GPF-OCEX 1403 Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios de computación en la nube.

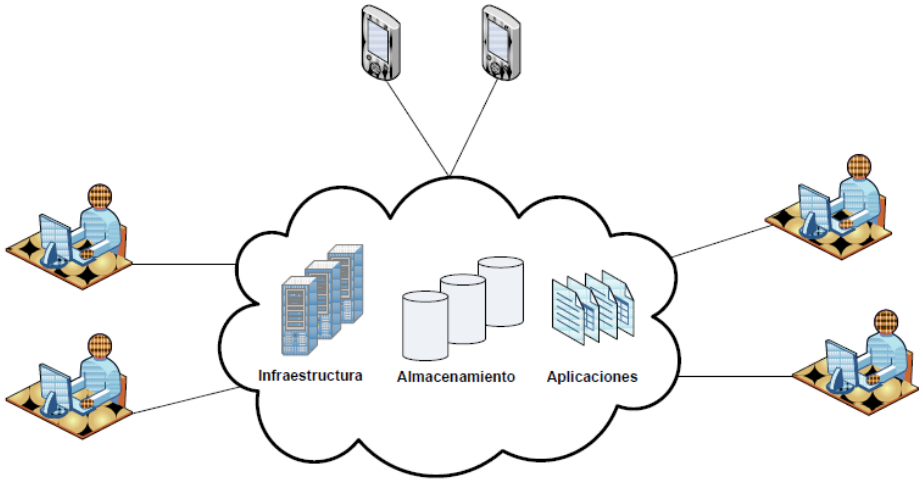
Referencia: NIA-ES-SP 1402 Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios

Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de la ASOCEX el 20/05/2020.
Guía revisada por la Conferencia de Presidentes de ASOCEX el 03/12/2020

1. La computación en la nube

En los últimos años, en paralelo a la expansión de la digitalización en todos los niveles de la gestión pública, se ha incrementado el acceso a servicios públicos a través de Internet desde diferentes dispositivos. Este hecho ha supuesto un importante auge en el uso de las tecnologías web y también en la externalización de muchos sistemas de información.

Surge así el modelo de servicios en la nube, donde entidades o proveedores (CSP, *Cloud Service Provider*) ofrecen servicios en red, con independencia de dónde se encuentren alojados los sistemas de información que soportan dichos servicios, y de forma transparente para el usuario final.



Fuente: CCN-STIC-823

Una de las definiciones de servicios en la nube con mayor aceptación es la propuesta por el NIST[1]: "**La provisión de servicios en la nube es un modelo para permitir el acceso por red, de forma práctica y bajo demanda, a un conjunto de recursos de computación configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser suministrados y desplegados rápidamente con una mínima gestión o interacción con el proveedor de servicio**".

1 National Institute of Standards and Technology [NIST SP-800-145]

El modelo de computación en la nube o cloud computing se utiliza cada vez más, tanto en el sector privado como en el público. Ofrece a las organizaciones **grandes beneficios**[2], como la deslocalización, alta disponibilidad, acceso a la información desde cualquier lugar, flexibilidad en la asignación de recursos y ahorros económicos, pero también conlleva **riesgos significativos** que deben ser previstos por las entidades que las utilizan, y también deben ser considerados en los trabajos de auditoría.

Numerosos países occidentales han establecido como política pública que el despliegue de los nuevos sistemas de información sea en la nube de forma prioritaria y, solo si esta alternativa no fuera viable o económica, se efectuará mediante medios propios[3].

Las **características esenciales** de la computación en la nube destacadas en el marco NIST son:

- **Autoservicio bajo demanda**. El cliente puede ajustar la capacidad necesaria de forma unilateral, sin necesidad de involucrar al personal del proveedor.
- **Amplio acceso a la red.** Todos los recursos están disponibles en una red, sin necesidad del acceso físico directo; la red no es necesariamente parte del servicio.
- **Agregación y compartición de recursos.** Los recursos del proveedor se agregan y se ponen a disposición de múltiples clientes para su compartición. La agregación incluye equipos físicos y equipos virtuales que se asignan dinámicamente bajo demanda. El cliente se independiza de la ubicación física de los recursos, aunque se pueden delimitar ubicaciones a un cierto nivel (país, UE).
- **Adaptación inmediata**. La elasticidad rápida permite a los usuarios ampliar o contraer los recursos que utilizan (aprovisionamiento y desaprovisionamiento), a menudo de forma completamente automática. Esto permite relacionar más estrechamente el consumo de recursos con la demanda (por ejemplo, agregar servidores virtuales cuando la demanda aumenta y luego desconectarlos cuando baja la demanda). Desde el punto de vista del consumidor los recursos parecen ilimitados, pudiendo disponer de cualquier volumen en cualquier momento.
- **Servicio medido.** El proveedor puede controlar el servicio efectivamente prestado en cada momento con el indicador que se especifique por contrato; por ejemplo, capacidad de almacenamiento, capacidad de procesamiento, ancho de banda, cuentas de usuario, etc. El uso de recursos puede ser monitorizado, controlado y reportado, proporcionando una gran transparencia tanto para el proveedor como para el consumidor del servicio utilizado.

2. Objetivos de la guía

Desde la perspectiva de un OCEX, se pueden adoptar **dos enfoques principales para revisar la seguridad de la información y los controles internos en un entorno de computación en la nube,** según el objetivo de la auditoría:

- Realizar una **auditoría específica** de los servicios de computación en la nube utilizados por un determinado ente.

  Este tipo de auditorías profundizará en la revisión de:

  - El marco de control aplicado por el ente auditado sobre el proveedor de servicios de computación en la nube.
  - La evaluación del diseño, implementación y eficacia operativa de los controles que, en función del tipo de servicio (IaaS/PaaS/SaaS), sean responsabilidad directa de la entidad auditada.

2 Guía de seguridad *TIC CCN-STIC-823, Utilización de servicios en la nube*

3 En un ámbito de actuación cercano a los OCEX, la "Estrategia de inteligencia artificial de la Comunitat Valenciana" de 2019 fija como una de las líneas de acción: "Establecer políticas de uso de sistemas informáticos basados en la nube (Cloud First) que, dentro de los marcos nacional y europeo, permitan el desarrollo de proyectos de IA competitivos".

Para realizar estas auditorías podrán utilizarse alguna de las guías señaladas en la bibliografía, incluyendo la GPF-OCEX 5330, la GPF-OCEX 5313 y la presente guía.

- Realizar la revisión del servicio de computación en la nube **en el contexto de una auditoría financiera.**

  La revisión del entorno de TI en el contexto de una auditoría financiera, cuando el ente fiscalizado utiliza servicios de computación en la nube, es la finalidad principal de esta guía. Además, son aplicables la NIA-ES-SP 1402, la GPF-OCEX 1315 y la GPF-OCEX 5330.

Esta guía recoge los aspectos más relevantes que deberán contemplarse en la fiscalización de entidades cuyas aplicaciones de gestión significativas a efectos de la auditoría estén alojadas en la nube mediante un contrato con un proveedor externo o CSP.

El **objetivo** de esta guía es ayudar al auditor a:

a) Comprender los conceptos fundamentales relacionados con el procesamiento en la nube para facilitar el conocimiento y comprensión del sistema de información y de control interno de la entidad auditada.

b) Identificar los principales riesgos específicos existentes cuando se utiliza el procesamiento en la nube desde el punto de vista del auditor y valorar su impacto en una auditoría.

c) Identificar posibles controles internos que aborden los riesgos identificados.

d) Diseñar procedimientos de auditoría para revisar la eficacia de los controles relevantes.

e) Considerar otros aspectos de la auditoría afectados cuando la entidad utiliza la nube en procesos significativos: evidencia, necesidad de expertos, utilización de herramientas de análisis de datos, etc.

f) Revisar el cumplimiento de los marcos legislativos aplicables, en especial el Esquema Nacional de Seguridad (ENS) o la normativa vigente en materia de protección de datos personales por parte de la entidad auditada y del CSP.

g) Señalar los principales aspectos que deben tenerse en cuenta al revisar el cumplimiento de la legalidad cuando se fiscaliza la contratación de un servicio de computación en la nube.

La presente guía se fundamenta en la NIA-ES-SP 1402 y en códigos de buenas prácticas o estándares reconocidos nacional e internacionalmente.

No es el objetivo principal de esta guía considerar el efecto en las fiscalizaciones de la utilización de soluciones en la nube puestas a disposición de las Administraciones Públicas por otra Administración Pública, para dar respuesta a necesidades comunes. Tampoco se consideran los entornos del tipo que más adelante denominamos “Nube privada”. No obstante, en estos casos, cuando sea pertinente, se seguirán criterios similares a los expuestos en esta guía.

3. Modelos de despliegue y tipos de servicios en la nube

Las diversas modalidades de servicios en la nube se pueden clasificar atendiendo a dos aspectos principales: el modelo de despliegue y el tipo de servicio de computación en la nube que se ofrece.

