

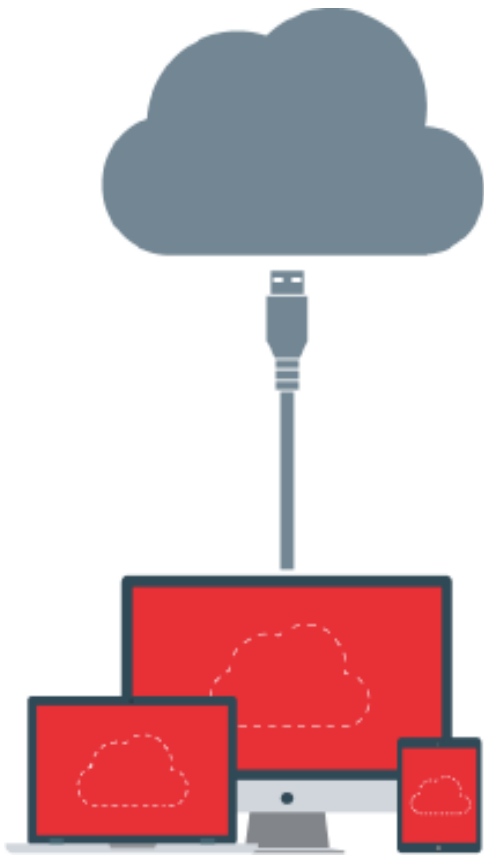


INICIO GRABACIÓN



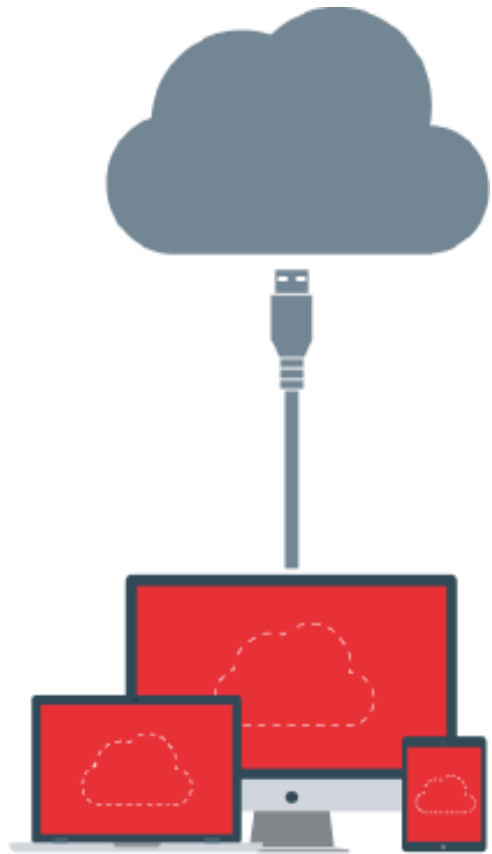
SANJOSÉ
FUNDACIÓN DE EDUCACIÓN SUPERIOR

INTRODUCCIÓN



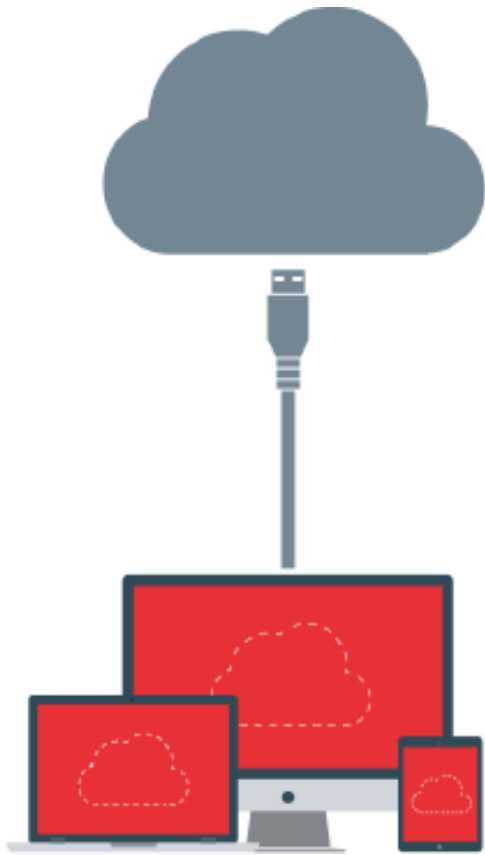
Frente a las estrategias de computación tradicionales, es decir, el alquiler de equipos y centros de datos internos, **el cloud pone al alcance de las pymes aplicaciones informáticas sin necesidad de adquirirlas, sólo contratándolas como servicio.** Se ha pasado de comprar o alquilar las máquinas a pagar únicamente por el uso que necesitemos.

INTRODUCCIÓN



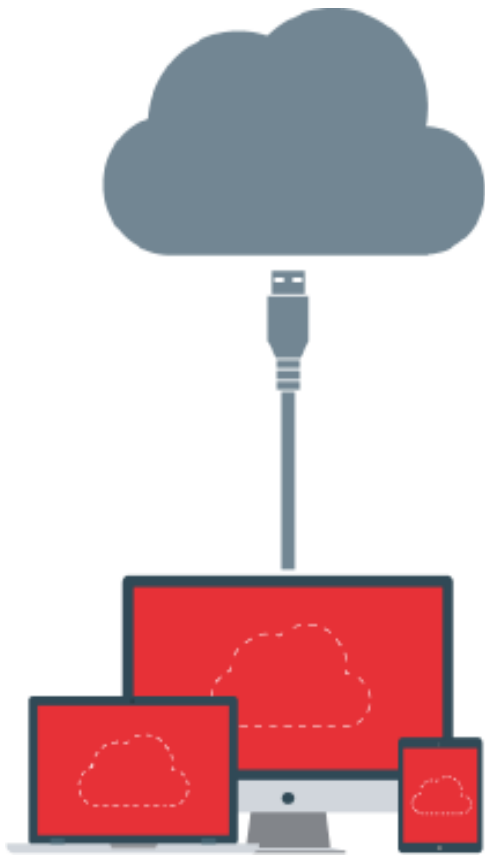
La tecnología de la nube permite al proveedor ofrecer aplicaciones y servicios tecnológicos accesibles a través de la red. Se puede acceder a estos servicios desde cualquier lugar y con disponibilidad total todos los días del año. Además, **se puede contratar al proveedor el despliegue de las aplicaciones de la empresa en la nube.** En cualquier caso se establecen acuerdos de nivel de servicio (o SLA del inglés *Service Level Agreements*) en los que se definen las responsabilidades del mantenimiento, actualización, incidencias, disponibilidad y recuperación.

INTRODUCCIÓN

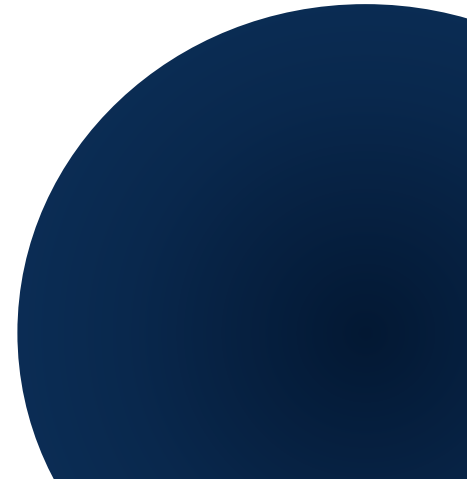


El cloud se basa en ofrecer «**los mismos**» recursos a los clientes **desde equipos en red**. Esto quiere decir que se ofrece el mismo software (en las mismas versiones) para todos por lo que se consigue mayor fiabilidad, flexibilidad y escalabilidad, y mejoras en el rendimiento. Por esto también **es más interoperable**, es decir, se puede integrar con mayor facilidad y rapidez con el resto de las aplicaciones empresariales (en *cloud* o no).

INTRODUCCIÓN



Este nuevo modelo **evita al cliente** (la empresa que contrata el servicio cloud) **la preocupación de comprar y mantener la infraestructura y los elementos técnicos de la misma**, que son ofrecidos por el proveedor como un servicio



