TLP:CLEAR

Estudio
Infraestructuras cloud en SCI

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

TLP:CLEAR

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

FEBRERO 2026

INFRAESTRUCTURAS_CLOUD_EN_SCI_V1

Índice

ÍNDICE DE FIGURAS

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

1. Sobre este estudio

A lo largo de este estudio se va a explicar cómo funciona el mundo *cloud* y las ventajas y desventajas que puede ofrecer al implementar dicha tecnología en el mundo industrial.

La elección de esta temática reside en que la tecnología *cloud* está constantemente evolucionando y cada vez hay más usuarios que la utilizan, por ello, muchos responsables creen conveniente implementarla dentro de su organización. Tanto es su auge que en muchas empresas se plantean utilizarla en el ámbito de la operación sin saber los posibles problemas que puede conllevar.

Por eso, con este estudio, se esperan aclarar las múltiples dudas que puedan surgir sobre la implementación de los sistemas *cloud* en el mundo industrial, aportando un mayor conocimiento sobre esta tecnología, así como las ventajas y desventajas que conlleva su implementación.

2. Organización del documento

Este estudio cuenta con nueve apartados, siendo el primero el de '**3.Introducción',** que trata de poner en situación al lector sobre la tecnología *cloud*, aportando un conocimiento básico que facilite la comprensión de los siguientes apartados.

Posteriormente, en el punto '**4.Infraestructuras cloud',** se explicarán las diferentes estructuras utilizadas en este ámbito, en la actualidad. En los apartados siguientes '**5.Cloud computing'** y '**6.Arquitectura segura en la nube',** se explicarán los diferentes tipos de servicios, capacidades y aplicaciones, así como las '**7.Buenas prácticas'** que deben de adoptarse para un uso seguro.

El apartado '**8.Sistemas cloud en el mundo industrial'** trata sobre las diferentes funcionalidades y aportaciones que puede tener la tecnología *cloud* en el mundo industrial, que ira seguido del apartado '**9.Ventajas y desventajas'** de su implementación.

El estudio se cierra con el apartado de '**10.Conclusiones'** que resume los conceptos e ideas más importantes de todo lo trasmitido a lo largo del estudio, aportando una visión general.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

3. Introducción

En las últimas décadas, la evolución de las infraestructuras *cloud* ha sido una de las transformaciones más significativas en el panorama tecnológico. Esta evolución empezó con una idea de compartir información y recursos informáticos hasta su posición actual, como un pilar fundamental de la tecnología empresarial.

En sus comienzos, las infraestructuras *cloud* se centraban en la virtualización de servidores físicos. Las empresas adoptaron la virtualización para poder consolidar sus recursos de hardware, reducir los costes y tener una mayor flexibilidad. Esta tendencia provocó que los proveedores viesen la necesidad de sus clientes y empezasen a ofrecer servicios en la nube, como, por ejemplo, máquinas virtuales bajo demanda a través de Internet, lo que permitía a las organizaciones escalar sus recursos de una manera rápida y eficiente, sin necesidad de adquirir más *hardware*.

A medida que la demanda de servicios en la nube crecía progresivamente, los proveedores comenzaron a diversificar su oferta, agregando una variedad de servicios gestionados, como almacenamiento, bases de datos y redes. Esto, permitió a las empresas externalizar aún más sus operaciones de TI, para poder enfocarse en sus aplicaciones y servicios principales, mientras delegaban tareas de gestión a los proveedores de la nube.

Con el tiempo, la nube evolucionó hacia modelos de entrega más especializados, como la computación sin servidor, que eliminó la necesidad de gestionar la infraestructura subyacente, permitiendo a los desarrolladores centrarse exclusivamente en escribir código y desplegar funciones individuales de manera rápida y eficiente.

Hoy en día, la infraestructura en la nube es mucho más que simplemente servidores virtuales y almacenamiento. Los servicios en la nube abarcan una amplia gama de capacidades, desde inteligencia artificial y aprendizaje automático, hasta análisis de IoT y *big data*. Los avances en la nube híbrida y el *edge computing* están llevando la computación más cerca de los usuarios finales, permitiendo nuevas aplicaciones y casos de uso en tiempo real.

Como se ha podido observar, la evolución de las infraestructuras en la nube ha sido impulsada por la búsqueda constante de una mayor agilidad, escalabilidad y eficiencia operativa. A medida que se produzcan nuevos avances, surgirán nuevas innovaciones que impulsen la adopción y la madurez de la nube en todos los ámbitos de la tecnología empresarial.