3.1. Modelo de despliegue

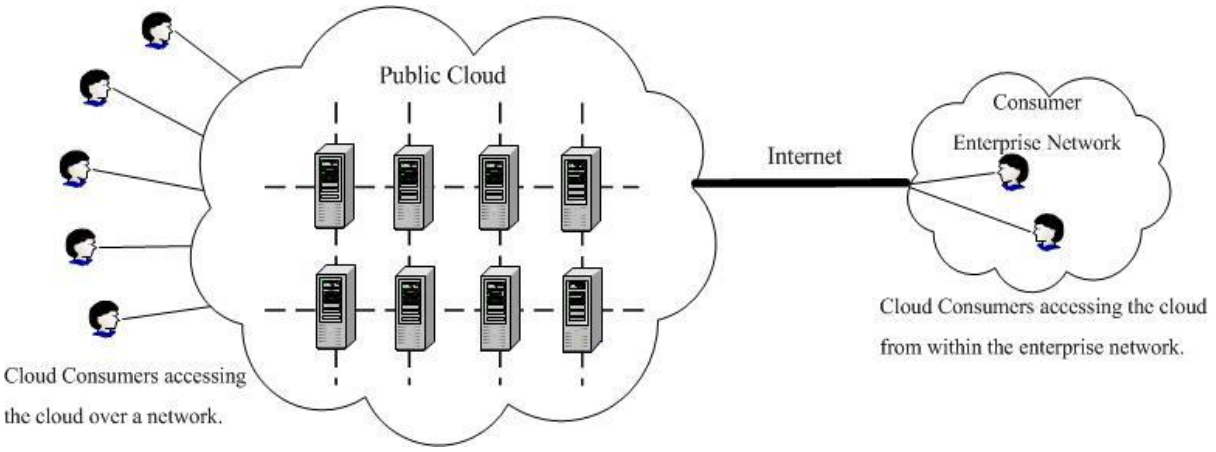
En cuanto al modelo de despliegue podemos hablar de:

Nube pública

Pueden definirse las nubes con modelos de despliegue público como **aquellas cuya infraestructura es ofrecida al público general o a un gran grupo de industria, y dicha infraestructura es controlada por un proveedor de servicios en la nube**.

Los recursos son propiedad de un proveedor de servicios en la nube (CSP), público o privado, quien los administra y los ofrece para el público en general a través de internet.

El consumidor recibe accesibilidad y escalabilidad bajo demanda sin el alto coste de adquirir y mantener el hardware físico y el software. El CSP es responsable de la gestión y el mantenimiento del sistema, mientras que el consumidor paga sólo por los recursos que utiliza.



Fuente: Evaluation of Cloud Computing Services Based on NIST 800-145, (NIST SP 500-322)

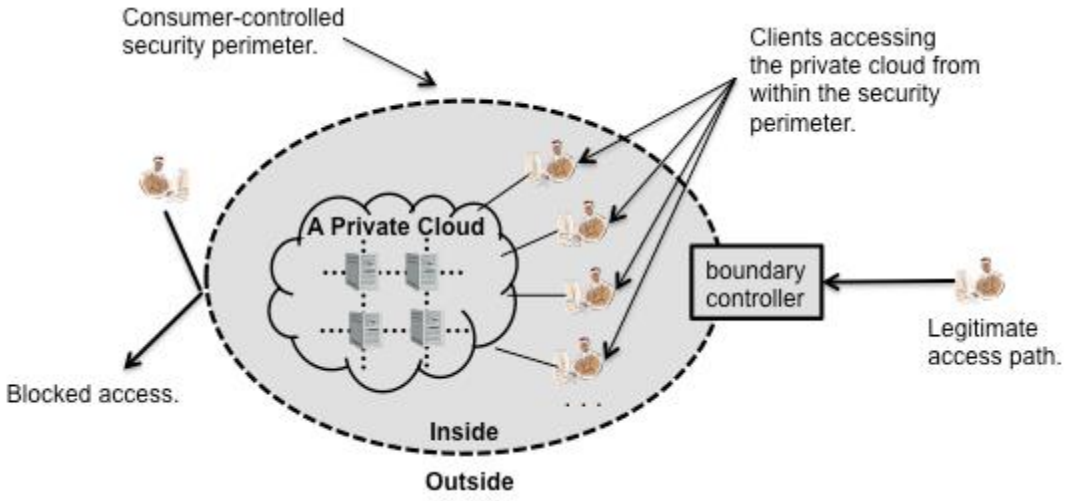
Nube privada

Tal como la define NIST, las nubes con modelos de despliegue privados se definen como **aquellas que se basan en una infraestructura operada únicamente para una organización y que ofrecen servicios únicamente a esa misma organización.**

Puede ser administrada por la entidad o por un tercero, y puede estar alojada en las instalaciones de la organización (es decir, nubes privadas en modo local) o subcontratadas a una empresa de alojamiento (es decir, nubes privadas alojadas en terceros).

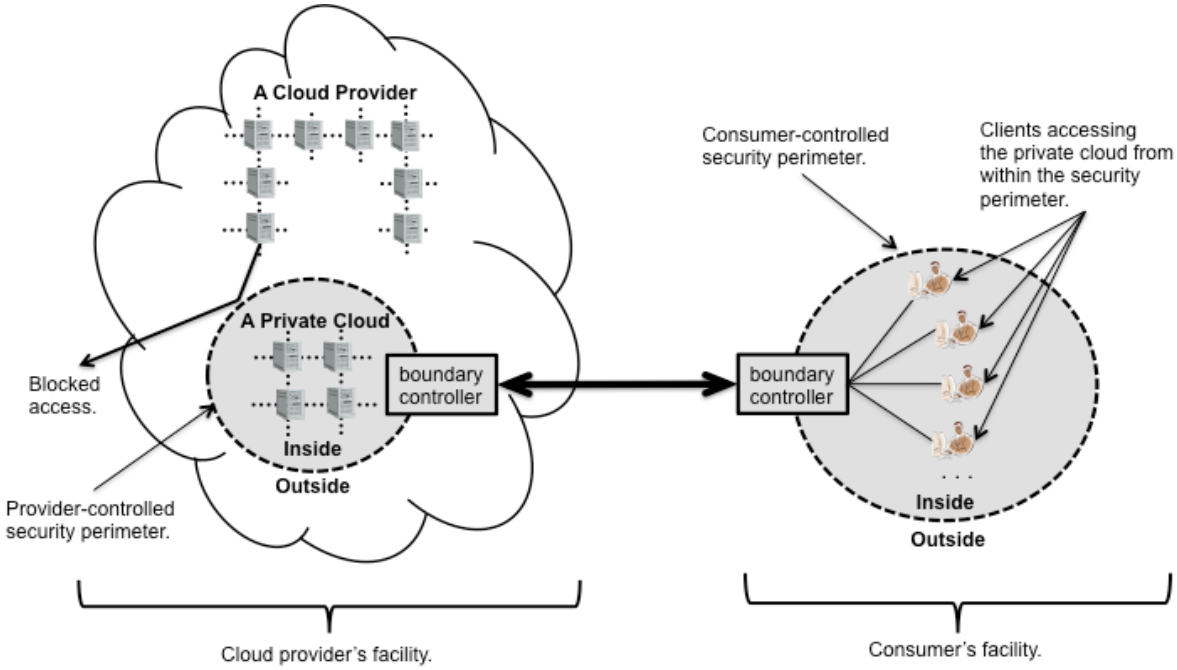
De esta forma, se puede distinguir entre:

- **Nube privada (en modo local).** Todos los recursos informáticos son alojados y utilizados exclusivamente por una entidad usuaria dentro de sus propias oficinas y centros de datos. La entidad usuaria es responsable de los costos operativos, hardware, software y los recursos necesarios para construir y mantener la infraestructura, es decir, requieren los mismos gastos que la propiedad tradicional del centro de datos.



Fuente: Cloud Computing Synopsis and Recommendations, (NIST-SP 800 146)

- **Nube privada (alojada en terceros).** Es una nube privada alojada en infraestructuras contratadas a proveedores externos. El tercero proporciona un entorno de nube exclusivo para la entidad usuaria y administra el hardware.



Fuente: Cloud Computing Synopsis and Recommendations, (NIST-SP 800 146)

Las nubes privadas ofrecen un mayor nivel de seguridad y privacidad a través de los firewalls de la empresa (el entorno normalmente se ejecuta detrás del firewall del usuario) y del alojamiento interno para garantizar que las operaciones y los datos confidenciales no sean accesibles para proveedores externos.

Es decir, en estos casos **la entidad mantiene un mayor control sobre la nube**.

