República Bolivariana de Venezuela

Ministerio del Poder Popular para la Educación Superior

Universidad Nacional Experimental de la Gran Caracas "UNEXCA"

Trayecto III, semestre II

Unidad Curricular: Electiva III

TEI Taller 4 La Nube (Cloud Computing)

Docente: Vladimir Peña

Estudiante: Ronaldo Rivero

C.I: 31169960

Caracas Enero del 2026

Introducción

El Cloud Computing o computación en la nube representa el eje central de la transformación digital contemporánea. Según estudios de consultoras como Forrester, la nube ha superado su primera década de consolidación para convertirse en la plataforma definitiva donde reside el "core" de los negocios modernos. A diferencia del modelo tradicional de computación local, la nube ofrece un acceso ubicuo y bajo demanda a un conjunto compartido de recursos configurables. Este cambio de paradigma permite a las organizaciones incrementar su productividad, facilitar la movilidad de sus equipos y relacionarse de forma más eficiente con sus clientes, aprovechando las ventajas de seguridad, eficiencia y escalabilidad que solo un entorno virtualizado masivo puede ofrecer.

La adopción de esta tecnología es el motor de la Cuarta Revolución Industrial, permitiendo que la infraestructura tecnológica deje de ser una barrera de entrada para convertirse en un servicio flexible. En este documento, se desglosan los conceptos fundamentales basándose tanto en los estándares del NIST como en las tendencias actuales del mercado, analizando los modelos de servicio, despliegue y los aspectos críticos de seguridad y gobernanza. A través de estos veinte puntos, exploramos cómo la nube ha evolucionado desde sus orígenes hasta convertirse en la infraestructura crítica que sostiene la economía digital global.

1) ¿Qué es la Cloud Computing (La Nube)?

El Cloud Computing es un modelo tecnológico que permite el acceso bajo demanda a través de la red a un catálogo de recursos de computación altamente escalables. En esencia, es la entrega de servicios informáticos —incluyendo servidores, almacenamiento, bases de datos y software— a través de Internet con un modelo de pago por uso. Esta modalidad traslada la carga de la gestión técnica y el mantenimiento del hardware desde la empresa hacia proveedores especializados. Históricamente, este concepto comenzó a tomar fuerza entre 2006 y 2007 con el lanzamiento de Amazon Web Services (AWS), marcando el inicio de una era donde la capacidad de cómputo se consume de la misma forma que un suministro público.

Operativamente, la nube se define por su capacidad de abstracción: el usuario no necesita conocer la ubicación física exacta ni la configuración del hardware que sostiene sus aplicaciones. Esto permite una agilidad empresarial sin precedentes, ya que los recursos pueden ser aprovisionados o liberados de forma instantánea según la demanda. Este enfoque transforma el modelo de inversión de las compañías, pasando de gastos de capital fijos (CapEx) a gastos operativos variables (OpEx), lo que democratiza el acceso a tecnología de punta para startups y grandes corporaciones por igual, fomentando un ecosistema de innovación constante.

2) De por lo menos tres definiciones de la nube.

La primera definición fundamental proviene del **NIST (National Institute of Standards and Technology)**, que la describe como un modelo para habilitar el acceso a red ubicuo, conveniente y bajo demanda a un fondo compartido de recursos de computación configurables (redes, servidores, almacenamiento, aplicaciones y servicios). Estos recursos se pueden aprovisionar rápidamente con un esfuerzo de gestión mínimo o interacción mínima con el proveedor. Esta definición es el estándar técnico global, ya que establece los criterios específicos que debe cumplir cualquier servicio para ser considerado verdaderamente "Cloud".

Una segunda definición se enfoca en la **visión de negocio y utilidad**, describiendo la nube como una plataforma donde los recursos informáticos se entregan como un servicio medido. En este contexto, la computación se convierte en una "utility" similar a la electricidad, donde la complejidad de la infraestructura queda oculta tras una interfaz de servicio. Finalmente, una tercera definición proveniente de la **industria tecnológica (como Forrester o Gartner)** la define como la base de la transformación digital, un ecosistema de servicios interconectados que permite a las empresas externalizar su infraestructura para ganar en movilidad, seguridad y capacidad de respuesta ante un mercado global altamente volátil.

3) ¿Cuáles son las características fundamentales del cloud computing según el NIST y explique cada una de ellas?