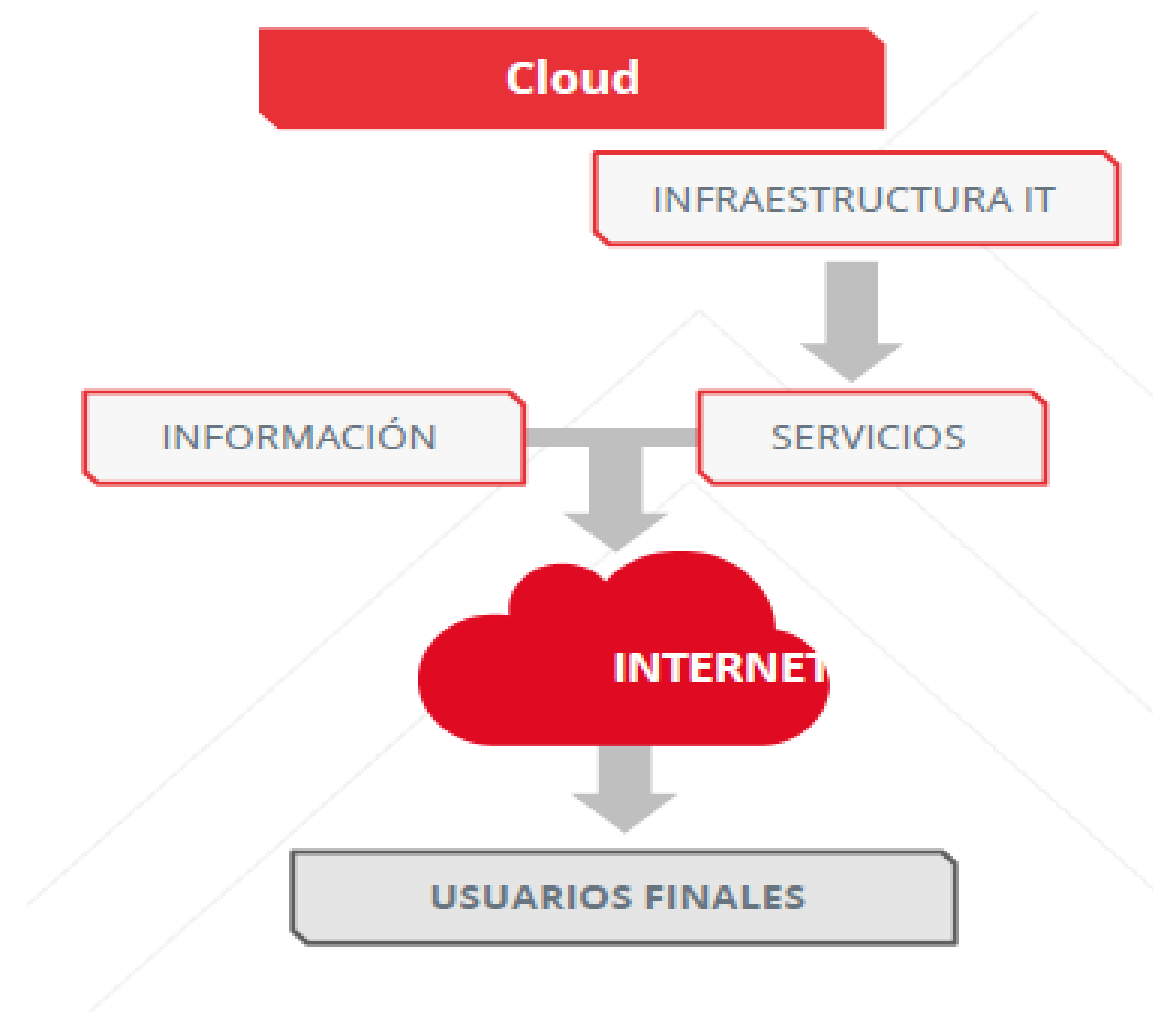
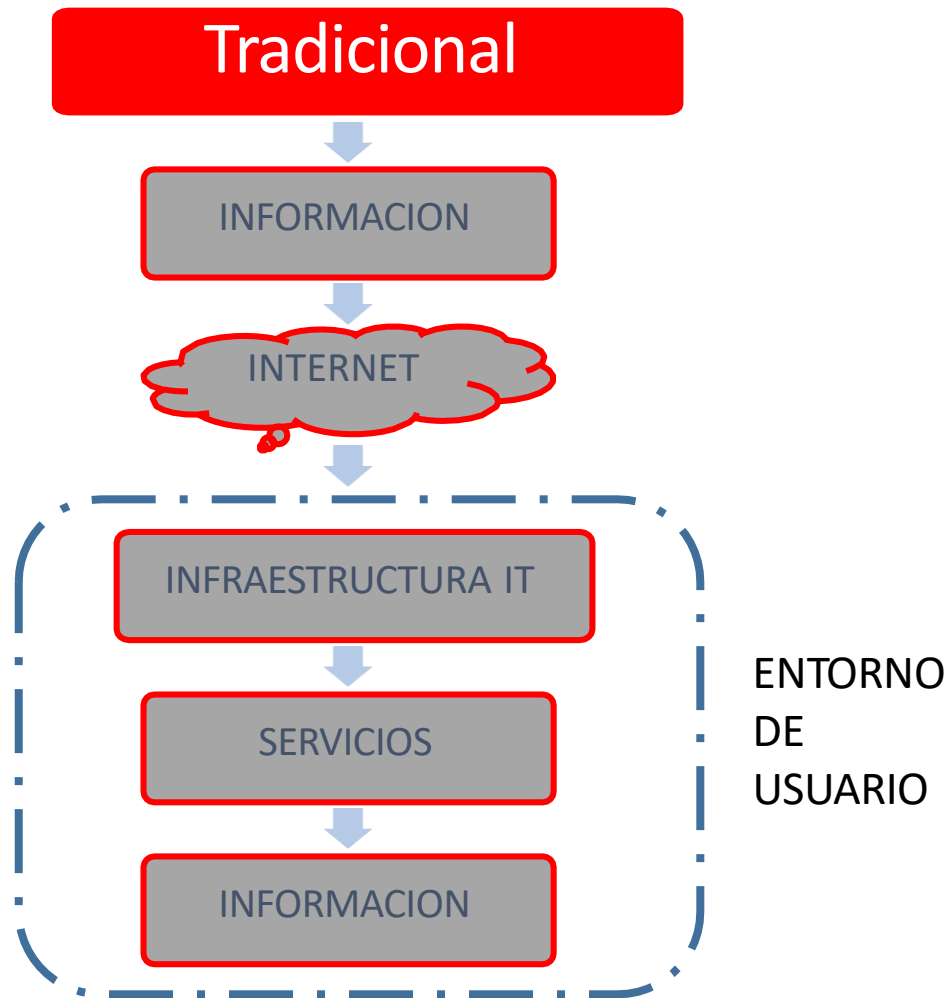


INTRODUCCIÓN



Los servicios que se pueden contratar en la nube pueden ser: **bases de datos, servidores de correo electrónico, almacenamiento, servidores web, herramientas de gestión, servidores de aplicaciones, entornos de desarrollo, redes, etc.**

Modelo tradicional vs Modelo cloud.



Modelo tradicional vs Modelo cloud.



Así, desde la empresa o desde dispositivos conectados a internet (mediante interfaces web o con apps) los empleados y colaboradores **tendrán acceso a los servicios que necesiten**, como por ejemplo:

Salesforce CRM: software para la administración de la relación con clientes (ventas, marketing,...) o CRM.

Dropbox: servicio que permite a los usuarios almacenamiento en la nube y sincronización de ficheros en línea desde diferentes dispositivos.

Office 365: suite de servicios como correo, gestión documental, mensajería instantánea, etc.

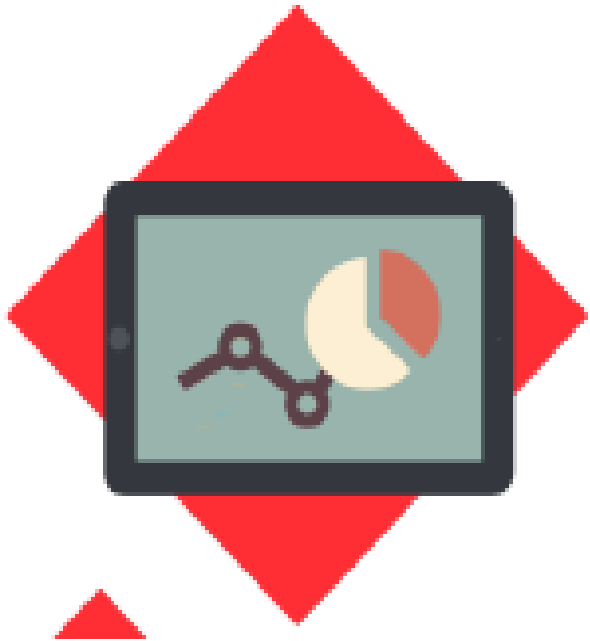
Gmail: servicio de correo electrónico que forma parte de Google Apps (Calendar, Drive, Docs) un paquete de productividad en cloud para negocios

El cloud es posible debido a la evolución y unión de varias tecnologías:



Capacidad de procesamiento o de cálculo.

Desde la aparición de la informática, la capacidad de cálculo de los ordenadores ha ido creciendo de forma exponencial. La evolución de la tecnología permite crear clústeres de ordenadores (ordenadores conectados con redes de alta velocidad) cuya capacidad de procesamiento es aún mayor. **Los proveedores de *cloud* han visto en esto una oportunidad de negocio: ofrecer capacidad de**



El cloud es posible debido a la evolución y unión de varias tecnologías:



Capacidad de almacenamiento. La evolución tecnológica hace posible infraestructuras de almacenamiento más eficientes en cuanto a capacidad y velocidad de transferencia. **El *cloud* permite a las pymes tener al alcance sistemas de almacenamiento rápidos y de gran capacidad sin necesidad de disponer de infraestructura.**

El cloud es posible debido a la evolución y unión de varias tecnologías:



Acceso a internet.

La conexión a Internet se ha extendido y abaratado, permitiendo que el número de conexiones aumente y aparezcan nuevos tipos de negocio que aprovechan esta conectividad, como por ejemplo, las redes sociales o el *ecommerce*. **Para los proveedores de servicios en *cloud*, internet es esencial como medio de acceso de sus clientes.**

El cloud es posible debido a la evolución y unión de varias tecnologías:



Dispositivos móviles.