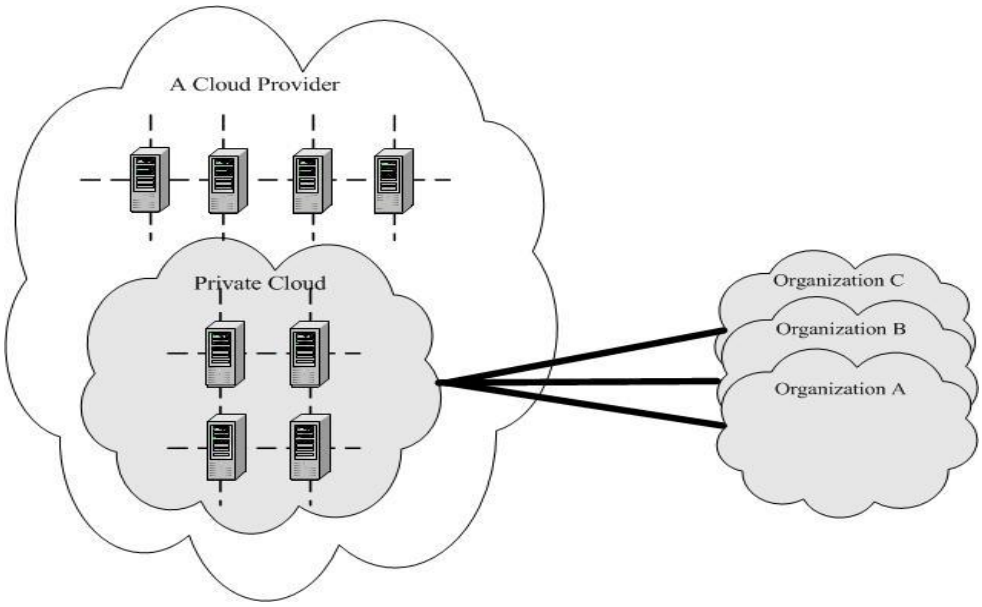
Las entidades que optan por las nubes privadas suelen ser entidades grandes y complejas que necesitan centralizar los recursos informáticos y/o mantener un control total sobre sus procesos críticos y, a la vez, ofrecer flexibilidad en la disponibilidad de los mismos, por ejemplo, administraciones públicas y grandes corporaciones.

La Norma de Seguridad TIC *CCN-STIC-220 Arquitecturas virtuales*, de julio de 2020 regula determinados aspectos de las nubes privadas. Esta norma de seguridad se centra precisamente en el modelo de nube privada, la cual está apoyada en tecnologías de virtualización y de hiperconvergencia. Según señala esta guía, "el objetivo que se busca cuando se plantea el despliegue de una nube privada es que la organización logre alcanzar los beneficios tecnológicos de un modelo de computación de nube (autoservicio, escalabilidad, automatización, monitorización, etc.) pero sin renunciar a las medidas de seguridad y el control de la infraestructura adaptado a los requerimientos y normativas aplicables a la organización."

Nube comunitaria o compartida

Las nubes con modelos de despliegue comunitarios se definen como **aquellas alojadas en infraestructuras compartidas por varias organizaciones relacionadas entre ellas, compartiendo requisitos de servicio** (son los centros de servicios compartidos[4]).

La nube comunitaria (compartida) es una modalidad de despliegue en la que los recursos informáticos y la infraestructura se comparten entre varias organizaciones para su uso exclusivo. Los recursos se pueden administrar internamente o por un tercero y se pueden hospedar en instalaciones propias de una o más de las organizaciones de la comunidad (modo local), externamente en una empresa de alojamiento, o alguna combinación de ellos.



Fuente: Evaluation of Cloud Computing Services Based on NIST 800-145, (NIST SP 500-322)

Las organizaciones comparten el coste y a menudo tienen requisitos de seguridad en la nube y objetivos similares.

Nube híbrida

Combina dos o más modelos de los anteriores. A menudo llamadas "lo mejor de ambos mundos", las nubes híbridas combinan infraestructura local, o nubes privadas, con nubes públicas para que las organizaciones puedan aprovechar las ventajas de ambas. Los servicios se ofrecen de forma pública y privada. Un usuario es propietario de unas partes y comparte otras, aunque de una manera controlada.

En una nube híbrida, los datos y las aplicaciones pueden moverse entre nubes privadas y públicas para una mayor flexibilidad y más opciones de implementación. Por ejemplo, puede

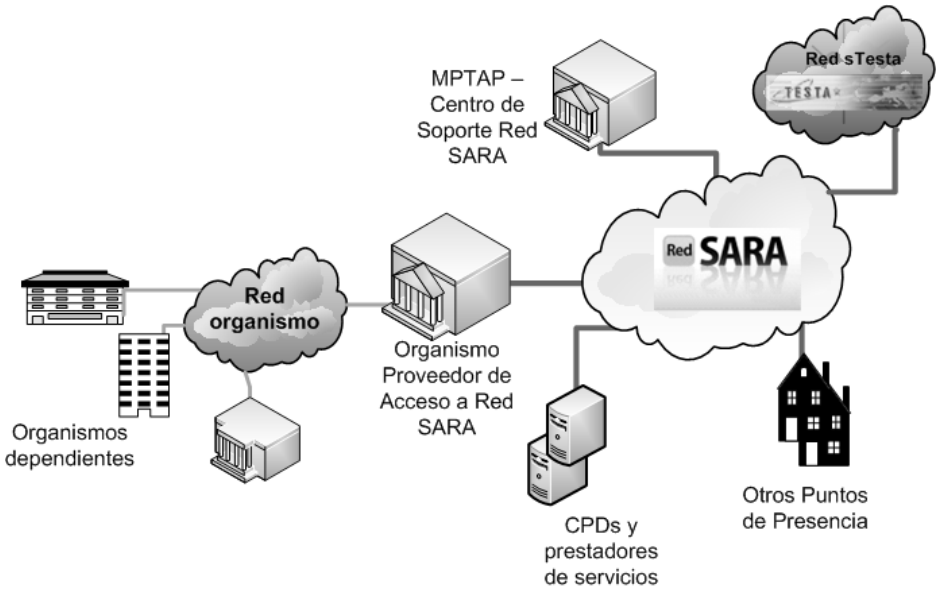
4 El 15 de septiembre de 2015 se publicó, en el ámbito de la Administración General del Estado, el "Marco regulador para la declaración de servicios compartidos" (Ministerio de Hacienda y AAPP).

usar la nube pública para necesidades de gran volumen y menor seguridad, como el correo electrónico basado en web, y la nube privada (u otra infraestructura local) para operaciones confidenciales y críticas para el negocio, como informes financieros.

En una nube híbrida, el "cloud bursting" también es una opción. Esto es cuando una aplicación o recurso se ejecuta en la nube privada hasta que hay un aumento de la demanda (como eventos estacionales como la presentación de impuestos), momento en el que la organización puede "atravesar" a la nube pública para aprovechar sus recursos adicionales.

Un ejemplo de nube híbrida es la Red SARA. En el *Plan de Transformación Digital de la Administración General del Estado y sus organismos públicos 2015-2020*, se fijó como meta la constitución de una nube híbrida (nube SARA) que ofreciera software, plataforma e infraestructura como servicio (SaaS, PaaS e IaaS). Se trata de un servicio que proporciona servicios de computación y almacenamiento en nube híbrida para la AGE y sus Organismos Públicos, mediante la configuración de nodos de consolidación tanto en centros de datos de la Administración (nube privada) como de proveedores externos (nube pública). Todos los nodos son gestionados mediante un portal común de aprovisionamiento multi-organismo. Esta conformación de nube supone en la práctica varias arquitecturas de ejecución normalizadas, industrializadas, predecibles, medibles y comparables en un escenario de pago por uso optimizado para el consumo granular de infraestructura TIC por parte de las diferentes unidades. Aunque inicialmente se centraba en la infraestructura como servicio, ha proporcionado gradualmente servicios de mayor madurez, tales como plataforma como servicio y aplicación como servicio (por ejemplo, gestión de la nómina en la nube).

La Red SARA tiene la siguiente estructura:



Fuente: Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública

Resumen comparativo

	Nubes privadas	Nubes públicas	Nubes híbridas
Flexibilidad	Alta (personalización del entorno)	Media	Combina las ventajas de ambas. Parte de los servicios se mantienen como nube privada y simultáneamente se dispone de acceso al resto de servicios de la nube pública cuando se precise. Se mantiene la seguridad, se gana en flexibilidad y se paga por lo que se usa.
Seguridad	Alta (recursos no compartidos)	Media (servicios compartidos con otros usuarios)	
Escalabilidad	Sí (adaptación a las necesidades del usuario)	Sí (adaptación a las necesidades del usuario)	
¿Requiere instalación HW/SW?	Sí	No	
Coste	Alto (asociado a la adquisición y mantenimiento hardware/software)	Medio: pago por servicio usado (sin mantenimiento)	
Usuarios	AA.PP., entidades financieras, empresas grandes o medianas	Todo tipo de entes públicos y privados	
Operaciones más usuales	Operaciones esenciales	Aplicaciones web (correo, ofimáticas, almacenamiento, etc.)	

3.2. Categorías de servicios de computación en la nube

En cuanto a las categorías o tipos de servicios de computación en la nube existentes, las principales son:

Infraestructura como servicio (Infrastructure-as-a-Service o IaaS)

El servicio que se ofrece es la infraestructura, es decir, capacidad de procesamiento, almacenamiento, redes y otros recursos informáticos fundamentales (administrados por el CSP) donde el cliente puede implementar y ejecutar software, incluyendo sistemas operativos y aplicaciones.

