



# Conectividad y la estrategia de adopción de las soluciones en la nube

**Junio 2024**

---

**Grupo**  
Telecomunicaciones

1.	Introducción.....	2
1.1.	Definición de Cloud/Nube a través de sus características .....	4
	Características:.....	4
1.2.	Tipos de modelos de servicio en la nube.....	5
1.3.	Tipos de Nubes por modelo de despliegues. Características y principales ventajas y desventajas (seguridad, coste, flexibilidad, conectividad, etc.).....	5
1.4.	Características de cada tipo y principales ventajas y desventajas (seguridad, coste, flexibilidad, conectividad, etc.). .....	6
	Ventajas.....	6
	Desventajas .....	7
1.5.	Desafíos de la nube híbrida .....	8
1.6.	A modo general. ....	8
2.	Estado de Situación .....	9
2.1.	Principales conclusiones de la encuesta.....	9
	Principales Hallazgos:.....	9
2.2.	Estado de adopción de Cloud.....	10
2.3.	Estado de adopción de la Cloud Publica .....	12
	IaaS (Infrastructure as a Service - Infraestructura como Servicio):.....	12
	PaaS (Platform as a Service - Plataforma como Servicio): .....	12
	SaaS (Software as a Service - Software como Servicio): .....	13
	Flexibilidad:.....	16
	Rapidez:.....	17
	Amplitud de Porfolio: .....	17
2.4.	Desafíos y Soluciones de Conectividad .....	19
2.5.	Detalles de la encuesta.....	23

Sobre la encuesta: .....	23
3. La Hiperconectividad como Solución .....	24
3.1. Introducción.....	24
3.2. Soluciones básicas de Conectividad en la interconexión de nubes .....	25
3.3. ¿Qué es la Hiperconectividad? .....	28
Entornos y tendencias.....	29
Hiperconectividad entre aplicaciones/infraestructuras .....	31
Hiperconectividad entre usuarios y aplicaciones .....	43
Ejemplos prácticos .....	48
3.4. Seguridad, Gestión, Observabilidad y Talento.....	58
Seguridad.....	58
Gestión y Monitorización .....	60
La importancia del Talento, el papel de la automatización .....	62
3.5. Conclusiones y Recomendaciones .....	64
4. Agradecimientos.....	66

## 1. Introducción

El Data center tradicional sigue siendo, para muchas compañías, un elemento clave en su infraestructura TIC, pero para poder aprovechar las ventajas, que sin duda pueden aportar las nubes públicas, servicios que actualmente residen en estos Data Center se están complementando con distintas soluciones en las nubes de los principales proveedores o migrándolas a estas.

Este cambio implica nuevos retos de conectividad. Los equipos de TIC están acostumbrados a trabajar con un alto nivel de rendimiento en la conectividad de los sistemas albergados en sus propios Data Center. Al complementar o migrar sistemas a la nube pública, se debe tener en cuenta que puede haber un

empeoramiento de este nivel de rendimiento, como, por ejemplo, peores tiempos de latencia tanto en la conectividad entre las aplicaciones como en los usuarios que acceden a estas. También es importante considerar que esta nueva necesidad de conectividad debe ir acompañada de requisitos de seguridad y por supuesto de capacidades de monitorización y gestión.

Por esta razón es importante que estos retos o desafíos de conectividad estén contemplados dentro de la estrategia de adopción de las soluciones en la nube y que se puedan proponer soluciones que permitan resolverlos y asegurar que ni el rendimiento de nuestras aplicaciones empeorará, ni los requisitos de seguridad y cumplimiento se reducirán, ni que se verán comprometidas las capacidades de gestión.

La variedad de situaciones de las compañías es muy amplia desde casos muy complejos con varios Data Centers y distintas nubes a otros mucho más simples con muchos menos elementos.

El objetivo del trabajo es el de analizar las distintas soluciones de conectividad que permitan una adopción de soluciones híbridas con garantías de rendimiento, seguridad y gestión. Se enfoca principalmente en un escenario de nube híbrida abordando la extensión del Data Center privado a una o varias nubes públicas, también se incluyen escenarios de soluciones de Conectividad MultiCloud con soluciones emergentes, sin olvidar de acceso de los usuarios, para tener así una visión completa

Hemos planteado el trabajo en dos bloques. Un primer bloque donde se introducen los conceptos de nube y su clasificación y donde se plantean los desafíos para su adopción. Además, hemos querido complementar esta información con el estado de la situación en España realizando una encuesta en la que además de preguntar sobre la existencia de Data Centers tradicionales y el estado de adopción de la nube, se ha hecho foco en la problemática de conectividad. En general las empresas utilizan arquitecturas de nube híbrida y conectividad multicloud y los problemas de conectividad están presentes entre los encuestados.

El segundo bloque profundiza en las diferentes soluciones de conectividad según diferentes escenarios, concluyendo con varios ejemplos prácticos reales que ilustran de manera resumida las soluciones descritas.

Aunque como casi todo en las TIC, las soluciones de conectividad están en constante evolución y, por tanto, en un futuro próximo habrá otras posibilidades, el trabajo aporta soluciones a problemas actuales y puede ayudar a las compañías a tener éxito en distintos proyectos de adopción de la nube.

### 1.1. Definición de Cloud/Nube a través de sus características

Es el uso de una infraestructura de servidores interconectados en localizaciones en despliegue de granjas remotas y conectados a internet para almacenar, administrar y procesar datos, servidores, bases de datos, redes y software.

Es la opción para depender de un servicio físico instalado. Como tal se tiene acceso a una estructura remota contratada donde el software y el hardware están virtualmente integrados.

Este concepto ha evolucionado a medida que el ancho de banda disponible se incrementaba considerablemente reduciendo latencias de conectividad y creando un entorno de “proximidad” al usuario.

Características:

- **Autoservicio:** Provisión de Máquinas, Almacenamiento, Granjas de Sistemas y Aplicaciones mediante menú de opciones a la carta y respaldado por acuerdos sin requerir intervención humana del proveedor.
- **Acceso público desde cualquier sitio.** Teniendo un acceso Universal siempre que el usuario disponga de conexión a Internet.
- **Consumo en modo pool entre diferentes usuarios:** El usuario final no dispone de un recurso dedicado ad hoc. los recursos se comparten bajo condiciones de contratabilidad entre diferentes usuarios.

- **Elasticidad rápida (crecimiento y decrecimiento):** los recursos solicitados se pueden aprovisionar y liberar rápidamente según demanda casi a tiempo real. Ajustándose a los flujos y continuidades de negocio.
- **Facturación por consumo.** Como continuación, al ser un consumo de recursos coyuntural, si bien se pueden establecer servicios de tarifa “plana” bajo ciertas condiciones, la tendencia es establecer la Facturación a la demanda de consumo y este es el punto crítico y ventajoso de la nube.

## 1.2. Tipos de modelos de servicio en la nube

A continuación, se indican las modalidades de nube pública más habituales. Una descripción más detallada se encuentra en el capítulo 2.3.

- **IaaS:** Es una manera de entregar almacenamiento básico y capacidades de cómputo como servicios estandarizados en la red. Servidores, sistemas de almacenamiento, conexiones, Router, Firewall
- **PaaS:** Es la [encapsulación](#) de un ambiente de desarrollo y el empaquetamiento de una serie de módulos o complementos que proporcionan, una funcionalidad horizontal (persistencia de datos, autenticación, mensajería, etc.).
- **SaaS:** Caracteriza una aplicación completa ofrecida como un servicio bajo demanda sirviendo a múltiples organizaciones, bajo una estructura común. Suelen ser accesibles a través de web sin control por parte del usuario. El usuario con ello no asume la necesidad de instalar y mantener la aplicación

## 1.3. Tipos de Nubes por modelo de despliegues. Características y principales ventajas y desventajas (seguridad, coste, flexibilidad, conectividad, etc.)

- **Nube pública.** Es una nube computacional mantenida y gestionada por terceras personas no vinculadas con la organización. Tanto los datos como los procesos de varios usuarios se mezclan en los servidores, sistemas de

almacenamiento y otras infraestructuras de la nube. Los usuarios finales de la nube no conocen qué trabajos de otros usuarios pueden estar corriendo en el mismo servidor, red, sistemas de almacenamiento.

- Las Aplicaciones, almacenamiento y otros recursos están disponibles al público a través del proveedor de servicios, que es propietario de toda la infraestructura en sus centros de datos; el acceso a los servicios solo se ofrece de manera remota, normalmente a través de internet.
- **Nube Privada.** Están en una infraestructura bajo demanda, gestionada para un solo usuario que controla qué aplicaciones debe ejecutarse y dónde.
  - Son propietarios del servidor, red, y disco y pueden decidir qué usuarios están autorizados a utilizar la infraestructura.
- **Nube Híbrida.** Combinan los modelos de nubes públicas y privadas. Un usuario es propietario de una parte y comparte otra, aunque de manera controlada. “grosso modo” Es una mezcla de nube privada local y nube pública de terceros, pero conectados entre ellos.
- **Multicloud:** Se combina más de un servicio de nube formada, por lo menos, de dos proveedores de nube pública o privada. Surge por una expansión de las organizaciones. Puede confundirse con la nube híbrida. La multinube combina servicios de diferentes proveedores no conectados entre sí.

#### **1.4. Características de cada tipo y principales ventajas y desventajas (seguridad, coste, flexibilidad, conectividad, etc.).**

Ventajas.

- La Tecnología se puede integrar en nube con mucha mayor facilidad y rapidez con el resto de las aplicaciones empresariales, ya sean desarrolladas de manera interna o externa.

- Las infraestructuras de cloud computing proporcionan mayor capacidad de adaptación, recuperación completa de pérdida de datos (con copias de seguridad) y reducción al mínimo de los tiempos de inactividad.
- Permite también al proveedor de contenidos o servicios en la nube prescindir de instalar cualquier tipo de software.
- La simplicidad y el hecho de que requiera mucha menor inversión para empezar a trabajar.
- Portabilidad de la información.
- Implementación más rápida y con menos riesgos.
- Actualizaciones automáticas que no afectan negativamente a los recursos de TI.
- Uso eficiente de la energía.

#### Desventajas

- La centralización de las aplicaciones y el almacenamiento de los datos origina una interdependencia de los proveedores de servicios.
- La disponibilidad de las aplicaciones está sujeta a la disponibilidad de acceso a [Internet](#).
- La confiabilidad de los servicios depende de la "salud" tecnológica y financiera de los proveedores de servicios en nube.
- La disponibilidad de servicios altamente especializados podría tardar meses o incluso años para que sean factibles de ser desplegados en la red.
- La madurez funcional de las aplicaciones hace que continuamente estén modificando sus interfaces, por lo cual la curva de aprendizaje en empresas de orientación no tecnológica tenga unas pendientes significativas, así como su consumo automático por aplicaciones.

- Seguridad. La información de la empresa debe recorrer diferentes modos para llegar a su destino
- Escalabilidad a largo plazo. A medida que más usuarios empiecen a compartir la infraestructura de la nube, la sobrecarga en los servidores de los proveedores aumentará, si la empresa no posee un esquema de crecimiento óptimo puede llevar a degradaciones en el servicio o altos niveles de retardo en la accesibilidad.

### 1.5. Desafíos de la nube híbrida

- Añaden la complejidad de determinar cómo distribuir las aplicaciones a través de estos ambientes diferentes. Puede ser atractiva la nube híbrida, pero está reservada a aplicaciones simples sin condicionantes, que no requieran de ninguna sincronización o necesiten bases de datos complejas.
- Es importante adoptar protocolos centralizados para acceder a los datos. Se recomienda gestionar accesos de inicio de sesión únicos.
- El equipo de TI muchas veces no está preparado para trabajar en nubes híbridas.
- La nube privada requiere mantenimiento y por consiguiente la nube híbrida también.

### 1.6. A modo general.

La computación en la nube tiene una serie de ventajas que hemos visto anteriormente y se amplían en mayor detalle en el capítulo 2.3, pero también es necesario contemplar:

- La computación en nube no permite a los usuarios poseer físicamente los [dispositivos de almacenamiento](#) de sus datos
- Limita la libertad de los usuarios creando dependencia del proveedor de servicios.

- la computación en nube pone en peligro las libertades de los usuarios, porque estos dejan su [privacidad](#) y datos personales en manos de terceros.

## 2. Estado de Situación

### 2.1. Principales conclusiones de la encuesta

La encuesta revela una adopción progresiva pero aún no masiva de servicios de nube pública, con una tendencia hacia soluciones híbridas que combinan la nube y centros de datos tradicionales. El impulso inicial se observa en soluciones SaaS, especialmente en el ámbito de productividad, acelerado por las demandas del trabajo remoto durante la pandemia de COVID-19.

Principales Hallazgos:

#### **Adopción Gradual e Hibridación:**

- La adopción de la nube pública es progresiva, con una preferencia por soluciones híbridas.
- Destaca la combinación de soluciones en la nube y centros de datos tradicionales.

#### **Enfoque Inicial en SaaS:**

- La adopción comienza con soluciones SaaS, especialmente en productividad.
- La necesidad de trabajo remoto durante la pandemia acelera esta tendencia.

#### **Centros Cloud en Europa y Futuros en España:**

- Existe una notoria utilización de centros Cloud en Europa.
- Se observa un interés creciente en el establecimiento de centros en España.

#### **Ventajas y Desafíos:**

- Ventajas principales: flexibilidad, rapidez y acceso a un amplio portfolio.
- Inconvenientes destacados: regulación, privacidad y escasez de talento.

### Costes de Nube Pública:

- Los costes de la nube pública son percibidos más como un inconveniente que como una ventaja.

### Soluciones de Conectividad:

- Soluciones privadas (enlaces autogestionados) son preferidas para la conectividad de infraestructura.
- Soluciones públicas (internet o VPNs) son más comunes para la conectividad a nivel de usuario.

### Desafíos en Conectividad:

- Desafíos notables en seguridad y falta de talento, especialmente en el área de seguridad.

## 2.2. Estado de adopción de Cloud

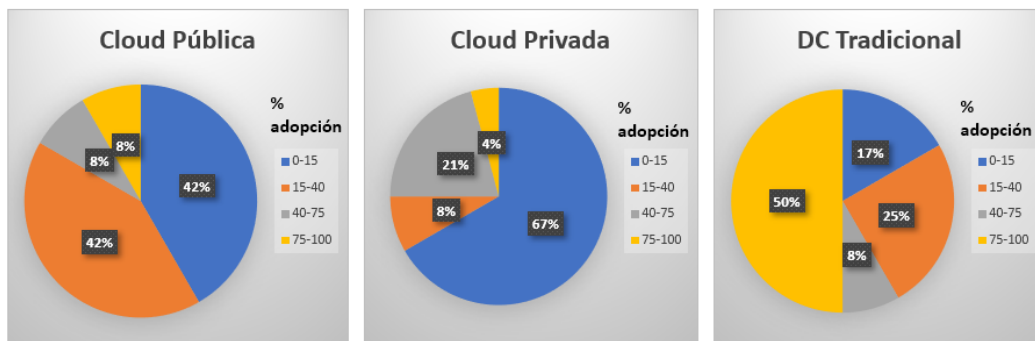


Ilustración 1 Estado de la adopción cloud

Respecto a la adopción de la **nube pública**, es interesante observar dos tendencias clave que se derivan de la información proporcionada:

- **Lenta Adopción:** La adopción de la nube pública por parte de las empresas parece avanzar a un ritmo más lento de lo que podría esperarse. Esto podría

deberse a varios factores, como la preocupación por la seguridad, la falta de experiencia en la migración a la nube o las necesidades de soluciones de conectividad para integrarlo con los entornos on-premise.

- **Distribución de Cargas en la Nube Pública:** Los datos revelan que solo el 60% de las empresas encuestadas tiene más del 15% de sus cargas de trabajo en la nube pública. Sin embargo, solo un 16% de estas empresas supera el 40% de cargas en la nube. Esto implica que, aunque muchas empresas han comenzado a migrar cargas de trabajo a la nube pública, la mayoría aún no ha alcanzado una adopción significativa.

La adopción de la **nube privada**, según los datos proporcionados, parece ser más rápida en comparación con la nube pública. Con un 25% de las empresas que tienen más del 40% de sus cargas en la nube privada, podemos destacar algunos puntos clave:

- La preferencia por la nube privada puede estar relacionada con la necesidad de mantener un mayor control sobre los datos y las aplicaciones. Las empresas que manejan información altamente sensible o que operan en industrias altamente reguladas a menudo optan por la nube privada debido a su capacidad para ofrecer mayor seguridad y personalización.
- La persistencia de cargas de trabajo en **centros de datos tradicionales**<sup>1</sup> es la situación común en la mayoría de las empresas encuestadas. Los datos proporcionados muestran una imagen interesante de la adopción de la nube y la permanencia de cargas en centros de datos tradicionales:

---

<sup>1</sup> La nube privada contempla que los servidores pueden estar ubicados en una instalación propia o en un centro de datos de tipo colocation, donde la empresa alquila espacio físico y servicios básicos. En el caso de los datacenters tradicionales, hacen referencia justamente al caso en la que la empresa dispone de una instalación propia propiedad o alquilada por la empresa.

- **Prevalencia de Centros de Datos Tradicionales:** A pesar del auge de las tecnologías de nube, muchas empresas todavía dependen en gran medida de centros de datos tradicionales para alojar sus cargas de trabajo. El hecho de que un 50% de las empresas mantenga más del 75% de sus cargas en centros de datos tradicionales destaca la persistencia de esta infraestructura.
- **Reducción Gradual de la Dependencia de Centros de Datos Tradicionales:** Sin embargo, también es alentador ver que un 17% de las empresas ha logrado reducir significativamente su dependencia de centros de datos tradicionales, con menos del 15% de sus cargas alojadas allí. Esto sugiere que algunas organizaciones están adoptando un enfoque más ágil para la migración a entornos más modernos.

### 2.3. Estado de adopción de la Cloud Publica

Las siglas "IaaS," "PaaS," y "SaaS" se refieren a diferentes modelos de servicios en la nube que ofrecen diversas capacidades y niveles de control a los usuarios.