4. Infraestructuras *cloud*

El entorno *cloud* se encuentra en constante evolución, por lo que las infraestructuras que se utilizaban al principio son muy diferentes a las que se utilizan en la actualidad. Sin embargo, todas estas infraestructuras cuentan con unas soluciones similares, siendo estas:

- **El *hardware*:** aunque en ocasiones se piensa que los entornos *cloud* no cuentan con dispositivos físicos, realmente se utilizan muchos recursos, dependiendo de las necesidades que tenga que cumplir el entorno. Para ello se suele utilizar todo tipo de *hardware*, como conmutadores, enrutadores, *firewalls*, balanceadores de carga, matrices de almacenamiento o dispositivos de almacenamiento para hacer las copias de seguridad.
- **La virtualización:** esta tecnología permite separar las diferentes funciones y los servicios de la tecnología de la información (TI) del sistema de *hardware*.
- **La gestión del almacenamiento:** cuya principal funcionalidad es poder almacenar todos los datos e información que el usuario crea conveniente, pudiendo permitir agregar o eliminar unidades de almacenamiento de una forma mucho más flexible.
- **La conexión por red:** consiste en permitir las comunicaciones entre los diferentes dispositivos, las cuales anteriormente se realizarían con cables o conmutadores, pero que, en el entorno *cloud*, se realizan mediante VLAN, siendo estas redes de área local virtuales que permiten asignar las direcciones de forma eficiente.

A continuación, se explicarán los diferentes tipos *cloud* que más se están utilizando en la actualidad:

- **Nubes públicas:** se tratan de un conjunto de recursos virtuales que han sido desarrollados a partir de un sistema de *hardware* el cual suele pertenecer a empresas externas que además se encargan de gestionarlo. Dicha nube se pone a disposición de distintos clientes mediante una interfaz de autoservicio de una forma automática que permitirá ampliar de forma horizontal las cargas de trabajo, ya que puede experimentar variaciones inesperadas en la demanda.
- **Nubes privadas:** la principal característica de este tipo de nube es que está diseñada exclusivamente para el usuario final y que normalmente se encuentra dentro de la infraestructura del usuario, lo que provoca que dicho usuario es el responsable del mantenimiento.
- **Nubes híbridas:** en este caso se trata una unión de nubes públicas y nubes privadas que permitiría tener las ventajas de ambos tipos de nubes.

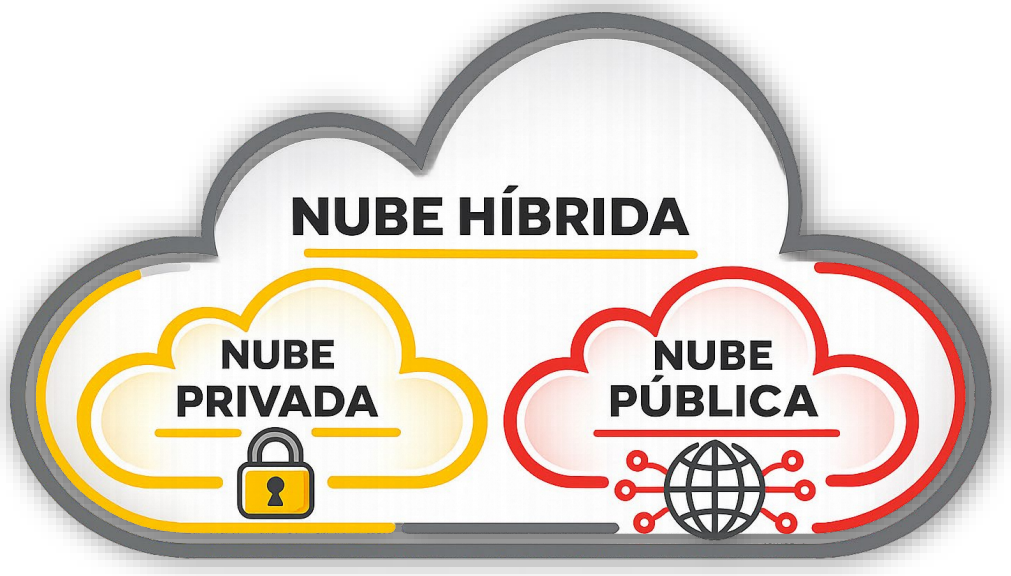


Ilustración 1: Nube hibrida.

- **Nubes Multicloud:** este tipo de nubes suelen confundirse con las nubes híbridas ya que ambas están formadas por las nubes de tipo pública y de tipo privada. A diferencia de las híbridas, en este caso, existe la diferencia de que al menos dos implementaciones de nube son del mismo tipo, pero provienen de diferentes proveedores.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

5. Cloud computing

El *cloud computing* se puede definir como la disponibilidad bajo demanda de los recursos de computación, como servicios a través de internet. Esta tecnología, permite evitar que las empresas se encarguen de aprovisionar, configurar o gestionar los recursos, permitiendo pagar únicamente por lo que vayan a utilizar. En la actualidad hay varios tipos de servicios:

