir de allí tener su rentabilidad.

Google Platform, Amazon Web Service, Azure, Vblock y EC2, son ejemplos de compañías que ofrecen este tipo de servicios IaaS en su forma más extendida o completa. Hay muchos proveedores de alojamiento de páginas webs, que también son un ejemplo de este tipo de uso de la nube, más simples pero muy utilizados por programadores y analistas digitales.

Si bien puede resultar complejo de comprender para un no técnico, se debe pensar que es un formato de renta o alquiler. La conectividad y velocidad de internet actual, ha dado la posibilidad de alojar el servidor (que es una computadora grande, con mucho procesador, memoria y almacenamiento) en cualquier lugar del mundo. Esto genera la oportunidad de, en lugar de invertir en la compra, puesta a punto y administración de un servidor, simplemente lo alquilemos, y tengamos expertos realizando las tareas de base y mantenimiento especializado. Esto nos independiza de actividades secundarias para nuestro negocio.

Existen, además, otros modelos de servicios en la nube como: FaaS (almacenamiento de archivos como servicio), MaaS, (monitoreo como servicio), BPaaS (procesos de negocio como servicio) y otras alternativas más, lo que sí es relevante comprender es que el IaaS, estará siempre en la base de estos modelos. Analicemos a continuación en la **Tabla 2**, estos servicios versus los tradicionales.

Tabla 2. Comparativo de servicios ofrecidos desde Internet

Concepto a Evaluar	*Software* propietario (licencia mensual)	*Software* propietario (licencia única)	Aplicaciones en la nube
Inversión inicial	Baja	Alta	Baja
Mantenimiento	Alto	Alto	Bajo
Instalación	Sí	Sí	No
Seguridad	Alta	Alta	Media
Confiabilidad de datos	Alta	Alta	Media
Actualizaciones automáticas	Sí	No	Sí
Gasto energético	Medio	Medio	Bajo
Necesidad de técnicos	Sí	Sí	No
Acceso a Internet	No	No	Sí

Fuente: Colubriale, 2017.

La tabla precedente nos da una vista de inversión, complejidad de instalación, gastos, y otros aspectos a tener en cuenta entre la opción del uso de *software* instalado en *hardware* propio, y las aplicaciones en la nube.

"Casi el 70% de las organizaciones y empresas utilizan algún tipo de servicio de nube para trabajar"
(Universia México, 2017, https://bit.ly/38xqErA).

3.1.3 Todo como servicio: PaaS

PaaS, responde a plataforma como servicio. Este sea tal vez, el más complejo de analizar para los no técnicos, porque el mismo incluye todo lo de IaaS y, además, todo lo necesario a nivel plataforma para que los desarrolladores o programadores trabajen en un proyecto.

El proveedor pone a disposición herramientas, configuraciones, esquema de trabajo que simplifican los desarrollos y, además, tiene embebido el proceso o la metodología que los programadores usan en todos sus proyectos. Estos pasos, tal vez, te sean familiares o los has

escuchado en tu organización: construcción/desarrollo, *testing* y puesta en marcha. El servicio de los proveedores PaaS, contempla en líneas generales los siguientes ítems:

- *Hosteo* de aplicaciones
- Capacidad de almacenamiento
- Soporte especializado
- Bases de datos
- Aplicaciones y herramientas de diseño
- Plataforma de desarrollo
- Sistema operativo y software de base para los servidores

Para intentar bajar a tierra este concepto, piensen que los programadores para comenzar a trabajar hace algunos años debían: instalar el servidor, bajar el *software* del lenguaje de programación, agregar librerías y objetos de desarrollo, diseñar en una aplicación y luego pasar esos diseños a código, y seguir todo el proceso de construcción con alguna herramienta de proyectos.

Gracias a este tipo de servicios PaaS, todo lo citado anteriormente está concentrado en una gran *suite on line*, lo que genera que para desarrollar ciertas aplicaciones no debamos tener demasiado *expertise* en algunos de los campos como, por ejemplo, instalación de *servers*. Como sucede en el caso de las empresas de *host web*, tenemos muchos *packs* y módulos que se instalan con un clic, plantillas, y principalmente todas las aplicaciones y herramientas para desarrollar en un lugar.