IaaS (Infrastructure as a Service - Infraestructura como Servicio):

IaaS proporciona una infraestructura de TI virtualizada. Esto incluye recursos como servidores virtuales, almacenamiento, redes y máquinas virtuales.

Uso común: IaaS es ideal para empresas que necesitan una infraestructura escalable y personalizable para alojar aplicaciones y servicios específicos. Es especialmente útil para el desarrollo y la implementación de aplicaciones personalizadas.

PaaS (Platform as a Service - Plataforma como Servicio):

PaaS proporciona una plataforma de desarrollo y alojamiento en la nube que incluye herramientas y servicios para desarrolladores. Esto facilita la creación, el despliegue y la gestión de aplicaciones sin preocuparse por la infraestructura subyacente.

Uso común: PaaS es adecuado para desarrolladores que desean centrarse en la creación de aplicaciones sin preocuparse por la infraestructura. Es ideal para el desarrollo de aplicaciones web y móviles.

SaaS (Software as a Service - Software como Servicio):

SaaS ofrece aplicaciones de software alojadas en la nube que están disponibles para los usuarios a través de internet. Los usuarios acceden al software a través de un navegador web, en lugar de instalar y ejecutar aplicaciones en sus propios dispositivos.

Uso común: SaaS es ampliamente utilizado para aplicaciones empresariales como la gestión de relaciones con usuarios (CRM), correo electrónico y colaboración, y aplicaciones de productividad. También se encuentra en aplicaciones de consumo, como servicios de transmisión de video.

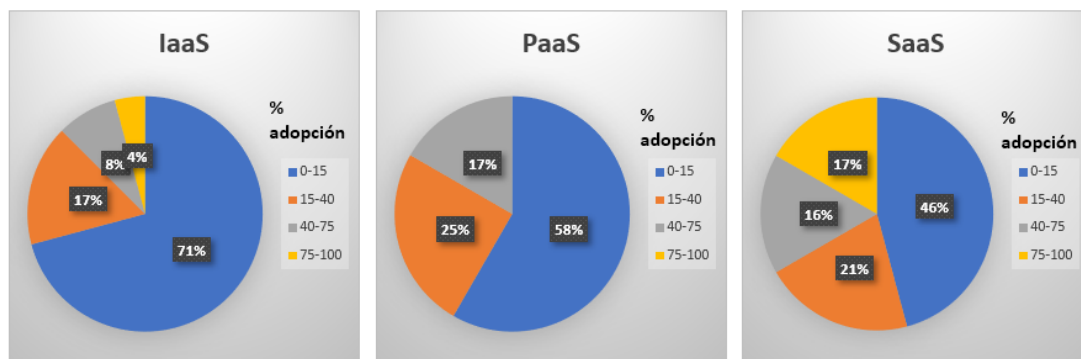


Ilustración 2 Adopción de los diferentes modelos de servicios

La baja adopción de IaaS (Infrastructure as a Service) en la encuesta indica que muchas empresas aún no han migrado una parte significativa de sus cargas de trabajo a esta infraestructura en la nube.

Esto puede deberse a varias razones, como la falta de comprensión de los beneficios de la nube, la inversión inicial requerida para migrar y la preocupación por la seguridad y el cumplimiento.

El hecho de que el 25% de las empresas utilice PaaS, especialmente para soluciones de desarrollo, es una señal positiva. Esto sugiere que las empresas

reconocen el valor de PaaS en el proceso de desarrollo de aplicaciones y están dispuestas a adoptarlo en este contexto.

El hecho de que la mayoría de las cargas de trabajo de los encuestados se hayan movido a soluciones SaaS (Software as a Service) refleja una tendencia creciente en la adopción de este modelo en la nube.

El crecimiento en la adopción de soluciones SaaS, especialmente en áreas como la productividad, el correo electrónico y las aplicaciones empresariales (ERPs, CRMs, recursos humanos, etc.), resalta la eficacia de este modelo en el cumplimiento de las necesidades empresariales cotidianas por su facilidad de Implementación y acceso desde cualquier lugar con una conexión a Internet.

Al adoptar SaaS, las empresas se benefician de un servicio completo llave en mano que reduce significativamente su carga de infraestructura y costes de mantenimiento, ya que el proveedor de SaaS se encarga de estos servicios.

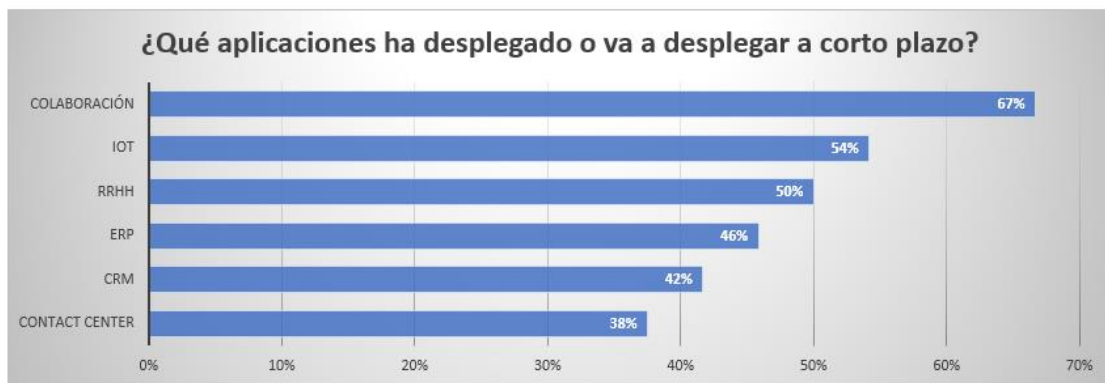


Ilustración 3 Tipos de aplicaciones y porcentaje desplegados

Las soluciones de colaboración basadas en SaaS (Software as a Service) experimentaron una adopción masiva durante la pandemia de COVID-19 debido a las ventajas que ofrecen en el entorno laboral y de comunicación remota al permitir a los usuarios acceder a herramientas y recursos de colaboración desde cualquier lugar con una conexión a Internet, lo que es esencial para el trabajo remoto y la flexibilidad laboral.

Las soluciones de colaboración en SaaS se convirtieron en una parte fundamental del entorno empresarial durante la pandemia debido a su capacidad para facilitar

la comunicación y la colaboración en un mundo cada vez más digital y distribuido. Las ventajas clave de accesibilidad, facilidad de implementación, actualizaciones automáticas y escalabilidad contribuyeron a su adopción masiva y seguirán siendo relevantes en el futuro del trabajo.

La incorporación por parte de los fabricantes de soluciones de IA, de manera nativa a este tipo de productos, en modo “Copilot” seguramente impulsará su uso para mejorar la productividad de las empresas

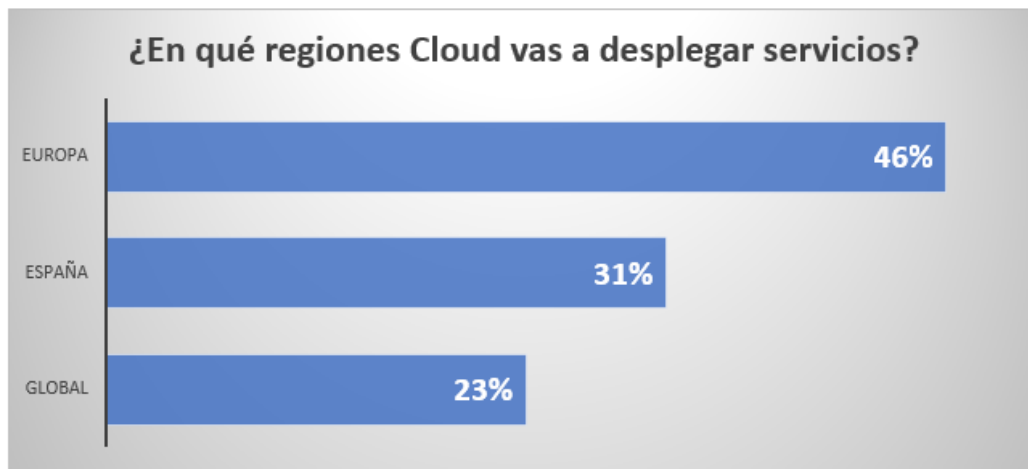


Ilustración 4 Región cloud en la que se va a desplegar servicios

El despliegue de cargas en la nube en regiones específicas, como España, debido a motivos de cumplimiento normativo como el GDPR (Reglamento General de Protección de Datos) y la búsqueda de cloud soberana, es un fenómeno que refleja la importancia de la privacidad de datos y la regulación en la toma de decisiones empresariales.

El GDPR establece estrictos requisitos de protección de datos para las empresas que operan en la Unión Europea. Como resultado, la mayoría de las empresas optan por alojar sus datos y cargas de trabajo en regiones de la nube dentro de la UE, incluidas las que se están estableciendo en España, para cumplir con estas regulaciones y garantizar la privacidad de los datos de sus usuarios.

El rápido interés de estas regiones de nube en España resalta la urgencia con la que las empresas desean cumplir con las regulaciones y garantizar la privacidad de los datos. Esto también puede deberse a una mayor conciencia de los riesgos

asociados con el almacenamiento de datos en ubicaciones fuera de su país de origen y con el concepto de Cloud soberana que se refiere a la preferencia de las empresas y los gobiernos por almacenar y procesar datos críticos dentro de las fronteras nacionales. Esto se hace para mantener un mayor control sobre los datos y garantizar su seguridad y privacidad.

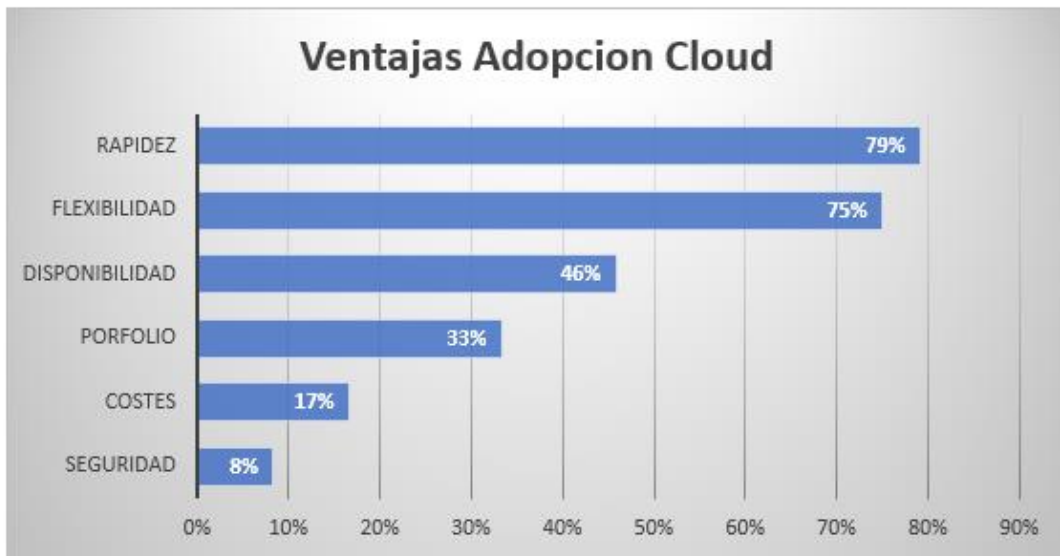


Ilustración 5 Ventajas de adopción de la cloud

Las empresas encuestadas destacan la flexibilidad, rapidez y amplitud de portfolio como las ventajas principales de la adopción de Cloud pública.

Flexibilidad:

- **Escalabilidad:** La nube pública permite a las empresas escalar sus recursos de manera rápida y eficiente, lo que se traduce en flexibilidad para adaptarse a las cambiantes necesidades de la empresa.
- **Acceso Remoto:** Los servicios en la nube pública son accesibles desde cualquier lugar con conexión a Internet, lo que brinda flexibilidad en la ubicación y el acceso a los recursos.

### Rapidez:

- **Implementación Rápida:** La nube pública permite implementar recursos informáticos en minutos u horas en lugar de semanas o meses, lo que acelera los procesos de desarrollo y despliegue.
- **Actualizaciones Automáticas:** Los proveedores de nube pública gestionan actualizaciones y parches de seguridad automáticamente, lo que garantiza la rapidez en la aplicación de mejoras.

### Amplitud de Porfolio:

- **Diversidad de Servicios:** La nube pública ofrece una amplia variedad de servicios, desde máquinas virtuales y almacenamiento hasta inteligencia artificial y análisis de datos, lo que proporciona un amplio portfolio de opciones para las necesidades de la empresa.
- **Ecosistema de Aplicaciones:** Existe un ecosistema de aplicaciones y servicios de terceros que se integran fácilmente con la nube pública, ampliando aún más las posibilidades y el portfolio de soluciones disponibles.

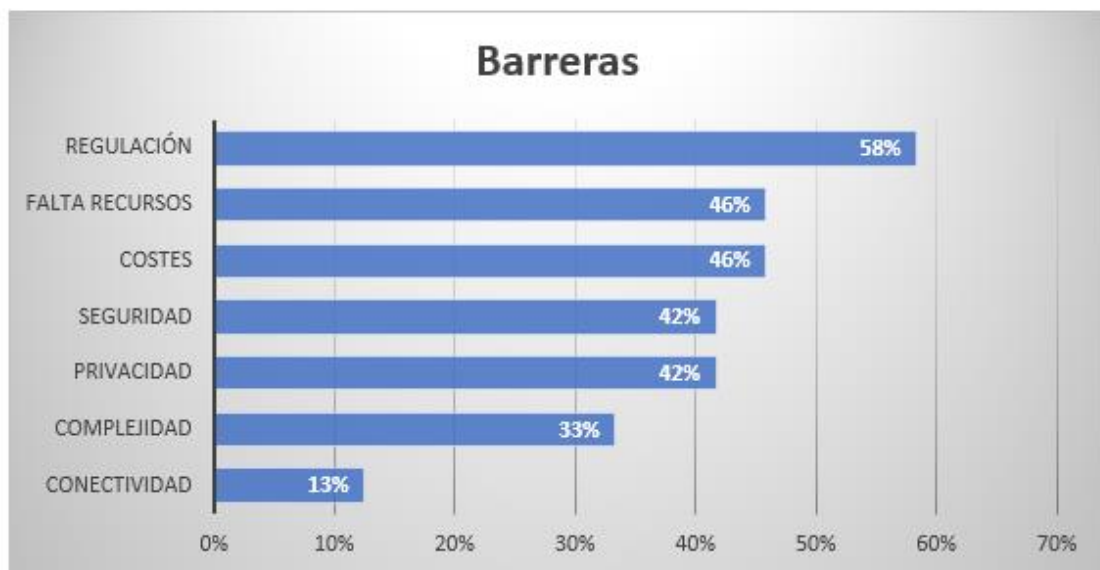


Ilustración 6 Barreras para la adopción de la cloud

Siguen muy presentes las barreras relacionadas con temas regulatorios, privacidad, seguridad y recursos capacitados que siguen siendo un desafío significativo en la adopción de tecnologías de la nube.

**Barreras Regulatorias y Cumplimiento Normativo:** Las regulaciones como el GDPR en Europa y otras leyes de privacidad de datos imponen restricciones estrictas sobre cómo se deben manejar y proteger los datos personales. Las empresas deben cumplir con estas regulaciones al usar servicios de nube pública, lo que puede requerir cambios en las prácticas y la infraestructura.

**Privacidad de Datos y Seguridad:** Las empresas a menudo son reacias a almacenar datos sensibles o críticos en entornos de nube pública debido a preocupaciones sobre la privacidad y el control de los datos.

**Falta de Recursos:** La falta de recursos y experiencia en la nube puede ser un obstáculo. La capacitación del personal y la contratación de talento con experiencia en la nube son esenciales para una implementación exitosa.

Entre los encuestados, se da la percepción de que la nube es un **entorno más caro** que los entornos clásicos. Esta es una preocupación común entre algunas organizaciones, pero es importante tener en cuenta que la evaluación de costos en la nube puede variar según varios factores y que depende en gran medida de la flexibilidad y rapidez requerida.

Estas preocupaciones han de ser mitigadas por la adopción y desarrollo de prácticas **FinOps**, así como la **modernización de aplicaciones** hacia soluciones **cloud-native** que permitan crecer o decrecer en función de la necesidad de negocio, aprovechando de ese modo la flexibilidad cloud de un verdadero pago por uso.

## 2.4. Desafíos y Soluciones de Conectividad

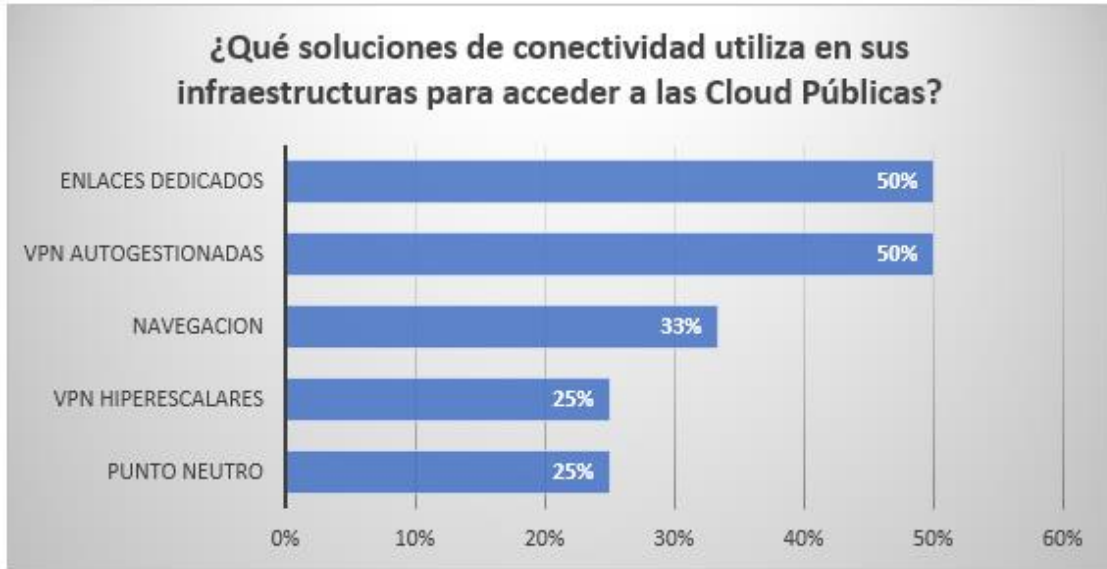


Ilustración 7 Soluciones de conectividad usadas para acceder a nubes públicas

Dar conectividad entre entornos de nube privada y centros de datos tradicionales, históricamente ha requerido como requisito fundamental el uso de conexiones privadas, bien a través de enlaces dedicados o circuitos autogestionados.