El cliente no administra ni controla la infraestructura de nube subyacente, pero tiene control sobre los sistemas operativos, el almacenamiento y las aplicaciones implementadas, y posiblemente un control limitado de determinados componentes de red (por ejemplo, firewalls).

Un ejemplo lo tenemos en máquinas virtuales o servidores como Amazon web services (AWS), donde se puede instalar después una base de datos.

Plataforma como servicio (Platform-as-a-Service o PaaS)

PaaS agrega una capa adicional, el sistema operativo, a lo que facilita IaaS (procesamiento, almacenamiento y redes). Una nube PaaS proporcionará a la entidad usuaria la capacidad de implementar aplicaciones desarrolladas o adquiridas para su utilización posterior. La entidad usuaria no administra ni controla la infraestructura de nube subyacente, incluida la red, los servidores, los sistemas operativos o el almacenamiento, pero tiene control sobre las aplicaciones implementadas y, posiblemente, los valores de configuración para el entorno de hospedaje de aplicaciones.

Tomando como ejemplo una base de datos, en PaaS la base de datos se expandiría (o contraería)

según fuese necesario en función de su uso, de forma transparente para el cliente, quien tampoco tendría que administrar los servidores individuales sobre los que estuviese la base de datos, las redes que la comuniquen, etc.

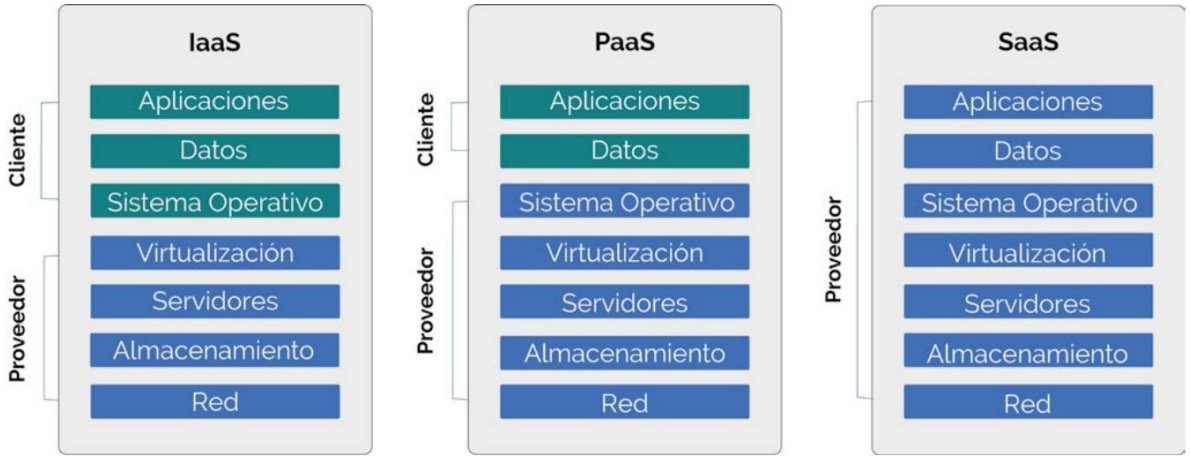
Un ejemplo reciente de utilización de PaaS por las administraciones públicas es la adjudicación de un ERP de gestión económica con esta modalidad por la Generalitat Valenciana[5].

Software como servicio (Software-as-a-Service o SaaS)

El proveedor ofrece al cliente aplicaciones como un servicio desde una infraestructura cloud. Estas aplicaciones son accesibles por los clientes (mediante el navegador, aplicación móvil, etc.), quienes no administran ni controlan la infraestructura en que se basa el servicio (red, servidores, sistemas operativos, almacenamiento o incluso aplicaciones individuales, con la posible excepción de los valores de configuración de aplicaciones que sean específicos del usuario).

Ejemplo: suites ofimáticas online, Dropbox, Gmail, TeamMate (versión web), etc. Muchos ayuntamientos han optado por contratar los servicios TIC de gestión tributaria y recaudación, de nóminas, entre otros muchos, con esta modalidad de nube.

Cada uno de estos modelos implica diferentes niveles de responsabilidad del usuario y del proveedor sobre el control interno, la seguridad y la configuración del servicio. Siguiendo el esquema de sistema de información por capas o niveles visto en la GPF-OCEX 5330, las principales diferencias de estos tres tipos de servicios de computación en la nube en cuanto a la responsabilidad y capacidad de supervisar cada uno de sus componentes son:



Fuente: CSA, Cloud Audit & Forensics

4. Riesgos significativos del uso de la computación en la nube

La adopción de servicios en la nube aporta notables ventajas, pero introduce nuevos riesgos, relacionados fundamentalmente con la seguridad de la información procesada y almacenada en la nube, que han de ser identificados y controlados. La identificación de los riesgos asociados al servicio de computación en la nube contratado es una actividad que debe desarrollar cada organización, puesto que el tipo, las características y el uso de los servicios contratados determinarán en gran medida los riesgos a los que está expuesta.

La computación en la nube cambia las responsabilidades y los mecanismos para la implementación y la gestión de los controles. Los servicios serán prestados a través de contratos y acuerdos de nivel de servicio, que deberán definir las responsabilidades y mecanismos para la gobernanza. Áreas no

5 (http://www.dgtic.gva.es/es/actualidad/-/asset_publisher/0YobAjUX6lT2/content/id/167776858).

incluidas en el contrato pueden provocar brechas de seguridad, que requerirán que el cliente ajuste sus propios procesos para gestionar los riesgos asociados.

Los **principales riesgos** derivados o acentuados por el uso de soluciones cloud son:

Pérdida de control

El uso de un entorno de computación en la nube conlleva la transferencia de algunas de las tareas de gestión de riesgos al CSP y, por tanto, existen responsabilidades compartidas. Si éstas no son bien gestionadas, pueden existir lagunas de responsabilidad que deriven en brechas de seguridad.

Por tanto, la entidad debe tener reguladas todas las responsabilidades y cuestiones que afecten a la seguridad de la nube, y todo ello debe estar adecuadamente recogido en los acuerdos de nivel de servicio y en cláusulas ad hoc en los pliegos y en el contrato. En este sentido, debe recordarse que la responsabilidad final sobre los datos sigue siendo de la entidad.

Riesgos legales

Al contratar servicios en la nube es responsabilidad de la entidad usuaria garantizar que el proveedor del servicio cumple con la legislación vigente.

Si por ley se exigen una serie de controles a distintos niveles, que un determinado modelo de servicio no garantiza, es responsabilidad del cliente tomar la decisión más adecuada sobre el modelo de servicio elegido, el proveedor más apropiado e incluso, en última instancia, la decisión de migrar o no cierta información a la nube.

En la revisión de servicios de computación en la nube por parte de los OCEX se prestará siempre atención a la normativa vigente, en especial al cumplimiento con el ENS, ENI[6], LOPD[7] y el RGPD[8].

Normalmente un CSP se convertirá en un encargado del tratamiento respecto a los datos personales del cliente. La DA 1ª de la LOPD obliga a aplicar las medidas del ENS: "*En los casos en que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración Pública de origen y se ajustarán al ENS*".

El cumplimiento de las leyes y normativas citadas anteriormente, así como el cumplimiento respecto a estándares de seguridad de la información por parte de los proveedores de servicio suele acreditarse mediante informes de auditoría externa y certificaciones de seguridad, que podrán servir para complementar los trabajos de auditoría.

Brechas/Fuga de datos

Al igual que los entornos tradicionales, las tecnologías de computación en la nube pueden verse afectadas por las amenazas clásicas presentes en aplicaciones, sistemas y redes. Sin embargo, la superficie de exposición en un servicio de computación en la nube es mayor (ya que dicho servicio es utilizado por varias organizaciones y es accesible desde Internet) así como su potencial impacto en el caso de que exista un alto volumen de datos.

El nivel de impacto vendría dado por el carácter y sensibilidad de los datos expuestos -piénsese como ejemplo aquellos relacionados con la salud- así como por el volumen de los datos afectados por la brecha que, en ciertos servicios de computación en la nube, suele ser alto (entornos cloud para uso de big data).

6 ENI: Esquema Nacional de Interoperabilidad, regulado por el Real Decreto 4/2010.

7 LOPDP: Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de Derechos Digitales.

8 RGPD: Reglamento General de Protección de Datos, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Uso inadecuado de usuarios administradores

La revisión de los usuarios administradores es un aspecto muy relevante en cualquier auditoría. Cuando se audita un entorno de computación en la nube aún es más crítico puesto que habrá administradores ajenos a la entidad cuya existencia no será "visible" (en la mayoría de los casos) ni para los auditores ni para la propia entidad auditada. A veces las entidades con servicios de computación en la nube contratados confían, sin verificar, en la buena gestión de los usuarios realizada por el CSP incurriendo en riesgos importantes.