- **SaaS (Software as a Service):** se trata de un servicio que es capaz de ofrecer a los usuarios finales una aplicación de nube junto a toda su infraestructura de TI y plataformas subyacentes, mediante un explorador de internet. En la actualidad, los usuarios muestran desinterés en asumir la responsabilidad de adquirir o mantener la infraestructura, las plataformas o el *software* local, además prefieren una gestión de costos más sencilla, optando por gastos operativos en lugar de inversiones en gastos de capital. Los desafíos enfrentados requieren una personalización mínima para su resolución. Finalmente, también se puede observar una clara preferencia por los modelos de suscripción de *software*.
- **PaaS (Plataform as a Service):** este tipo de servicio representa una forma de *cloud computing* donde un proveedor externo suministra una plataforma de *software* para aplicaciones. Es especialmente adecuada para desarrolladores y programadores, ya que les permite crear, ejecutar y administrar sus propias aplicaciones sin necesidad de diseñar ni mantener la infraestructura o plataforma asociadas. Las PaaS pueden operar tanto en la nube, como en una infraestructura local. En el caso de las soluciones gestionadas, el proveedor de PaaS hospeda *hardware* y *software* en su propia infraestructura, ofreciendo al usuario una plataforma integrada, una gama de soluciones, o un servicio a través de Internet.
- **IaaS (Infrasture as a Service):** se trata de un modelo de *cloud computing* que proporciona recursos informáticos virtualizados, como almacenamiento, redes y máquinas virtuales, a través de Internet. Los usuarios pueden acceder a estos recursos bajo demanda y configurarlos según sus necesidades específicas, lo que les permite implementar y ejecutar aplicaciones sin la necesidad de gestionar la infraestructura física subyacente. IaaS ofrece escalabilidad instantánea, pagando solo por los recursos utilizados, lo que lo convierte en una opción ideal para empresas que requieren flexibilidad y control sobre su infraestructura de TI.

En la siguiente imagen se podrá visualizar múltiples tecnologías que están relacionadas con cada servicio anteriormente comentado.

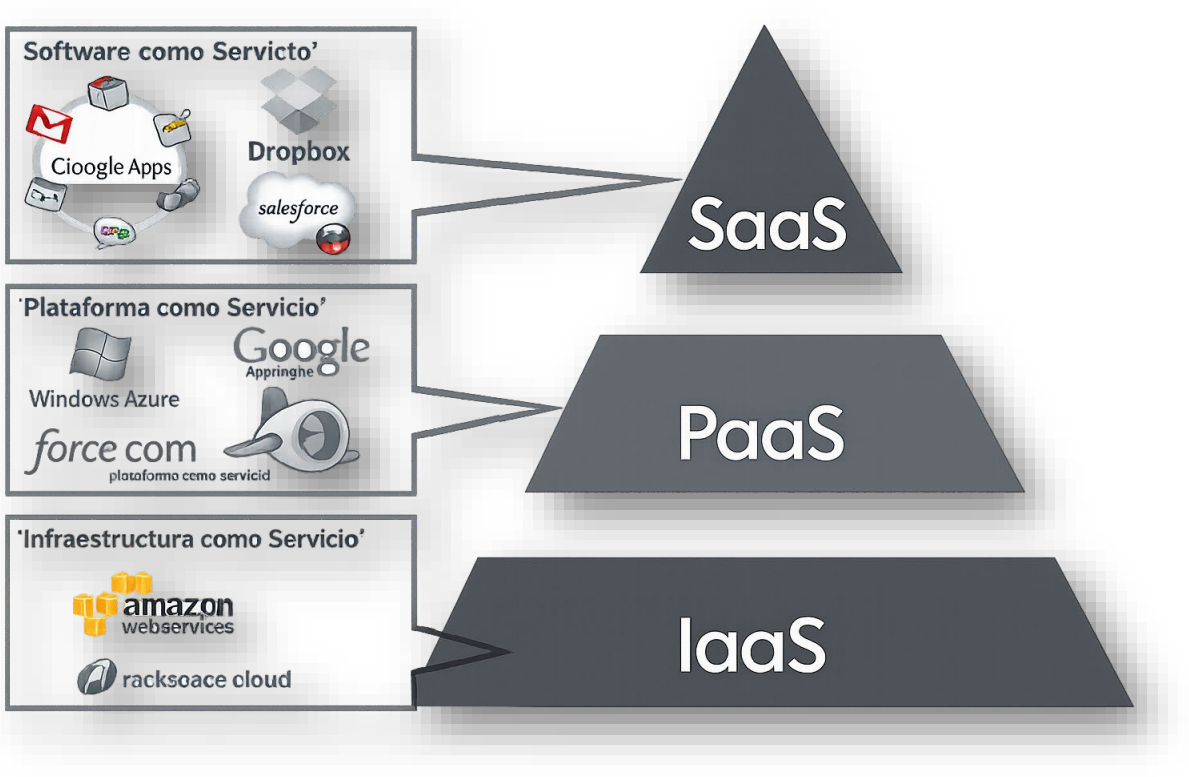


Ilustración 2: Tecnologías utilizadas en diferentes servicios cloud.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

6. Arquitectura segura en la nube

La adopción generalizada de la computación en la nube ha transformado la forma en que las organizaciones gestionan sus recursos tecnológicos. Sin embargo, con la creciente dependencia de la nube para almacenar datos sensibles y ejecutar aplicaciones críticas, la seguridad se ha convertido en una preocupación central. Es en este contexto, en el que surge la necesidad de una arquitectura segura en la nube, ya que, no solo aborda los desafíos tradicionales de seguridad, como el acceso no autorizado y la pérdida de datos, sino que también se adapta a las complejidades inherentes al entorno de la nube, como la compartición de recursos, la movilidad de datos y la gestión de identidades. En esta introducción, se explorarán los principios fundamentales de la arquitectura segura en la nube y cómo ayuda a proteger los activos digitales de una organización en un entorno dinámico y en constante evolución.