En entornos de infraestructura de nube pública es una elección estratégica que se basa en una serie de consideraciones importantes como mayor control y seguridad, rendimiento, aislamiento de redes y reducción de latencias. Debido al tamaño de las empresas encuestadas, vemos como las soluciones de enlaces dedicados (junto con el acceso desde puntos neutros) ocupan el mayor porcentaje, seguidos de los circuitos autogestionados.

Un dato interesante es el incremento del porcentaje que hace uso de tráfico de navegación sin cifrado. Suponemos que el principal uso de este tipo de tráfico se debe al consumo de soluciones SaaS, como por ejemplo las principales soluciones de colaboración, donde el cifrado se realiza a nivel de aplicación.

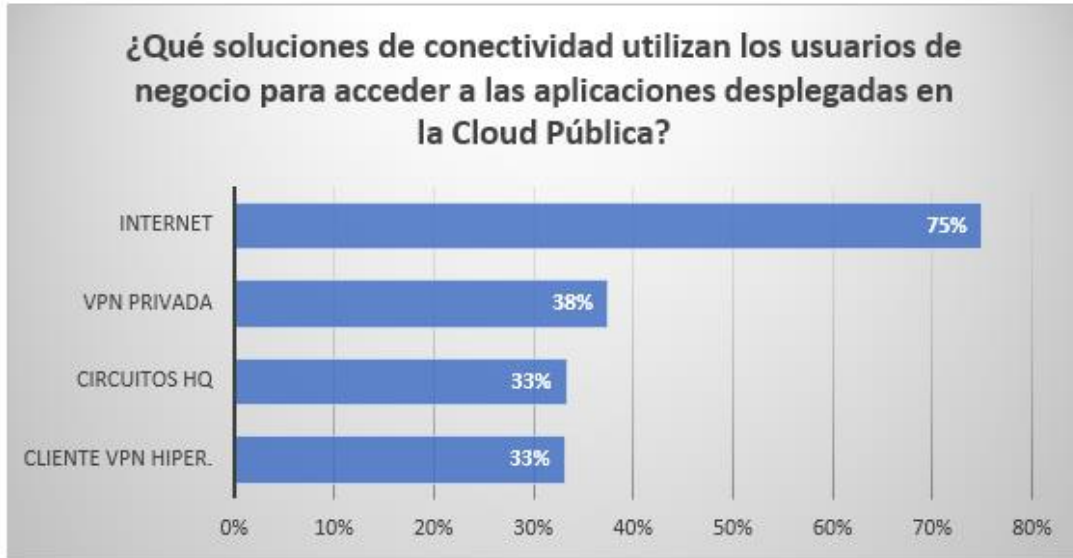


Ilustración 8 Soluciones para acceder a nubes públicas desde los usuarios de negocio

Si ponemos el foco en los usuarios finales, la foto es radicalmente distinta. Los aplicativos desplegados en las nubes públicas se consumen en su mayoría a través de tráfico sin cifrado, especialmente cuando se trata de acceder a soluciones SaaS y herramientas de colaboración, es una elección lógica por el acceso universal de estas soluciones, la facilidad de acceso y el rendimiento adecuado para estos servicios.

La siguiente categoría de soluciones más utilizada serían las soluciones de VPN corporativas y el tráfico centralizado desde las sedes corporativas, y en menor medida el uso de usuarios VPN de la plataforma destino.

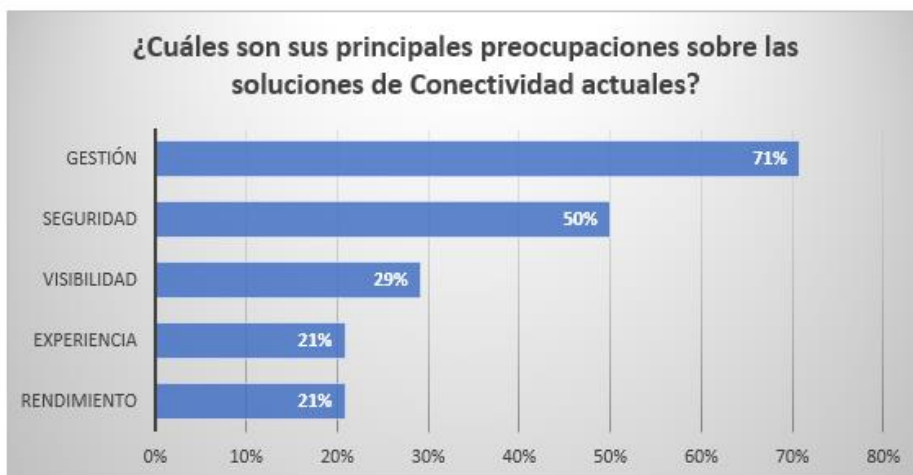


Ilustración 9 Principales preocupaciones sobre la conectividad con la nube pública

La mayor preocupación sobre las soluciones de conectividad son los relacionados con la gestión, seguido por la seguridad.

**Gestión de la Conectividad:** La gestión de soluciones de conectividad puede ser compleja, especialmente cuando se trata de redes distribuidas en la nube. La falta de visibilidad y control puede dificultar la resolución de problemas y el mantenimiento eficiente.

Mantener un rendimiento óptimo y orquestar el despliegue de los entornos de conectividad puede ser un desafío. Las organizaciones deben supervisar y optimizar constantemente la red para garantizar un acceso rápido y confiable a aplicaciones y servicios.

**Falta de Talento y Habilidades:** En muchos casos, las organizaciones carecen de talento y habilidades especializadas en conectividad y redes. Esto puede dificultar la configuración, el mantenimiento y la resolución de problemas de la infraestructura de conectividad. La capacitación y el desarrollo de habilidades son esenciales para abordar la falta de talento. Las organizaciones deben invertir en la formación de su personal o considerar la contratación de expertos en conectividad.

**Seguridad de la Conectividad:** La conectividad expone a las organizaciones a amenazas cibernéticas, como ataques de malware, ransomware y fuga de información. Garantizar la seguridad de la red es fundamental para proteger los datos y las operaciones.

La gestión de acceso y la autenticación son preocupaciones clave para garantizar que solo usuarios autorizados tengan acceso a recursos y datos críticos.

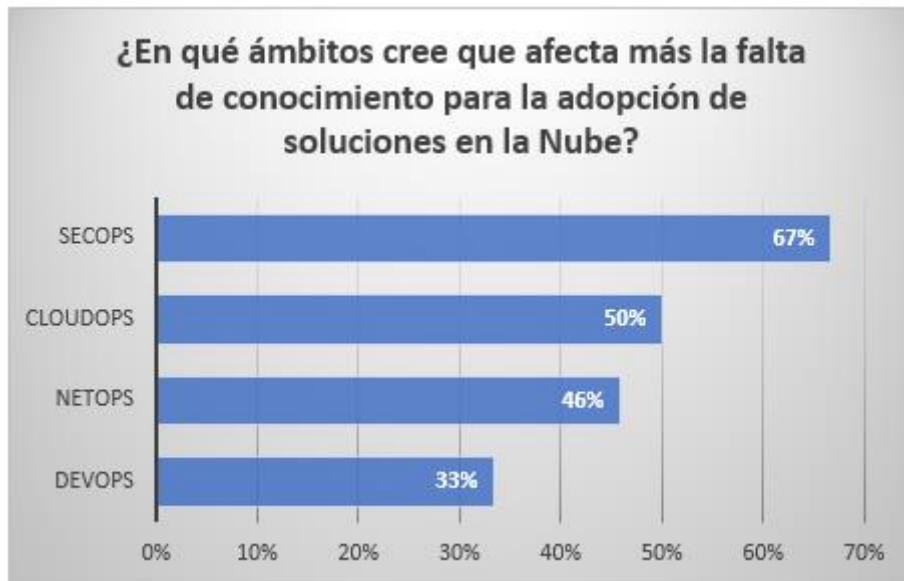


Ilustración 10 Ámbitos en los que afecta más la falta de conocimiento para la adopción de la nube pública

La falta de talento en áreas críticas como operaciones de seguridad, cloud y redes es un desafío importante que muchas organizaciones enfrentan actualmente. Esta escasez de habilidades puede obstaculizar la capacidad de las empresas para gestionar de manera efectiva sus operaciones de TI y ciberseguridad, y por ende ralentizar su adopción Cloud.

Razones de la Falta de Talento:

**Demanda en Crecimiento:** La creciente dependencia de la tecnología, la migración a la nube y el aumento de amenazas cibernéticas han aumentado la demanda de profesionales en estas áreas.

**Evolución Tecnológica:** La rápida evolución de la tecnología significa que los profesionales deben mantenerse actualizados con nuevas habilidades y conocimientos constantemente.

**Competencia por el Talento:** La competencia por los talentos más calificados es feroz, lo que puede hacer que sea difícil para las organizaciones atraer y retener a los expertos.

## 2.5. Detalles de la encuesta

La encuesta ha sido distribuida entre los miembros de Autelsi para tener una foto objetiva del estado de adopción de Cloud, los mecanismos de conectividad utilizados y las principales ventajas y problemáticas que han tenido.

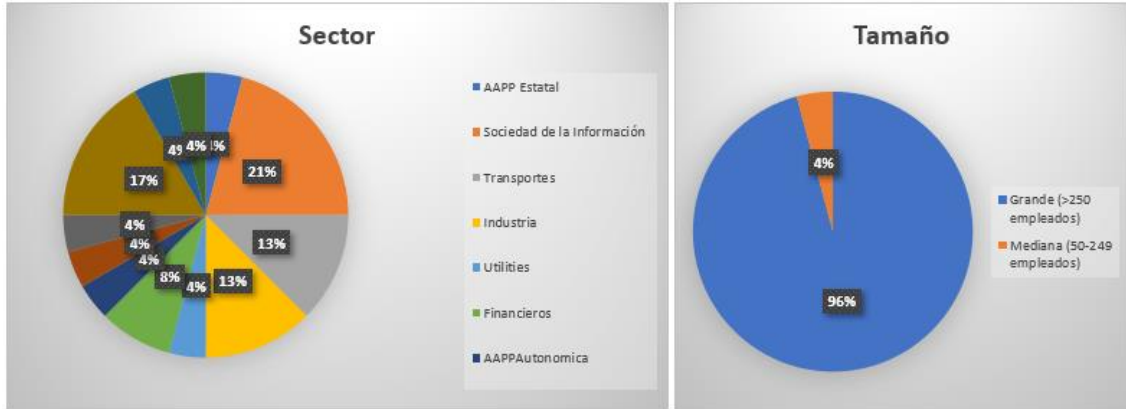


Ilustración 11 Adopción de la nube pública dependiendo del sector y el tamaño

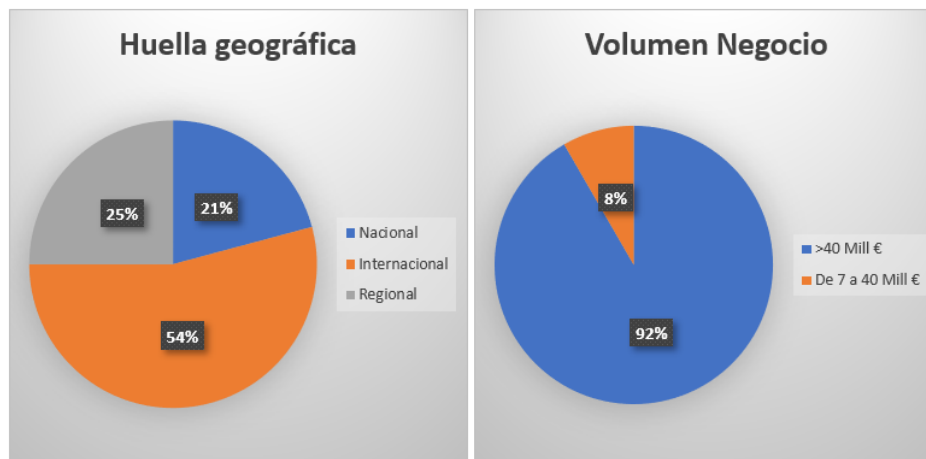


Ilustración 12 Adopción de la nube pública dependiendo de la huella geográfica y el volumen de negocio

Sobre la encuesta:

### Buena representación de Sectores:

Es positivo que la encuesta tenga una buena representación de sectores, ya que esto proporciona una visión más completa de las tendencias y desafíos en diferentes industrias. Esto permite obtener información valiosa sobre cómo la adopción de tecnologías de la nube y la hiperconectividad varía en diferentes sectores.

### **Empresas Grandes con Implantación Internacional:**

La encuesta esta principalmente contestada por empresas grandes con implantación internacional en la mayoría de los casos sujetos a complejos procesos internos y regulaciones.

### **Baja Participación (24 Empresas):**

Si bien la representación de sectores es buena, la baja participación de 24 empresas puede limitar la generalización de los resultados. Cuanto mayor sea la muestra de participantes, mayor será la validez estadística de los hallazgos. Es importante considerar que los resultados pueden no ser representativos

## **3. La Hiperconectividad como Solución**

### **3.1. Introducción**

Hasta ahora hemos visto como la adopción de la nube puede ofrecer nuevas oportunidades a las empresas para abordar su transformación digital, aportando mayor agilidad y rapidez en el desarrollo de nuevas soluciones de negocio.

Según datos de Gartner en el 2025 el 85% de las empresas utilizarán principios de “la nube primero”.

La encuesta que hemos realizado como parte de este trabajo muestra que efectivamente la adopción de la nube es una realidad, si bien la existencia de cargas de trabajo en centros de datos tradicionales es una situación común en la mayoría de las empresas encuestadas, aunque poco a poco parece que reducirán su dependencia.

Aunque la encuesta muestra que la conectividad no es una de las barreras identificadas más importantes para la adopción de la nube, siendo los temas relacionados con la seguridad y marco normativo junto con la complejidad los que están más presentes, la conectividad es, a nuestro modo de ver, un elemento clave

en el éxito de la adopción de la nube impactando considerablemente en aspectos como el rendimiento, la seguridad y la complejidad de la gestión del entorno.

En los siguientes capítulos se aborda la problemática de la conectividad intentando dar una visión lo más completa posible, tratando la conectividad entre aplicaciones e infraestructuras y las comunicaciones entre los usuarios y las aplicaciones en distintos escenarios (Data centers privados con una o varias nubes o Conectividad MultiCloud).

Se incluyen unos ejemplos prácticos de casos reales que ilustran las soluciones descritas y que pueden servir como una guía para escoger la solución que mejor se adecue a la casuística y requisitos concretos de cada empresa.

Por último, también se tienen cuenta aspectos como la seguridad, la monitorización o la automatización que son reconocidos como factores clave para una adopción exitosa de la nube.

### **3.2. Soluciones básicas de Conectividad en la interconexión de nubes**

Tradicionalmente las tecnologías para interconectar datacenters se han agrupado debajo de las siglas DCI, de su nombre *Data Center Interconnect*, un concepto que agrupa soluciones de conectividad a lo largo de las diversas capas de la red.

A lo largo de los años las tecnologías DCI han evolucionado de forma significativa para adaptarse a nuevas necesidades y tendencias (aparición de nubes públicas, gestión centralizada, SDN, por mencionar algunas), con nuevas soluciones incorporándose paulatinamente. Actualmente el catálogo de soluciones para interconectar las ubicaciones donde residen las aplicaciones es amplio y variado.

Como punto de partida y desde una perspectiva de *Underlay* o de la pura conectividad física, se encuentran las siguientes soluciones tradicionales sobre las que se basan las conexiones DCI:

- **Conexiones sobre Internet:**

Popularizadas en los últimos años gracias a su mejora sobre todo en velocidad y performance. Son la opción de conectividad más económica, *best effort* en la mayoría de los casos (aunque algunos proveedores ya proporcionan calidad de servicio dentro de su red/backbone para ciertos tipos de tráfico SaaS, como O365) y, en general necesitan de otras soluciones que se despliegan por encima o *over the top*, para poder conectarse a los entornos privados (ya sea de usuario como en nubes públicas- i.e IaaS). Como mínimo, será necesaria una tecnología de tunelización por encima para habilitar el tráfico de capa 2 extremo a extremo y que al mismo tiempo garantice la privacidad, seguridad e integridad del tráfico empresarial.

- **Conexiones directas tipo fibra oscuras o punto a punto:**

La fibra oscura es una de las soluciones más utilizadas cuando los datacenters se encuentran en el mismo campus o relativamente cercanos (en cuyo caso se pueden alquilar fibras a través de operadores). Para distancias mayores las conexiones punto a punto, como su nombre indica, son habituales cuando se quiere interconectar datacenters privados entre ellos o bien con datacenters privados alojados en terceros (co-location) y se desea una conexión directa, de alta velocidad, máxima seguridad y menor latencia.

- **Conexiones privadas (MPLS o VPN):**

La interconexión vía MPLS ofrecida por las operadoras de telecomunicaciones permite sortear la problemática de la distancia de la opción de fibra oscura y punto a punto, permitiendo al mismo tiempo la interconexión a nivel 2 que ofrece ésta. A pesar de tener un precio más elevado que la conectividad vía Internet, son una opción relevante para los datos críticos de las compañías o *business critical* (datos sensibles, tráfico de disaster recovery...) ya que garantizan seguridad de forma intrínseca y los

operadores además de ofrecer SLAs y calidades de servicio, pueden también ofrecer la interconexión vía MPLS hacia los hiperescalares.