Inadecuada gestión de identidades, accesos y credenciales

La asignación de permisos y la gestión de usuarios conllevan un esfuerzo y dificultad que en muchos casos provoca que se cometan errores, otorgándose permisos y accesos a información y sistemas a usuarios que no deberían tenerlos.

Igualmente, los mecanismos de asignación de contraseñas o los propios sistemas de autenticación, cuando no disponen de controles para robustecerlos y evitar que un usuario ilegítimo acceda a donde no debe, son amenazas que deben preocupar a los responsables de seguridad de cualquier organización y a los auditores.

Por otro lado, han de valorarse los riesgos que implica compartir la gestión de identidades con un proveedor de servicios de computación en la nube frente a su centralización en un repositorio único. En un entorno de computación en la nube, el auditor debe analizar si la organización ha revisado los controles de seguridad que el proveedor ofrece para proteger los accesos.

Dependencia del proveedor

Externalizar servicios crea una dependencia con un tercero, que puede dar lugar a un riesgo alto para la continuidad del servicio en el caso de desaparición del proveedor. No es un riesgo exclusivo del cloud computing.

Portabilidad

Los servicios de computación en la nube están diseñados para que el cliente pueda abstraerse de la tecnología y acceder de forma sencilla y rápida a unas necesidades tecnológicas específicas. Sin embargo, derivado en parte de esta abstracción, así como de la localización de los datos en un entorno controlado por un tercero, se puede llegar a producir una situación de bloqueo en la que el cliente no sea capaz de migrar el servicio de computación en la nube a la infraestructura de otro proveedor o a una propia.

Esto suele deberse a la incompatibilidad surgida entre la tecnología desplegada por dos proveedores distintos, o por restricciones en el acceso a los datos depositados en la nube. Asimismo, esta situación también puede estar causada por una mala negociación de las cláusulas del contrato con el proveedor del servicio de computación en la nube.

Disponibilidad

Dependiendo de la criticidad de la información que esté alojada en la nube, los controles sobre su disponibilidad serán más o menos relevantes. Por ejemplo, no es lo mismo un servicio SaaS para la gestión de cuentas de correo corporativas que uno para compartir archivos de forma puntual con agentes externos a la entidad, o la gestión tributaria y recaudatoria. Los proveedores de servicios de computación en la nube deben tener definida una política de recuperación de datos y servicio en caso de desastre.

Pérdida de trazabilidad

El cliente o consumidor desconoce el nivel de trazabilidad de los servicios hasta que los necesita.

Otros riesgos o riesgos no vinculados solo a la nube

Desastres naturales, acceso no autorizado a instalaciones, robos o problemas en la red, etc.

De todos los riesgos existentes, entre los que se encuentran los que se acaban de citar, el auditor debe, aplicando su juicio profesional, determinar cuáles son riesgos significativos a efectos de la auditoría financiera, es decir aquellos que pueden suponer un impacto significativo en las cuentas anuales y por tanto representan un riesgo de incorrección material.

5. Responsabilidades del proveedor del servicio y del auditado en relación con la seguridad y con el ENS

5.1. Aspectos generales

En función de la propiedad y de la administración de la infraestructura cloud, el cumplimiento legal y normativo recaerá sobre la organización usuaria, el proveedor de servicios o ambos. En el supuesto de que sea el organismo usuario el propietario y administrador de la infraestructura, la responsabilidad por la adecuación a la normativa vigente recae en dicho organismo; por el contrario, en el caso de estar la infraestructura operada por un tercero, éste deberá cumplir los requisitos establecidos en la normativa de seguridad que le sea de aplicación.

En cualquier caso, la responsabilidad del cumplimiento de las normas aplicables y el correcto tratamiento de los datos recaerá siempre sobre el organismo propietario de la información, con independencia de la existencia de acuerdos, seguros u otras medidas compensatorias.

Cuando se utilizan servicios externalizados (mediante contrato, convenio, encomienda, etc.), es frecuente que la entidad prestadora o CSP (pública o privada) cuente con un Responsable de la Seguridad al que será exigible el mantenimiento de la seguridad de los sistemas de información concernidos, sin que ello suponga merma de la responsabilidad exigible al Responsable de Seguridad de la entidad pública destinataria de los servicios y propietaria de los datos.

La *Guía de seguridad de las TIC CCN-STIC 801* aclara y delimita los distintos roles establecidos en el ENS, el RGPD y la LOPD en materia de seguridad de la información.

En cuanto a las responsabilidades de las partes y el cumplimiento legal, el CSP queda obligado a cumplir todas las medidas del Anexo II del ENS que sean pertinentes. En este sentido la *Guía de seguridad de las TIC CCN-STIC 823* (2020), proporciona orientación detallada respecto al cumplimiento de medidas de seguridad, enfatizando la identificación de responsabilidades del organismo usuario, las exclusivas del CSP o las responsabilidades compartidas.

5.2. Soluciones y servicios prestados por el sector privado a entidades públicas

Además de los aspectos señalados en el apartado anterior, la *Guía de Seguridad de las TIC CCN-STIC 809 Declaración y certificación de conformidad con el ENS y distintivos de cumplimiento* señala:

"40. Como se ha señalado con anterioridad, es muy frecuente que las organizaciones del sector privado participen en la provisión de soluciones tecnológicas o en la prestación de servicios a las entidades públicas (a través, por ejemplo, de servicios en la nube).

41. **Cuando las organizaciones del sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del ENS, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el ENS** (cuando se trate de sistemas de categoría BÁSICA) **o la Certificación de Conformidad con el ENS** (obligatoriamente, cuando se trate de sistemas de categorías MEDIA o ALTA, y de aplicación voluntaria en el caso de sistemas de categoría BÁSICA), **utilizando los mismos procedimientos que los exigidos para las entidades públicas**.

42. Es **responsabilidad de las entidades públicas contratantes** notificar a los operadores del sector privado que participen en la provisión de soluciones tecnológicas o la prestación de servicios, la obligación de que tales soluciones o servicios sean conformes con lo dispuesto en el ENS y posean las correspondientes Declaraciones o Certificaciones de Conformidad, según lo señalado en esta Guía.

43. Cuando la provisión de las soluciones o la prestación de los servicios sujetos al cumplimiento del ENS sean realizados por organizaciones del sector privado, estas utilizarán los mismos modelos documentales utilizados para las Declaraciones, las Certificaciones o los Distintivos de Conformidad recogidos en la presente Guía, sustituyendo las referencias a las entidades públicas por las correspondientes a las entidades privadas. Análogamente, los Distintivos de Conformidad, cuando se exhiban por parte de dichos operadores privados, deberán enlazar con las correspondientes Declaraciones o Certificaciones de Conformidad, que permanecerán siempre accesibles en la página web del operador de que se trate.

44. Además del Centro Criptológico Nacional, las entidades públicas usuarias de soluciones o servicios provistos o prestados por organizaciones del sector privado que exhiban una Declaración o Certificación de Conformidad con el ENS podrán solicitar en todo momento a tales operadores los Informes de Autoevaluación o Auditoría correspondientes, al objeto de verificar la adecuación e idoneidad de las antedichas manifestaciones".

5.3. Aplicación del ENS en sistemas Cloud Privados y Comunitarios en modo local

En diciembre de 2019 se publicó la guía *CCN-STIC-886 Perfil de cumplimiento específico para Sistemas Cloud Privados y Comunitarios.* Este perfil será de aplicación en sistemas alojados en infraestructuras propias de la entidad auditada, que tenga la categoría de seguridad MEDIA y se trate de un servicio PaaS.

Según el CCN se hace necesario[9] establecer unos requisitos de seguridad adicionales en los sistemas de información, que originalmente hubieran sido desplegados como soluciones en la nube, instalados en modo local por entidades proveedoras y así garantizar la seguridad de los sistemas implicados y velar por el cumplimiento de los requisitos establecidos en el ENS.

Requisitos de seguridad del proveedor

Las entidades del sector público que requieran la contratación en modo local de un proveedor de servicios, que afecte a sus sistemas de información, deberán exigir al proveedor la adecuación al ENS del sistema instalado en modo local y su consiguiente Declaración o Certificación de Conformidad, según la categoría de seguridad que la entidad contratante haya determinado para la correcta operación de los sistemas concernidos.

En aquellos casos que no existiese ningún proveedor que disponga de la Declaración o Certificación de Conformidad de los sistemas que prestan el servicio, se dará un plazo de dos (2) meses para iniciar el Procedimiento de Adecuación con el ENS y se definirán las medidas técnicas que es obligatorio que cumplan los sistemas implicados para poder comenzar a prestar el servicio.

Tanto los requisitos relativos a la adecuación del ENS del sistema del proveedor como las medidas que es necesario cumplir, en el caso de no disponer de una Declaración o Certificación de Conformidad, **deberán aparecer reflejadas en el PPT** publicado por la entidad contratante.