Los principales proveedores de este tipo de servicio son:

1. Amazon Web Services – Elastic Beanstalk
2. Salesforce
3. Software AG – LongJump
4. Microsoft – Azure
5. IBM – Bluemix
6. RedHat – OpenShift
7. VMware – Pivotal CF
8. Google – App Engine
9. AppFog
10. Engine Yard

Analicemos a continuación las ventajas y desventajas.

Tabla 3. Ventajas y desventajas de servicios tipo PaaS

+	-
Administración simple para entornos de desarrollo	Alta dependencia del proveedor
Simplificación de actividades de desarrollo y programación	Código compartido.
Integración con otras plataformas simplificada.	Baja seguridad en datos
	Bajo nivel de estandarización

Fuente: Elaboración propia.

Si revisamos el cuadro anterior, podemos indicar que PaaS es tal vez, el menos desarrollado de los servicios, porque aún está en busca de la estandarización y su líder. Más allá de esto, cuenta con un gran empuje por parte de la comunidad y de los grandes líderes tecnológicos.

3.1.4 Modularidad y API´s

Desde hace mucho tiempo que los sistemas se comenzaron a particionar, pasando de una gran aplicación que contenía todo, a un conjunto de módulos independientes y especialistas. La modularidad es una forma muy potente de abordar grandes proyectos dividiéndolos por fases. Esto nos permite ir iterando a medida que tenemos partes de la solución, pero principalmente da lugar a la especialización en el *software*. Para comprender este fenómeno haremos la analogía con la industria automotriz.

Cuando un diseñador de autos hace el borrador del nuevo modelo, parte siempre de componentes que ya están estandarizados. Las cubiertas pueden tener distintas pulgadas, pero está claro que salvo en algún modelo de súper lujo, las mismas estarán dentro de los que los fabricantes de cubiertas provean. Y así podemos seguir con los motores, las cajas de velocidad, los artículos de audio, etc.… En definitiva, la lógica del diseñador parte de armar un nuevo auto, ensamblando muchos componentes que ya existen. Ej.: Ford, no se pone a diseñar y desarrollar los equipos de audio, sino que hace un acuerdo con Sony y este le provee los mismos. En la industria del *software* ya sucede lo mismo. El nivel de especialización y estandarización ha llegado al punto de que siempre antes de desarrollar algo, debemos buscar lo que ya está hecho.

Diseñar de esta manera, simplifica y acelera los procesos y, por otro lado, permite mantener de manera independiente algún competente en paralelo sin tener que modificar toda la aplicación. Siguiendo con el ejemplo, si analizamos como algunos modelos de Ford populares evolucionaron su tecnología interna, veremos que el tablero del algún modelo no cambió mucho y sí lo hizo el equipamiento, pasando de estéreos muy simples a pantallas táctiles. Esto permite evolucionar la aplicación de una manera mucho más simple y eficiente.

Cada módulo o componente se ocupa de resolver un problema o tarea dentro de un diseño o proceso general. Otra gran ventaja es que cuando surge un error, se puede aislar al módulo

que lo contiene. Este modelo de desarrollo minimiza tiempos y recursos si lo ponemos en comparación con las grandes soluciones integrales.

La comunicación entre módulos de un mismo proyecto y módulos de distintos proyectos, es fundamental en el avance tecnológico actual. Con la diversidad de aplicaciones que el ciudadano común utiliza con naturalidad, ha sido necesario crear una conexión entre ellas, así como también de cada aplicación con el sistema operativo del dispositivo del usuario. Así nacen las APIs, siglas que corresponden a Interfaz de Programación de Aplicaciones. Esta interfaz compuesta por una serie de reglas en código, permite acceso limitado a los datos necesarios para la conexión entre dos programas. Limitado, porque provee la información necesaria sin vulnerar la seguridad de ninguno de los extremos de conexión. Esta es la magia de la API, habilitar funciones relacionadas a un programa, para que usuarios y otros programas se valgan de dichas herramientas sin brindar el código que corresponde a esa programación. Ahora bien, seguramente nos surge la pregunta ¿cómo conectamos los módulos o aplicaciones entre sí? La respuesta es a través de las APIs (Interfaz de Programación de Aplicaciones).

Una API es un conjunto de funciones, procesos, y procedimientos, que cumplen una o muchas tareas con el fin de ser utilizadas por otro *software*. En la definición de API está siempre el sentido de que puedan ser utilizados por terceros. Esta es la gran diferencia de desarrollo con los métodos anteriores que hacían una aplicación para que resuelva un problema, pero nunca se tenía presente la interacción con otros productos.