La selección entre estas diferentes opciones se basa mayoritariamente en criterios de adaptabilidad a la naturaleza del datacenter o datacenters (datacenters tradicionales, clouds públicas, privadas, alojamiento en datacenters de terceros, IaaS o PaaS, entre otros) a la arquitectura concreta del datacenter, a los requisitos de seguridad y también recientemente a los escenarios de casos de uso.

De hecho, de entre los encuestados, las principales soluciones utilizadas son justamente soluciones privadas tipo enlaces o VPN autogestionadas. Sin embargo, los servicios en la nube se han acelerado y siguen predominando los modelos híbridos de interconexión con la nube pública y multicloud. Según un estudio reciente (IDC 2023) el 45% de las empresas españolas ha adoptado una estrategia de nube híbrida, y el 90% de ellas utiliza un escenario multicloud.

A nivel general, podemos decir que las empresas utilizan conectividad multicloud, y de ellas una amplia mayoría corresponden a arquitecturas de nube híbrida. Cabe también notar que se ha observado un ligero incremento de las empresas que implementan una sola nube (en este caso pública), esta consolidación en un único vendor puede venir motivada por una búsqueda de menor complejidad y también de un menor acceso a talento para gestionar estos entornos, motivos por los que el desarrollo de soluciones de hiperconectividad de integración fácil son de importancia.

La flexibilidad y rapidez de despliegue que ofrecen los hiperescalares en el entorno Cloud (el poder desplegar “a un clic”) se ha extendido como demandas de las empresas de cara a la conectividad contra sus aplicaciones. La expectativa consiste en poder provisionar de forma sencilla la conectividad y otros servicios relacionados para aplicaciones que pueden encontrarse distribuidas en múltiples localizaciones dependiendo de los proveedores cloud utilizados. Otras demandas que también se les une a las anteriores, son las de alta velocidad y baja latencia, ya que gracias a la aparición de tecnologías como el *Edge Computing* las empresas

contemplan la posibilidad de poder interactuar con los datos de la nube pública en tiempo real, lo que les permite ser más ágiles y competitivas.

Esto ha generado evoluciones en servicios y productos por parte de proveedores de diferentes ámbitos para adaptarse a esta demanda, lo que ha traído consigo una transformación de la conectividad con el objetivo de que sea cada vez más ágil, dinámica y adaptable. Profundizamos en ello en los siguientes capítulos.

### 3.3. ¿Qué es la Hiperconectividad?

Estos entornos híbridos que han crecido rápidamente fomentado por la rapidez y la innovación que las capacidades del Cloud nos han traído, ha generado una serie de *challenges* o desafíos a los que debe dar respuesta la conectividad y que tratamos de resumir a continuación:



#### Infraestructura y Diseño

Conectividad ágil y transparente que permite el despliegue de aplicaciones distribuidas en entornos heterogéneos

Facilidad de diseño que facilita la abstracción y la aplicación consistente de políticas (versus soluciones tipo silo)

Seguridad e Integridad del dato (Privacidad y Regulación)



#### Operativa y Funcionamiento

Adaptación del modelo operativo a un modelo *cloud-like*

Automatización y softwarificación de la red

Gobierno/Orquestación/ Integración de las diferentes soluciones

Observabilidad y Troubleshooting *end-to-end*



#### Negocio

SLAs y Garantías de Servicio

FinOps y Billing integrado

Continuidad de Negocio y Resiliencia

Talento y Conocimiento

Ilustración 13 Desafíos de los entornos de Nube Híbrida/Multicloud

Las empresas en esta era multi-cloud necesitan poder extender aplicaciones a través de diferentes entornos, y eso significa *levantar* la conectividad entre cualquier servidor (físico o virtual) y/o nube de forma consistente, aplicando las políticas de enrutado, seguridad y automatización independientemente de las

múltiples redes y las nubes públicas. Y, además, con herramientas de gestión y observabilidad que permitan una visión extremo a extremo de la conectividad.

**La hiperconectividad**, por lo tanto, debe tener como misión resolver estas necesidades y, en consecuencia, proporcionar una experiencia ágil, unificada y bajo demanda, a través (e indistintamente) de las redes o nubes públicas y privadas, en donde residan los datos y/o usuarios.

#### Entornos y tendencias

Hasta ahora hemos visto la conectividad base sobre la que se sustentan las soluciones DCI y los requisitos que deben cubrir las soluciones en el mercado para poderse considerar como *hiperconectividad*. Antes de continuar, merece la pena distinguir los dos entornos o casos de uso principales que nos encontramos para evaluar estas soluciones y, asimismo, hacer un breve repaso de las tendencias en la tecnología de redes empresariales que pueden ayudar a dar forma a las estrategias de evolución de red de la compañía.

Los principales casos de uso asociados son los siguientes:

1. Hiperconectividad de las aplicaciones y sus infraestructuras entre sí
2. Hiperconectividad de los usuarios (corporativos y proveedores) con las aplicaciones

Los desafíos más retadores se encuentran en el primer entorno y allí encontraremos también un mayor número de soluciones, algunas más universales y otras según casuísticas soportadas.

A nivel de tendencias, en los últimos años se ha identificado un auge de soluciones sobre tecnologías nuevas y tecnologías ya existentes. Soluciones por ejemplo como SASE, redes multinube, 5G, NetDevOps y la red como servicio (NaaS).

- **Redes SASE:**

El stack de Tecnologías y funcionalidades de SASE (*Secure Access Service Edge*) conecta y protege a los usuarios, los dispositivos y las ubicaciones que acceden a las aplicaciones. Ofrece múltiples capacidades de red y seguridad convergentes, como WAN definida por software (SD-WAN), Proxy Web seguro (SWG), gestor de acceso seguro a la nube (CASB), firewall de próxima generación (NGFW) y aplicando políticas de acceso basadas en la confianza cero (ZTNA). SASE es un habilitador de la transformación empresarial digital moderna, que incluye el trabajo desde cualquier lugar, la confianza cero y la adopción de la computación perimetral y las aplicaciones en la nube.

- **Redes multinube (MCNs y MCN NaaS)**

El software de red multinube (MCNS, *Multicloud Networking Services*) permite el diseño, la implementación y el funcionamiento de una red dentro de múltiples entornos de nube pública. Los productos MCNS permiten una política de red, seguridad de red, gobierno y visibilidad de red consistentes en múltiples entornos de nube a través de un único punto de administración.

- **NetDevOps:**

NetDevOps implica la aplicación de prácticas de DevOps y/o integración continua/implementación continua (CI/CD) a las actividades de red, como el aprovisionamiento y la resolución de problemas. El término "NetDevOps" ha ganado popularidad en la industria, los operadores de red y los proveedores durante los últimos meses.

SASE y las redes multinube ya están experimentando aceptación entre los usuarios empresariales, mientras que 5G, NetDevOps y NaaS son tendencias incipientes con un fuerte crecimiento previsto durante los próximos años. A continuación, analizamos algunas de estas soluciones en los dos entornos de uso que se han mencionado antes.

### Hiperconectividad entre aplicaciones/infraestructuras

En este escenario se debe cubrir la capacidad de las infraestructuras para conectarse entre sí estén donde estén, tanto si se encuentran alojadas en una o varias nubes privadas o el caso equivalente en nubes públicas.

En este punto, y para poder entender mejor las soluciones que se van a describir, es importante tener claros los tramos a nivel de conectividad que existen en esta comunicación entre aplicaciones.

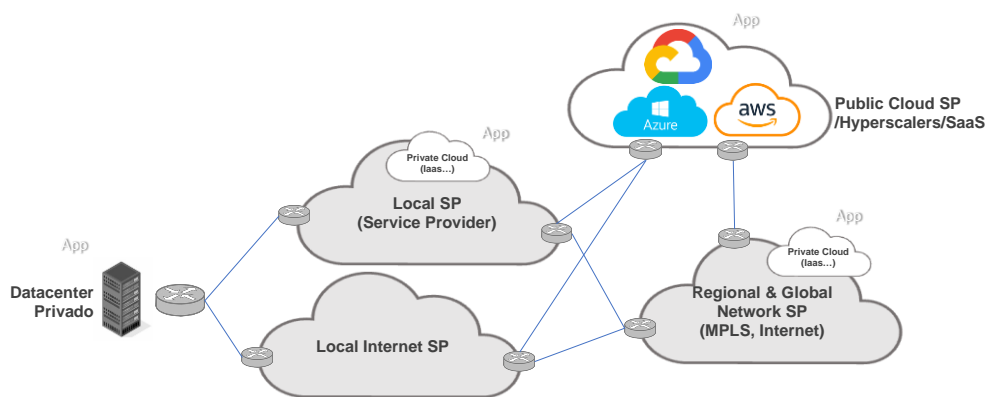


Ilustración 14 Tramos de Conectividad Underlay en la comunicación Aplicación - Aplicación

Partimos de una situación común en general con aplicaciones que se encuentran alojadas en datacenters privados (ya sean propiedad del usuario, *col-location* en datacenters de proveedores terceros, etc).

La situación de cada compañía obviamente será diferente (habrá compañías con varios datacenters, otras con sólo uno que se quieran interconectar con la nube pública, o incluso compañías con servicios en IaaS de terceros). El volumen de datos también será diferente, teniendo usuarios que sólo estén utilizando las nubes externas para un volumen determinado de datos y otros usuarios que hayan migrado la gran mayoría de sus datos en una estrategia *cloud-first* y otros a medio camino donde, por seguridad o soberanía y/o garantía de continuidad de negocio, mantengan las bases de datos sensibles en su datacenter privado).

Algunos ejemplos de los escenarios que podemos encontrarnos en la conectividad de aplicaciones/infraestructuras entre sí son:

### **Escenario 1:**

#### **Data Center – to – Cloud Distribuido y variaciones de este:**

- a. Extender un Cloud (o n+1) a los distintos CPDs/Edge del usuario
- b. Escenario de housing + integración con CPD propio o bien con IaaS/Nube pública
- c. Escenario Edge hiperescalar integrado onprem con CPD de usuario

### **Escenario 2:**

**Cloud – to – Cloud o Multicloud híbrido**, según si queremos conectar infra o apps, varían las soluciones:

- a. Desde el punto de vista de red: Multicloud Networking
- b. Desde el punto de vista de aplicaciones: App delivery Network

Volviendo al ejemplo de la imagen, este datacenter privado se interconecta a través de operadores locales (Local Access o Local Mile) tanto de conexiones privadas como también Internet (aunque es necesario securización en este último), que a su vez se conectan con otros Operadores de Conectividad Regional y Global (Middle Mile) que disponen a su vez de backbones privados y peering directo de Internet e interconectan con las regiones de los hiperescalares (Public Cloud). Si el hiperescalar dispone de región en el país, la conectividad se puede realizar a través de proveedores locales (privados e Internet). En el caso de una interconexión vía Internet, a parte de la necesidad de securización al ser redes abiertas, es importante mantener presente que la calidad (en cuanto a latencia, por ejemplo) dependerá de los acuerdos de *peering* entre los operadores globales de internet con sus homólogos locales en cada país.

Cabe destacar que en España está aumentando el número de nuevos datacenters que se están abriendo o en construcción, así como la apertura de Zonas y Puntos de presencia Locales de los principales hiperescalares. Este punto facilitará la

capacidad de conexión con las nubes públicas, simplificando las soluciones de hiperconectividad que, en algunos casos, se resolverá con arquitecturas basadas en la *adyacencia* (estarán co-ubicados el cloud público y el privado), como por ejemplos los POPs (*Point of Presence*) que veremos más adelante.

Hasta ahora se ha hablado de la conectividad física o también denominada *Underlay*. Por encima de esta conectividad, existen soluciones de tipo *Overlay* que se basan en la creación de una red virtual de túneles extremo a extremo que buscan comunicar los centros de la compañía como si estuvieran dentro de la misma red corporativa, pero de forma agnóstica a la conectividad física subyacente por debajo. Ejemplo de ellos son las soluciones SD-WAN o MCN mencionadas que veremos más adelante. Pero, independientemente de la solución de Overlay escogida, el performance, los SLAs y el soporte técnico a la conectividad viene en gran medida determinada por la selección de Underlay realizada y por ello, es importante el conocimiento de sus características y prestaciones.

Sintetizando este flujo de conectividad en un conjunto de piezas, podemos observar las siguientes:

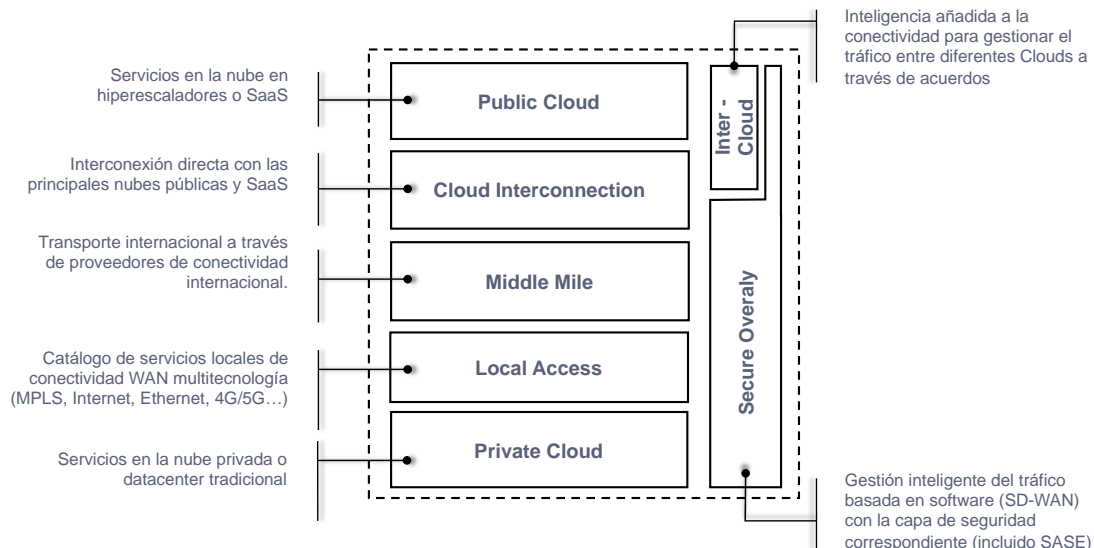


Ilustración 15 Elementos de la conectividad aplicación-aplicación en entornos de nube híbrida

Para cubrir los desafíos descritos en cuanto a *hiperconectividad*, sería deseable que las soluciones abordarán una serie de requisitos<sup>2</sup> tales como:

- Conectividad segura y *cloud-agnostic*
  - Integrar de forma única, escalable y segura los datacenters privados con el Cloud (uno o varios)
  - Facilidad para integrar la conectividad *underlay* manteniendo la convergencia de la solución.
  - Soporte para baja latencia y calidades de servicio (anchos de banda garantizados)
  - Flexible y fácil de escalar
  - Soporte de cargas distribuidas
  - Protege la soberanía e integridad de los datos
- Self Service
  - Permite la definición de SLAs.
  - Mejora los tiempos operativos
- Soporte de funcionalidades L3-L7 de forma cross a las plataformas
  - Despliegue sencillo y consistente de políticas de red, seguridad y relativos al resto de capas (4-7) en los entornos híbridos y multicloud
- Modelos de precio flexibles

---

<sup>2</sup> Funciones clave de las plataformas NaaS (Analysis Mason 2022: Multi-cloud Networking a framework for understanding the opportunity and ecosystem)

- Exposición mediante APIs
  - Facilitar la automatización, orquestación y gestión end to end

Teniendo en cuenta estos requisitos, se puede completar el diagrama anterior de la siguiente forma:

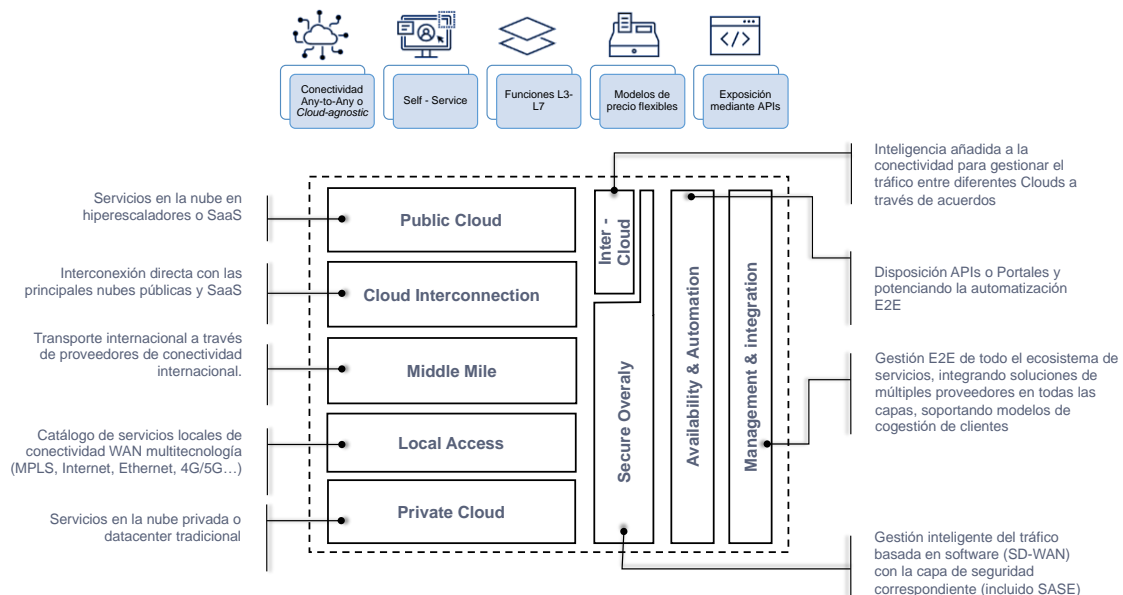


Ilustración 16 Elementos de la hiperconectividad aplicación-aplicación en entornos de nube híbrida

Los beneficios que traen para las compañías:

- Acelera la adopción de la nube (Híbrida y Multicloud)
- Gestión de Políticas Comunes para las aplicaciones y APIs (independientemente de su ubicación)
- Ayuda a cumplir requerimientos regulatorios
- Mejora del rendimiento de la red y de las aplicaciones

Es importante contemplar que la selección de solución dependerá del caso de uso de cada compañía. Habrá compañías que sólo estarán interesadas en soluciones concretas para resolver necesidades específicas y, otras que, para alcanzar todos los beneficios descritos anteriormente que se desean de la *hiperconectividad*, encontrarán que una única solución puede no abordarlos completamente, y por

ello, conllevar el despliegue de una o varias soluciones de forma complementaria de acuerdo con el escenario del usuario. Todavía es necesario más tiempo para disfrutar de soluciones de *ventanilla única* extremo a extremo. Tener presente los elementos que debe tener una solución de hiperconectividad (Ilustración 16) y compararlos contra las necesidades del usuario/escenario y la propuesta de la solución del vendor que se esté analizando, garantizará un mayor éxito en conseguir los objetivos buscados.