La aparición de *tablets*, *smartphones*, etc... hace posible que podamos estar **siempre conectados y acceder a los recursos de la empresa incluso cuando estamos de viaje o desplazándonos**. Las aplicaciones *cloud* aprovechan esta funcionalidad para ofrecer servicios y aplicaciones móviles (gestión de flotas, partes de obra...).



El cloud es posible debido a la evolución y unión de varias tecnologías:



Virtualización.

Es un mecanismo software que permite utilizar un equipo para «hospedar» a otros diferentes.

El software de virtualización hace que una máquina pueda albergar «virtualmente» a otras distintas y comportarse como ellas. Esta tecnología se aprovecha en algunos servicios *cloud* y proporciona al proveedor flexibilidad para mover y reservar los recursos.

¿Sabías qué?

- ♦ El **99%** de las pymes y grandes empresas tiene **ordenadores** y el **98%** dispone de **conexión a Internet**, frente al **95,3%** de **teléfono móvil**.
- ♦ Empresas que han comprado alguno de los siguientes **servicios de computación en la nube (%)**



Fuente: ONTSI. Elaborado con datos INE 2014

PAGO POR USO	<p>Se refiere al cálculo del precio en función de las necesidades del cliente de una manera flexible.</p> <p>Si necesito más capacidad de proceso por un pico de trabajo solicitaré más recursos y sólo tendré que pagar más por el tiempo de uso extra.</p>
ACCESO DESDE LA RED	<p>Debido a que los recursos están alojados en la red, se puede acceder a los mismos desde cualquier lugar.</p> <p>Es posible acceder a la gestión de nuestras aplicaciones y como usuarios, desde distintas oficinas o desde el teléfono móvil</p>
RECURSOS COMPARTIDOS	<p>Los recursos computacionales (servidores, comunicaciones, almacenamiento, máquinas virtuales, etc.) están en reservas comunes para aquellos clientes que contraten un servicio de nube pública, es decir, se comparte hardware y software. Disponemos de recursos que de otra forma no podríamos costear.</p>

RECURSOS A LA CARTA

Los clientes pueden redimensionar sus propias necesidades de recursos (memoria, almacenamiento, comunicaciones,...) de manera rápida y eficaz en casi cualquier momento.

Si aumenta nuestra necesidad de recursos podemos cambiarla desde el panel de control de cloud y estará a nuestra disposición al instante.

SERVICIO SUPERVISADO

El control y optimización de recursos se hace de manera automática por los servicios de la nube gracias a su capacidad de evaluación, siendo este proceso, transparente para el cliente.

No tenemos que prever la compra de más equipos o de nuevas licencias de software, ni tendremos que contratar técnicos para mantenimiento de equipos.



VENTAJAS DEL USO DE LA NUBE

AHORRO DE COSTES	Este ahorro se debe a la reducción de los costes de infraestructura y su mantenimiento, licencias de uso, personal, etc. Se paga por uso de recursos.
OPTIMIZACIÓN DE RECURSOS	Los recursos (equipos, técnicos, etc.) se utilizan cuando se necesitan y se paga por este uso. Si tenemos un pico pagaremos más. Esto supone un ahorro en la infraestructura que tendríamos que comprar si queremos cubrir esos picos.
RECUPERACIÓN ANTE DESASTRES	La información y las aplicaciones están almacenadas en la nube y en distintas ubicaciones. Si se produjera algún incidente grave, esa información seguiría estando accesible.



VENTAJAS DEL USO DE LA NUBE

TECNOLOGÍA ACTUALIZADA Y SEGURA	El proveedor del servicio en la nube es el encargado de realizar las tareas de mantenimiento, que son transparentes para el cliente.
DEDICACIÓN AL NEGOCIO	Al reducir la carga de trabajo para la administración de los sistemas TIC podemos dedicar mayor esfuerzo en la gestión de nuestro negocio.

PÉRDIDA DE CONTROL	Como cliente de servicios cloud no tendremos acceso a instalaciones donde se están ejecutando nuestras aplicaciones. Dejamos nuestros datos y aplicaciones en manos del proveedor. Debemos leer con detalle el contrato de suministro: ubicación, disponibilidad, responsabilidades, etc.
CONFIDENCIALIDAD Y SEGURIDAD EN LOS DATOS	La información de nuestra empresa (datos de clientes, facturas,...) va a estar almacenada en los servidores del proveedor y, en caso de que sufra un problema técnico o de seguridad, nuestra información puede verse comprometida.
DISPONIBILIDAD DEL SERVICIO	La nube, como cualquier otro servicio, no está exenta de problemas y puede ocurrir que se caiga. Como consecuencia de ello los servicios que ofrece podrían no estar disponibles.
ACCESO A INTERNET	El acceso a las aplicaciones está condicionada a que tengamos acceso a Internet. Si no tenemos acceso por algún motivo, no tendremos acceso a las aplicaciones.

SERVICIOS DISPONIBLES EN LA NUBE

- aplicaciones finales que podrá administrar desde una interfaz web
- plataformas para almacenamiento, desarrollo, servidores web, etc.
- infraestructuras completas (centros de datos, comunicaciones,)



OPCIONES DE CONTRATACIÓN

Los servicios que una empresa puede contratar en la nube se ofrecen en tres niveles diferentes, en función del control que el usuario final tenga sobre la infraestructura tecnológica.

Como es lógico, no todos los clientes tienen las mismas necesidades y, por lo tanto, existen diferentes opciones de contratación.

SERVICIOS DISPONIBLES EN LA NUBE



OPCIONES DE CONTRATACIÓN

1

SaaS

Software as a
Service
(Software como
Servicio)

2

PaaS

Platform as a
Service
(Plataforma como
Servicio)

3

IaaS

Infrastructure as
a Service
(Infraestructura
como Servicio)

SERVICIOS DISPONIBLES EN LA NUBE

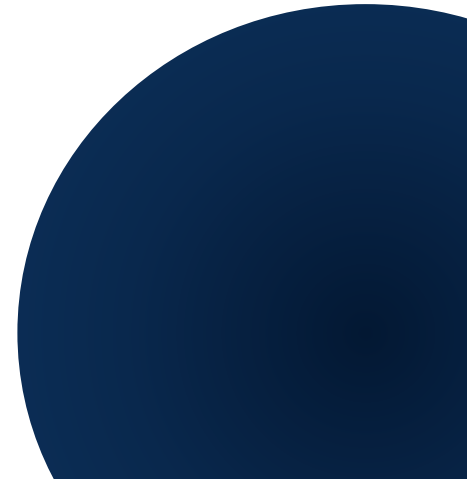


SaaS - Software como Servicio

El cliente utiliza **software**, como por ejemplo una aplicación de nómina alojada en la nube, que el **proveedor** le proporciona.

Se puede **acceder y administrar las aplicaciones** desde diferentes dispositivos a través de una interfaz web o una app.

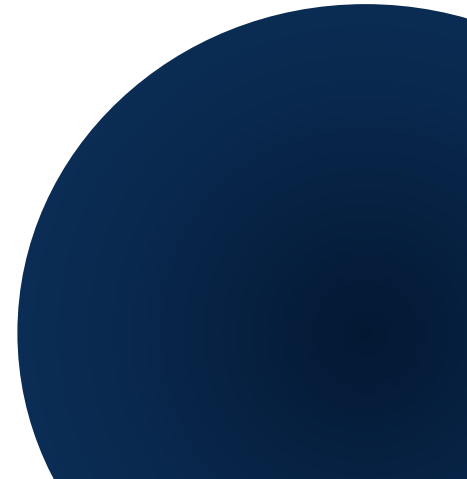
El **cliente no gestiona ni controla la infraestructura** existente en la nube. Este proceso es totalmente transparente para él





SaaS - Software como Servicio

Ejemplo: correo electrónico a través de web, almacenamiento tipo Dropbox, un blog sencillo (tipo Blogger o Wordpress.com) o herramientas para creación sencilla de páginas web tipo Wix, Weebly, Jimdo, etc.

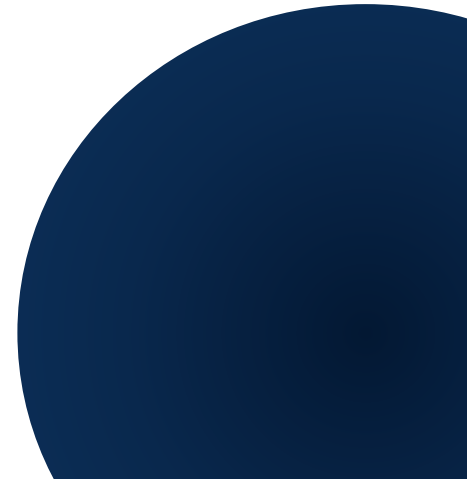




SaaS - Software como Servicio

Adecuado para organizaciones que solamente necesitan aplicaciones que el proveedor proporciona y se ajustan a sus necesidades.

No existen costes tecnológicos de hardware, software y soporte técnico.
Suele ser atractivo para pymes.