Requisitos de seguridad de la entidad contratante

El sistema a instalar en modo local, que presumiblemente interactuará con un sistema previamente configurado de manera segura y conforme con el ENS, deberá formar parte del Análisis de Riesgos del

9 Para más información consultar el documento del CCN *Requisitos de Seguridad Adicionales para Soluciones en la Nube (SaaS) implementadas en Modo Local.*

sistema global y tener en cuenta el resto de acciones contempladas en los Procedimientos de Gestión y Autorización de Cambios de la entidad contratante.

La entidad contratante deberá realizar un Análisis de Riesgos contemplando todos los aspectos de los sistemas con los que interactuará el sistema instalado en modo local y valorar las salvaguardas a aplicar para minimizar el riesgo, siendo este riesgo aceptado por la autoridad responsable de la entidad contratante. Si la entidad contratante quiere que el citado Análisis de Riesgos lo realice el proveedor, deberá reflejarlo en el PPT publicado por la misma.

Requisitos de seguridad adicionales

Una vez garantizada la seguridad en los sistemas implicados (sistema propio de la entidad contratante y sistema contratado en modo local) se deberán establecer ciertos requisitos de seguridad adicionales que cubran las necesidades propias de los sistemas en modo local y satisfagan los controles requeridos en el ENS. Este tipo de necesidades adicionales de seguridad se dan principalmente en dos niveles:

- en la configuración y administración del sistema,
- y en el uso del sistema por parte de los usuarios finales.

Es importante determinar las responsabilidades que son propias del usuario al utilizar el servicio/aplicación y las que son del proveedor. Todo ello permitirá concretar y determinar cómo deben operarse este tipo de sistemas instalados en modo local, salvaguardando los requisitos de seguridad y no poniendo en riesgo la adecuación al ENS.

5.4. Aplicación del ENS en sistemas SaaS en modo local

La guía *CCN-STIC 858 Implantación de sistemas SaaS en modo local (on-premise*), proporciona una propuesta de reparto de la responsabilidad de implantar las correspondientes medidas de seguridad, estableciendo de manera preliminar aquellas que deben ser implantadas por la entidad y aquellas que deberá implantar el CSP.

Mientras que en las soluciones prestadas desde la nube las medidas de seguridad corresponden casi en exclusiva al prestador del servicio, en las soluciones implantadas en modo local desde las instalaciones del cliente, las medidas de seguridad se reparten entre ambos: proveedor que suministra y organización cliente que contrata.

El Anexo I de la guía *CCN-STIC 858* contiene una propuesta de reparto de la responsabilidad de implantar las correspondientes medidas de seguridad, que deberá acomodarse a cada caso en particular. Adicionalmente, la guía considera parte de la responsabilidad del proveedor de la solución que entregue a su cliente tres guías diferenciadas:

- la guía de instalación, dirigida a los administradores del Sistema de Información del cliente que contrata, para posibilitar la integración del sistema en la infraestructura tecnológica del cliente.
- la guía de uso seguro, dirigida a los usuarios del sistema con objeto de que estos dispongan de todos los recursos necesarios para hacer un uso seguro de este.
- y la guía de relación entre proveedor y cliente, que deberá contener recomendaciones para la gestión de la relación entre el proveedor de la solución y el cliente contratante.

5.5. Decálogo de recomendaciones para la utilización de servicios en la nube

La nueva guía CCN-STIC-823 (2020) establece el siguiente decálogo que por su interés y sencillez reproducimos textualmente, aunque son materias tratadas con detalle en la presente GPF-OCEX 1403:

1. Determinar la categoría del sistema (BÁSICA, MEDIA o ALTA) que soportará la solución en la nube, según el ANEXO I del Real Decreto 3/2010.

2. Elaborar la declaración de aplicabilidad, según el ANEXO II del Real Decreto 3/2010.
3. Realizar un análisis de riesgos, para identificar requisitos adicionales de seguridad, que se reflejarán en la declaración de aplicabilidad.
4. Acogerse a un Perfil de Cumplimiento Específico (en caso de que sea de aplicación).
5. Establecer las condiciones contractuales, con carácter previo a la contratación, en los pliegos y/o peticiones de oferta.
6. En las condiciones contractuales, además de las relativas al cumplimiento de requisitos legales, detallar aspectos relativos al servicio, su infraestructura, el dimensionamiento, los registros de actividad, la gestión de incidentes, copias de seguridad, etc. y establecer condiciones relativas a la finalización del servicio.
7. Supervisar el cumplimiento, por parte del CSP, de los requisitos legales establecidos en las condiciones de contratación.
8. Realizar un seguimiento periódico del cumplimiento de los Acuerdos de Nivel de Servicio (SLA), establecidos con el CSP.
9. Planificar revisiones periódicas de la información, que el CSP proporciona a través de diversos mecanismos, como por ejemplo los registros de actividad, la capacidad, el almacenamiento, etc.
10. Elabora una normativa de seguridad específica para los usuarios de la nube.

Tanto para la contratación de un servicio de computación en la nube como para su fiscalización es de lectura obligada la citada guía CCN-STIC-823 (2020).

6. Consideraciones al fiscalizar la contratación de un servicio de computación en la nube

En las auditorías de los OCEX un área recurrente es la fiscalización de la contratación. Los contratos de servicios de computación en la nube suelen ser significativos tanto por su valor estimado como por su objeto y posiblemente sean seleccionados para su revisión. En estos expedientes, además de las cuestiones que con carácter general se deben tener en consideración al fiscalizar un contrato de servicios, al tratarse de servicios de computación en la nube hay que tener en cuenta los aspectos que se mencionan a continuación.

Con carácter previo a la contratación y tal y como se describe en la g*uía de seguridad de las TIC CCN-STIC 823* (2020), será necesario que la entidad identifique los requisitos de seguridad a solicitar al CSP. Resulta especialmente relevante el establecimiento de responsabilidades y obligaciones del CSP y del organismo contratante respecto a la implantación de medidas, mediante el análisis detallado de la declaración de aplicabilidad, identificando las medidas que son responsabilidad exclusiva del CSP o compartida.

Los pliegos y el contrato deben recoger con claridad las responsabilidades del proveedor y los niveles de seguridad de la información y los servicios afectados, de forma que el proveedor aplique las medidas de seguridad oportunas en cumplimiento de las diferentes leyes y normativas que le sean de aplicación.

Además, es muy importante que el contrato (en los pliegos) contemple de **forma explícita** cómo la entidad contratante, que es **la responsable** de los posibles riesgos que afecten a la información y a los servicios prestados, va a controlar la forma de prestar tales servicios por el CSP. Para ello se deben definir con precisión las características del servicio y establecer acuerdos de nivel de servicio para definir la calidad del servicio contratado, tal y como se recoge el apartado *[op.ext.1] Contratación y acuerdos de nivel de servicio* del Anexo II del ENS y en el apartado *C.5 Servicios Externos* de la GPF-OCEX 5330.

Para garantizar el cumplimiento de las medidas de seguridad aplicables, la entidad deberá disponer del **derecho de auditoría sobre el CSP** y exigir:

- Certificación de conformidad con el ENS (ver apartado 5.2 anterior).
- Auditoría que verifique con evidencias el cumplimiento de las medidas del Anexo II del ENS que sean de aplicación de acuerdo con la categoría de seguridad del sistema (el ENS es aplicable a una empresa privada contratada por un ente público).
- Auditorías de cumplimiento de la LOPD para satisfacer requisitos de seguridad de información.
- Otras certificaciones o acreditaciones en materia de seguridad en función de la actividad de la entidad y de los datos almacenados (por ejemplo, la auditoría de PCI/DSS[10], ISO 27000 de Gestión de Seguridad de la Información, etc.).
- Informes de auditoría tipo 1 o tipo 2 (se explican en el apartado 7 más adelante).

Cuando no se recoja esta exigencia en los pliegos de cláusulas administrativas particulares (PCAP) o en los pliegos de prescripciones técnicas (PPT) deberemos considerarlo un **grave defecto de control interno** y **un incumplimiento del ENS**, tanto más grave cuanto más crítico o relevante sea el sistema o servicio afectado.

Asimismo, siempre que la prestación de servicios en la nube albergue **datos de carácter personal**, deberán cumplirse, además de los requisitos establecidos por el ENS (DA 1ª LOPDP), todos aquellos exigidos por la normativa en materia de protección de datos. Para más detalle sobre esta materia puede consultarse el apartado 2.2.3 de la guía CCN-STIC-823 (2020).

En los pliegos correspondientes a los contratos cuya ejecución implique la cesión de datos por las entidades del sector público al contratista será obligatorio el establecimiento de una condición especial de ejecución que haga referencia a la obligación del contratista de someterse a la normativa nacional y de la Unión Europea en materia de **protección de datos**, advirtiéndose además al contratista de que tiene el carácter de obligación contractual esencial.