El NIST identifica cinco características esenciales. La primera es el **Autoservicio bajo demanda**, donde el consumidor puede proveerse de capacidades de computación (tiempo de servidor, almacenamiento) de forma automática. La segunda es el **Acceso amplio a la red**, asegurando que los servicios estén disponibles a través de mecanismos estándar que promuevan el uso por parte de plataformas heterogéneas (móviles, laptops, tablets). La tercera es la **Agrupación de recursos (Resource Pooling)**, que utiliza un modelo de multiarrendamiento para servir a múltiples consumidores utilizando recursos físicos y virtuales asignados dinámicamente según la demanda.

La cuarta característica es la **Rápida elasticidad**, que permite que las capacidades de cómputo crezcan o disminuyan de manera inmediata, dando al usuario la percepción de que los recursos son infinitos. Por último, el **Servicio medido** garantiza que el uso de los sistemas se controle y reporte de forma transparente para ambas partes. Esto permite un modelo de facturación basado en el consumo real, optimizando el uso de los recursos y permitiendo a las organizaciones pagar únicamente por lo que utilizan, eliminando el desperdicio de capacidad ociosa en los centros de datos.

4) ¿Qué otras características añaden ventajas adicionales a la nube?

Además de las características del NIST, la nube ofrece **economías de escala masivas**, ya que los proveedores compran hardware y energía en volúmenes gigantescos, trasladando esos ahorros a los clientes. Esto permite a las empresas acceder a infraestructuras de seguridad y redundancia que serían prohibitivas de implementar de forma privada. Otra ventaja crucial es la **ubicuidad y movilidad**, facilitando que los empleados accedan a sus herramientas de trabajo desde

cualquier lugar del mundo, lo cual es vital para las estrategias actuales de teletrabajo y equipos distribuidos.

La **actualización tecnológica continua** es otra característica distintiva; el proveedor es responsable de mantener el hardware y el software actualizados, asegurando que el cliente siempre trabaje sobre las versiones más recientes y seguras. Asimismo, la nube potencia la **experimentación ágil**, permitiendo a los departamentos de innovación lanzar prototipos y probar nuevas ideas en cuestión de horas sin inversiones iniciales. Finalmente, la **resiliencia y recuperación ante desastres** se ven fortalecidas, ya que la naturaleza distribuida de la nube permite replicar datos en múltiples geografías, garantizando la continuidad del negocio ante fallos físicos localizados.

5) Mencione y Explique los modelos de la nube.

Los modelos de la nube se dividen principalmente según la arquitectura de control y acceso. Un modelo emergente es el de **Computación sin servidor (Serverless)**, donde el cliente se desprende totalmente de la gestión de la infraestructura; el código se ejecuta en respuesta a eventos y el proveedor escala los recursos automáticamente. Este modelo es altamente eficiente para microservicios y aplicaciones modernas que requieren una respuesta rápida y un costo optimizado al milisegundo de ejecución.

Otro modelo relevante es la **Nube Federada**, que consiste en la colaboración de múltiples proveedores de servicios de nube para compartir recursos y garantizar la interoperabilidad. Esto evita el "bloqueo" por un solo proveedor y permite una distribución de carga más inteligente a nivel global. También encontramos la **Nube de Borde (Edge Computing)**, que acerca el procesamiento de los datos al lugar donde se generan (dispositivos IoT, sensores), reduciendo la latencia y permitiendo que solo la información procesada y relevante sea enviada a la nube centralizada, optimizando el uso del ancho de banda.

6) Mencione y Explique los modelos de servicio que se ofertan a los clientes y usuarios en la nube.

El modelo **IaaS (Infraestructura como Servicio)** proporciona acceso a recursos fundamentales como servidores virtuales, almacenamiento y redes. Es la capa más baja y ofrece el mayor control al cliente, quien debe gestionar el sistema operativo y las aplicaciones. El modelo **PaaS (Plataforma como Servicio)** ofrece un entorno de desarrollo completo (sistemas operativos, bases de datos, herramientas de programación) para que los desarrolladores creen aplicaciones sin preocuparse por la infraestructura subyacente.

Finalmente, el modelo **SaaS (Software como Servicio)** es el más común para el usuario final, entregando aplicaciones listas para su uso a través de un navegador (como Office 365 o Salesforce). En este modelo, el proveedor gestiona absolutamente todo, desde el hardware hasta las actualizaciones de la aplicación. Estos modelos forman lo que se conoce como la "pila" de servicios de la nube, donde cada nivel ofrece un grado distinto de abstracción, responsabilidad compartida y flexibilidad, permitiendo a las empresas elegir el modelo que mejor se adapte a su capacidad técnica y objetivos de negocio.