SaaS - Software como Servicio



VENTAJAS

- Reducción drástica de costes
- Reducción de tiempos debido a que el software ya está instalado
- Escalabilidad
- Facilidad de uso

INCONVENIENTES

- Integración con aplicaciones existentes en la organización
- Incertidumbre en relación al dueño de las aplicaciones
- Gran dependencia del proveedor




PaaS - Plataforma como Servicio



El **cliente despliega sus propias aplicaciones** en la infraestructura proporcionada por el proveedor, que da una plataforma de procesamiento completa al usuario.

El **cliente no gestiona ni controla la infraestructura** existente en la nube. Este proceso es totalmente transparente para él.

El **proveedor proporciona** al cliente la **capacidad de gestionar las aplicaciones desplegadas** y la posibilidad de **controlar las configuraciones de entorno** (tipo de base de datos, capacidad de almacenamiento, número de usuarios, permisos...)






PaaS - Plataforma como Servicio



Ejemplo: correo electrónico corporativo que instalamos en la plataforma o una web que creamos y mantenemos nosotros, instalando aplicaciones como el gestor de contenidos o CMS (Drupal, Joomla, Wordpress.org) en un servicio de alojamiento compartido (que nos proporciona la base de datos y el entorno de desarrollo web).



PaaS - Plataforma como Servicio



VENTAJAS

- Facilidad para administrar la plataforma
- Sencillez a la hora de permitir un desarrollo propio
- Facilidad de integración con el resto de la plataforma

INCONVENIENTES

- Dependencia del proveedor
- Dudas sobre la confidencialidad de los datos



PaaS - Plataforma como Servicio



Adecuado para organizaciones que deseen desarrollar sus propias aplicaciones sobre la infraestructura que proporciona el proveedor.

Conlleva unos costes de soporte y software.

Bastante atractivo para las pymes.





IaaS - Infraestructura como Servicio



El **cliente dispone de la infraestructura completa**, es decir, del hardware necesario como servidores, sistemas de almacenamiento, dispositivos de comunicaciones, etc.

El **cliente** puede instalar el software necesario y **desplegar sus propias aplicaciones desde cero**.

Ejemplos: redes internas de empresa (infraestructura corporativa), sistemas de respaldo, hosting virtual y centros virtuales de datos.





IaaS - Infraestructura como Servicio



Adecuado para organizaciones que necesitan una mayor versatilidad ya que permite ejecutar prácticamente lo que la organización desee.

Coste elevado, ya que la organización es la encargada de mantener todo el software y el hardware virtual.

No es muy atractivo para las pymes.





IaaS - Infraestructura como Servicio



VENTAJAS

- **Flexibilidad en relación a la infraestructura necesaria por el cliente**
- **Rapidez de instalación**
- **Facilidad al desplegar las aplicaciones del cliente**

INCONVENIENTES

- Soporte ofrecido ya que al estar externalizado el servicio es más complicado solucionar el problema de una forma rápida



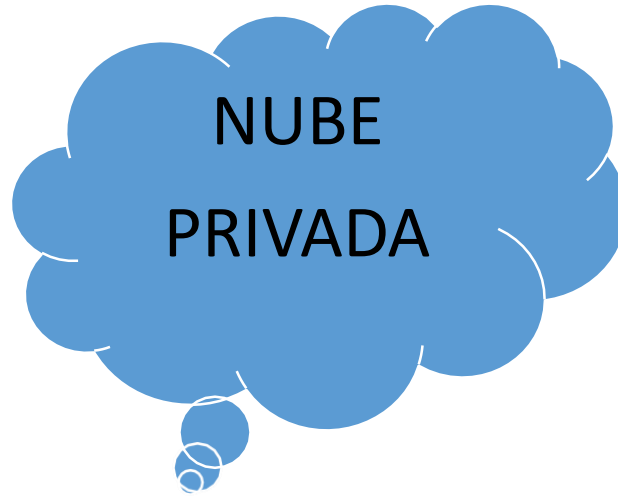
Independientemente de las diferentes formas de contratación que hemos visto, **existen distintas formas de prestar los servicios *cloud*** según el grado en el que se comparten los recursos.

Por ello, dependiendo de las necesidades de la organización, de dónde se encuentren instaladas las aplicaciones de la misma y de qué clientes puedan usarlas, se hace una distinción entre los siguientes **tipos de nube**.



Una
infraestructura
cloud para
muchos clientes.

- Adecuado para negocios que no temen compartir recursos.
- Gran capacidad de expansión (escalabilidad) a bajo coste.



Uso exclusivo para cada cliente de cloud.

- Adecuado para cuando no se prevé aumentar recursos a corto plazo.
- Diseño específico

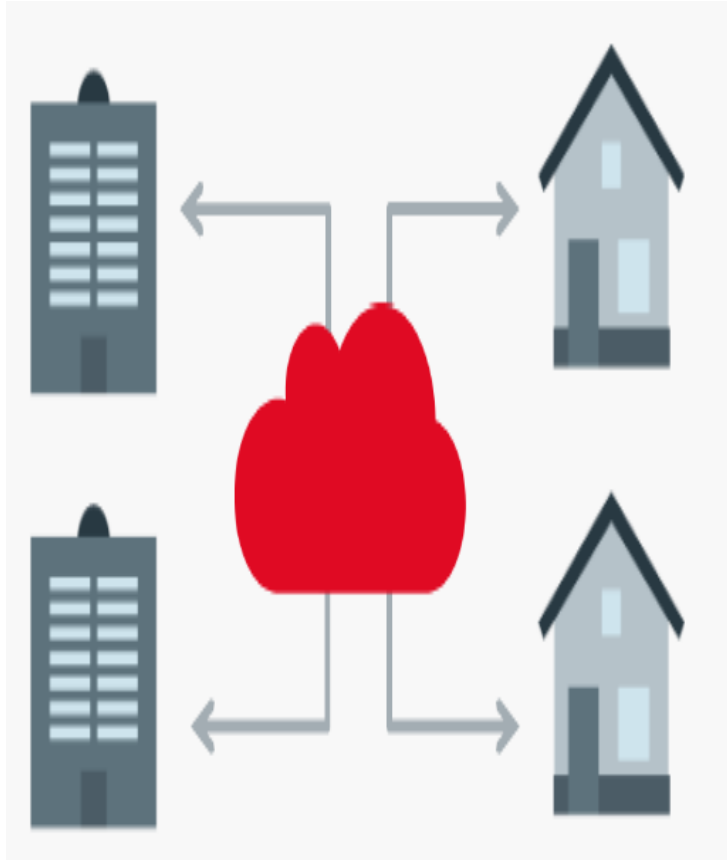
NUBE HÍBRIDA



Una parte en nube privada y otra en nube pública.

- Las aplicaciones fundamentales para el negocio en la parte privada.
- Útil si se necesita aumentar recursos a corto plazo (sobre la parte pública).

NUBE PÚBLICA



- La **infraestructura es compartida** entre varios clientes de cloud.
- Está **disponible para el público en general**.
- La **propiedad** de la nube es de una **organización externa**.

Ejemplo:

- Google Drive gratuito
- Dropbox



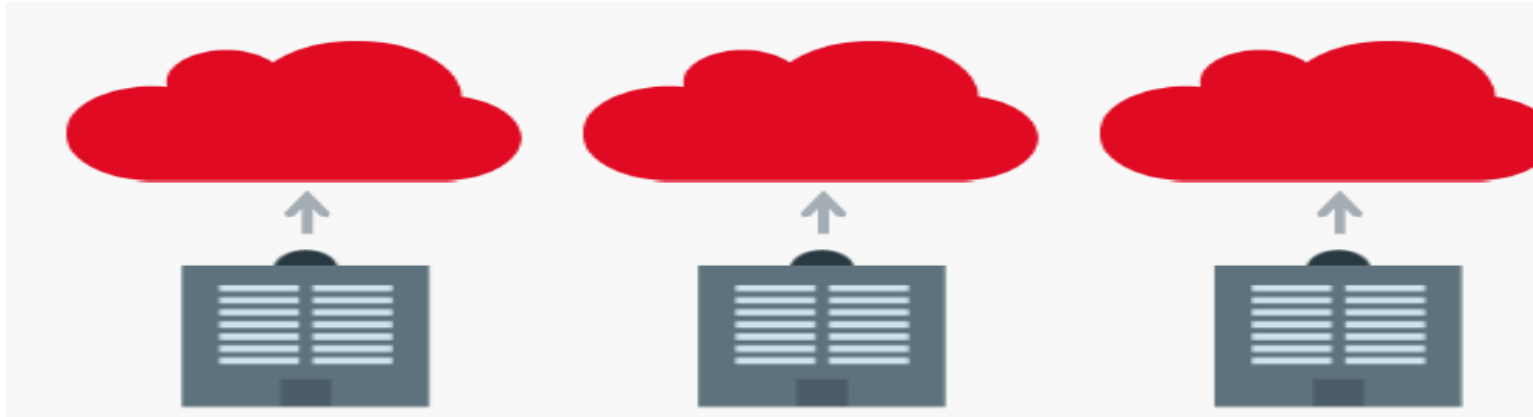
VENTAJAS

- Escalabilidad
- Ahorro de tiempo y costes
- Mayor eficiencia de los recursos

INCONVENIENTES

- La infraestructura es compartida
- Hay poca transparencia para el cliente de cloud ya que no se sabe el resto de recursos que se pueden estar compartiendo

NUBE PRIVADA



- La **infraestructura es única** para una organización.
- La nube puede ser **manejada por la organización o por un tercero**.
- Puede estar **dentro o fuera de las instalaciones**.