Por otra parte, según la redacción vigente en el momento de aprobarse esta guía, el artículo 122. 2 de la Ley de Contratos del Sector Público, exige en aquellos contratos cuya ejecución requiera el tratamiento por el CSP de datos personales por cuenta del responsable del tratamiento (la entidad contratante), que en el pliego se haga constar, entre otras cuestiones:

- La obligación del futuro contratista de someterse en todo caso a la normativa nacional y de la Unión Europea en materia de protección de datos.
- La obligación de la empresa adjudicataria de presentar antes de la formalización del contrato una declaración en la que ponga de manifiesto **dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos**. Y la obligación de comunicar cualquier cambio que se produzca al respecto, a lo largo de la vida del contrato.
- La obligación de los licitadores de indicar en su oferta, si tienen previsto subcontratar los servidores o los servicios asociados a los mismos, el nombre o el perfil empresarial, definido por referencia a las condiciones de solvencia profesional o técnica, de los subcontratistas a los que se vaya a encomendar su realización.

Estas obligaciones en todo caso deben ser calificadas como esenciales a los efectos de ser consideradas como causa de resolución del contrato.

Por tanto, dado que en la contratación de un servicio de computación en la nube muchos de los aspectos que determinarán la seguridad de la información y el cumplimiento legal y regulatorio

10 PCI DSS – Payment Card Industry Data Security Standard. Normativa que han de cumplir las entidades que procesen o almacenen datos de tarjetas bancarias.

vendrán determinados por lo recogido en el contrato del servicio (pliegos), la revisión de éste es un punto fundamental en el trabajo de auditoría, con efecto tanto en el control interno como en el cumplimiento legal.

Aunque es un aspecto más técnico, otro aspecto importante al revisar contratos cloud es verificar que exista un adecuado conjunto de indicadores para medir el servicio prestado o *Service Level Agreements* (SLA). La incorporación de SLA en un contrato de computación en la nube es importante porque garantiza que los servicios se realizan en los niveles especificados en el contrato, puede contribuir significativamente a evitar conflictos y puede facilitar la resolución de un problema antes de que se convierta en una disputa. Un SLA típico describe los niveles de servicio mediante varios atributos, como la disponibilidad, la capacidad de servicio o el rendimiento, y especifica los umbrales y las sanciones financieras asociadas con el incumplimiento de estos umbrales. Puede consultarse a este respecto el documento *Cloud Service Level Agreement Standardisation Guidelines*[11], elaborado en 2014 como parte de la *Commission's European Cloud Strategy*.

En el **Anexo 2** se incluye una guía para realizar la revisión de los pliegos de contratación.

7. Consideraciones que deben realizarse en una auditoría financiera

7.1. Consideraciones generales

Un auditor debe, como parte esencial de sus procedimientos de auditoría financiera, conocer el sistema de información y de control interno de la entidad auditada, identificar riesgos y controles, incluidos los TIC, y diseñar y ejecutar las pruebas pertinentes. En la medida que alguna de las áreas significativas para la auditoría (por ejemplo, la gestión tributaria en un ayuntamiento, las nóminas o la gestión económica y contable en una entidad) se gestione mediante aplicaciones en la nube, el auditor deberá adaptar convenientemente sus procedimientos para tener en cuenta las características y riesgos específicos de este entorno tecnológico. Un entorno de computación en la nube no es sino una particularidad de un entorno TIC, con sus características y riesgos específicos.

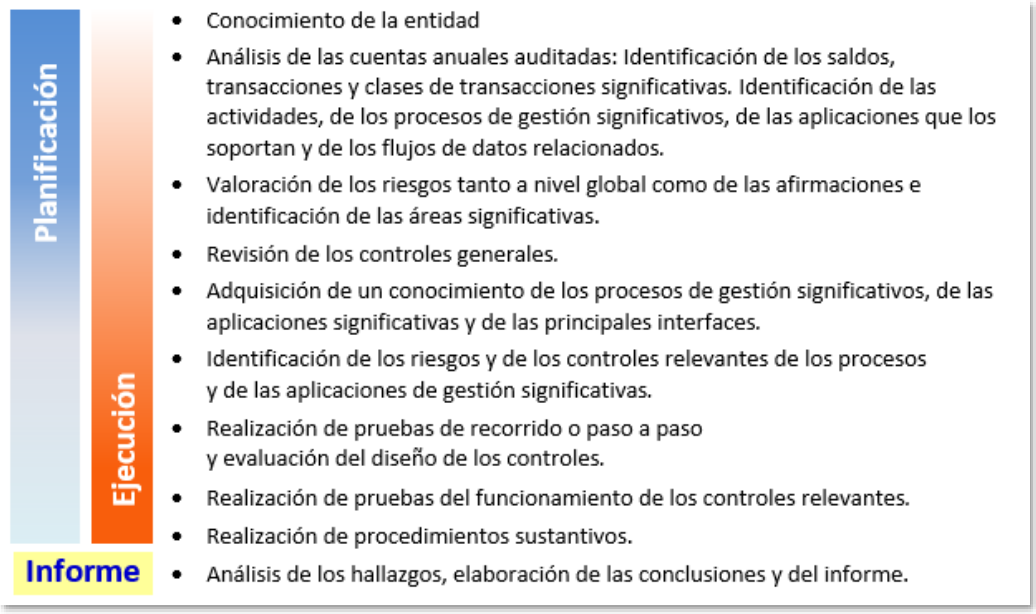
De acuerdo con el enfoque de riesgo y lo previsto en la *NIA-ES-SP 1315/GPF-OCEX 1315 Identificación y valoración de los riesgos de incorrección material mediante el conocimiento de la entidad y de su entorno*, el auditor deberá tener en cuenta en cada etapa de la auditoría el efecto sobre su trabajo del hecho de que una parte de la gestión del ente auditado esté soportada mediante sistemas TI y, si fuera el caso, mediante el procesamiento en la nube.

Los servicios de computación en la nube o cloud computing son un caso particular de los servicios contemplados en la ***NIA-ES-SP 1402 Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios***. Su amplia y creciente utilización en el sector público aconseja la elaboración de la presente guía, en la que se exponen sus principales características y las consideraciones que se deben realizar en una fiscalización. La lectura de esta GPF-OCEX 1403 es complementaria de la NIA-ES-SP 1402, y no ha de sustituir el análisis profundo ni el obligado conocimiento de la NIA-ES-SP 1402 por parte del auditor público.

La NIA-ES-SP 1402 y la GPF-OCEX 1403 se aplican cuando una entidad auditada (usuaria) recibe servicios de computación en la nube de otra entidad (organización de servicios, entidad prestadora o CSP) relacionados con aquellas áreas significativas de la entidad (contabilidad, compras, nóminas, ingresos, etc.) en las cuales el auditor tiene que valorar el riesgo, aplicar procedimientos de auditoría, revisar el sistema de control interno y obtener evidencia de auditoría, en definitiva, aplicar lo previsto en la NIA-ES-SP/GPF-OCEX 1315 y en la NIA-ES-SP 1330.

11 https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines

El objetivo de una auditoría financiera no varía por el hecho de que una entidad tenga varios servicios y aplicaciones significativas operando en la nube mediante un contrato de servicios con un CSP. Con carácter general, el desarrollo de la auditoría con enfoque de riesgo debe seguir las siguientes etapas[12]:



La auditoría en entornos de computación en la nube debe orientarse en principio a la evaluación de riesgos y controles derivados de su uso por el ente auditado y al grado de seguridad (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) que proporciona el sistema de control interno para la elaboración de la información financiera.

Será necesario concretar qué sistemas van a revisarse. Por tanto**, en la planificación de cada trabajo de revisión de entornos de computación en la nube se definirá el alcance concreto del mismo, de** acuerdo con los objetivos de la auditoría.

Los principales aspectos de una auditoría financiera que se ven afectados por un entorno cloud son:

a) El conocimiento de la entidad auditada, de sus sistemas de información y de control interno.

b) La identificación y valoración de riesgos.

c) La evaluación del sistema de control interno (CGTI + controles aplicación).

d) Las características de la evidencia de auditoría y los procedimientos para obtenerla.

e) Las competencias del equipo auditor y el uso de especialistas.

f) El análisis de los hallazgos y la evaluación de las deficiencias de control interno observadas.

7.2. Conocimiento de la entidad auditada, de sus sistemas de información y de control interno

Un paso fundamental en la etapa de planificación consiste en lograr un conocimiento profundo de la actividad del ente auditado y de su entorno, a partir de la comprensión en profundidad de la naturaleza de su actividad y sus operaciones. Se seguirá en esta fase lo previsto en la *GPF-OCEX 1316 El conocimiento del control interno de la entidad*.

Se deben conocer y entender los sistemas de contabilidad y control interno afectados por el entorno TIC. En esta fase también son de aplicación los apartados 9 a 13 de la NIA-ES-SP 1402. El auditor debe adquirir una clara comprensión del proceso de gestión auditado y conocer qué parte de este y qué

12 Según el esquema general reflejado en el Anexo 4 de la GPF-OCEX 1315 (18/11/2015)

actividades se realizan directamente por la entidad auditada, y cuáles son los servicios prestados por el proveedor de servicios en la nube, qué aplicaciones significativas hay en la nube e identificar las interfaces significativas.