La API genera un avance tecnológico en base a la especialización y colaboración. Lo ya desarrollado, se pone a disposición para que otros puedan conectarse. Si volvemos al ejemplo de las cubiertas, la empresa Bridgestone va a seguir evolucionando los materiales, la resistencia y demás características de sus productos, pero siempre va a tener en cuenta que las llantas vienen de determinados tamaños, simplemente porque el fabricante de llantas ya ha estandarizado las mismas en xxx pulgadas. Parece algo obvio y simple, pero en la industria del *software*, antes de las API no se desarrollaba bajo este concepto, sino que cada uno hacía sus cubiertas a medida, para seguir con la analogía.

El uso de la API ha traído grandes beneficios en lo que refiere al impacto económico se:

- redujeron los costes de IT en un 41%;
- aumentó en el volumen de transacciones en un 42%;
- mejoró la satisfacción del cliente un 43% más que antes de su aplicación.

Para enlazar con lo que venimos desarrollando, el proveedor IaaS, PaaS, SaaS entrega una plataforma al cliente, con el servicio contratado, pero en todos los casos con determinadas APIs que permiten desarrollar o conectar aplicaciones a dicha plataforma, por lo que parte de la exploración al momento de contratar tiene que ver con que variedad o disponibilidad de APIs nos ofrece.

3.2 Seguridad en la nube

Cloud computing y los servicios en la nube, traen aparejado un cambio en la concepción de la seguridad informática y su forma de gestionarla. Dado que en este nuevo contexto la misma está casi completamente a cargo del proveedor, debemos contar con los recaudos suficientes en la hora de la selección, así como también establecer ciertos controles y mecanismos sobre los usuarios y sus roles. Desde ya que sobre la seguridad física no tenemos ningún tipo de inferencia, pero en la parte lógica tendremos que estar alertas en las asignaciones de perfiles administradores. Pensemos que hemos eliminado el edificio, la seguridad del mismo, las claves de cada sistema y servidor, y pasamos a tener uno o varios usuarios que controlan todo de manera remota. Además de la seguridad, los aspectos legales, contractuales, y de protección de datos, también poseen una vista distinta. En este módulo intentaremos clarificar la mejor manera de abordarlos.

Del mismo modo, deberá mantener sus equipos actualizados tanto a nivel *hardware* como *software*, para hacer frente a las amenazas existentes en Internet. Esto no significa que el proveedor de servicios se encargue de todo y que ya no sean necesarios los administradores del sistema en nuestra organización. Tanto si se utiliza un servidor en la nube (IaaS) como si se utiliza un entorno de desarrollo (PaaS), somos responsables de mantener el sistema operativo y las aplicaciones que instalemos correctamente configuradas, actualizadas a las últimas versiones y con todos los parches de seguridad que vayan apareciendo. Sea cual sea la forma de contratación y el modelo de despliegue en la nube, tendremos que mantener las políticas de seguridad que aplicaban a los servicios que hemos trasladado a la nube. Tendremos que cumplirlas o revisar su cumplimiento por parte del proveedor.

Elegir la forma de contratación y el modelo de despliegue que nos interesa, va a depender del servicio que queramos subir a la nube y de sus requisitos de seguridad. Así, no es lo mismo contratar un servicio para el correo electrónico, para almacenar y compartir ficheros o alojar una web, que migrar por completo nuestra empresa a la nube.

A continuación, en la figura 3 detallamos los distintos tipos de niveles de seguridad y la responsabilidad dependiendo del tipo de servicios en la nube, versus los sistemas *On Premise*.

Figura 3. Responsabilidad de seguridad en la nube según servicio

Responsabilidad	On Premise	SaaS		Paas		Iaas	
Gobierno de datos	C		C		C		C
Protección de puntos finales	C		C		C		C
Gestión de acceso a usuarios	C		C		C		C
Identidad	C		C		C		C
Aplicación	C	CSP		CSP			C
Control de red	C	CSP		CSP			C
Seguridad de sistema operativo	C	CSP		CSP			C
Host	C	CSP		CSP		CSP	
Red	C	CSP		CSP		CSP	
Data Center	C	CSP		CSP		CSP	

C= Cliente / CSP= Proveedor de servicios cloud

Fuente: Evaluando Cloud, 2018, https://bit.ly/2TQuyaZ

Como resumen, analicemos las generalidades de la seguridad en la nube presentada por una empresa de ERP en la Nube como Sage.