Ejemplo:

- Amazon VPS
- IBM Softlayer



NUBE PRIVADA

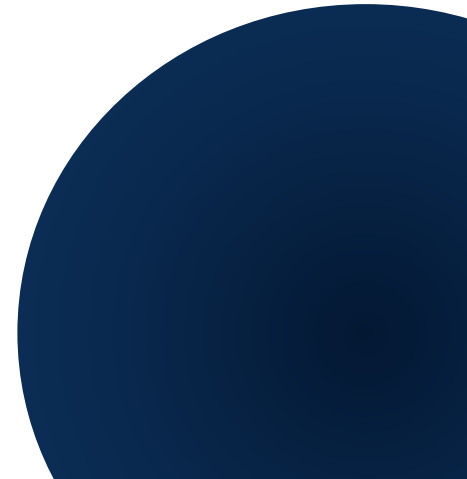


VENTAJAS

- Cumple con las políticas internas, ofreciendo mayor seguridad que la pública
- Control total de los recursos

INCONVENIENTES

- Elevado coste
- Dependencia de la infraestructura contratada

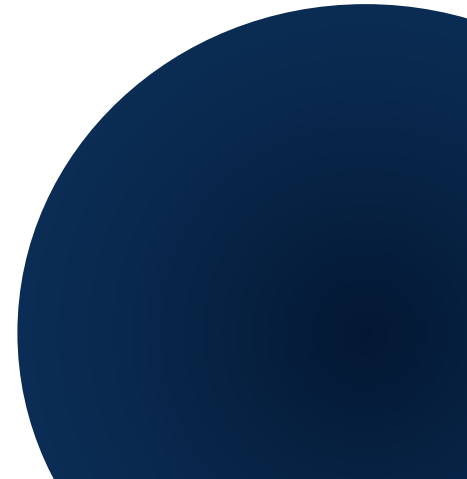




NUBE HÍBRIDA

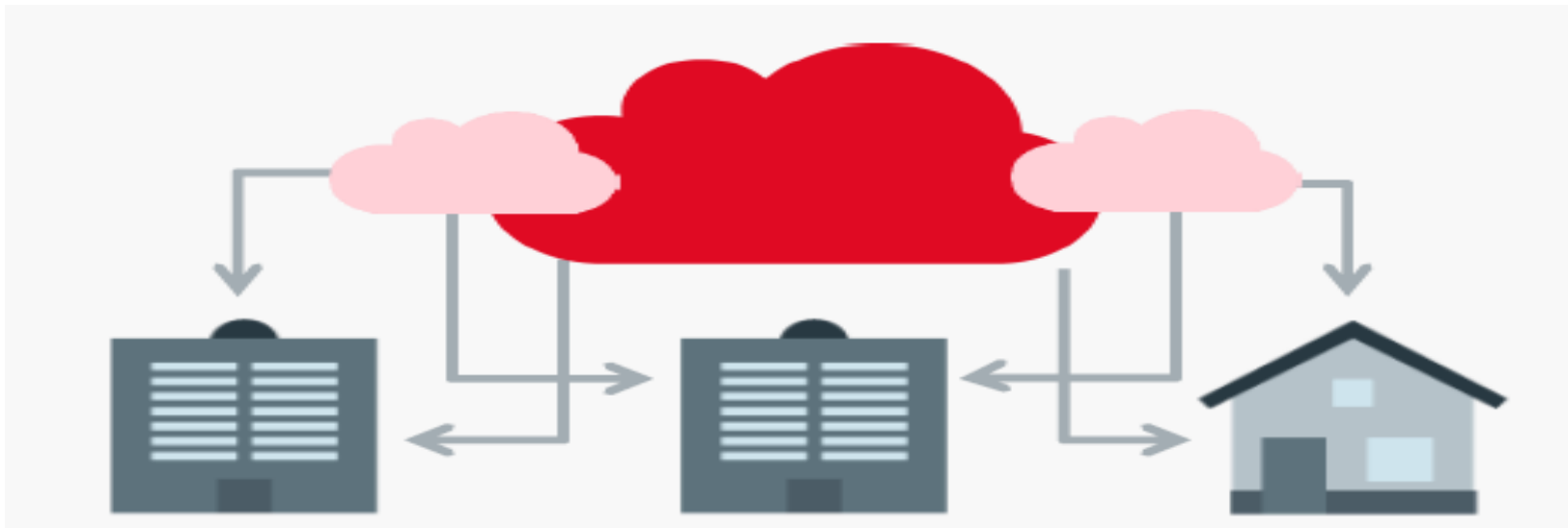


- La nube híbrida es **una combinación entre nube pública y privada.**
- Los diferentes usuarios (clientes de cloud) tienen **partes compartidas y partes privadas.**
- Las diferentes nubes que la forman son **entidades separadas**, pero unidas por la misma administración.



Ejemplo:

- VMware vCloud Air
- IBM Bluemix



NUBE HÍBRIDA



VENTAJAS

- **Maximiza el valor al utilizar recursos privados y compartidos**
- **Reducción de costes**

INCONVENIENTES

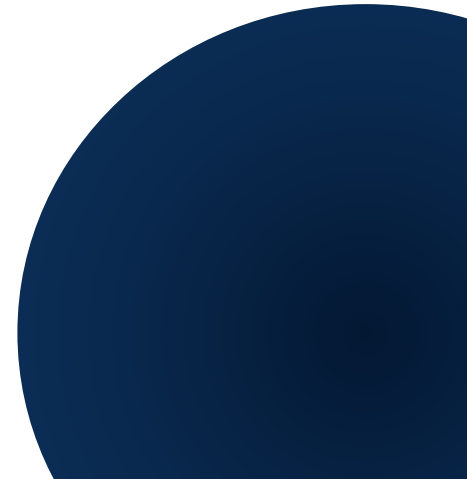
- Riesgo al combinar dos modelos de implementación diferentes
- Control de la seguridad entre ambas nubes

● CONTRATACIÓN DE SERVICIOS EN LA NUBE



A la hora de **elegir un proveedor**, se deben tener en cuenta diferentes aspectos:

- **Tratamiento** de los datos.
- **Localización** de los datos.
- Opciones de **portabilidad** de los datos.
- **Servicios** ofrecidos.



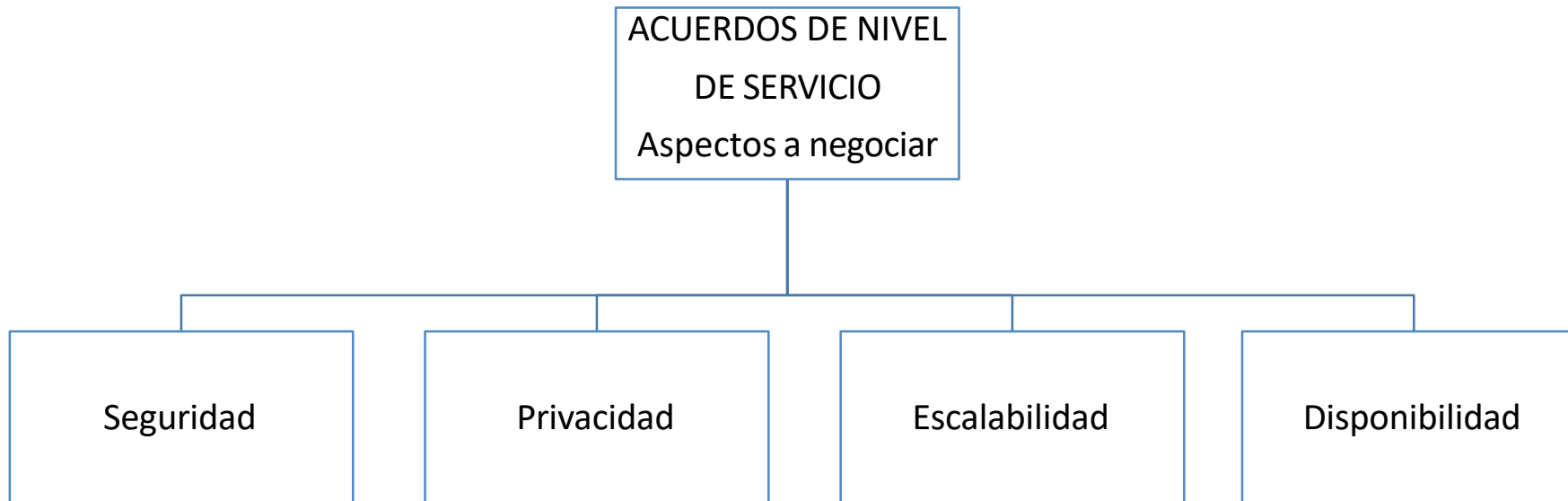
CONTRATACIÓN DE SERVICIOS EN LA NUBE



- **Acuerdos de nivel de servicio:**
 - **Unilateral:** no se puede negociar el acuerdo; se da en nubes públicas.
 - **Parcialmente definido:** se pueden negociar algunas cláusulas del acuerdo; se suele dar en nubes híbridas y privadas.
 - **Negociable:** se puede negociar casi en su totalidad; se suele dar en nubes privadas.