7) Mencione y Explique los modelos de despliegue en la nube.

La **Nube Pública** es el modelo donde los servicios se ofrecen sobre una red abierta al uso general. Es propiedad de un proveedor que gestiona los recursos para miles de clientes simultáneamente, ofreciendo la mayor escalabilidad y el costo más bajo. Por otro lado, la **Nube Privada** es una infraestructura operada exclusivamente para una única organización. Puede ser gestionada internamente o por un tercero, y ofrece el mayor nivel de control y seguridad, siendo la opción preferida para entidades gubernamentales o financieras con requisitos regulatorios estrictos.

La **Nube Híbrida** combina los dos modelos anteriores, permitiendo que datos y aplicaciones se compartan entre nubes públicas y privadas según sea necesario. Esto da a las empresas la flexibilidad de mantener cargas de trabajo críticas en su entorno privado mientras aprovechan la escala de la nube pública para picos de demanda. Por último, la **Nube Comunitaria** es compartida por varias organizaciones que tienen intereses comunes (como requisitos de seguridad o

misiones compartidas), permitiendo dividir los costos de una infraestructura especializada entre un grupo cerrado de usuarios.

8) ¿Qué se puede decir en cuanto al criterio de selección en la nube?

El criterio de selección debe ser un proceso estratégico que evalúe no solo el costo, sino la **alineación con los objetivos de negocio**. Las organizaciones deben analizar la criticidad de sus aplicaciones y la sensibilidad de sus datos; por ejemplo, una aplicación de cara al cliente puede beneficiarse de la escala de una nube pública, mientras que un sistema de registros médicos podría requerir la seguridad de una nube privada. Es fundamental considerar la **soberanía de los datos**, asegurándose de que el proveedor cumpla con las leyes locales de almacenamiento y privacidad de la información.

Además, se debe evaluar la **interoperabilidad y la portabilidad**, evitando quedar atrapado con un solo proveedor (vendor lock-in). La madurez del proveedor, su historial de disponibilidad (SLA) y la calidad de su soporte técnico son factores determinantes. Una buena selección implica también analizar el ecosistema de servicios adicionales (IA, Big Data, IoT) que ofrece el proveedor, ya que la nube moderna no es solo almacenamiento, sino un conjunto de herramientas avanzadas que pueden potenciar la ventaja competitiva de la empresa a largo plazo.

9) ¿Qué es un proveedor en la nube?

Un proveedor de servicios en la nube (CSP) es una entidad comercial que ofrece componentes de computación (IaaS, PaaS o SaaS) a través de Internet. Estas empresas operan infraestructuras masivas compuestas por múltiples centros de datos distribuidos geográficamente. Los CSP más grandes, como Amazon (AWS), Microsoft (Azure) y Google (GCP), dominan el mercado gracias a su capacidad de inversión en hardware, seguridad y desarrollo de software de orquestación. Su función principal es abstraer la complejidad técnica para el cliente, garantizando la disponibilidad y el rendimiento.

El proveedor actúa como un socio tecnológico que asume los riesgos de obsolescencia y mantenimiento. Al operar a una escala global, estos proveedores pueden implementar medidas de seguridad física y lógica que superan por mucho las capacidades de una empresa individual. El CSP cobra por el uso de estos recursos y ofrece contratos de nivel de servicio (SLA) que definen las garantías de tiempo de actividad y soporte. En la actualidad, el rol del proveedor ha evolucionado de ser un simple hospedador a ser un habilitador de tecnologías disruptivas como el aprendizaje profundo y el procesamiento de datos masivos.

10) ¿Qué elementos hay que considerar para seleccionar un proveedor en la nube?

El primer elemento es el **Cumplimiento Normativo y Seguridad**. Es vital verificar que el proveedor posea certificaciones internacionales como ISO 27001 o SOC 2, y que cumpla con normativas específicas de la región (como el RGPD en Europa). El cliente debe entender cómo se gestionan las claves de cifrado y cuáles son las políticas de acceso físico a los servidores. Sin una confianza total en la integridad y privacidad que ofrece el proveedor, la migración a la nube representa un riesgo inaceptable para cualquier organización seria.