Video 1. Seguridad en la nube

Fuente: **Sage España** [Sage España]. (11 de octubre de 2013). *La seguridad en la nube* [YouTube]. Recuperado de https://www.youtube.com/watch?v=vqyuNha0Rek

3.2.1 Amenazas y riegos del *cloud computing*

El cambio que conlleva la seguridad de los servicios en la nube, nos pone en alerta respecto a algunos procesos críticos tales como las copias de seguridad de los datos, o los usuarios que ya no pertenecen a la compañía o no tienen determinada actividad.

Sabemos que todo lo relacionado a lo físico, estará a cargo del proveedor, es decir un *router*, una placa, un *server*, o cualquier otro elemento electrónico que tenga fallas será gestionado por ellos, y que en unos pocos minutos estará resuelto sin que nos demos cuenta. En este sentido las ventajas del *cloud computing* frente a las infraestructuras propietarias son muy grandes.

Gracias a las técnicas de virtualización, el proveedor puede garantizarnos copias, *back ups* y realmente independizarnos de estos temas. Ahora bien, las responsabilidades de seguridad deben estar bien detalladas en los contratos, y como usuarios firmaremos ANS (Acuerdos de Nivel de Servicio) en lo que esto debe estar muy explícito, por lo que debemos revisar con mucha precaución estas condiciones ya que tenemos muchas variantes al respecto y tendremos que evaluarlas al momento de adherirnos a un servicio en la nube.

Los objetivos de seguridad están en muchas situaciones ligados a los requisitos del negocio, no es lo mismo subir una página web de una Pyme, que manejar la base de datos de una empresa *worldclass*, por lo que costos, niveles y protecciones, son aspectos para clasificar. Lo mismo

sucede con determinadas industrias como la financiera que son muy propensas a ataques de ciberseguridad, por lo que el nivel de auditoría y seguimiento de fallas o ataques, es también un factor para poner en la balanza.

Por otro lado, debemos revisar la información sensible de la empresa, como los contratos, datos de clientes, presupuestos y otras transacciones. Esta debe estar almacenada de tal manera que nos garantice la seguridad y la exportación en el caso de que tengamos que cambiar de proveedor. El cliente debe garantizar la autenticidad, usabilidad, y en muchos casos, los niveles de confidencialidad de sus datos, por lo que no todos los proveedores en la nube pueden estar en condiciones de soportar nuestro servicio.
El uso del *cloud computing* lleva asociados amenazas y riesgos, por lo que a continuación los detallamos para que como managers de un proyecto en la nube podamos gestionarlos.

- **Amenazas**

  Si bien estas dependerán del tipo de contrato o acuerdo de servicio, podemos clasificarlas en las siguientes categorías.

  - **Accesos no autorizados:** el proveedor y el cliente deben estar en condiciones de garantizar el bloqueo a filtraciones, código malicioso, y otros tipos de robos de datos muy comunes. El esquema de control de acceso, roles y permisos, debe ser gestionado y el proveedor debe garantizar que se cuenta con las capas de seguridad acordes al tipo de organización o proyecto.

  - **Amenazas internas:** en muchas situaciones los empleados actuales o exempleados, generan situaciones de riesgo. Los permisos y privilegios de acceso están muy expuestos en estos modelos ya que se eliminan algunas capas de seguridad tradicionales como las VPN´s (redes privadas) o los controles de acceso físicos. Ya sea gestionado por el proveedor con nuestras notificaciones o perfiles de superadmin, del lado del cliente deben usarse para mitigar estas falencias.
  - **Interfaces inseguras:** gran parte de los ataques de ciberseguridad, se inician desde interfaces desactualizadas o redes que no poseen las capas y actualizaciones correspondientes. El proveedor debe tener la capacidad de identificar estos accesos, notificar al momento que se presentan y poner a disposición métodos de doble autenticación.

  - **Tecnologías compartidas:** si contratamos una infraestructura compartida, tenemos el riesgo de que otro cliente que está sobre la misma, introduzca un virus o un *software* malicioso. El proveedor debe garantizar que es capaz de aislar o de no permitir estos fallos.

  - **Robo de información:** algo muy común en estos días, los *malwares*, ataques por ingeniería social y otros métodos, ponen a disposición de los hackers datos sensibles como los de tarjetas de crédito. Es indispensable que el proveedor asegure los protocolos y estándares de seguridad para cada tipo de servicio.