CONTRATACIÓN DE SERVICIOS EN LA NUBE



CONTRATACIÓN DE SERVICIOS EN LA NUBE



En cualquier caso, **todo los puntos a tratar dependerán del servicio que se contrate**, aunque es recomendable tener en cuenta lo siguiente:

- Medidas de seguridad adoptadas por el proveedor para conservar nuestros datos.
- Confidencialidad de los datos almacenados por el proveedor.
- Calidad de servicio por parte del proveedor.
- Seguridad en las transacciones de datos.

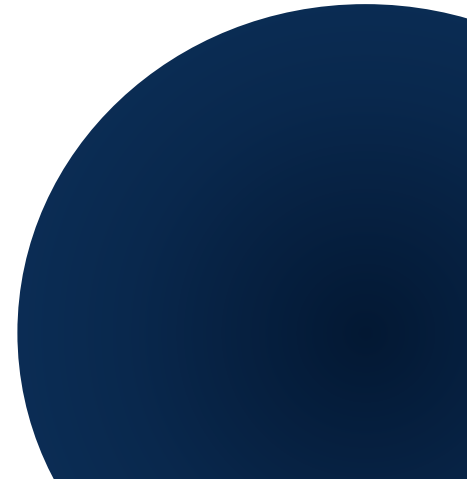




CONSIDERACIONES LEGALES



Cuando se decide implementar una solución *cloud* es necesario tener en cuenta el **marco legal existente, tanto del país donde reside la organización como del país del proveedor del servicio en la nube.**



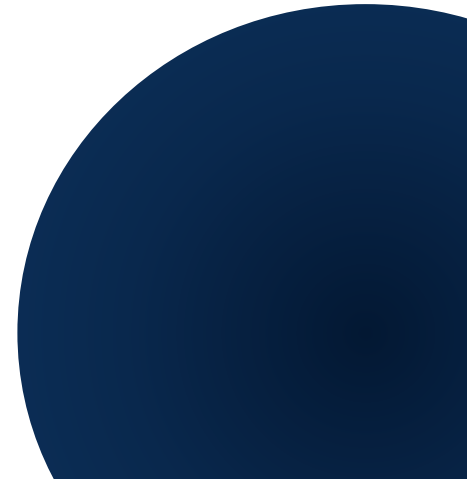


CONSIDERACIONES LEGALES



Esta ley pretende:

«**Garantizar y proteger**, en lo que concierne al tratamiento de los **datos personales**, las **libertades públicas** y los **derechos fundamentales de las personas físicas**, y especialmente de **su honor e intimidad personal y familiar**».



CONSIDERACIONES LEGALES

LOCALIZACIÓN DEL PROCESO (INFRAESTRUCTURA)

Es importante conocer la **localización del proceso** que vamos a subir al cloud, pues el proveedor puede proporcionar la estructura directamente desde sus instalaciones o contratar a su vez los servicios a terceros.



CONSIDERACIONES LEGALES



- LOCALIZACIÓN DEL PROCESO (INFRAESTRUCTURA)

SUBCONTRATACIÓN

Se da cuando el proveedor no dispone de los recursos e infraestructura propias y la subcontrata a terceros.

Este proceso puede ser sucesivo, permitiendo redimensionar los recursos de la nube adaptándose a las necesidades de los clientes.

LOCALIZACIÓN

Cuando se contrata un servicio cloud es importante saber dónde están localizados los proveedores.

Este hecho condicionará las consecuencias legales por incumplimiento, como verás después.

TRANSPARENCIA

Los servicios cloud pueden ser auditables o transparentes en función de:

- La posibilidad de reclamar información acerca de dónde, cuándo y quién ha almacenado o procesado sus datos
- Las condiciones de seguridad

CONSIDERACIONES LEGALES



- LOCALIZACIÓN DE LOS DATOS

Si tratamos con datos de carácter personal, es importante saber **en qué país residirán** los datos que subimos al cloud, pues si se encuentran alojados en países del **Espacio Económico Europeo (EEE)** se **considera que son países adecuados para la recepción de datos** porque se encuentran regulados por normativas alineadas con directivas comunes de los países miembros (por ejemplo Directiva 95/46/CE).




CONSIDERACIONES LEGALES



- LOCALIZACIÓN DE LOS DATOS

En caso de que estén fuera del EEE podría tratarse de una transferencia internacional de datos, y en este caso sería necesario asegurar que dicho país ofrece unos niveles jurídicos de protección de datos equivalentes a las del EEE.

Las transferencias de datos internacionales tienen que contar con la autorización expresa del Director de la Agencia Española de Protección de Datos. En caso de que el prestador de servicios se encuentre en un país considerado con un nivel adecuado de protección se considerará preceptada la autorización.

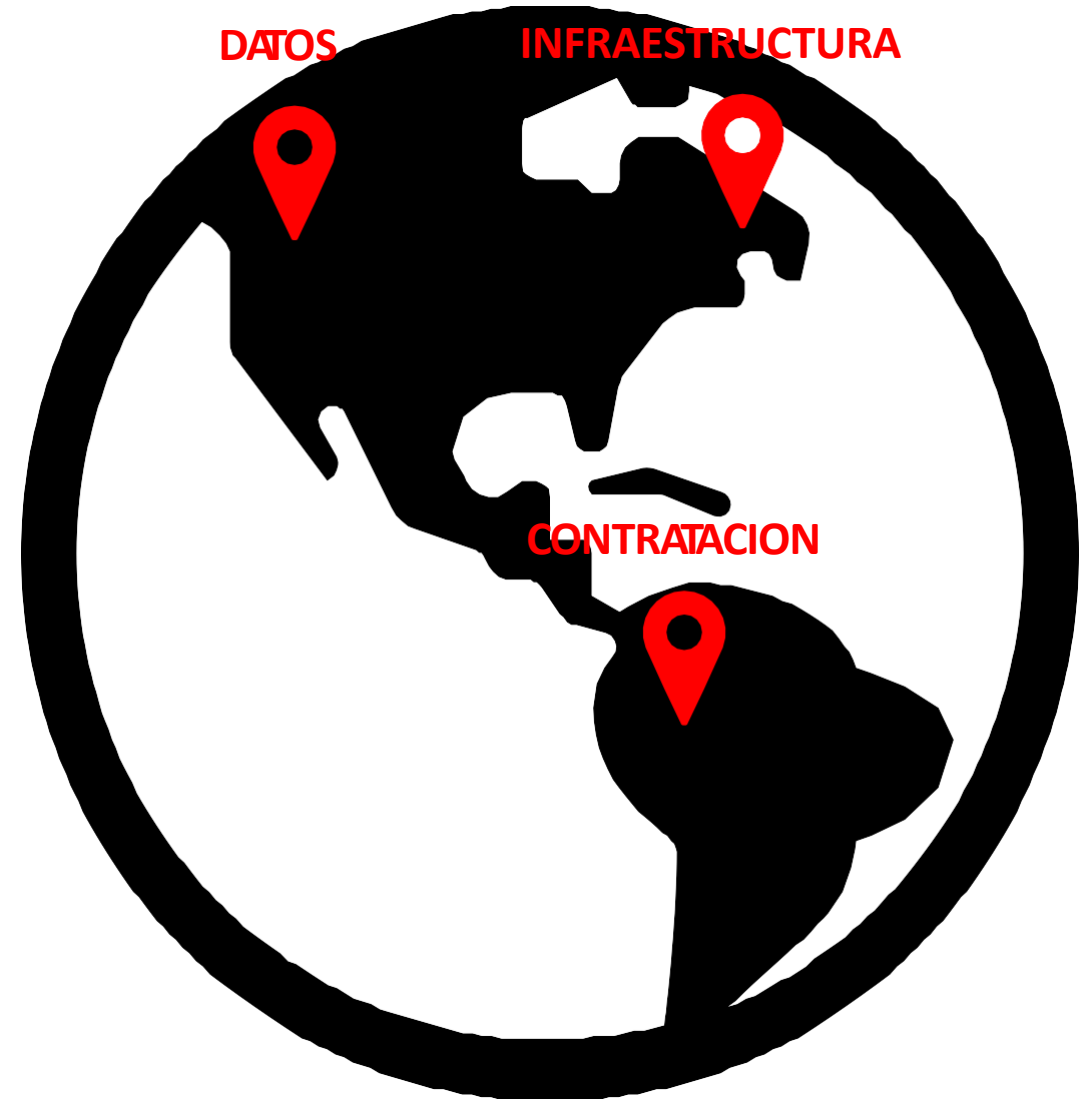


CONSIDERACIONES LEGALES



- LOCALIZACIÓN DE LOS DATOS

Ejemplos de Transferencia de Datos Internacional:
transferencia monetaria entre un banco canadiense y un banco americano, registro de un usuario en eBay.es, etc.