6.1. Factores que afectan a la arquitectura

Hay multitud de factores que afectan a la arquitectura segura en la nube y se encuentran en constante evolución. Actualmente, algunos de los factores más destacables son:

- **Requisitos de cumplimiento normativo:** existen gran cantidad de regulaciones que imponen estándares específicos de seguridad y privacidad que se tienen que cumplir en el diseño de la arquitectura en la nube.
- **Datos utilizados y su sensibilidad:** se refiere a la importancia de comprender la naturaleza de los datos que una organización maneja y cómo esta sensibilidad influye en los requisitos de seguridad y privacidad. La clasificación de estos datos se puede realizar en diferentes categorías dependiendo de su sensibilidad y su impacto en la organización, como por ejemplo datos personales, financieros o de propiedad intelectual. Por lo tanto, es fundamental que las organizaciones realicen diferentes evaluaciones exhaustivas de los tipos de datos que manejan y comprendan su sensibilidad para diseñar una arquitectura en la nube para así poder proteger de forma adecuada la información más crítica y valiosa.
- **Amenazas y vulnerabilidades:** la identificación y mitigación de amenazas y vulnerabilidades son aspectos fundamentales de la seguridad en la nube. Esto implica la implementación de medidas de seguridad adecuadas. Además, la monitorización continua y la respuesta rápida a incidentes son esenciales para proteger eficazmente los diferentes sistemas y datos en la nube contra la multitud de amenazas que existen y que además se encuentran constante evolución.
- **Gestión de identidades y accesos:** la autenticación y autorización adecuadas, junto con la gestión de claves y certificados, son cruciales para garantizar que solo usuarios autorizados accedan a los recursos y datos en la nube.

6.2. Roles

Debido a los diferentes factores que se han comentado anteriormente y a la posible complejidad de la arquitectura, suelen existir varios roles y responsabilidades clave que

desempeñan un papel fundamental en la protección de los sistemas y datos. Los roles más importantes son:

- **Administrador de seguridad en la nube:** este rol es responsable del diseño, la implementación y el mantenimiento de las políticas y controles de seguridad en la nube.
- **Arquitecto de la nube:** encargado de elaborar el esquema general de la arquitectura en la nube, abarcando la configuración de redes, la elección de servicios y la integración de sistemas. Además, este rol es el que garantiza que la estructura tenga que cumplir con los estándares de seguridad y privacidad de la organización.
- **Ingeniero de seguridad en la nube**: centrado en la implementación y mantenimiento de los controles de seguridad en la nube, así como trabajar en estrecha colaboración con el administrador de seguridad y el arquitecto en la nube.
- **Administrador de identidades y accesos:** este rol es responsable de gestionar las identidades de usuarios y controlar el acceso a los recursos en la nube. Esto incluye la creación y gestión de cuentas de usuario, la implementación de políticas de acceso basadas en roles y la monitorización de actividades de usuario para detectar comportamientos sospechosos o no autorizados.

7. Buenas prácticas

Como se ha podido observar en los anteriores apartados, el nuevo uso de las infraestructuras en la nube ha provocado en la forma en la que las organizaciones son capaces de gestionar sus datos, aplicaciones y operaciones. Aunque esta nueva tendencia tiene muchísimas ventajas, también provoca una multitud de desafíos significativos en términos de seguridad cibernética. Por ello, es aconsejable realizar las siguientes pautas para proteger este tipo de infraestructuras.

- **Gestión de accesos:** es recomendable controlar quién se introduce a la infraestructura y las actividades que tiene que realizar, para ello, se recomienda implementar una autenticación y autorización robustas.
- **Cifrado de los datos:** esta práctica es importantísima para proteger la confidencialidad y la integridad de los datos que son almacenados o que se encuentran en tránsito, un ejemplo sería utilizar el protocolo HTTPS en vez de HTTP.
- **Monitorización:** se recomienda conocer las diferentes actividades que se están realizando en la infraestructura en tiempo real, ya que si hubiese alguna que no fuese normal se podría detectar y anticiparse antes de que pueda producir problemas serios.
- **Gestión de vulnerabilidades:** es aconsejable estar atento a las nuevas vulnerabilidades que puedan afectar a la infraestructura ya que podrían ser una brecha de seguridad que permitiría que los ciberdelincuentes puedan atacar. Para ello se recomienda aplicar los parches de seguridad o implementar contramedidas.
- **Realización de *backups*:** esta práctica permite garantizar la disponibilidad y la recuperación en caso de que el *hardware* falle, se produzcan errores humanos o se sufra algún ataque ciberseguridad. Por ello, se recomienda realizar copias periódicas y, a su vez, probarlas para que cuando se produzcan los problemas anteriormente comentados sea posible recuperar con eficacia el sistema.
- **Concienciación:** es aconsejable que el personal responsable de la infraestructura y de la gente que la utiliza, tenga un cierto conocimiento y concienciación en ciberseguridad ya que el fallo humano es una de las principales técnicas que los ciberatacantes aprovechan para introducirse en la infraestructura.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