- **Falta de capacitación:** las interfaces y entornos de *cloud computing* son complejas, por lo que es muy común que personal no capacitado opere plataformas y genere riesgos por el simple desconocimiento de las configuraciones básicas. El proveedor debe proporcionar las alertas del caso para que no pasen desapercibidas.

- **Ataque de ciberseguridad:** es conocido que los hackers siempre tienen en la mira a los grandes *vendors* de soluciones o plataformas. Poner en jaque a Google, Amazon, u otro proveedor, es algo que nos deja expuestos como compañías si confiamos en ellos para alojar nuestros datos.

- **Riesgos**

  Los sistemas no son perfectos y las amenazas que citamos anteriormente se transforman en incidentes y en problemas para los clientes. Revisemos a continuación estos riesgos y como mitigarlos.

  - **Usuarios sin privilegios**: algo muy común es asignar roles indebidos a usuarios que pueden poner en riesgo la integridad de la solución.

  - **Regulaciones:** las obligaciones legales y formales de determinados países e industrias, nos exponen a sanciones graves que pueden poner en jaque a la compañía y a sus directivos.

  - **Localización de datos:** no tener control sobre dónde están nuestros datos, nos genera que en determinados contextos estemos en infracción. Por ejemplo, la comunidad europea tiene normas muy especiales respecto a la protección de datos. Es un aspecto muy crítico a tener en cuenta en estos tiempos.

  - **Caídas del servicio:** los incidentes graves pueden darse, por ejemplo, ante catástrofes naturales. Si el proveedor no posee un esquema de réplica o *backup* puede dejarnos fuera de línea o del negocio.

  - **Auditorias:** ya sea por incidentes técnicos o por aspectos legales, podemos recibir una auditoría. El no contar con los *logs* (archivos de back up de transacciones) puede ser un riesgo ante la justicia inclusive.

  - **Garantías del proveedor:** si este ingresa en quiebra o tiene algún problema que lo lleva a no prestar más el servicio, nos expone a perder nuestra operación. Debemos exigir mecanismos de contingencia para estas situaciones.

Desde ya que, al repasar estas amenazas y riesgos, nos preguntaremos si el contar con nuestra infraestructura no nos genera las mismas situaciones. Y la respuesta es muy directa: tenemos tal vez las mismas situaciones, pero con la gran diferencia de que no las gestionamos nosotros sino un externo. Este simple hecho puede ser un factor clave en la decisión de tomar o no un servicio

en la nube. Desde ya que los proveedores *worldclass* nos garantizan la mayoría de estos servicios, pero el tema es que en el medio tenemos muchas alternativas y en determinados casos por costo, cercanía, u otra conveniencia, terminamos eligiendo un *vendor* que no tiene todos los *features* de seguridad o responsabilidad empresarial.

Figura 4. Resumen de beneficios y riesgos de *cloud computing*

BENEFICIOS	RIESGOS
Escala	Pérdida de gobernanza
Diferenciador del mercado	Vinculación
Interfaces normalizadas	Fallo de aislamiento
Escalada rápida de recursos	Cumplimiento
Auditoría	Interfaz de gestión
Actualizaciones	Protección de datos
Concentración de recursos	Supresión de datos insegura o incompleta
	Miembro malicioso

Fuente: Evaluando Cloud, 2015, https://bit.ly/2tCavTf

Por todo esto, es clave identificar el tipo de proveedor, analizar su cartera de clientes, solicitar pruebas y dejar por contrato todo lo que consideremos que es clave para nuestra operatoria. Entonces estamos en condiciones de revisar en detalle los aspectos legales en el próximo capítulo de este módulo.

3.2.2 Aspectos legales

Cuando se decide implementar una solución *cloud*, es necesario tener en cuenta el marco legal existente, ya sea del proveedor, de la actividad, y desde ya del país en el cual está asentada nuestra empresa. Las contrataciones de *cloud* son similares a cualquier otra, en la cual las partes tienen responsabilidades y obligaciones. En este tipo de acuerdos son muy comunes los acuerdos de servicios (ANS) con sus respectivos niveles y detalles.

Un aspecto para revisar en detalle son las condiciones de uso. Los proveedores de la nube presentan estas de manera estándar y en general tienen pocas variaciones, por lo que debe mirarse punto por punto ya que una vez adherido, será complejo litigar o buscar una salida especial. Desde ya que el precio, las características del servicio, los plazos y otros aspectos son claves, pero es muy común pasar por alto estos acuerdos de uso ya que parecen todos similares, pero en esencia no lo son y dependerá de cada tipo de prestación.