El segundo elemento clave es la **Estructura de Costos y Flexibilidad**. El modelo de precios debe ser transparente y predecible, permitiendo al cliente escalar sin enfrentar costos inesperados. También es fundamental evaluar el **Rendimiento y la Latencia**, verificando que el proveedor tenga centros de datos o "puntos de presencia" cerca de los usuarios finales del cliente para garantizar una experiencia de usuario fluida. Por último, se debe considerar el **Ecosistema y Soporte**, analizando si el proveedor ofrece las herramientas específicas que la empresa necesita y si cuenta con una comunidad robusta de socios y expertos para asistir en la implementación.

11) ¿Qué elementos se deben tener en cuenta para adaptar la nube a organizaciones y empresas?

Adaptar la nube requiere una **transformación cultural profunda**. El departamento de TI debe pasar de ser un "gestor de cajas" a un "gestor de servicios". Esto implica capacitar al personal en nuevas metodologías como DevOps y FinOps (gestión financiera de la nube), para asegurar que el uso de los recursos sea eficiente y no genere gastos descontrolados. La creación de un Centro de Excelencia en la Nube (CCoE) es una práctica recomendada para centralizar las mejores prácticas, establecer estándares de gobernanza y guiar a las distintas unidades de negocio en su proceso de adopción.

Asimismo, se debe considerar la **arquitectura de las aplicaciones**. No basta con mover un software antiguo a la nube; para obtener beneficios reales, las aplicaciones deben ser "cloud-native", aprovechando microservicios y contenedores que permitan el escalado independiente y la resiliencia. La integración con los sistemas "legacy" (heredados) que aún permanecen en las instalaciones locales es otro desafío técnico que requiere una estrategia de red híbrida sólida, utilizando conexiones seguras y de alta velocidad para mantener la coherencia de los datos en todo el entorno empresarial.

12) Defina Centro de Datos como soporte a la Nube (o Cloud Computing).

Un Centro de Datos (Data Center) es la infraestructura física que constituye el cimiento de la nube. Son instalaciones de alta seguridad diseñadas para albergar sistemas informáticos y sus componentes asociados, como telecomunicaciones y almacenamiento. En el contexto de la nube, estos centros de datos operan con niveles de redundancia y eficiencia extremos. Cuentan con sistemas de alimentación ininterrumpida (SAI), generadores de respaldo y sistemas de refrigeración de precisión para garantizar que el hardware funcione 24/7 sin interrupciones, independientemente de las condiciones externas.

Estos centros de datos son los que permiten la virtualización masiva de recursos. Un solo edificio puede albergar miles de servidores físicos que, a través de software especializado, se dividen en millones de servidores virtuales para distintos clientes de todo el mundo. La ubicación estratégica de estos centros es

vital; se agrupan en "Regiones" para ofrecer baja latencia y se subdividen en "Zonas de Disponibilidad" para asegurar que, si un edificio falla por una inundación o incendio, los datos y aplicaciones sigan funcionando en otro edificio cercano, proporcionando la base de la alta disponibilidad de la nube.

13) ¿Qué importancia tienen internet y los centros de datos en la conformación de entornos industriales?

En la Industria 4.0, Internet y los centros de datos son los habilitadores de la **hiperconectividad industrial**. Internet actúa como el sistema nervioso que transporta datos en tiempo real desde los sensores de las máquinas en la fábrica hasta la nube. Sin una red de alta velocidad y baja latencia, sería imposible monitorear procesos productivos a distancia o coordinar cadenas de suministro globales de forma sincronizada. La red permite que la planta de producción deje de ser una isla para convertirse en un nodo activo dentro de un ecosistema digital inteligente.

Los centros de datos, por su parte, proporcionan el "cerebro" donde se procesan esos volúmenes masivos de datos industriales (Big Data). Gracias a la capacidad de cómputo en la nube, las fábricas pueden implementar algoritmos de inteligencia artificial para el mantenimiento predictivo, optimizando el consumo de energía y reduciendo los tiempos de inactividad. En conjunto, internet y los centros de datos permiten la creación de "Gemelos Digitales", representaciones virtuales de activos físicos que permiten simular cambios y mejoras en la producción antes de implementarlos en el mundo real, aumentando drásticamente la eficiencia y la competitividad industrial.

14) ¿Cuáles son los aspectos a considerar a la migración a la nube o (Cloud Computing)?