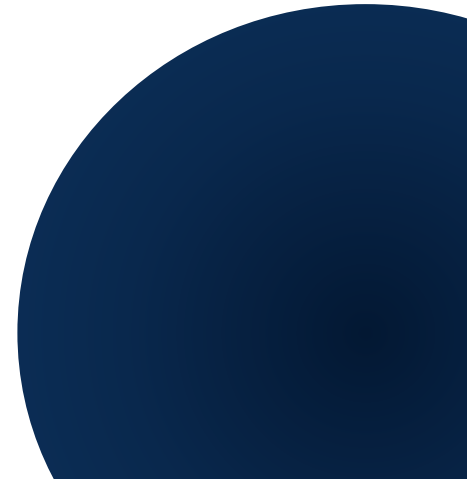
CONSIDERACIONES LEGALES



- El contrato de prestación de servicios entre proveedor y cliente puede ser:

NEGOCIADO

- El cliente puede fijar las condiciones de contratación en relación a:
 - tipo de datos que va a procesar
 - medidas de seguridad
 - localización de los datos
 - portabilidad de los mismos






CONSIDERACIONES LEGALES



- El contrato de prestación de servicios entre proveedor y cliente puede ser:

ADHESIÓN

- El cliente no puede fijar las condiciones de contratación.
 - Se tiene que adaptar a las que fija el proveedor, que son iguales para todos sus clientes.
 - Este suele ser el caso más común en cloud pública o híbrida.
- 




CONSIDERACIONES LEGALES



- El contrato de prestación de servicios entre proveedor y cliente puede ser:

MIXTO

- En este caso, el cliente va a poder fijar únicamente parte de las condiciones del contrato, otras vendrán determinadas por el propio proveedor.
 - Estas condiciones que el cliente va a poder determinar varían en función de la flexibilidad del proveedor.
- 

CONSIDERACIONES LEGALES



- ¿qué medidas de seguridad debo exigir?

Las medidas de seguridad exigibles van a **dependen de la sensibilidad de los datos que se quieren tratar** y serán las necesarias para:

- asegurar la integridad de los datos y su recuperación

- evitar accesos no autorizados Así, los datos relacionados con la salud, ideología, religión, etc son más sensibles que los meramente identificativos

Además, si deseas acceder a los datos a través de redes de comunicaciones (internet o redes inalámbricas, por ejemplo) se tendrán que contemplar medidas de seguridad que garanticen un nivel de seguridad equivalente al acceso en local.

CONSIDERACIONES LEGALES




- ¿qué forma tengo de saber que estas medidas se están cumpliendo correctamente?
 - El cliente tiene derecho a acceder a los quiénes han accedido a los datos
 - El proveedor puede acreditar haber superado una **certificación de seguridad**
 - El cliente de cloud puede **requerir que un** estándares establecidos
 - El proveedor del servicio **debe notificar cliente sobre cualquier incidente** seguridad.



CONSIDERACIONES LEGALES



¿cómo puedo estar seguro de que voy a recuperar los datos de los que soy responsable?

- El proveedor debe **entregar toda la información de forma segura** al cliente para que éste la guarde en sus propios sistemas o la transfiera a otro proveedor.
- 

CONSIDERACIONES LEGALES



Pero una vez que ya he migrado mis datos a otro sitio... ¡El proveedor que tenía puede haberse quedado con mi datos!

¿Qué hago para saber si realmente los ha borrado?!

Antes de extinguir el contrato deben establecerse la medidas adecuadas que aseguren el borrado seguro de los datos cuando el cliente lo desee o cuando el contrato finalice. Esto se puede hacer a través de una **certificación de destrucción** de que emite el proveedor.

CONSIDERACIONES LEGALES

En Colombia




La publicación de la **“Guía de Protección de Datos en los servicios de computación en la nube”** por parte la autoridad colombiana de protección de datos personales (**SIC**) sobre la realidad del llamado contrato de transmisión internacional de datos incorporado en la legislación colombiana con el **decreto 1377 de 2013 (hoy Decreto 1074 de 2015)**

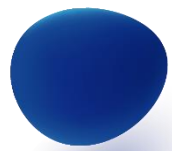


RIESGOS Y AMENAZAS



Las **AMENAZAS** que se van a citar a continuación tienen como objetivo **ayudar a las organizaciones en la toma de decisiones y en su estrategia de *cloud***. Las amenazas más críticas que se identifican son las siguientes:

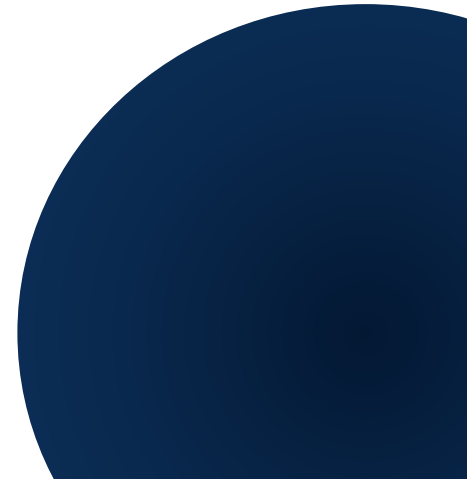




RIESGOS Y AMENAZAS



ACCESO. Si no se toman las medidas de seguridad adecuadas con el proveedor de *cloud* no habrá posibilidad de controlar los accesos de los empleados a la información de la organización, lo que puede provocar robo de datos, inyección de código malicioso, etc.



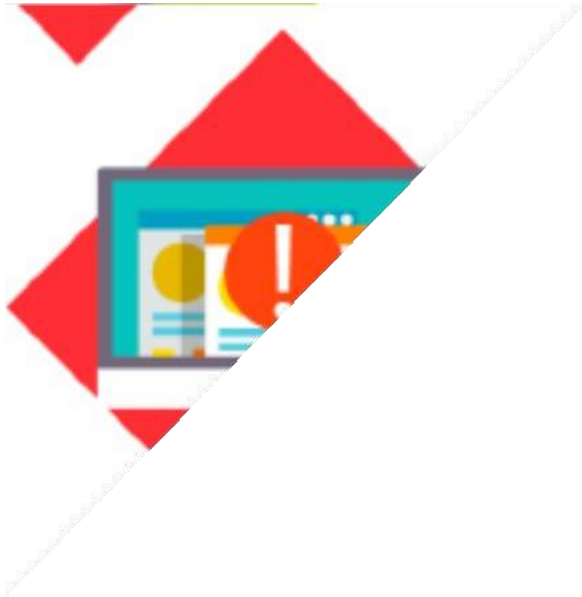


AMENAZAS INTERNAS.

Cuando los trabajadores salen de la organización (fin de contrato o despido), se debe notificar al proveedor de servicios *cloud* su baja para evitar que sigan teniendo acceso a la información.

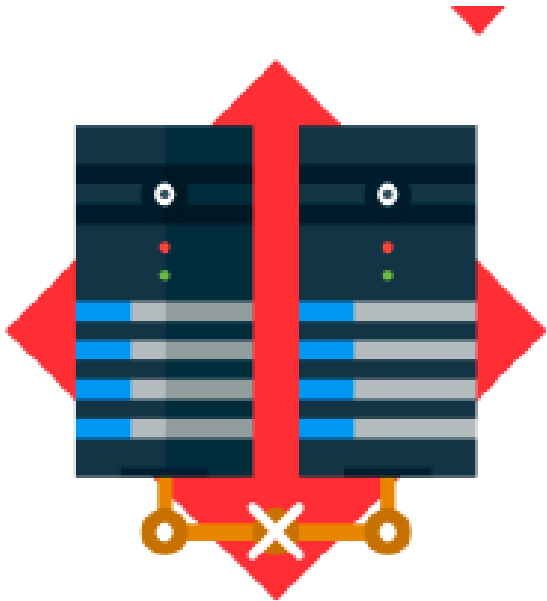


RIESGOS Y AMENAZAS

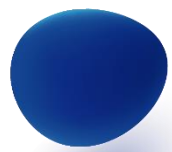


INTERFACES. El problema aparece cuando las interfaces que proporciona el proveedor para acceder a la plataforma en la nube no son del todo seguras y presentan fallos de seguridad que pueden ser explotados por terceros.

RIESGOS Y AMENAZAS



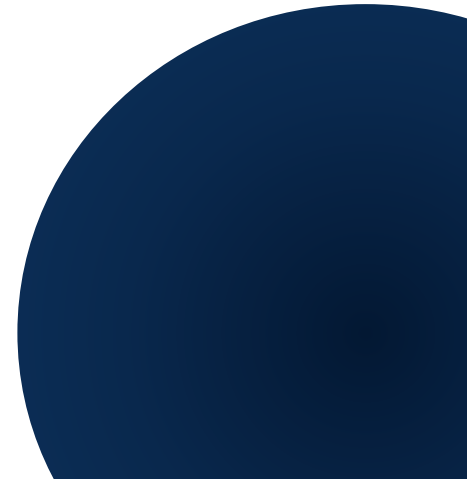
PROBLEMAS DERIVADOS DEL USO DE LAS TECNOLOGÍAS COMPARTIDAS. Se suele dar en modelos de Infraestructura como Servicio (IaaS). Si contratamos una infraestructura compartida existe la amenaza de que por un fallo de seguridad otras empresas puedan acceder a nuestra información.



RIESGOS Y AMENAZAS



FUGA DE INFORMACIÓN. Si nuestra organización lleva a cabo muchas operaciones con cliente al cabo del día y estas no están cifradas, puede producirse una fuga de información.