Los ANS tienen además anexos muy específicos respecto a las penalidades que surgen de los incumplimientos de las partes, algunas de ellas son:

- *Performance*: tiempos de respuesta, tiempos en servicio, etc.
- Seguridad: mecanismo de autenticación, protocolos de seguridad, normativas, registro de *logs*, etc.

- Datos: *back ups*, importaciones, exportaciones, etc.
- Privacidad: normativas, roles, métodos de control, etc.

Desde el punto de vista del tipo de contratos, nos encontraremos con tres variantes.

1) **Adhesión**: es tal vez la más común en *cloud computing*. Es fundamental comprender que no tenemos posibilidad de cambiar o ajustar cláusulas, simplemente debemos aceptar lo que propone el proveedor por lo que debemos buscar un escenario que se ajuste a nuestras necesidades.

2) **Ad Hoc:** el cliente y el proveedor se ponen de acuerdo en cada uno de los ítems, ya sea seguridad, disponibilidad, datos, etc. No es común que se de en este extremo, sino más bien se presentan distintas alternativas parametrizadas.

3) **Mix de 1 y 2:** algunas cláusulas son fijas y otras a medida o negociables. Esta suele presentarse por los vendedores más experimentados como una solución Ad Hoc, pero en esencia son modelos preseteados que ya están analizados por el mismo.

Luego de haber analizado muchas situaciones de este tipo, podemos indicar que los proveedores tienen esquemas que están siempre propensos a favorecer la venta y a captar clientes. Es decir, en principio podemos encontrarnos con un contrato de adhesión sin posibilidades de modificación, pero ante escenarios de gobierno, industrias muy reguladas, grandes volúmenes, el proveedor se suele flexibilizar entendiendo que el negocio lo requiere. Como indicaba al inicio, la venta consultiva es gran parte de la clave de estos acuerdos y nos toparemos con proveedores que nos escuchan, toman nota, y vuelven a nosotros con soluciones que parecen *ad hoc*, pero que en realidad son una combinación de las alternativas que ya tienen en su caja de herramientas. Nosotros desde el lado del cliente debemos estar prestos a negociar y a revisar en detalle aquellas cláusulas que están cerradas a cualquier modificación.

Ya veremos más adelante las modalidades de contratación, pero encontraremos algunas diferencias contundentes entre las nubes públicas y las privadas. Estas últimas en general nos dan mucho más margen de negociación, pero desde ya, que siempre a nivel de costos, serán algo superiores a las públicas, las cuales están diseñadas para satisfacer la demanda genérica. En conclusión, desde lo legal debemos tener en cuenta que:

- *Cloud computing* no es un servicio de telecomunicaciones regulado;
- el proveedor y el cliente establecen una relación jurídica de tipo civil;
- las partes deben regular dicha relación jurídica mediante la suscripción de un contrato privado.

Revisemos en detalle las variantes de contratación para tener un panorama más amplio de las opciones que tendremos a nivel contractual.

3.2.3 Modalidades de contratación

Los servicios en la nube se ofrecen bajo tres alternativas. Es importante comprender las diferencias entre estas variantes, dado que las mismas nos darán opciones de flexibilidad en la configuración y, como citamos anteriormente, en la negociación de los servicios. En resumen, estas opciones son:

1) **Nube pública:** espacios y servicios compartidos por distintos clientes.
2) **Nube privada:** recursos exclusivos para nuestra empresa.
3) **Nube híbrida:** mix entre servicios públicos y privados.

A continuación, profundizamos en cada modelo.

- **Servicios en nube pública:** las instalaciones del proveedor se comparten con distintitos clientes, es decir, almacenamiento, procesamiento, seguridad, y todo lo que un data center tiene, está dividido en secciones o porciones físicas o lógicas que son asignadas de manera dinámica a los clientes. Esto genera grandes beneficios tales como:

  - escalabilidad
  - ahorro de tiempo y costes
  - mayor eficiencia de los recursos.

  Empresas de almacenamiento de correo, hosting web, y otros, son un ejemplo y en general se trabaja en esta modalidad con contratos de adhesión.