En los siguientes capítulos veremos en mayor detalle algunas soluciones para este entorno.

#### *Soluciones basadas en extensión single-cloud*

Este tipo de soluciones buscan resolver la complejidad de la conexión contra una nube pública (interconexión con la red privada, contención del dato, routing a través de regiones...).

Entre las diferentes soluciones que se pueden encontrar, podemos diferenciar tres tipos:

- **Soluciones basadas en mejora del rendimiento de la interconexión física:**

No cumplen con todos los elementos que hemos descrito para la *hiperconectividad*, pero son de relevancia para aquellos usuarios que quieren asegurar a nivel físico la seguridad de la interconexión y/o una conexión mucho más rápida de su compute en la nube (reducción de latencia). Principalmente, encontramos dos posibles soluciones: las interconexiones con cloud públicas a través de MPLS (Telefónica Wan2Cloud o Kyndryl GNPP, por ejemplo) y también la conexión a través de *puntos de presencia* (POP) de los hiperescalares, los cuales acercan sus nubes de cómputo a través de su red de POPs para tener una mayor capilaridad de forma que es posible una conexión al hiperescalar a través de algunos operadores locales y/o regionales.

▪ **Soluciones basadas en overlay virtual (SD-WAN/SASE):**

Se basan en crear una red overlay por encima de la conectividad física que interconecta los datacenters (también las sedes) del usuario con la nube pública (dependiendo del vendor, se puede soportar más de una nube pública).

Aquí se pueden encontrar soluciones de los propios hiperescalares (Azure Virtual WAN, AWS Cloud WAN...), también de vendors de infraestructura de red (Cisco, Aruba, Fortinet, Vmware...) junto con servicios de integradores y operadores para su despliegue y gestión.

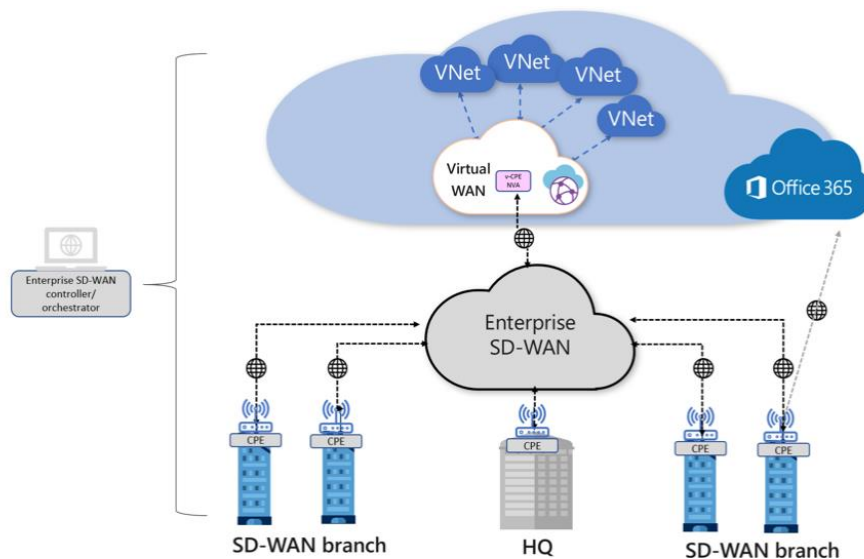


Ilustración 17 Ejemplo Azure Virtual WAN

A parte de establecer los túneles para la comunicación *overlay*, estas soluciones ofrecen un dashboard único para gestionar la comunicación extremo a extremo así como también el estado y configuración de diferentes servicios (SD-WAN, seguridad, políticas...). Cabe mantener presente el tipo de *underlay* que se consume por debajo y que no puede ser reconfigurado por este *overlay*.

Actualmente la diversidad de soluciones SD-WAN en este ámbito es muy amplia pero cada solución tiene funciones en dominios específicos ya que influye bastante el origen/experiencia y la evolución particular del vendor de la solución (si originariamente viene del entorno de networking, de

seguridad...). Por eso, también se pueden desplegar soluciones mixtas (por ejemplo, AWS Transit Gateway con soluciones SD-WAN de terceros).

- **Soluciones Edge:**

Se trata principalmente de soluciones de proveedores de nube pública que se instalan onprem en los datacenters del usuario. Son soluciones de racks o servidores físicos, permitiendo ejecutar los servicios del hiperescalar desde el datacenter privado local del usuario. Como ejemplos, podemos encontrar Azure Stack, AWS Outpost o Wavelength.

#### *Soluciones MCN o extensión Multicloud*

Este tipo de soluciones buscan resolver la complejidad de que una empresa se conecte contra varias nubes (más de una pública) sobre todo con el objetivo de facilitar el despliegue y consumo de aplicaciones con cargas distribuidas.

Si bien las soluciones que se comentan a continuación resuelven este tipo de escenario multicloud, también pueden emplearse para extensión a sólo una única nube pública.

- **Soluciones MCNS:**

Como se comentaba anteriormente, una de las tendencias que marca el desarrollo de soluciones de *hiperconectividad*, son justamente las soluciones MCNS (Multicloud Network Software). Estos productos pueden extender funcionalidades del plano de control, datos y gestión a través de cualquier nube mediante una única interfaz de gestión. Además, implementan políticas de seguridad, visibilidad y networking, por ejemplo, en algunos casos implementando sus propias funcionalidades de SD-WAN o integrándose con soluciones de SD-WAN de terceros para extenderse entre los datacenters.

Entre sus funciones, se encuentran:

- Intra-cloud networking con funcionalidades de automatización que mejoran la integración con el hiperescalar (*extensión single-cloud*)
- Cross-cloud networking que permite la creación de una arquitectura mallada y segura en un único entorno de gestión a través de diferentes hiperescalares
- App-to-app networking para conexión entre aplicaciones en todo el resto de capas (4-7). Éste es uno de sus valores diferenciales al preocuparse de la conectividad extremo a extremo desde la perspectiva de las aplicaciones para asegurar el performance.

Pioneros de estas soluciones han sido empresas “*born in the cloud*” como Aviatrix, Volterra (ahora parte de F5) o Proximo, pero también otros vendedores (networking tradicional, SDN...) están rápidamente desarrollando sus propias soluciones MCNS. En este punto se puede considerar si las soluciones SD-WAN también se pueden utilizar para entornos multinube y, así es.

Pero las funcionalidades y soportes de nubes como se comentaba en el anterior capítulo dependen del expertise del vendedor y suelen estar más fragmentadas. Las soluciones MCNS intentan abordar el extremo-extremo de la solución. Esto no significa bajo ningún concepto que las soluciones MCNS tengan que prevalecer sobre una solución SD-WAN. Como se puede observar, este tipo de soluciones tienen un perímetro de integración mucho más grande que puede no ser el caso de todos los usuarios.

Y es que esta aproximación extremo-extremo trata frontalmente la convergencia entre cloud, networking y seguridad, siendo una tendencia que puede significar la siguiente fase evolutiva en la transformación del cloud y la WAN para las redes empresariales. Aunque todavía estamos en una fase muy inicial y falta tiempo para ver cómo maduran este tipo de soluciones y si entregan el valor esperado de ellas.

Con todo, este tipo de productos no dejan de ser una solución de tipo *overlay*, no incluyen la capa física de conectividad hacia la nube (el *underlay*). Por eso, una de las características de este tipo de soluciones y que permite diferenciar las soluciones de diferentes vendedores, es su integración mediante APIs que les permite por un lado interactuar dinámicamente con los entornos de nube en la capa superior y de red física en la capa inferior.

Es por eso por lo que, si bien este tipo de productos se pueden obtener como soluciones DIY, varios proveedores están colaborando con vendedores de software MCNS para construir servicios MCN NaaS (como veremos en el siguiente capítulo) ofreciendo de forma complementaria sus capacidades *overlay/underlay* con los beneficios de estos productos/soluciones MCNS.

- **Servicios NaaS:**

Los servicios NaaS se proponen como un *fabric* intermedio que conecta los diferentes entornos (nubes públicas, datacenters, colocation, XaaS, sedes...) del usuario a través de un conjunto de POPs/accesos locales y que proporciona una interfaz de gestión centralizada. Este tipo de soluciones se pueden utilizar en entornos *multicloud* como *single-cloud*. En ese caso, también hay que tener en cuenta que, las soluciones de Azure Virtual WAN o AWS Cloud Connect se podrían considerar también NaaS, aunque sólo para *single-cloud* y además exclusivamente el de su propia nube pública.

Volviendo al entorno *multicloud*, podemos encontrar diferentes proveedores de servicios NaaS, aunque no todos ellos disponen de capacidades extremo a extremo para cubrir todas las funcionalidades descritas en la Ilustración 16 y en algunos casos las cubren mediante acuerdos con terceros o integraciones.

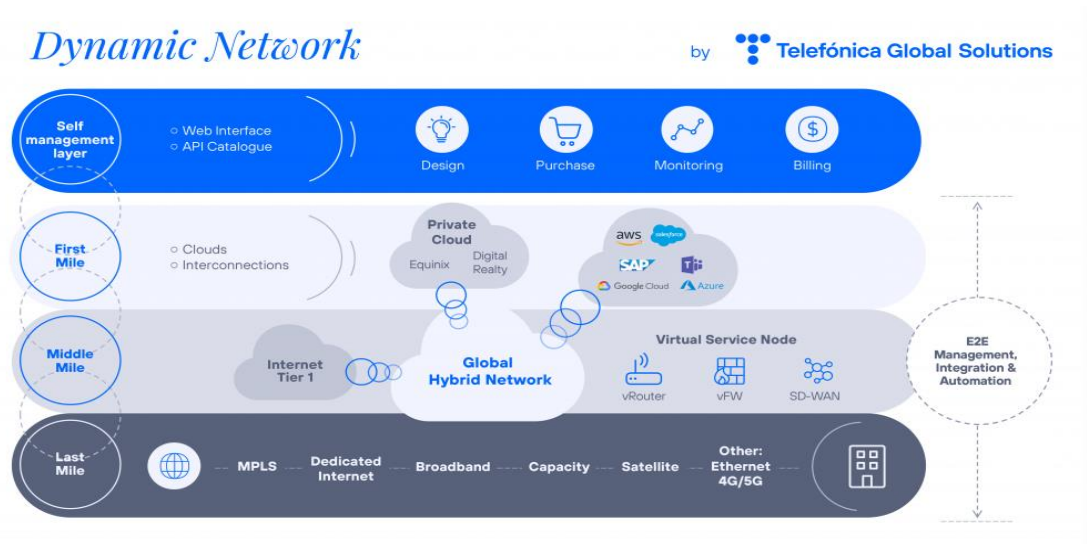


Ilustración 18 Ejemplo de arquitectura de un ejemplo de Servicio NaaS

Este tipo de soluciones se basan en cinco elementos principales:

1. El **fabric**, el cual se basa en un *overlay* SDN extendido a través de los diferentes entornos. Cada vendor puede utilizar tecnologías de tunelizado específicas.
2. La existencia de **múltiples POPs** distribuidos globalmente para aumentar el alcance, sobre todo conveniente para compañías internacionales con multitud de sedes o puntos de conexión. Otros proveedores en vez de disponer de POPs pueden ofrecer directamente **accesos de operadores locales** (MPLS/Internet) hasta la sede del usuario.
3. **Dotar de disponibilidad las interconexiones/peering con los hiperescalares** y proveedores SaaS más demandados, eliminando la necesidad del usuario de tener que desplegar una integración de este tipo que no sólo es costosa económicamente (ahorro de integraciones y del coste del tráfico directo vía Internet...) sino también en tiempo y seguridad (reducción del perímetro de ataque).

Cabe mencionar la **importancia de la apificación** que soporte el vendor para garantizar una actualización dinámica de capacidades dentro de la red y un provisionamiento rápido de servicios. En este punto, por su poder

revolucionario, es relevante mencionar la **iniciativa OpenGateway**, una iniciativa global del sector telco liderada por la GSMA que aspira a transformar las redes de comunicaciones en plataformas, exponiendo las capacidades de las telcos mediante APIs globales y estandarizadas y en la que están participando las tres principales telcos del país y más de 30 operadoras a nivel mundial, que suman cerca del 60% de las líneas móviles del mundo.

4. *Underlay*, compuesto tanto por su **red backbone de interconexión global** como también sus redes de acceso de interconexión local (como se mencionaba en el punto 2). En este punto es cuando el proveedor se diferencia disponiendo de su propia red local o bien con acuerdos con proveedores de internet terceros.
5. La **interfaz de gestión** que no sólo gestionará el *overlay*, sino otras funcionalidades de cloud y seguridad dependiendo de las integraciones del vendor, así como también elementos del ciclo de vida del servicio como facturación, soporte técnico, etc.

Principalmente en el mercado español encontramos soluciones de proveedores Cloud Exchange como Equinix, Kyndryl, Megaport, Intercloud o también de operadores como Telefónica, con su unidad Telefónica Global Solutions. También por ejemplo Google ofrece interconexión vía Internet a otras nubes públicas a través suyo con el servicio de Google Cross-Cloud Interconnect.

Por lo tanto, a la hora de considerar un proveedor en esta categoría, es necesario analizar el caso de uso y plantear la necesidad de:

- **Funcionalidad:** Catálogo de las funcionalidades y entornos de dominio (networking, seguridad, extensión al cloud) incluidas en su network fabric y en su plataforma de gestión hacia usuarios.

- **Capacidad:** Capilaridad, Velocidad e Interconexión que puede proporcionar una conectividad/routing hacia los centros del usuario a través de sus POPs o si lo hacen a través de acuerdos con partners terceros
- **Garantía:** Capacidad de poder ofrecer mejoras de performance, QoS y SLAs
- **Seguridad:** Mecanismos y funcionalidades que garantizan la integridad de la seguridad en sus interconexiones.

#### Hiperconectividad entre usuarios y aplicaciones

En este escenario se debe cubrir la capacidad de los usuarios para conectarse desde cualquier ubicación y desde cualquier dispositivo a las aplicaciones corporativas estén donde estén.

En cuanto al tema principal de este informe *Camino hacia la hiperconectividad de la nube*, el perímetro del escenario de nube híbrida principalmente aborda la extensión de un datacenter privado (donde residen aplicaciones) a una o varias nubes públicas (donde residen aplicaciones). Por eso, en el apartado “0 Entornos y tendencias” se mencionaba que el reto principal se encuentra principalmente en el tráfico aplicación-aplicación descrito en el capítulo anterior, sobre todo de cara a escenarios futuros con aplicaciones distribuidas en diferentes clouds y que se encuentren sincronizadas como si siguieran estando en el mismo servidor con una gestión transversal a los diferentes dominios (red, seguridad y cómputo).

No obstante, aunque no principal, también se incluye el escenario de acceso usuarios-aplicaciones para tener una visión completa. Por lo tanto, si comparamos con la conectividad aplicación-aplicación, observamos algunas diferencias:

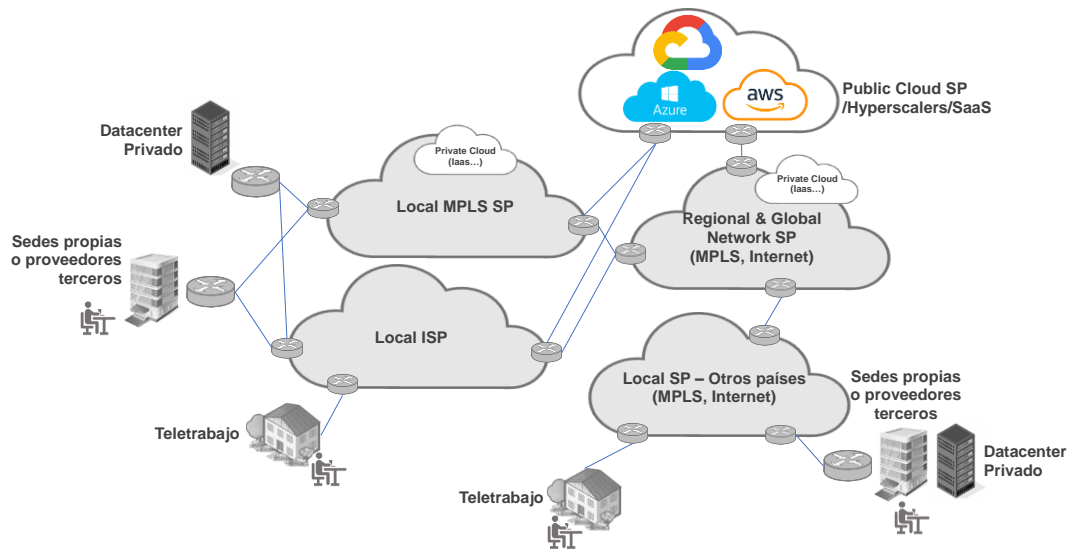


Ilustración 19 Tramos de Conectividad Underlay en la comunicación Usuarios – Aplicación

- **Ubicaciones:** Aumento de ubicaciones de conexión al contemplar tanto las sedes propias del usuario, como también el teletrabajo o incluso también el caso de proveedores externos.
- **Tipo de aplicaciones que consumen los usuarios:** Dependiendo del sector de la empresa, puede haber grandes variaciones. Hay una tendencia generalizada al consumo de aplicaciones tipo SaaS (autocontenidas en nubes públicas con alguna integración mínima (por ejemplo, para el Directorio Activo) y accesibles mediante Internet principalmente). Éste, sería el caso principal de las aplicaciones de ofimática, pero en sectores como la Industria, por ejemplo, existe un gran peso de aplicaciones corporativas alojadas en datacenters privados. En resumen, existe un perímetro mixto de aplicaciones fuera y dentro de la red física de la empresa a la que los usuarios necesitan acceder.
- **Requisitos diferentes:** A diferencia del escenario anterior, aquí los requisitos sobre todo se centran en habilitar una conectividad homogénea, agnóstica y segura, donde la identidad y el rol del usuario cobran especial importancia teniendo en cuenta la diversidad de usuarios que pueden acceder a las aplicaciones y el acceso al que están autorizados a las mismas.