8. Sistemas *cloud* en el mundo industrial

Como se ha podido observar a lo largo de este estudio, las infraestructuras *cloud* tienen muchas ventajas, por eso los responsables e integradores de los dispositivos y tecnologías desean aprovecharlas, ya que con el crecimiento de la industria 4.0 y el aumento exponencial del uso de datos, resulta un modo de infraestructura muy atractivo. A continuación, se podrá observar algunos ejemplos de cómo poder utilizar la infraestructura *cloud* en el mundo industrial.

8.1. Aplicaciones SCADA

En este tipo de aplicaciones, el *software* y los datos se almacenan en servidores a los que se accede a través de Internet. En este caso se puede dividir en dos apartados.

- **Almacenada de forma interna y datos publicados externamente:** este modo se caracteriza porque la parte de supervisión y control se mantienen dentro de la red industrial de la empresa, mientras que los datos se encuentran almacenados en la nube para ser analizados, como por ejemplo los comandos, las mediciones que se realizan en tiempo real o los datos que se almacenan en el histórico.

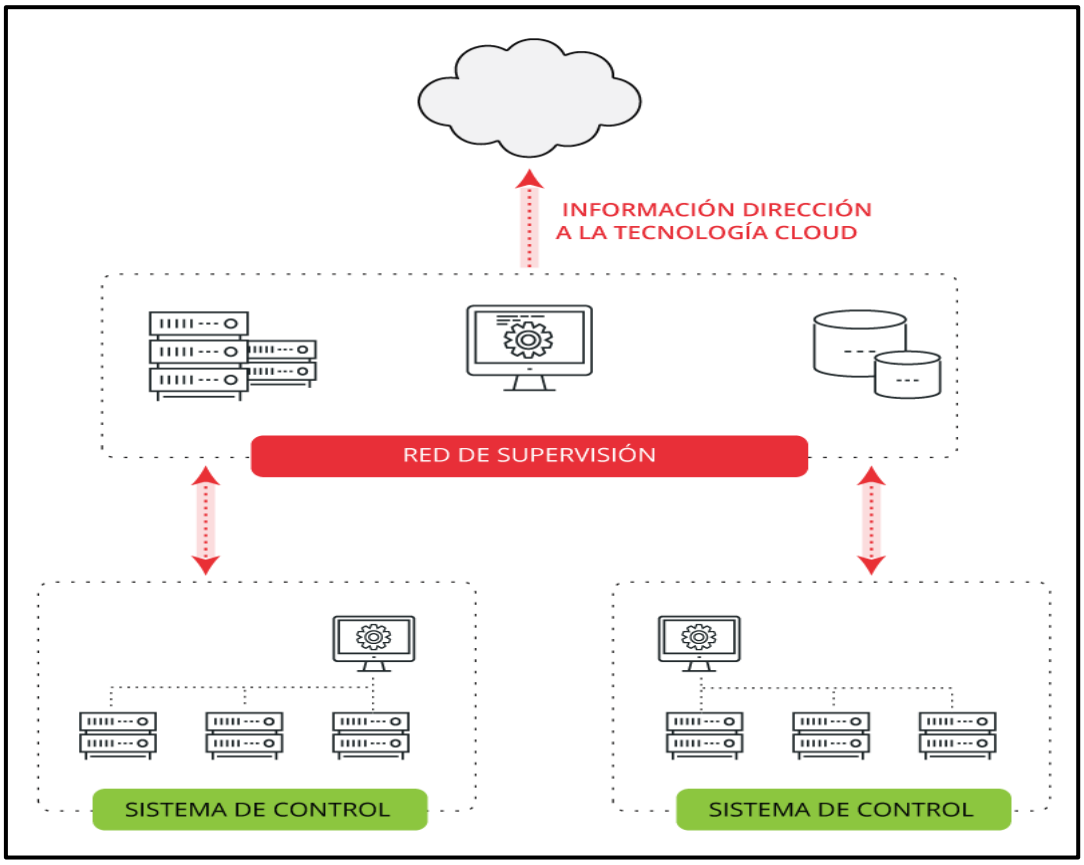


Ilustración 3: Arquitectura de una aplicación SCADA almacenada de forma interna y con datos publicados externamente[1] Fuente: [1] https://www.incibe.es/incibe-cert/blog/tecnologia-cloud-entornos-industriales

[1] https://www.incibe.es/incibe-cert/blog/tecnologia-cloud-entornos-industriales

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

- **Almacenada completamente en la nube**: esta forma consiste en almacenar toda la información generada y los datos creados en la nube. Para ello, ya existen diferentes plataformas como las siguientes:
  - PetroCloud[2]
  - Iconics[3]
  - RealiteQ[4]