- **Servicios en nube privada:** el proveedor garantiza la separación de los servicios y mayores niveles de control y auditoría por parte del cliente. Las principales ventajas que podemos encontrar son:

  - cumplimiento de normativas y políticas corporativas;
  - mayor seguridad que la pública (a mayor costo);
  - control total de los recursos.

  En estos casos nos encontraremos con acuerdos a medida y muchas opciones de negociación, pero sin dudas costos y gestión más elevados. En esta categoría nos encontramos con proveedores locales de infraestructura como las Telcos o empresas de telecomunicaciones, que nos permiten alojar nuestras aplicaciones en sus *data centers*.

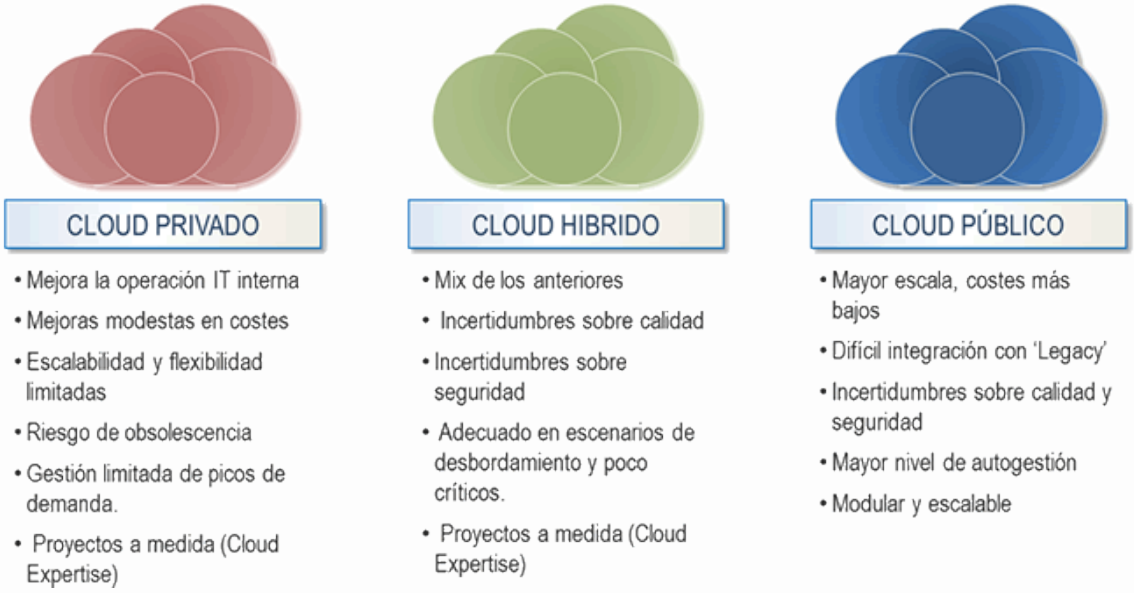
- **Servicios en nube híbrida:** desde una misma consola de administración nos permiten acceder a servicios públicos y privados. En muchos casos también facilitan la administración de aplicaciones *On premise* o instaladas en nuestros equipos. Las principales ventajas son:

  - potenciar la capacidad operativa, aprovechando lo mejor de cada mundo;

- reducción de costos, frente a una nube privada;
- seguridad entre ambos entornos.

Proveedores como Oracle, los cuales brindan servicios de CRM y ERP suelen ofrecer esta variante en la cual el CRM (datos de relacionamiento de clientes) está en la versión pública, y el ERP que maneja todos los datos contables, en un entorno privado. Aquí las modalidades de contratación mixtas son las que prevalecen. Como podemos apreciar el concepto de la nube se ha extendido y las variantes son muchas, por lo que es relevante siempre conocer el escenario de negocio, legal y fiscal, para luego iniciar la evaluación de soluciones.

Figura 5. Comparativo entre soluciones *cloud*.



Fuente: Nexica, 2013, https://bit.ly/2RMifd8

3.2.4 Protección de datos

Desde hace ya varios años, determinados organismos internacionales se han concentrado en la protección de los datos personales y la intimidad de los usuarios. Normas como RGPD, LOPD, ISSI y otras, han buscado estandarizar y garantizar a los consumidores que sus datos estarán seguros y serán utilizados de acuerdo con lo que hemos aceptado en los términos y condiciones.

Para poner un ejemplo RGDP (Reglamento General de Protección de Datos), es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. El RGPD considera datos personales a toda información (tales como el aspecto físico o incluso datos biométricos) sobre una persona física identificada o identificable.