El aspecto más crítico es la **Estrategia de Migración**, comúnmente resumida en las "6 R": Rehost (mover sin cambios), Replatform (ajustes menores), Repurchase (cambiar a SaaS), Refactor (rediseñar), Retire (eliminar) o Retain

(mantener local). Elegir el camino correcto para cada aplicación es vital para no inflar los costos. Un error común es el "Lift and Shift" (Rehost) de aplicaciones que no fueron diseñadas para la nube, lo que puede resultar en un rendimiento pobre y facturas mensuales elevadas. Se requiere un inventario detallado y una priorización basada en el valor de negocio.

Otro aspecto fundamental es el **Gobierno y Seguridad de los Datos durante el proceso**. La transferencia de grandes volúmenes de información requiere protocolos de cifrado robustos y una planificación del ancho de banda para evitar interrupciones en el servicio. Además, se deben rediseñar los modelos de acceso; en la nube, el perímetro de seguridad ya no es el firewall de la oficina, sino la identidad del usuario (IAM). La migración es también el momento ideal para implementar la automatización, permitiendo que la infraestructura se despliegue mediante código (IaC), lo que reduce errores humanos y garantiza la consistencia del entorno.

15) Mencione los dominios a considerar para tomar una decisión sobre la seguridad en la nube.

La seguridad en la nube se divide en varios dominios críticos. El primero es la **Gobernanza y Gestión de Riesgos**, que implica definir quién es responsable de qué según el modelo de servicio (IaaS, PaaS, SaaS) y cómo se alinean los controles de la nube con las leyes locales. Otro dominio esencial es la **Seguridad de los Datos**, que abarca el cifrado en reposo y en tránsito, así como la gestión de las claves criptográficas. Es vital asegurar que el proveedor no tenga acceso a los datos del cliente sin autorización explícita.

También se debe considerar el dominio de la **Arquitectura y Virtualización**, analizando cómo el proveedor aísla las cargas de trabajo de diferentes clientes para evitar ataques de "canal lateral". La **Gestión de Identidades y Accesos (IAM)** es quizás el dominio más importante para el cliente, ya que permite controlar los privilegios de los usuarios y aplicar autenticación de múltiples factores. Finalmente, la **Seguridad en las Operaciones** incluye el monitoreo continuo, la detección de intrusos y los planes de respuesta ante incidentes, asegurando que la organización

pueda reaccionar rápidamente ante cualquier anomalía detectada en su infraestructura virtual.

16) ¿Cuáles son los puntos importantes que se deben incluir según la AEPD en los contratos de servicio en la nube?

La Agencia Española de Protección de Datos (AEPD) enfatiza que los contratos deben ser exhaustivos en la **definición de las responsabilidades del tratamiento**. Debe quedar claro que el cliente es el "responsable del tratamiento" y el proveedor es el "encargado". El contrato debe especificar que el proveedor solo tratará los datos siguiendo las instrucciones documentadas del responsable y nunca para fines propios. También se debe incluir la obligación de implementar medidas de seguridad técnicas y organizativas adecuadas para proteger los datos personales contra accesos no autorizados o pérdidas accidentales.

Otro punto crucial es la transparencia sobre las **Subcontrataciones y Transferencias Internacionales**. El proveedor debe informar si utiliza terceros para prestar parte del servicio y el cliente debe dar su autorización. Si los datos se almacenan fuera de la Unión Europea, el contrato debe garantizar que se cumplen los estándares de protección equivalentes (como las Cláusulas Contractuales Tipo). Por último, el contrato debe regular el destino de los datos al finalizar el servicio, obligando al proveedor a devolver o destruir la información de forma segura, y garantizando el derecho del cliente a realizar auditorías para verificar el cumplimiento de estas obligaciones.

17) En un contrato de Cloud Computing enumere lo que se debe incluir según las diferentes agencias y asociaciones internacionales como: Cloud Security Alliance, ENISA y el INCIBE.

Estas organizaciones recomiendan que los contratos incluyan de forma obligatoria la **Transparencia en la Cadena de Suministro**. Es vital conocer no solo al proveedor principal, sino a cualquier sub-proveedor involucrado en el almacenamiento o procesamiento. También subrayan la importancia de los **SLA de Seguridad específicos**, que definen compromisos de tiempo para la notificación de brechas de seguridad y protocolos claros de respuesta ante incidentes. La seguridad no debe ser una promesa vaga, sino una métrica contractual medible con penalizaciones claras por incumplimiento.