Las soluciones SASE ayudan a abordar estos retos. De nuevo, este tipo de soluciones son, sintetizando mucho, tecnologías *overlay* que se basan en appliances HW en las sedes o agentes software en los dispositivos de los usuarios, pero, además, con funciones de seguridad enriquecidas. Para garantizar un funcionamiento acorde a las expectativas de servicio del usuario, es necesario contemplar el *underlay* (red física) que se vaya a utilizar y si cumple y garantiza los SLAs que requiere la compañía.

En concreto SASE consiste en un *framework* de funcionalidades avanzadas de red y de seguridad. En el caso de red, aparte de funcionalidades de optimización y aceleración WAN, la más reconocida es SD-WAN. Las funcionalidades de Seguridad se agrupan bajo el nombre SSE (*Secure Service Edge*) que representa un conjunto de funcionalidades que securizan el acceso de los usuarios a las aplicaciones basándose en identidad y política/acreditación agnósticamente a si aplicaciones y usuarios se encuentran dentro o fuera de la red física de la empresa.



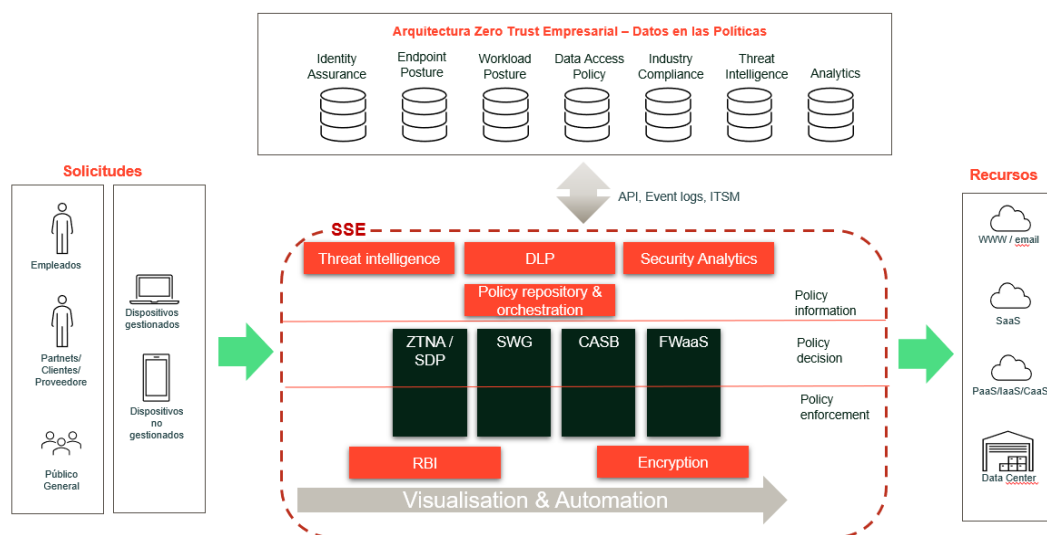
Ilustración 20 SASE framework (funcionalidades destacadas)

De las funcionalidades SSE, diseñadas principalmente pensando en los desafíos del acceso mediante Internet, las tres principales corresponden con (una lista más completa se puede ver en la Ilustración 21):

- **ZTNA (Zero Trust Network Access):** Permite la conexión segura de usuarios a aplicaciones en donde el acceso se concede en base a identidad y política, sin necesidad de estar conectado a la red corporativa. Las políticas son adaptativas al contexto usuario-dispositivo. Debido a estas ventajas, esta

solución está desplazando otras soluciones de usuario VPN para usuarios remotos principalmente.

- **CASB (Cloud Access Security Broker):** Es un agente que actúa como intermediario aplicando políticas de seguridad en el tráfico de los usuarios a las aplicaciones en la nube pública y garantizando el cumplimiento de las normativas corporativas en ambos extremos.
- **SWG (Secure Web Gateway):** Previene que el tráfico malicioso desde internet pueda infectar al usuario. Se diferencian de un firewall, en que funcionan a nivel de aplicación, por lo tanto, pudiendo securizar mejor al usuario de la gran variedad de posibles ataques que puedan proceder desde Internet.



kyndryl

Ilustración 21 Funcionalidades SSE según escenario

Dependiendo de las características del escenario, el uso de determinadas funcionalidades en la parte de networking o en la parte de seguridad tiene mayor relevancia. Por ejemplo:

- **Escenario 1:**

**Conectar de forma segura las oficinas del usuario a los CPDs y al Cloud:**

En este escenario, la funcionalidad SD-WAN es la que proporciona mayores ventajas ya que crea una red virtual por encima de las redes físicas que permite que sedes (normalmente con accesos mixtos MPLS e Internet) se puedan conectar virtualmente bajo la misma red al datacenter privado (MPLS normalmente) y/o a la nube pública (Internet/MPLS). Una alternativa a este escenario es utilizar conectividad privada MPLS e interconectar también a través de MPLS la nube pública y privada. En ese caso, una solución SD-WAN no sería necesaria.

- **Escenario 2:**

**Conectar de forma segura los usuarios remotos (corporativos y proveedores) a aplicaciones en Internet (Web/SaaS/Public Cloud):**

En este escenario, las funcionalidades SSE son las que entran en juego. El tráfico del usuario se redirige a la nube SASE del proveedor para análisis. ZTNA acredita la identidad y autorización del usuario, CASB analiza que el acceso a la aplicación sea seguro y SWG previene que el tráfico desde internet no infecte al usuario en el caso que sea malicioso.

- **Escenario 3:**

**Aplicar políticas Zero Trust a los usuarios (corporativos y proveedores) en el acceso a aplicaciones y recursos corporativos:**

En este caso estamos hablando de proteger principalmente aplicaciones que se encuentran en datacenters privados o tradicionales. SD-WAN permitirá que el usuario pueda conectarse como si estuviera en la red corporativa, y ZTNA proporcionará la garantía de que el usuario tiene rol y acreditación para acceder y actuar a ella.

La realidad es que estas situaciones se pueden dar de forma combinada en cada compañía. Dependiendo de la cantidad de sedes conectadas, el volumen de teletrabajadores y el uso de aplicaciones principalmente en SaaS, una mejor solución será aquella para interconectar las sedes bajo redes heterogéneas o bien

securizar al teletrabajador vía Internet. O soluciones combinables escogiendo lo mejor de ambos mundos.

En este ámbito existen multitud de posibilidades, soluciones HW/SW de vendors de red y seguridad las cuales pueden destacar en todas las funcionalidades SASE de forma homogénea o enfatizar sus ventajas en SD-WAN o SSE. Asimismo, también existen tanto operadores como integradores que ofrecen servicios de despliegue, mantenimiento y gestión a través de estas tecnologías.

Para concluir, podemos observar que una mejora de la conectividad usuario-aplicación en entornos de teletrabajo o sedes distribuidas con aplicaciones en nubes híbridas y SaaS, aporta los siguientes beneficios:

- Mejora de la experiencia de usuario y del trabajo Híbrido
- Control más granular del acceso de los usuarios y Gestión de Políticas de Seguridad comunes (independientemente de la ubicación)
- Reducción de la superficie de ataques y el riesgo de brechas de seguridad

#### Ejemplos prácticos

Como se ha podido observar en los anteriores apartados, las casuísticas de los usuarios en cuanto a conectividad hacia la nube híbrida pueden ser muy variadas, y existen diferentes soluciones tecnológicas para abordarlas.

A continuación, como ejemplos prácticos se plantean algunas casuísticas genéricas en diferentes tipologías de usuarios empresariales y posibles opciones de hiperconectividad para resolver los retos planteados. Es importante tener en cuenta que son ejemplos prácticos basados en experiencias reales, y que es recomendable escoger la solución que mejor se adecue a la casuística y requisitos concretos de cada empresa.

## CASO 1:

*Usuario del sector público que ha implementado un modelo de Cloud Híbrido. Este modelo combina diversos entornos tecnológicos, como aplicaciones legacy, infraestructura de virtualización, un Cloud Privado y un Cloud Público (preferente). El objetivo principal de esta implementación es consolidar varios Centros de Procesamiento de Datos (CPDs) y Salas Técnicas en dos ubicaciones principales: un CPD principal y un CPD secundario.*

*El usuario se enfrenta al desafío de definir estrategias de alta disponibilidad (HA) para sus aplicaciones en este entorno híbrido. Cada aplicación puede requerir un enfoque de alta disponibilidad específico, como configuraciones activo-pasivo, activo-activo o recuperación ante desastres (DR). Estas estrategias de HA son esenciales para garantizar que las aplicaciones críticas sigan funcionando de manera confiable incluso en caso de fallos o interrupciones.*

*Además, el usuario está aprovechando el Cloud Público para migrar la infraestructura como servicio (IaaS) de los diferentes CPDs satélites y salas técnicas en una primera fase. Posteriormente, planea migrar aplicaciones a la nube una vez que hayan sido modernizadas y estén preparadas para operar en un entorno de nube.*

Para garantizar una conectividad segura y confiable en este escenario, el usuario ha optado por conexiones directas redundantes con proveedores hiperescalares. Estas conexiones son privadas, lo que significa que no utilizan Internet público para la transmisión de datos.

Esta elección se basa en varias consideraciones importantes:

- **Control del enrutamiento:** El uso de conexiones privadas permite al usuario tener un mayor control sobre cómo se enrutan los datos entre su infraestructura y los proveedores de nube hiperescalares. Esto es fundamental para garantizar la eficiencia y la disponibilidad de los servicios.
- **Seguridad en tránsito:** Al utilizar conexiones privadas, el usuario puede mantener un alto nivel de seguridad durante la transferencia de datos. Los datos no viajan a través de redes públicas de Internet, lo que reduce significativamente el riesgo de exposición a amenazas de seguridad.
- **Rendimiento con SLAs:** Las conexiones privadas suelen ofrecer un rendimiento más consistente y predecible en comparación con las

conexiones a través de Internet público. Además, los proveedores de nube hiperescalares suelen respaldar estas conexiones con acuerdos de nivel de servicio (SLAs) que garantizan un cierto nivel de disponibilidad y rendimiento.

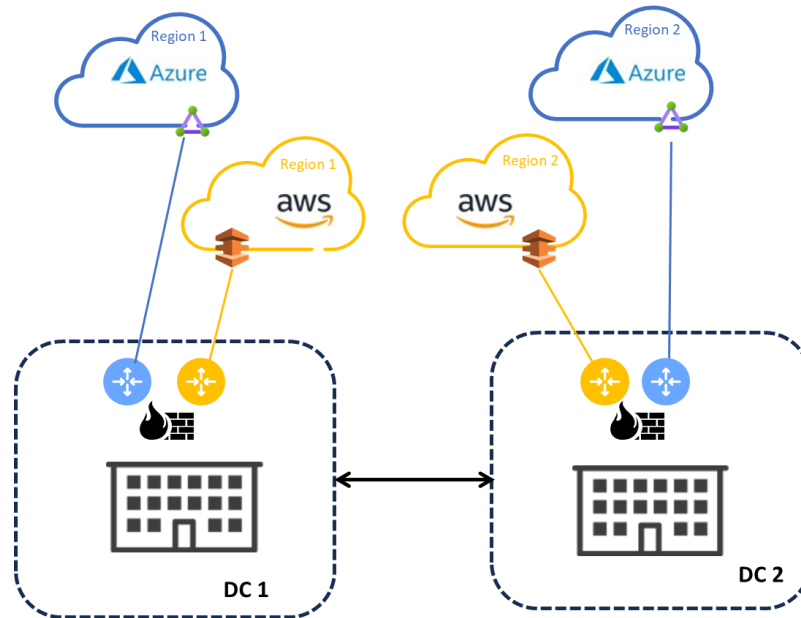


Ilustración 22 Arquitectura - Caso 1

En resumen, este caso representa un enfoque integral de migración hacia un modelo de nube híbrida en el sector público. El usuario aborda consideraciones críticas como la alta disponibilidad, la migración de aplicaciones y la conectividad segura para garantizar que su entorno de nube híbrida cumpla con los requisitos de rendimiento y seguridad necesarios para respaldar las operaciones críticas del sector público.

## CASO 2:

*Compañía del sector de venta en línea (Online Retail) cuyas aplicaciones de negocio están completamente desarrolladas nativamente en la nube. Lo que destaca en este escenario es que se trata de un entorno Multi-Cloud, lo que significa que se utilizan múltiples proveedores hiperescalares, cada uno proporcionando una parte importante de la solución global.*

*La arquitectura de esta compañía se distribuye entre varios proveedores hiperescalares. Un proveedor de hiperescalar se encarga de la infraestructura de la Aplicación Web, otro se encarga de los motores y analíticas, y un tercero gestiona las plataformas de bases de datos (BBDD). Esta estrategia Multi-Cloud*

tiene el propósito de aprovechar las fortalezas específicas de cada proveedor, lo que puede resultar en una solución más resiliente y de alto rendimiento.

Sin embargo, un desafío importante en este caso es garantizar que las aplicaciones puedan operar de manera efectiva en este entorno Multi-Cloud. Los requisitos de latencia y rendimiento son críticos, y las aplicaciones deben funcionar como si estuvieran todas alojadas en el mismo centro de datos, incluso cuando se ejecutan en infraestructuras de nube diferentes.

Para abordar este desafío, el usuario ha buscado una solución de adyacencia, que implica la co-ubicación de los proveedores hiperescalares en el mismo campus o ubicación física. Esto significa que los centros de datos de estos proveedores hiperescalares están geográficamente cercanos entre sí, lo que reduce la latencia en las comunicaciones entre ellos. Esto es fundamental para garantizar un rendimiento óptimo de las aplicaciones que requieren una interacción fluida entre los distintos servicios alojados en diferentes nubes.

Además, para conectar estos entornos de nube de manera efectiva y segura, el usuario ha contratado los servicios de un proveedor de Datacenter y Conectividad especializado. Este proveedor de Datacenter y Conectividad se encarga de crear enlaces de red dedicados y de alta velocidad entre los centros de datos de los hiperescalares, lo que permite una comunicación eficiente y de baja latencia. Esto ejemplifica el uso de soluciones tipo Puntos de Presencia (POPs) y Servicios de Acceso a la Red (NaaS) para habilitar la conectividad entre nubes que vimos en el capítulo “Hiperconectividad entre aplicaciones/infraestructuras”.

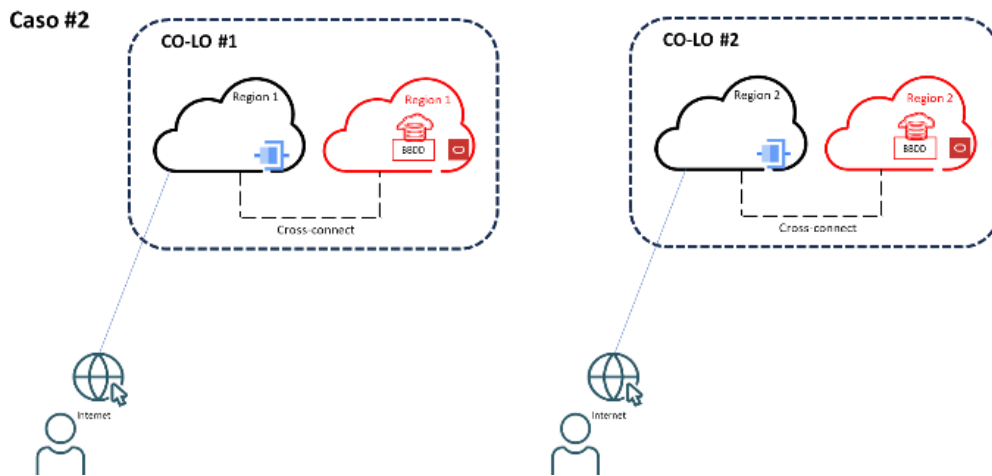


Ilustración 23 Arquitectura - Caso 2

### CASO 3:

*Multinacional con presencia en varias regiones que ha elegido utilizar un único proveedor de nube pública a nivel global para satisfacer sus necesidades tecnológicas. El enfoque (desde el punto de vista de arquitectura) de esta organización se centra en la creación de hubs regionales, o centros de datos regionales, que actúan como puntos estratégicos para sus usuarios internos en diferentes partes del mundo. Estos hubs regionales están conectados localmente a los PoPs (puntos de presencia) del proveedor de servicios de nube (CSP).*

La estrategia de conectividad del usuario se basa en aprovechar la solución de Cloud WAN nativa proporcionada por el CSP. Esta solución utiliza la infraestructura de red global del proveedor de nube y su propio backbone (columna vertebral de red) para conectar las distintas geografías con los centros de datos locales (On-premises) de la organización. Además, esta solución interconecta también las sedes de la empresa, lo que significa que las oficinas en diferentes ubicaciones regionales pueden comunicarse de manera eficiente a través de la red del CSP.