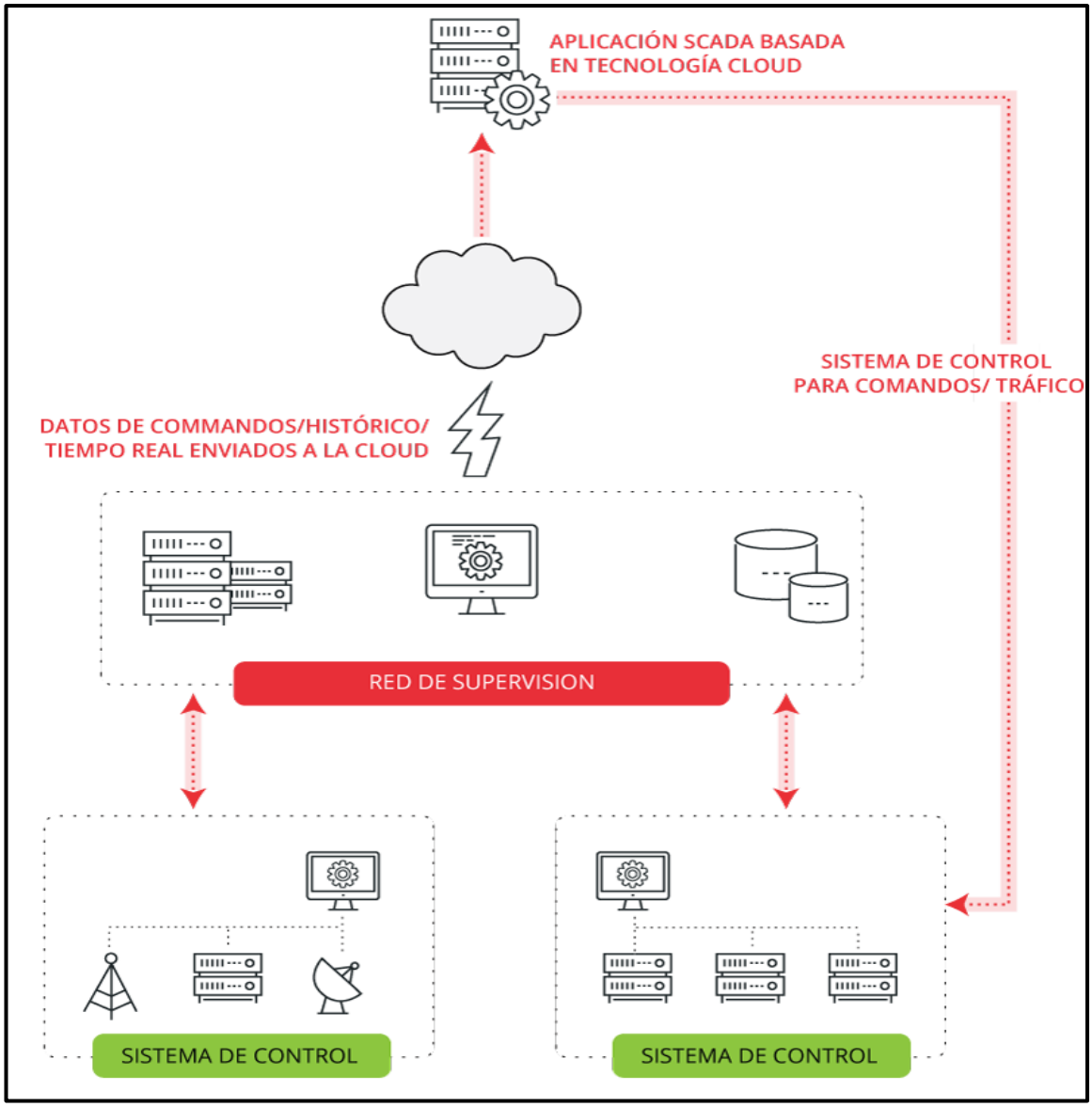


Ilustración 4: Arquitectura que posee una aplicación SCADA almacenada completamente en la nube[5] Fuente: https://www.incibe.es/incibe-cert/blog/tecnologia-cloud-entornos-industriales

[2] https://petrocloud.com/

[3] https://iconics.com/

[4] http://www.realiteq.com/

[5] https://www.incibe.es/incibe-cert/blog/tecnologia-cloud-entornos-industriales

8.2. Honeypots Industriales

Como se ha podido observar en otros artículos o guías[6] ya realizados, un *honeypot* consiste en simular sistemas, servicios o recursos que tengan algún tipo de vulnerabilidad o que puedan ser valiosos para el atacante, para así poder atraer y monitorizar las actividades que se realizan. Debido a la constante evolución de las tecnologías y al desempeño de los atacantes, continuamente se tienen que cambiar y mejorar los *honeypots,* ya que se podrían quedar anticuados y dejando de resultar atractivo para el atacante. Por ello, la flexibilidad que caracteriza este tipo de infraestructuras es muy atractivo para el uso de implementación de *honeypots*.