Además, se debe garantizar la **Portabilidad e Interoperabilidad de los Datos**. Las agencias sugieren cláusulas que impidan que el proveedor utilice formatos de datos propietarios que dificulten la migración hacia otro prestador. La **Gobernanza y Cumplimiento Legal** también deben estar detallados, especificando qué leyes rigen el contrato y cómo se resolverán las disputas. Finalmente, el INCIBE y ENISA recomiendan incluir requisitos de **Auditoría Independiente**, donde el proveedor se compromete a someterse a revisiones periódicas por parte de terceros y a compartir los resultados de dichas auditorías con sus clientes para fomentar una cultura de transparencia y confianza.

18) ¿Qué cláusulas se recomiendan sean de obligatorio cumplimiento en todo contrato en la nube (o Cloud Computing)?

Es imperativa la cláusula de **Propiedad y Control de los Datos**, que establezca sin ambigüedades que el cliente es el único dueño de la información y que el proveedor no tiene derechos de uso comercial sobre ella. También es vital la cláusula de **Disponibilidad y Continuidad**, que defina los porcentajes mínimos de tiempo de actividad (Uptime) y las compensaciones financieras en caso de caídas. Sin estas garantías, una interrupción del servicio del proveedor podría causar daños irreparables a la reputación y finanzas de la empresa cliente sin ninguna vía de resarcimiento.

Otra cláusula obligatoria es la de **Derecho de Inspección y Auditoría**, que faculte al cliente para verificar las medidas de seguridad del proveedor. Asimismo,

se debe incluir una cláusula de **Notificación de Brechas de Seguridad**, con plazos estrictos (usualmente 72 horas) para informar sobre cualquier incidente que pueda haber comprometido la información. Por último, la cláusula de **Terminación y Reversión** debe detallar cómo se realizará la salida del servicio, asegurando que el proveedor preste la asistencia necesaria para que la empresa pueda recuperar sus datos y aplicaciones de forma íntegra y segura al finalizar la relación contractual.

19) ¿Cuáles son las amenazas más comunes en la Cloud Computing (la nube)?

La amenaza más extendida es la **Configuración Incorrecta de los Recursos**. Debido a la complejidad de las plataformas de nube, es fácil dejar por error una base de datos o un contenedor de archivos abierto a Internet, lo que conduce a fugas masivas de información. Otra amenaza crítica es el **Secuestro de Cuentas y Credenciales**; si un atacante obtiene las llaves de acceso al portal de administración de la nube, puede destruir toda la infraestructura de la empresa, robar datos confidenciales o desplegar recursos costosos para actividades ilícitas como el minado de criptomonedas.

También son comunes los ataques a las **Interfaces de Programación de Aplicaciones (API)**, que son los puntos de entrada para la gestión de la nube. Si estas interfaces no están bien protegidas, pueden ser explotadas para saltarse los controles de seguridad. El **Abuso de Servicios de Nube** por parte de ciberdelincuentes (cómo usar servidores gratuitos para lanzar ataques DDoS) también es una amenaza constante. Finalmente, las **Amenazas Internas (Insiders)**, tanto del lado del proveedor como del cliente, representan un riesgo significativo, ya que personas con acceso legítimo pueden filtrar datos de manera intencionada o accidental, evadiendo los controles de perímetro tradicionales.

20) ¿Cuáles son los riesgos más importantes que enfrentan las empresas cliente de la nube según ENISA?

ENISA destaca como riesgo principal la **Pérdida de Control sobre la Seguridad**. Al externalizar la infraestructura, el cliente ya no tiene acceso físico a los servidores ni control total sobre la capa de red o el hipervisor. Si el proveedor cambia sus políticas o sufre un fallo interno, la empresa cliente puede verse afectada sin tener capacidad de reacción directa. Este riesgo se agrava si no existe una visibilidad clara (monitoreo) de las acciones que el proveedor realiza en la infraestructura compartida, lo que puede ocultar debilidades de seguridad hasta que sea demasiado tarde.

Otro riesgo fundamental es el **Bloqueo del Proveedor (Vendor Lock-in)**. Esto ocurre cuando una empresa se vuelve tan dependiente de las herramientas específicas de un proveedor que el costo de migrar a otro se vuelve prohibitivo. Esto quita poder de negociación al cliente y lo deja vulnerable a cambios de precios o a la obsolescencia tecnológica si el proveedor deja de innovar. ENISA también advierte sobre el riesgo de **Incumplimiento Normativo**, donde la falta de conocimiento sobre la ubicación física de los datos o la identidad de los sub-proveedores puede llevar a la empresa cliente a violar leyes de protección de datos, resultando en multas millonarias y daños reputacionales severos.