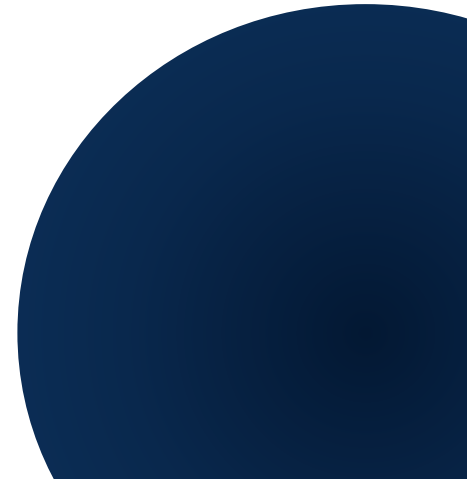




RIESGOS Y AMENAZAS



SUPLANTACIÓN DE IDENTIDAD. Esto sucede cuando a una persona le roban las credenciales de usuario y acceden a la plataforma en su nombre, pudiendo manipular la información.



RIESGOS Y AMENAZAS



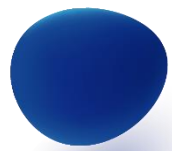
DESCONOCIMIENTO DEL ENTORNO. Si el personal encargado de implantar las políticas de seguridad no conoce el entorno *cloud* estas no serán eficientes.

RIESGOS Y AMENAZAS



ATAQUES DE HACKING.

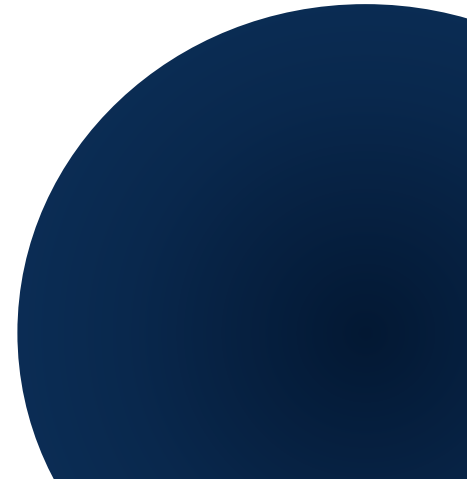
Sucede cuando una persona maliciosa intenta robar o acceder a la información que maneja alguno de los empleados de nuestra organización o el administrador de la plataforma.



RIESGOS Y AMENAZAS



Es necesario realizar una evaluación de los **RIESGOS** antes de implementar una solución cloud. A continuación se enumerar los riesgos que se han considerado más importantes:





RIESGOS Y AMENAZAS



ACCESO DE USUARIOS CON PRIVILEGIOS. Este riesgo aparece cuando un empleado con privilegios de administrador accede cuando no debería o actúa de forma maliciosa (empleados descontentos por ejemplo) alterando datos o configuraciones. También es posible que se den privilegios por error a empleados que no deban tenerlos y estos por desconocimiento provoquen daños.

RIESGOS Y AMENAZAS



CUMPLIMIENTO

NORMATIVO. Este tipo de riesgos aparecen cuando el proveedor cloud no cumple, o no nos permite cumplir con nuestras obligaciones legales. Por este tipo de infracciones nos podemos enfrentar a sanciones legales.



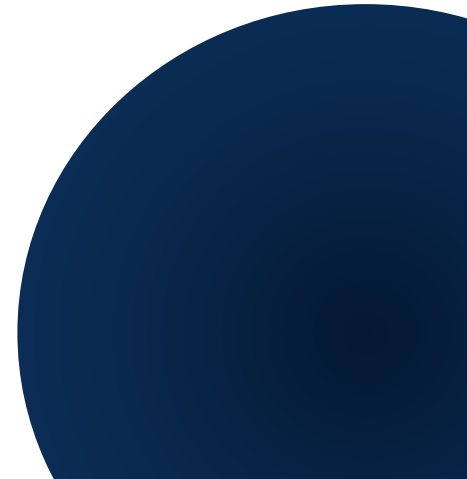


RIESGOS Y AMENAZAS



LOCALIZACIÓN DE LOS DATOS.

Surge cuando se contratan servicios *cloud* a una empresa que aloja nuestros datos en un Centro de Datos del cual desconocemos su ubicación. Por ello, si tratamos con datos de carácter personal, en caso de alojarse fuera del Espacio Económico Europeo es necesario que se proporcionen las garantías jurídicas necesarias.



RIESGOS Y AMENAZAS



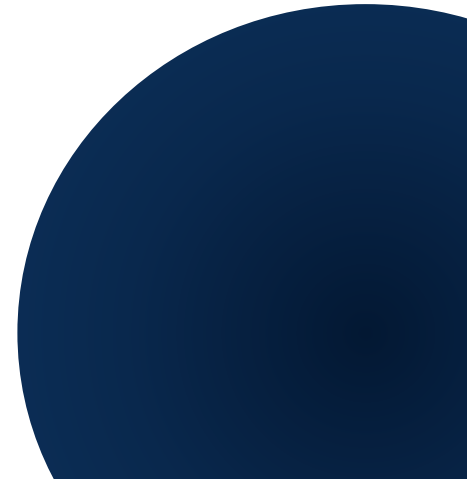
AISLAMIENTO DE DATOS. Si nuestra organización comparte la infraestructura con otra es necesario que el proveedor gestione que nuestros datos no se mezclen con los de la otra organización.



RIESGOS Y AMENAZAS



RECUPERACIÓN. Si nuestro proveedor sufre un incidente y no tiene los datos replicados en otro centro de datos no nos podrá seguir dando servicio.



RIESGOS Y AMENAZAS



SOPORTE INVESTIGATIVO. Si hay cualquier incidente y necesitamos revisar los accesos a los datos y es necesario que estos no estén «mezclados» con los de otros clientes.

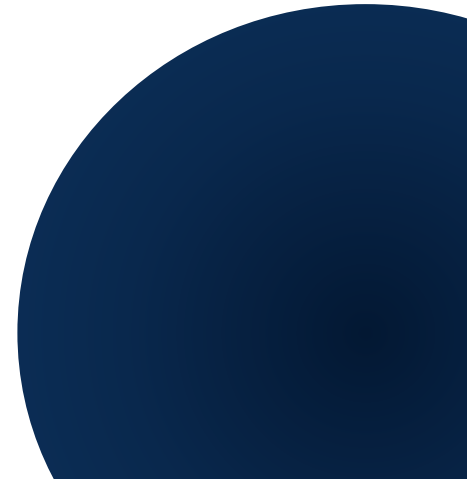
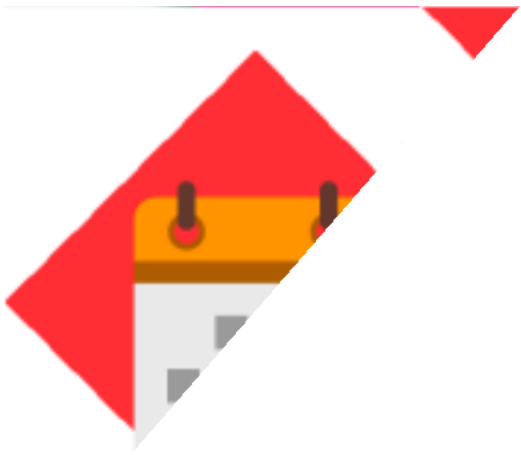


RIESGOS Y AMENAZAS



VIABILIDAD A LARGO PLAZO.

Existe el riesgo de que las condiciones del contrato sufran alguna modificación debido al cambio de estructura del proveedor, a la entrada en situación de quiebra del mismo o a que decida externalizar parte de sus servicios. Por ello es recomendable asegurarse el acceso a los datos y su recuperación.





PROTECCIÓN FRENTE A RIESGOS



RIESGOS	MITIGACIÓN	RESPONSABILIDAD DEL EMPRESARIO
Acceso de usuarios con privilegios	Consenso con el proveedor para que los usuarios que tienen privilegios sean sólo los que deban tenerlos.	Decidir qué privilegios de acceso tendrán sus empleados en función de la información a acceder.
Cumplimiento normativo	Realización de auditorías externas y certificaciones de seguridad.	Velar por el cumplimiento normativo dentro de su organización. Se asegurará de que estas auditorías se realizan adecuadamente.
Localización de los datos	Conocer el marco regulatorio aplicable al almacenamiento y procesamiento de datos. Es recomendable que el proveedor se adapte al marco legal del país del suscriptor del servicio.	Conocer la localización de sus datos para saber cuál será la legislación aplicable.



PROTECCIÓN FRENTE A RIESGOS

RIESGOS	MITIGACIÓN	RESPONSABILIDAD DEL EMPRESARIO
Aislamiento de datos	Los datos en reposo deberán estar aislados y los procedimientos de cifrado deben ejecutarse por personal experimentado.	Saber dónde está localizada la información más sensible para su negocio y adoptar las medidas de protección necesarias (cifrado de datos).
Recuperación	Es necesario exigir a los proveedores la capacidad de recuperación de los datos y el tiempo estimado.	Asegurarse que estas condiciones quedan establecidas en el acuerdo. Adicionalmente, sería conveniente tener los datos replicados en otra plataforma (servidores o equipos propios)
Soporte investigativo	El proveedor debe garantizar que los <i>logs</i> y los datos se gestionan de una forma centralizada.	
Viabilidad a largo plazo	El cliente debe tener la seguridad de que va a poder recuperar todos los datos en caso de que el proveedor cambie la estructura o la dirección.	



FUNDACIÓN DE EDUCACIÓN SUPERIOR

SAN JOSÉ

INSTITUCIÓN TECNOLÓGICA

FIN DE
GRABACIÓN