Un punto clave en este escenario es que el CSP proporciona todos los servicios y mecanismos de conectividad y seguridad necesarios a través de su catálogo de servicios. Esto incluye, entre otros, servicios de red privada virtual (VPN), enrutamiento, seguridad de red, balanceo de carga, gestión de identidad y acceso, y opciones de conectividad dedicada.

Esta estrategia tiene varias ventajas. En primer lugar, permite a la empresa multinacional utilizar una infraestructura de nube global para respaldar sus operaciones en todo el mundo, simplificando la administración y reduciendo la complejidad de la gestión de redes en diferentes regiones. Además, al aprovechar la solución de Cloud WAN nativa del CSP, el usuario se beneficia de la experiencia y la infraestructura global del proveedor de nube, lo que puede resultar en un rendimiento de red más eficiente y una mayor confiabilidad.

### Caso #3

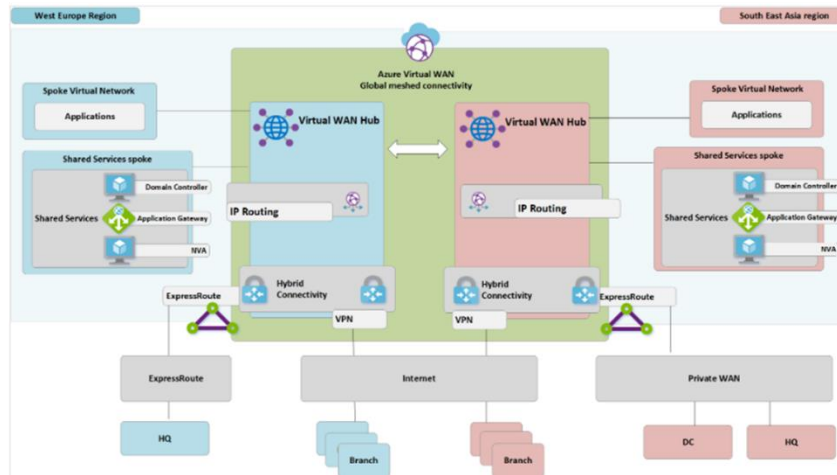


Ilustración 24 Arquitectura - Caso 3<sup>3</sup>

En resumen, este caso ejemplifica cómo una multinacional puede utilizar un único proveedor de nube pública a nivel global para establecer hubs regionales y habilitar una conectividad y comunicación eficiente entre sus usuarios internos y sus sedes en diferentes partes del mundo. La elección de la solución de Cloud WAN nativa del CSP proporciona una forma efectiva de gestionar la conectividad y la seguridad de la red en un entorno empresarial distribuido a nivel global.

<sup>3</sup> Ejemplo realizado con un CSP, cada empresa debe valorar el CSP que mejor se adecua a sus necesidades

#### CASO 4:

*Empresa multinacional con operaciones en varias regiones que ha elegido utilizar varios proveedores de nube pública a nivel global en lugar de depender de un único proveedor. Al igual que en casos anteriores, la arquitectura se enfoca en la creación de hubs regionales para satisfacer las necesidades de los usuarios internos. Estos hubs se conectan localmente a puntos de presencia (PoP) de proveedores de servicios de comunicaciones (SP de Comunicaciones).*

En este escenario, el usuario ha optado por apoyarse en la solución de conectividad Multi-Cloud proporcionada por un proveedor de servicios de telecomunicaciones (Telco). Esta solución utiliza el backbone internacional del proveedor de telecomunicaciones para conectar las diferentes geografías con los centros de datos locales (On-premises) de la organización y con los puntos de presencia de cada proveedor hiperescalar, según sea necesario.

El proveedor de servicios (SP) de comunicaciones en este caso proporciona la conectividad y los mecanismos de seguridad inherentes a una red de comunicaciones privada. Esto incluye la creación de redes privadas virtuales (VPN), gestión de enrutamiento, seguridad de red, calidad de servicio (QoS), y otras funcionalidades de red necesarias para garantizar la integridad y la confidencialidad de la comunicación de datos en una red global.

La elección de esta estrategia permite al usuario multinacional aprovechar la experiencia y la infraestructura global del proveedor de telecomunicaciones para gestionar su conectividad Multi-Cloud. Esto puede resultar en un rendimiento de red más eficiente y en una mayor seguridad de datos. Además, le da la flexibilidad de utilizar múltiples proveedores de nube pública para adaptarse a las necesidades específicas de cada región.

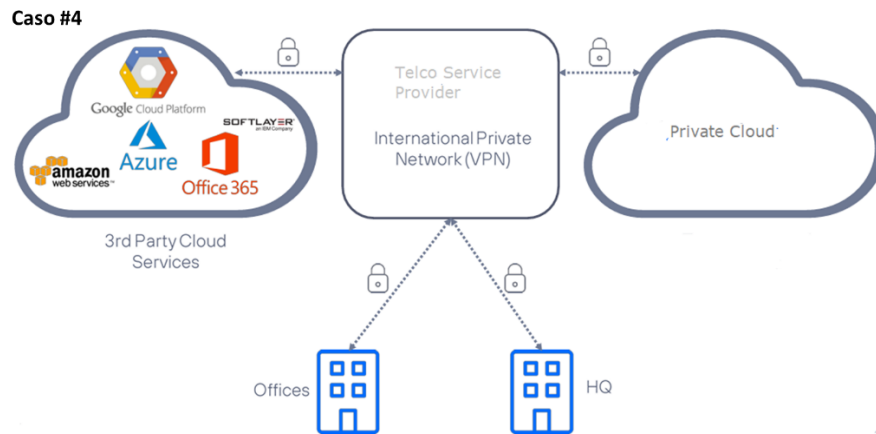


Ilustración 25 Caso 4

En resumen, el Caso 4 demuestra cómo una empresa multinacional puede utilizar varios proveedores de nube pública y confiar en un proveedor de servicios de comunicaciones para habilitar la conectividad y la seguridad de la red. Esto le permite gestionar hubs regionales y atender las necesidades de sus usuarios internos en una arquitectura Multi-Cloud, aprovechando la experiencia y la infraestructura de red de la Telco para lograr una comunicación eficiente y segura en una escala global.

### CASO 5:

*Compañía del sector industrial que busca mejorar el control de sus procesos de producción. Para lograr esto, ha decidido extender las soluciones de su proveedor de servicios en la nube (CSP) directamente a sus fábricas, lo que se conoce como Edge Computing.*

La idea principal detrás de esta estrategia es acercar el procesamiento y la aplicación de datos lo más cerca posible de la producción, lo que permite el cómputo en tiempo real en las instalaciones mismas.

En este contexto, el procesamiento en tiempo real se lleva a cabo "on-prem", es decir, en el lugar (en las fábricas). Esto significa que las fábricas están equipadas con la infraestructura de cómputo necesaria para realizar análisis y tomar decisiones en tiempo real a medida que los datos se generan en el entorno de producción. Esta capacidad es esencial para el control y la optimización de los procesos industriales.

Una característica importante de este escenario es que el procesamiento y análisis posteriores de los datos, así como las tareas analíticas más avanzadas, se realizan en la nube. Esto permite aprovechar el potencial de la nube para el almacenamiento de datos, la analítica avanzada y la generación de informes.

En este caso, el usuario no tiene los mismos requisitos estrictos de latencia que se mencionaron en casos anteriores. No necesita una solución de adyacencia para garantizar una baja latencia en la comunicación entre los entornos on-prem y la nube, como se vio en el Caso 2. En su lugar, el usuario ha utilizado las soluciones de Edge Computing proporcionadas por el CSP, así como los mecanismos de seguridad en la conectividad a Internet hacia la nube que éste ofrece.

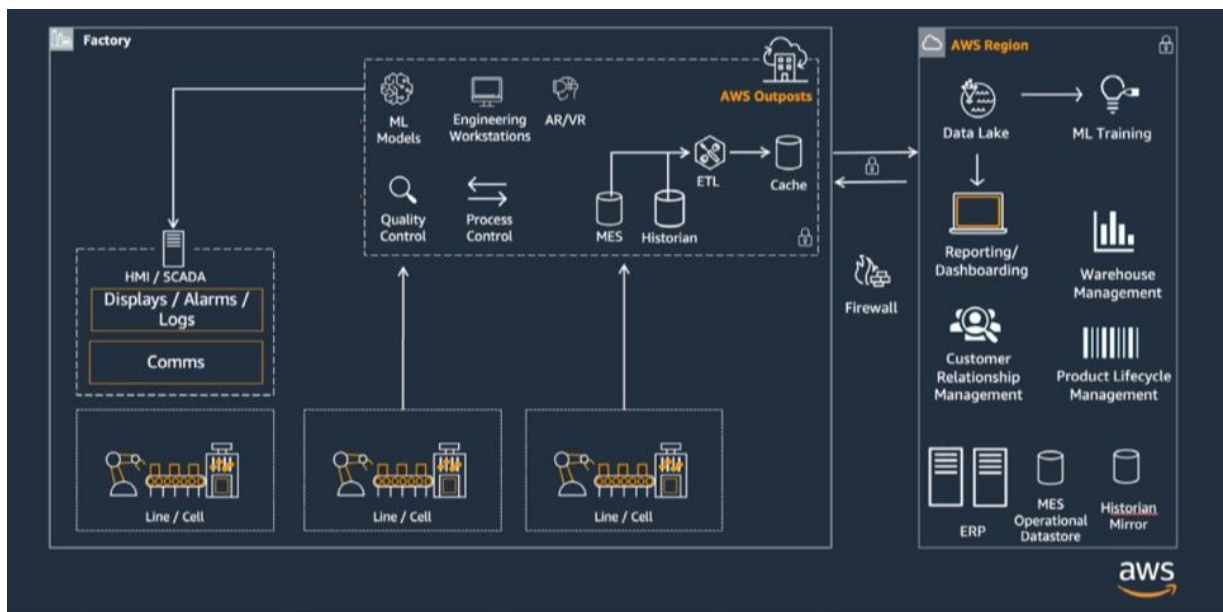


Ilustración 26 Arquitectura-Caso 5<sup>4</sup>

En resumen, este escenario ilustra cómo una empresa del sector industrial puede aprovechar las ventajas del Edge Computing para llevar a cabo procesos en tiempo real en sus instalaciones de producción. Al mismo tiempo, utiliza los recursos y la potencia de la nube para el procesamiento y análisis más avanzados. Esta estrategia permite una mayor eficiencia y control en la producción y se beneficia de

<sup>4</sup> Ejemplo realizado con un CSP, cada empresa debe valorar el CSP que mejor se adecua a sus necesidades

las soluciones proporcionadas por el CSP para garantizar la conectividad segura y eficiente entre los entornos de producción y la nube.

### CASO 6:

*Compañía que opera una gran cantidad de aplicaciones y frontales de usuarios, que se encuentran distribuidos en diferentes ubicaciones tanto en entornos On-Prem (en sus propios centros de datos locales) como en la nube (Cloud). La gestión y orquestación de estas aplicaciones y APIs se ha convertido en un desafío importante para la compañía, que busca asegurar una entrega uniforme y segura de estos recursos a través de una infraestructura denominada "App Delivery Network" (ADN).*

El enfoque principal en este escenario es desde el punto de vista de las aplicaciones y cómo se distribuyen a los usuarios finales.

Para resolver este desafío, el usuario ha optado por una solución proporcionada por un proveedor especializado que opera una App Delivery Network (ver capítulo "Soluciones MCN o extensión Multicloud"). Esta red actúa como un intermediario entre las aplicaciones y los usuarios, y su objetivo es garantizar la distribución eficiente, segura y controlada de las aplicaciones y APIs a través de múltiples ubicaciones y entornos.

El proveedor de la solución dispone de un backbone, una infraestructura centralizada y robusta de red, que integra tanto los entornos de nube pública como las ubicaciones On-Premises del usuario. A través de este backbone, el proveedor puede presentar, asegurar (securizar) y controlar el acceso de los usuarios a las aplicaciones. Esto implica que las aplicaciones se entregan de manera consistente y segura a los usuarios, independientemente de dónde se encuentren y de la ubicación de las aplicaciones.

**Caso #6**

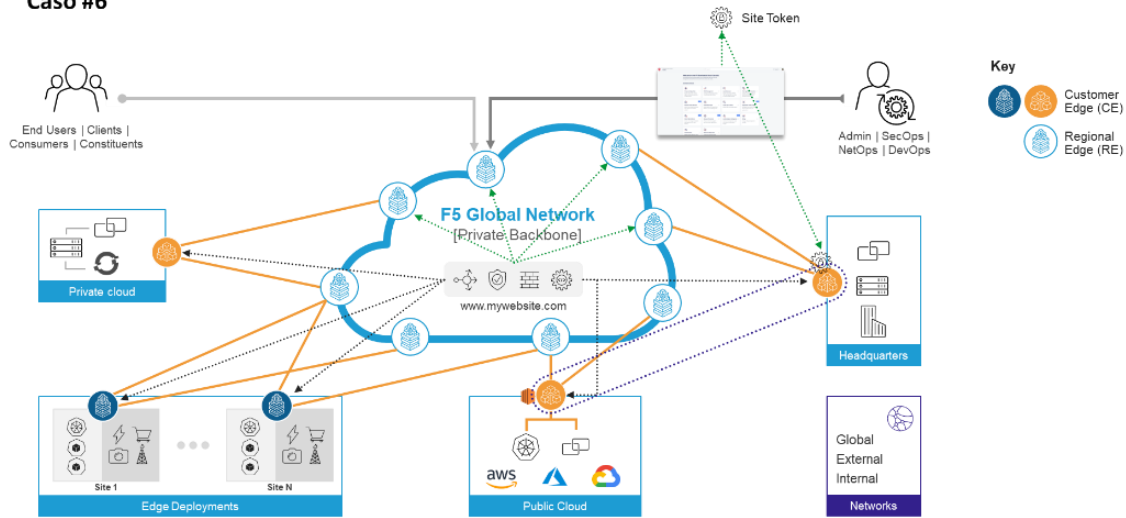


Ilustración 27 Arquitectura-Caso 6<sup>5</sup>

En resumen, este caso ilustra cómo un usuario con un entorno complejo y distribuido de aplicaciones ha adoptado una solución basada en una App Delivery Network para garantizar la distribución segura y eficiente de sus aplicaciones y APIs. Esta estrategia es fundamental para proporcionar una experiencia de usuario coherente y segura en un entorno de aplicaciones distribuidas a través de múltiples ubicaciones On-Prem y en la nube.

### 3.4. Seguridad, Gestión, Observabilidad y Talento

Hasta este punto, hemos estado abordando principalmente la conectividad en sus diferentes ámbitos para ser considerada como *Hiperconectividad*. Pero si recordamos los desafíos que hemos identificado en la Ilustración 13, existen otros elementos adyacentes de especial relevancia en entornos distribuidos y heterogéneos que también deben ser analizados en mayor detalle.

#### Seguridad

Tal y como hemos podido ver en los resultados de las encuestas realizadas, y como confirmación de lo que venimos observando en el mercado en lo que respecta a

---

<sup>5</sup> Ejemplo realizado con un proveedor, cada empresa debe valorar el proveedor que mejor se adecua a sus necesidades

volumetría, tipología de ataques y organizaciones objetivo de los atacantes, la seguridad es la segunda gran preocupación de las empresas encuestadas.

En el nuevo escenario de *hiperconectividad*, hay que tener en cuenta los siguientes aspectos en la gestión de la seguridad y los riesgos de una organización:

- Resulta cada vez más complicado aplicar el concepto de “seguridad perimetral” y de proteger y controlar el tráfico en puntos concretos sobre todo en aquellos escenarios con interconexión de aplicaciones, datos y usuarios desagregados e interconectados a en parte a través de Internet. En este aspecto, aquellas compañías que interconecten sus redes, datacenters privados y la nube pública a través de *underlays* privados como las redes MPLS, se encuentran en una posición más segura al tener un perímetro más controlado.
- Desaparecen o, al menos, se difuminan cada vez más, los conceptos de red privada/publica, red interna/externa, tráfico entrante vs saliente, etc...
- Aparece el concepto de [SASE](#) que propone una arquitectura basada en la nube que ofrece servicios de red y seguridad destinados a proteger a los usuarios, las aplicaciones y los datos
- Crece la necesidad de disponer de *Visibilidad y control* de los entornos IoT y OTs (*Operation Technology*) debido a su proliferación con diferentes casos de uso y al impacto de estos entornos en el negocio de las empresas (especialmente en el sector industrial).
  - Evitar el secuestro por parte de redes de Bots para desencadenar un ataque de DDoS (*Distributed Denial of Service*), o ser una víctima de estos ataques
  - Falta de visibilidad y gestión de dispositivos IoT/OT
  - Sistemas Operativos no actualizados de dispositivos OT, ni firmware actualizado

- Falta de estandarización y segmentación
- Las políticas y directivas de seguridad deben tener en cuenta 2 ámbitos:
  - Se aplican a “subjects” (normalmente usuarios), se evalúa el nivel (o “la postura”) de seguridad del dispositivo/equipo desde el que se establece la conexión y se debe de tener en cuenta el contexto desde el que se establece la conexión
  - Se aplica el concepto de *Zero Trust* o mínimo privilegio, es decir, permitir aquellas conexiones lícitas y denegar el resto por defecto
  - Aplicación del concepto *CARTA* (Continuous Adaptive Risk & Threat Assessment) que considera la implementación de arquitecturas de seguridad que se adaptan a su entorno con el fin de conocer comportamientos y eventos que permitan anticiparse a las amenazas.
- Conceptos nativos de seguridad Cloud (VPCs, subredes microsegmentación, microservicios...) deben de ser conocidos y aplicados para poder aplicar un modelo de seguridad completo y multicapa

Dado que la tecnología 5G es y va a ser uno de los principales habilitadores de la *hiperconectividad* y de la explotación de las tecnologías exponenciales, el marco regulatorio aplicable está evolucionando en esta dirección. Prueba de ello ha sido la aprobación y la introducción de la Ley de Ciberseguridad 5G y que incorpora al marco legal español las medidas estratégicas y técnicas de la caja de herramientas (tool box) consensuada entre los Estados Miembros de la Unión Europea.