Estos estándares, son muy importantes en el entorno de la nube, ya que debemos estar muy al día dado que el no cumplimiento de los mismos, presenta sanciones económicas y legales muy rigurosas.

Estos consideran la recogida de datos personales, desde algo tan elemental como la *cookie*, hasta algo tan detallado como la ficha de un contacto en una base de datos de gestión de relaciones con clientes (o CRM), o incluso más. Aunque los datos personales se recojan o traten únicamente en beneficio de esa persona, siguen quedando protegidos dentro del ámbito del RGPD (Excelius, s.f.).

Normas relativas a los datos personales: principios de la protección de datos, tratamiento lícito y limitaciones a las transferencias internacionales. Siempre se debe utilizar *software* o plataformas que garanticen la seguridad y privacidad de los datos en todos los entornos.
Algunos ejemplos de implementación de estas normativas son:

- Agregar leyendas y botones de aceptación sobre recolección de datos a través de cookies.

- Los formularios deben contar con la posibilidad de una declaración u otra acción afirmativa sobre cada acción que se realizará con el dato. No puede haber casillas pre completas y se debe detallar cada acción (uso, promoción, y difusión comercial institucional, aceptación de legales). La persona debe poder elegir la información que necesita o requiere. No es suficiente con aceptar la leyenda "Acepto términos y condiciones".

- Se debe agregar dentro de las secciones de "legales" que la protección de datos adoptada respeta RGPD, tiempo de guardado y uso de ese dato.

Tal vez estemos familiarizados con estas opciones como usuario, pero al momento de contratar proveedores en la nube, debemos estar seguros de que ellos irán actualizando estas normativas. Es parte de nuestro análisis seguir esta tendencia dado que se irá acentuando y poniendo cada vez más estricta con el paso del tiempo. A continuación, en la figura 6 presentamos los principales puntos de una de las reglamentaciones más extendidas.

Figura 6. Principales puntos de la normativa RGPD

Fuente: Gazquez, 2018, https://bit.ly/2ur1lmX

Referencias

Colubriale, F. (2017). Tecnologías de Marketing Digital. Cátedra de la Tecnicatura en Marketing Digital, Universidad Empresarial Siglo 21

Excelius. (s.f.). *Reglamento General de Protección de Datos (RGPD)* [entrada de blog]. Recuperado de http://excelius.cat/es/reglamento-general-de-proteccion-de-datos

Evaluando Cloud. (2015). *7 beneficios y 9 riesgos del Cloud Computing* [entrada de blog]. Recuperado de https://evaluandocloud.com/7-beneficios-y-9-riesgos-del-cloud-computing/

Evaluando Cloud. (2018). *Seguridad y privacidad en la nube ¿de quién es la responsabilidad?* [entrada de blog]. Recuperado de https://evaluandocloud.com/seguridad-privacidad-la-nube-quien-la-responsabilidad/

Gazquez, J. (2018). Se avecinan cambios: los negocios online ya se preparan para la nueva ley de protección de datos. En El Mundo [versión digital]. Recuperado de https://www.elmundo.es/economia/2018/05/14/5af9a194e2704e08648b463a.html

Kinsta. (2019). Cuota de mercado de la nube – una mirada al ecosistema de la nube en 2020 [entrada de blog]. Recuperado de https://kinsta.com/es/blog/cuota-de-mercado-de-la-nube/

Nexica. (2013). Modelos de despliegue cloud: Cloud privado, cloud público y cloud híbrido [entrada de blog]. Recuperado de https://www.nexica.com/es/blog/modelos-de-despliegue-cloud-cloud-privado-cloud-p%C3%BAblico-y-cloud-h%C3%ADbrido

Rodríguez, M. (2019). ¿Sabías que…? Qué son los microservicios y por qué son el futuro en la arquitectura de software [página web]. Recuperado de https://www.cloudmasters.es/sabias-que-que-son-los-microservicios-y-por-que-son-el-futuro-en-la-arquitectura-de-software/

Sage España [Sage España]. (11 de octubre de 2013). *La seguridad en la nube* [YouTube]. Recuperado de https://www.youtube.com/watch?v=vqyuNha0Rek

Universia México. (2017). El 70% de las empresas utilizan la nube para trabajar [página web]. Recuperado de http://noticias.universia.net.mx/practicas-empleo/noticia/2017/01/03/1148061/70-empresas-utilizan-nube-trabajar.html