A continuación, se explicará dos posibles ejemplos que permitan utilizar este tipo de tecnologías en la infraestructura *cloud*.

- Se podría crear diferentes máquinas virtuales que simulen dispositivos industriales, como por ejemplo PLC, HMI, RTU, etc. Estas máquinas podrían estar interconectadas como si estuviesen realmente conectadas ya que la infraestructura *cloud* permite crear múltiples VLAN lo que haría mucho más realista este tipo de simulaciones.
- Utilizar los diferentes *honeypots* industriales que ya existen, lo que permitirá que la instalación y la configuración sea mucho más simple. Algunos *honeypots* que se pueden implementar son las siguientes:
  - Conpot
  - Gridpot
  - SCADA-honeynet

8.3. Laboratorio de pruebas

Como se comentó anteriormente en el mundo actual, la tecnología no para de evolucionar por ello, es aconsejable tener una zona donde se pueda realizar múltiples pruebas, como por ejemplo el software que vas a utilizar para programar los dispositivos industriales, comprobar los nuevos parches que se van a implementar o incluso comprobar los *backups* que se realizan, ya que tienen que ser testeados por si en un futuro se llegaran a utilizar.

Por estas necesidades, las infraestructuras *cloud* son muy interesantes ya que gracias a su flexibilidad se puede crear los recursos necesarios para realizar la prueba necesaria y después si se quiere poder eliminarlo o guardarlos para otras posibles utilidades.

[6] https://www.incibe.es/incibe-cert/guias-y-estudios/guias/guia-de-implantacion-de-un-honeypot-industrial

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

9. Ventajas y desventajas

Ahora que ya se tiene un conocimiento más amplio sobre las infraestructuras *cloud,* se explicara las diferentes ventajas y desventajas que es capaz de ofrecer este tipo de tecnología.

9.1. Ventajas

Las principales ventajas son:

- **Flexibilidad:** es capaz de ofrecer una variedad de servicios y modelos de implementación que se adaptan a las necesidades específicas de cada organización.
- **Rentabilidad:** esta tecnología elimina la necesidad de adquirir y mantener *hardware* costoso e invertir en infraestructura física permitiendo pagar únicamente por los recursos que se van a utilizar.
- **Gestión:** los servicios gestionados en la nube simplifican la administración de sistemas, ya que los proveedores se encargan de tareas como mantenimiento, parcheo, seguridad y *backups,* lo que permite liberar carga de trabajo a los equipos de TI.

9.2. Desventajas

Las principales desventajas son:

- **Dependencia de la conectividad a Internet:** la conexión requerida a Internet debe ser estable y confiable para así poder acceder a los servicios y datos que se encuentran alojados en la nube. Una falta de conectividad puede afectar a la disponibilidad y el rendimiento de las aplicaciones y servicios en la nube, lo que podría provocar un impacto significativo en las operaciones comerciales.
- **Coste a largo plazo:** aunque la nube puede ofrecer ahorros de costos a corto plazo las tarifas de suscripción mensuales y el uso excesivo de recursos pueden dar lugar a facturas inesperadamente altas si no se gestionan adecuadamente.
- **Seguridad y privacidad:** aunque los proveedores de servicios en la nube implementan medidas de seguridad robustas, existen preocupaciones sobre la seguridad y la privacidad de los datos alojados en la nube.
- **Dependencias del proveedor:** dependiendo de un solo proveedor de servicios en la nube puede exponer a que las organizaciones tengan el riesgo de depender constantemente de este proveedor.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