#### Gestión y Monitorización

Llevar cargas a la nube no elimina la necesidad de una monitorización y gestión continua. Al contrario, el despliegue de aplicaciones de forma distribuida ya sea en entornos de nube híbrida o de nube pública aumenta esta necesidad justamente para controlar el estado de las aplicaciones cuando por debajo existe un conjunto de entornos heterogéneo.

Entrando ya en detalle a los ámbitos de gestión, monitorización y observabilidad (y Visibilidad), cabe destacar que el cambio más relevante que se ha producido recientemente es la aparición de las redes definidas por software (SDN). SDN centraliza la gestión abstrayendo el plano de control de la función de reenvío de datos en los dispositivos de red discretos.

¿Cuáles son las principales ventajas que introducen la gestión y monitorización de red de forma centralizada?

1. Permite la creación de redes programables que descubran y configuren automáticamente redes conectadas e infraestructura (switches...)
2. Mejora la analítica y la monitorización del tráfico de red mediante técnicas de Machine Learning o analítica predictiva que permite lograr una fase de troubleshooting o gestión de incidencias más ágil y dar visibilidad de lo que está sucediendo en la red
3. Permite la interrelación y la automatización en la aplicación de políticas entre distintos entornos (Redes locales, redes WAN, Cloud...)

La visibilidad y la observabilidad de la red se han desarrollado a partir de la necesidad de identificar de forma rápida y precisa la fuente de los problemas, incluso si están fuera de la pila tecnológica normal. La observabilidad ha ganado popularidad porque el mayor uso de la nube y las aplicaciones SaaS ha expuesto los límites de la monitorización de red tradicional. Adicionalmente, esta monitorización enfatiza las señales visibles externamente, mientras que la observabilidad se basa en representaciones detalladas del estado interno de un sistema.

Las herramientas de monitorización tradicionales son en su mayoría reactivas y se centran en la salud y el rendimiento de los elementos de red individuales. Además, las propias herramientas de red están aisladas por sus mecanismos de captura de datos. Las herramientas de monitoreo de infraestructura de TI (ITIM) y monitoreo y diagnóstico del rendimiento de la red (NPMD) están evolucionando hacia un

enfoque más centrado en el servicio y en toda la red, y algunos usuarios están comenzando a usar las herramientas de manera más proactiva.

El monitoreo de la red en la era digital y en la nube, necesita correlacionar la información de los elementos individuales no solo de la red en su conjunto, sino también de las aplicaciones que dependen de ella. La agilidad que exigen los negocios digitales, la nube y la infraestructura dinámica requiere un menor tiempo medio de reparación (MTTR) y detección (MTTD).

De hecho, según Gartner, Para 2027, el 80% de las organizaciones habrán visto una reducción en la red tradicional. Se reducen las necesidades de herramientas de monitorización debido al trabajo remoto, la migración a la nube y la visibilidad mejorada de la red a través de herramientas de observabilidad y análisis, en comparación con 2023.

De esta forma, las soluciones de observabilidad son parte del impulso por una visión más unificada de las redes de nube híbrida y solo de nube. Las capacidades automatizadas para las soluciones de observabilidad también son atractivas para los equipos de TI que intentan hacer más con menos a medida que su entorno se vuelve más complejo. La observabilidad exitosa de la red puede proporcionar un valor significativo a la organización en forma de tiempo medio de resolución reducido, empleados más productivos, usuarios más satisfechos y más tiempo para que el equipo de TI lo dedique a otros proyectos.

La importancia del Talento, el papel de la automatización

Habida cuenta de la diversidad y extensión de las diferentes soluciones, podemos llegar a la conclusión que la adopción no sólo de nubes públicas, sino de entornos híbridos público-privados a nivel de cómputo y de red que además cuenten con una seguridad garantizada extremo a extremo, requiere de conocimiento de las diferentes soluciones, arquitecturas y protocolos.

Y éste es otro de los grandes retos y acorde a los resultados de los encuestados, donde se ha identificado falta de talento con un nivel de conocimiento adecuado en cuanto a seguridad, cloud y networking en este orden.

Construir y sobre todo mantener equipos de soporte que agrupen este conocimiento especializado y lo que no es conocimiento (expertise, certificaciones oficiales y de fabricantes...) es difícil y costoso para las empresas, pero necesario para maximizar el retorno de las inversiones realizadas en los diferentes entornos de cloud, red y seguridad.

Las estrategias aquí también pueden variar dependiendo de la dirección que quiera tomar la empresa. Una opción consiste en invertir en programas de formación/certificación que identifiquen y proporcionen la formación adecuada para que los departamentos de TI puedan operar este tipo de entornos. Otra opción que considerar es justamente la capacidad que pueden ofrecer integradores/operadores mediante sus Centros de Excelencia para gestionar y operar los entornos multicloud, teniendo en cuenta que realizan considerables inversiones en este ámbito tanto a nivel de personas, certificaciones y formación para ofrecer diferentes servicios al respecto (consultoría, despliegue, monitorización y gestión).

Finalmente, aunque todavía es un momento inicial, la automatización de la mano por ejemplo de tecnologías como GenAI (*Inteligencia Artificial Generativa*) también jugará un papel relevante en este ámbito. A medida que los entornos son más heterogéneos, las configuraciones manuales no pueden aumentar, sino que deben disminuir. En este aspecto, soluciones que incluyan workflows automatizados para absorber estas configuraciones repetitivas y que descarguen al departamento de soporte, que permitan analíticas preventivas para mejorar la respuesta ante incidencias o consuman de forma automatizada APIs de integración entre plataformas abrirán el camino a una evolución más dentro de estos entornos híbridos.

### 3.5. Conclusiones y Recomendaciones

A lo largo de este informe hemos ido desgranando las diferentes piezas que conforman los escenarios de conectividad hacia la nube híbrida y también multicloud.

Primero hemos analizado los tres entornos diferentes de nube que, a grandes rasgos, podemos encontrar y, lo que es más importante, podemos ver que partimos de diferentes entornos de computación, con sus particularidades.

Como hemos podido ver en la encuesta realizada, las diferentes empresas utilizan diferentes soluciones de computación (nube pública, datacenters privados o tradicionales...). Los escenarios de nube híbrida son una realidad, aunque existen una gran variedad de escenarios y esto va a ser así en la medida que las empresas trasladen sus cargas a la nube pública y tengan que mantener datos sensibles en un perímetro privado.

En cuanto a las preocupaciones y/o necesidades que las empresas tienen, en primer lugar, existe una preocupación por la seguridad, regulación y privacidad de estos entornos. A nivel de conectividad, la principal preocupación es la gestión/orquestación de la conectividad en entornos heterogéneos para conseguir visibilidad extremo a extremo y garantizar el acceso seguro (identidad del usuario o aplicación que accede) a los datos y las aplicaciones.

Actualmente, existen numerosas soluciones de conectividad que se pueden plantear como hemos detallado en este informe. Dada la evolución que ha habido respecto a soluciones más tradicionales, podemos hablar de cierta *hiperconectividad hacia la nube híbrida y multicloud*, aunque el avance tecnológico persiste y, las redes están evolucionando según las demandas de los usuarios y nuevas soluciones tecnológicas están surgiendo para hacer frente a los retos que se plantean.

Hemos analizado en este informe una gran variedad de soluciones, tanto tradicionales como modernas, éstas últimas enfocadas sobre todo a la gestión,

orquestración, visibilidad y conectividad "*click to deploy*" alineada con el consumo que se puede hacer de la nube pública.

En los casos prácticos vemos cómo se pueden utilizar este tipo de soluciones en ejemplos de escenarios que se pueden dar en las empresas. Hemos plasmado la realidad de que las empresas pueden tener entornos muy diferentes (no existe un único escenario de nube híbrida) y que, para adaptarse a los requisitos de estos entornos, las posibles soluciones a nivel de conectividad pueden ser diferentes.

Es importante resaltar este último punto. Las opciones de conectividad no tienen que ser un mismo modelo o una única solución para todas las empresas. Por este motivo, se ha considerado importante detallar las diferentes soluciones y sus características, de forma que las empresas puedan tomar decisiones más informadas.

Se recomienda que las empresas conozcan y sean conscientes de las diferentes soluciones de conectividad tanto físicas como virtuales que existen y para qué entornos están mejor dirigidas para poder analizar qué solución se adapta más a su escenario concreto: si su solución actual ya cumple con sus necesidades, si quieren aumentar su solución existente de conectividad o bien hacer una migración más ambiciosa. Además de mantener presente de qué forma la solución escogida garantiza la seguridad tanto a nivel físico como de configuración o red virtual, y cómo garantiza la seguridad de los datos en tránsito y en reposo.

Finalmente, terminar enfatizando la importancia de la conectividad. El éxito de una organización no sólo depende de tener una infraestructura de cómputo adecuada, sino también de una red preparada y fuerte para acceder a ella.

## 4. Agradecimientos

Queremos manifestar nuestro agradecimiento a las entidades representadas en el Grupo de trabajo de Telecomunicaciones de AUTELSI; y a sus vocales, que han contribuido activamente al desarrollo y resultado positivo de esta iniciativa. En especial queremos destacar la colaboración de los siguientes integrantes:

Presidente:

**Carlos Varela Ávila**, licenciado en Ciencias Físicas por la Universidad Complutense de Madrid. Desde 2014 es el Director de Transformación Digital y Tecnología en la Dirección General de Estrategia y Desarrollo de Renfe Operadora. Anteriormente ha desempeñado distintos cargos en la organización TI de Renfe donde ha trabajado desde 1989, Entre otros: director de producción, Director de Ingeniería de sistemas y comunicaciones, Jefe de Técnica de sistemas y Jefe de Administración de bases de datos. También en el sector de los sistemas de información ha trabajado en Serbal informática Avanzada, Computing Technology Consulting (CTC) y Rank Xerox España.

Vocales:

**Juan Luis Blasco Salvador**, licenciado en Matemáticas con más de 25 años de experiencia en gestión de infraestructuras IT, gran parte de su carrera la realizó en el sector de telecomunicaciones (Orange), antes de unirse a Acciona en 2016, donde actualmente es el director de operaciones TIC.

**Jorge Carrasquilla Soares**, ingeniero de Telecomunicaciones con más de 20 años de experiencia en el sector de las Comunicaciones en Operadores y Proveedores de servicios. Apasionado de la tecnología y del impacto positivo que genera en los clientes. Actualmente trabaja como Associate Partner – Network & Edge de KYNDRYL.

**Jesus Coslado Santibañez**, graduado en Ingeniería del sector Agropecuario con mención especial Cum Laude en trabajo fin de grado y Máster de profesorado de secundaria en la especialidad de Tecnología. Carrera profesional desarrollada en el sector de la Tecnología y la Digitalización con 25 años de vida laboral. La carrera profesional comprende la dirección de proyectos tecnológicos en el ámbito de la empresa privada, liderando proyectos singulares en multinacionales del sector tecnológico, la formación en el ámbito privado y las responsabilidades como Concejal de Nuevas Tecnologías en el Ayuntamiento de Badajoz, siendo responsable también de las delegaciones de Transporte y Eficiencia energética entre otras. Cuenta además con la publicación de un manual tecnológico de difusión nacional.

**Carlos Gimeno Valverde**, licenciado en Administración y Dirección de Empresas bilingüe y con más de 11 años de experiencia en el Sector TIC. Comenzó su carrera en BT (British Telecom) hace algo más de 11 años como parte de Graduate Program, participando en proyectos nacionales e internacionales. Posteriormente, enfocó su carrera en ciberseguridad desde distintos roles de negocio (Product manager, ing. Preventa...). En su última etapa, ya en Evolutio, gestiona los Equipos de portfolio de Conectividad Telco-edge y telefonía y ciberseguridad, y con especial foco en el desarrollo de servicios de conectividad segura apoyándonos en Arquitecturas SASE.

**David González García**, profesional de Comunicaciones en Kutxabank, donde trabaja actualmente, desde 2022. Aquí desempeña labores de Diseño, Análisis y Gestión de Proyectos ligados con el ámbito tecnológico y, en especial, con Networking. Es precisamente en este campo donde intenta completar de forma continua su formación, con certificaciones, como el CCNP Enterprise, Microsoft Azure Fundamentals u otros anteriores, como el NSE7 o el Pulse Connect Secure. Máster en Ingeniería de Telecomunicación en la UC3M. Como paso previo en su experiencia laboral, durante 3 años y medio formó parte de SATEC donde realizó, en 2019, labores de Técnico de Networking y Ciberseguridad durante un año y, después, tareas de Preventa y Project Management durante más de 2 años, hasta

2022. Antes, en 2018, se inició en el trabajo en el área de Redes y Gestión de Proyectos en Euskaltel, a lo largo de un año.

**David Gutierrez Serrano**, director de ventas para España de IBM Public Cloud desde Abril de 2023. Licenciado en Ciencias Económicas Rama General en la especialidad Análisis Económico y Economía Cuantitativa por el Universidad Complutense de Madrid. MBA a través de la Henley School of Economics. Profesional con más de 25 años de experiencia en el área de IT, con diferentes roles en la venta de HW, SW y Servicios de Infraestructura y consultoría, tanto en IBM como en Viewnext.

**Gabriela Hurtado de Mendoza**, trabajó en IBM desde 1986 hasta 2021, en puestos varios, desde preventa de SW, vendedora de HW y desde 2010 como account manager de clientes de sectores como industria, banca, distribución y transportes. En 2021 entró en Seidor y desde entonces ocupa puesto de account manager, principalmente de empresas del sector del transporte, así como otros clientes públicos y privados.

**José Luis Iglesias Martínez**, jefe de Área de Comunicaciones en Adif. Ingeniero de telecomunicación por la UPM, y máster de Dirección Estratégica Internacional (UPM) y de Sistemas de Información Aplicados a la Empresa (UPM). Anteriormente ha desarrollado su carrera profesional en diferentes ámbitos de las telecomunicaciones, cómo son la consultoría de negocio y tecnológica, planificación e ingeniería de red, diseño y despliegue de sistemas OSS/BSS, etc. en Red Eléctrica de Telecomunicaciones, Nortel Networks y Telefónica. Profesor Asociado en la UCIIIM

**Alejandro Lisón**, ingeniero Técnico Telecomunicación por la Universidad de Alcalá de Henares Master Universitario MBA especialidad Marketing por la UNED. Cisco Certified CCIE/CCSP/CCNP Data Center/CCNP Enterprise/CyberOPs Associate. Network & Security Business Development Officer in Seidor.

**Sara Martínez García**, ingeniera de Telecomunicaciones con más de 13 años de experiencia en el sector TI. Desde hace 9 años trabaja en Telefónica donde ha

desarrollado su carrera profesional en diferentes roles siempre alrededor del mundo de la Conectividad empresarial (en sus diferentes entornos WAN, LAN, Campus, CPD, SDN...). Actualmente es Product Manager de Networking APIs en Telefónica OpenGateway, donde queremos evolucionar la Conectividad al siguiente nivel.

**Cristina Navarro Pitarch**, licenciada en Informática. Master en Dirección de Sistemas y Tecnologías de la Información y las Comunicaciones. Jefa de Servicio de Comunicaciones Corporativas en la Dirección General de Tecnologías de la Información y las Comunicaciones de la Generalitat Valenciana desde 2013. Empleada pública desde 1989 y ocupando diferentes cargos a lo largo de los años, en los últimos 25 con responsabilidades de jefatura de servicio o subdirección. En el puesto actual, responsable de la contratación y provisión de servicios de telecomunicaciones para todo el ámbito de la Generalitat.

**Antonio Rodríguez Perales**, tiene más de 25 años de experiencias en el sector, con un sólido conocimiento tecnología y amplia experiencia nacional. Actualmente es VP Desarrollo Negocio en Kyndryl. Anteriormente fue Managing Partner Global para empresas como BBVA y Telefónica o lideró el negocio de Cloud en IBM.

**Miguel Sánchez del Águila**, ingeniero de Telecomunicaciones especializado en Telemática. Durante su etapa profesional en Telefónica ha ejercido diferentes posiciones como: Ingeniero de soluciones para grandes empresas y Administración Pública, desarrollador del ecosistema de emprendimiento e innovación entre startups, responsable de generación de demanda de tecnologías TI, hasta llegar a su rol actual de responsable de desarrollo de negocio de tecnologías Cloud.

**Leonor Torres Moreno**, presidenta de ASTIC. Es licenciada en Informática por la UPM, Máster en Dirección de Sistemas TIC por INAP y UPM. Pertenece al Cuerpo Superior de Sistemas y Tecnologías de la Administración de la Seguridad Social. Comenzó trabajando en la AGE (Administración General del Estado) en diversos departamentos como Sanidad, IGAE, Administraciones Públicas y

Educación. Más tarde pasó a trabajar en la Administración local en el Ayuntamiento de Madrid y el Ayuntamiento de Alcobendas.

**Gregorio Villarrubia Martínez**, ingeniero Superior en Informática con 15 años de experiencia en seguridad y telecomunicaciones. Su trayectoria incluye roles como consultor de red y seguridad, Ingeniero y Arquitecto de soluciones para grandes redes, liderando proyectos en Telecomunicaciones y Seguridad informática. La colaboración en equipo, habilidades analíticas y capacidad para afrontar desafíos complejos ha sido fundamental para el éxito en proyectos estratégicos en sectores exigentes como aseguradoras, banca, infraestructuras críticas y telecomunicaciones. Actualmente, desempeña el rol de Jefe de Ingeniería de Seguridad en Renfe Operadora.

**También nos gustaría agradecer a ADIF por la cesión de su Aula Magna del Centro Formación, para la celebración del seminario en el que se presentó este informe el 25 de junio del 2024 y a las entidades patrocinadoras (Huawei, Kyndryl y Telefónica) y colaboradoras (Adif, Astic y Kutxabank) que hicieron posible la organización de dicho seminario.**