10. Conclusiones

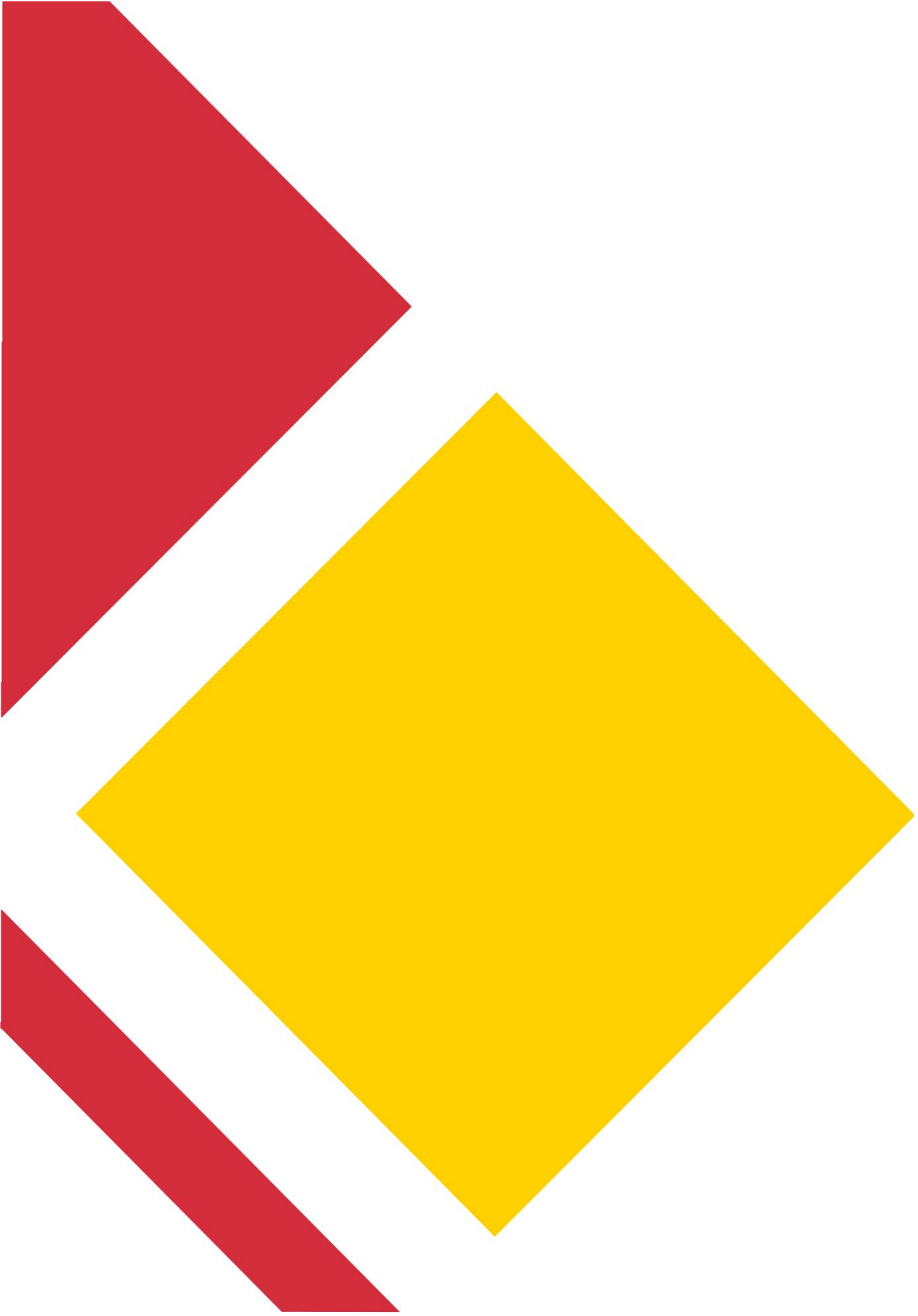
Los entornos *cloud* están en continuo crecimiento, proporcionando cada vez características y funcionalidades más atractivas y ya no solo para los entornos TI, en los que ya están afianzados, sino también para los entornos industriales en los que cada vez más se están desplegando este tipo de arquitecturas debido a las capacidades para reducir costes y mejorar la conectividad entre TI y TO.

Junto con la industria 4.0, los sistemas *cloud* en los entornos industriales, son otro de los aspectos más importantes en los últimos, pero esto no debe ocultar también las problemáticas que pueden ocasionar en los entornos industriales, ya que la seguridad de los sistemas puede verse comprometida sino existen diferentes medidas de seguridad y una correcta segmentación entre las redes TI y TO.

Es por ello, que, aunque las ventajas son muy atractivas, también hay que tener en cuentan las diferentes desventajas mencionadas a lo largo del estudio ya no solo en cuento a sobrecostes o caídas en rendimiento, sino también en cuanto a la seguridad de los sistemas industriales.

11. Referencias

Referencia	Título, autor, fecha y enlace web
[Ref.- 1]	"Tecnología cloud en entornos industriales". INCIBE-CERT. INCIBE (Instituto Nacional de Ciberseguridad de España). 14 de marzo de 2019. URL: https://www.incibe.es/incibe-cert/blog/tecnologia-cloud-entornos-industriales
[Ref.- 2]	"Arquitecturas de referencia de ciberseguridad de Microsoft". Microsoft. 21 de febrero de 2024 URL: https://learn.microsoft.com/es-es/security/adoption/mcra?bc=%2Fazure%2Fcloud-adoption-framework%2F_bread%2Ftoc.json&toc=%2Fazure%2Fcloud-adoption-framework%2Ftoc.json
[Ref.- 3]	"Ventajas y desventajas del cloud computing" Google. URL: https://cloud.google.com/learn/advantages-of-cloud-computing?hl=es#section-3
[Ref.- 4]	"¿Qué es una infraestructura de nube?". Red Hat. 28 de mayo de 2019. URL: https://www.redhat.com/es/topics/cloud-computing/what-is-cloud-infrastructure
[Ref.- 5]	"Cloud adoption framework". Oracle cloud. 12 de septiembre de 2023. URL: https://docs.oracle.com/es-ww/iaas/Content/cloud-adoption-framework/process-design.htm
[Ref.- 6]	"Cloud computing" Actualizado 31 de enero 2023 ¿Qué es cloud computing o computación en la nube ? (redhat.com)



Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

TLP:CLEAR