El conocimiento adquirido se documentará mediante narrativas y flujogramas. Incluirá dónde se almacenan los datos, los controles existentes, en quién recae la responsabilidad de su ejecución (entidad usuaria o CSP) y cómo se puede acceder a ellos para realizar muestreos, análisis de datos y todo tipo de pruebas.

Se indagará sobre el tipo y modo de despliegue del servicio cloud contratado, profundizando en la relación contractual establecida entre cliente y CSP y la distribución de responsabilidades. Es importante conocer los aspectos anteriores ya que condicionan de forma determinante los riesgos a considerar por el auditor.

Se deberá mantener una reunión con los responsables de la entidad para explicar el trabajo que se va a realizar, solicitando la documentación necesaria al Responsable de Seguridad de la entidad auditada, quien deberá estar presente en la reunión.

7.3. Identificación y valoración de riesgos

El auditor de la entidad usuaria valorará si la existencia de la entidad prestadora de servicios aumenta o disminuye el riesgo de incorrección material (por ejemplo, al ser la prestadora una organización especializada, pueden reducirse riesgos de ciberseguridad; sin embargo, éste puede verse aumentado cuando el servicio se ha exteriorizado buscando abaratar los costes y se ha desmantelado un servicio propio de la usuaria, y ésta no disponga de medios para supervisar el contrato de servicios de computación en la nube).

Para poder valorar el riesgo y aplicar la NIA-ES-SP/GPF-OCEX 1315 el auditor de la entidad usuaria habrá de:

- Conocer la naturaleza del servicio recibido y el efecto en las áreas y materias objeto de la auditoría, incluyendo el control interno.
- Considerar la naturaleza y materialidad de las transacciones involucradas, controladas por la prestadora del servicio.
- Tener en cuenta el control interno de la entidad usuaria en relación con los servicios o tareas externalizados.
- Valorar la evidencia obtenida para la identificación de riesgos.

Se identificarán los riesgos y los controles de la forma prevista en la GPF-OCEX 1316, teniendo en consideración el efecto del tipo de servicio de computación en la nube y el modo de despliegue que se utilice.

A partir del conocimiento obtenido, el auditor estará en condiciones de valorar el riesgo de auditoría del cliente; esto implica comprender las condiciones —internas y del entorno— que amenazan la habilidad de la organización para ejecutar debidamente su proceso de gestión y alcanzar sus objetivos.

El auditor debe identificar los “riesgos significativos”, aquellos que representan riesgo de incorrección material en los estados contables, ya que no todos los riesgos de negocio son relevantes para el auditor. Los riesgos significativos deben ser valorados en dos niveles: riesgos de incorrección material a nivel de estado financiero (riesgos globales o generales) y a nivel de las afirmaciones para las clases de transacciones, saldos de cuentas y revelaciones.

Se deben identificar únicamente aquellos que fueran significativos para la auditoría financiera dentro del conjunto amplio de riesgos que representa la computación en la nube. Así pues, además de los

riesgos inherentes a la actividad del ente se deberán considerar los riesgos señalados en el apartado 4 anterior y su efecto en la auditoria que se esté realizando.

En general, el riesgo de auditoría es creciente conforme se incrementa la complejidad del entorno informatizado.

Al realizar la reunión del equipo para analizar riesgos y al documentarla según el Anexo 3 de la GPF-OCEX 1315 se deberá señalar si alguna de las aplicaciones significativas se ejecuta en la nube y sus implicaciones en la auditoría.

La estrategia del auditor de la entidad usuaria para valorar el riesgo derivado del uso de computación en la nube y la eficacia de los controles consistirá en[13]:

- Tratar de obtener evidencia de los procedimientos de control interno sobre los servicios externalizados que tiene establecidos la propia entidad usuaria. Por ejemplo, la usuaria es la que autoriza todas las transacciones y la de servicios quien las contabiliza, siendo en este sentido la prestadora del servicio un mero instrumento.
- Obtener evidencia en la entidad prestadora del servicio (CSP):
  - Obteniendo informe tipo 1[14] (descripción de los controles preparados por la organización de servicios con opinión del auditor de dicha organización de servicios).
  - Obteniendo informe tipo 2[15] si lo hubiere (informe elaborado por el auditor de la organización de servicios opinando sobre la descripción de los controles y la eficacia operativa, así como descripción de las pruebas sobre controles realizadas).
  - Obteniendo información específica, a través de la entidad usuaria, sobre la prestadora del servicio.
  - Visitando y aplicando procedimientos sobre la prestadora del servicio.
- Recurriendo a otro auditor a fin de que aplique determinados procedimientos.

7.4. Revisión de los controles generales de TI (CGTI) y de los controles de aplicación

Una vez obtenido un adecuado conocimiento del ente a auditar e identificados y valorados los riesgos significativos, el auditor debe evaluar el diseño e implementación de los controles internos relevantes que sirven para prevenir, detectar o corregir los riesgos o errores relacionados con los servicios

13 Ver Nota explicativa de la NIA-ES-SP 1402.

14 De acuerdo con la NIA-ES-SP 1402, se entiende por "**informe tipo 1**" aquel informe sobre la descripción y el diseño de los controles del CSP, que comprende tanto:

- una descripción preparada por la dirección del CSP del sistema de la organización de servicios (CSP), de los objetivos de control y de otros controles relacionados que se han diseñado e implementado en una fecha determinada;
- un informe elaborado por el auditor del CSP, con el objetivo de alcanzar una seguridad razonable, que incluya su opinión sobre la descripción del sistema de la organización de servicios, de los objetivos de control y otros controles relacionados, así como de la idoneidad del diseño de los controles para alcanzar los objetivos de control especificados.

15 De acuerdo con la NIA-ES-SP 1402, se entiende por "**informe tipo 2**" aquel informe que contiene tanto:

- una descripción, preparada por la dirección del CSP, del sistema del CSP, de los objetivos de control y otros controles relacionados que se han diseñado e implementado en una fecha determinada o a lo largo de un período específico y, en algunos casos, su eficacia operativa a lo largo de un período específico;
- un informe elaborado por el auditor del CSP con el objetivo de alcanzar una seguridad razonable, que incluya su opinión sobre la descripción del sistema de la organización de servicios, de los objetivos de control y otros controles relacionados, así como la idoneidad del diseño de los controles para alcanzar los objetivos de control especificados **y la eficacia operativa** de dichos controles; y una descripción de las pruebas de controles realizadas por el auditor y de los resultados obtenidos.

prestados por el CSP, incluidos los que se aplican a las transacciones procesadas por el CSP[16], valorar el riesgo de control y determinar el enfoque de auditoría a aplicar (de cumplimiento o sustantivo).

El auditor obtendrá información referida al diseño e implementación de los controles y valorará el nivel de riesgo preliminar, en función del cual decidirá si es conveniente continuar con el testeo de los controles mediante pruebas que permitan evaluar su eficiencia operativa, aplicando un enfoque de cumplimiento si el riesgo de control es bajo o aplicando un enfoque sustantivo, cuando el riesgo de control sea muy alto.

Dicho análisis debe ser realizado para dos categorías de controles, los CGTI y los controles de aplicación, evaluándolos en ese orden, en la medida en que el mal funcionamiento de los primeros invalida los segundos.

La **revisión de los CGTI** será análoga al trabajo que se realiza cuando se auditan los sistemas de información en el marco de una auditoría financiera en una entidad que no utiliza servicios de computación en la nube. Es decir, se debe aplicar la GPF-OCEX 5330, *Revisión de los CGTI en un entorno de administración electrónica*, sobre los relacionados con las áreas significativas para la auditoría. Pero cuando el ente auditado haga uso de servicios de computación en la nube, se adaptará el trabajo anterior en dos aspectos principales:

- El alcance de la revisión de los CGTI incluirá los controles que, en función de la categoría de servicio (IaaS/PaaS/SaaS), sean responsabilidad directa de la entidad auditada.

  El Anexo 1 incluye una guía general para realizar esta tarea, si bien hay que tener en cuenta que ésta deberá ser adaptada convenientemente en función de las características propias de los sistemas de TI y el entorno cloud presente en cada entidad.

- Se deberá prestar especial atención a la revisión del contrato del servicio cloud y al seguimiento del cumplimiento de los indicadores de nivel de servicio establecidos en éste, tal y como se ha indicado en apartados anteriores de esta guía. La supervisión del cumplimiento de los requisitos legales y acuerdos de nivel de servicio establecidos en las condiciones de contratación, se encuentran específicamente incluidos en el decálogo de recomendaciones para la utilización de servicios en la nube de la guía CCN-STIC-823 (2020). En el Anexo 2 se incluye un programa de trabajo orientativo para facilitar esta revisión.

Por último, cabe señalar que determinadas comprobaciones de los CGTI podrán darse por cumplidas si el CSP dispone de auditorías de seguridad (ENS, protección de datos), tal como se señala en la GPF-OCEX 5330, o si se dispone de informes de auditoría **tipo 2**, con los requisitos que establece el párrafo 17 de la NIA-ES-SP 1402.

En la revisión de los **controles de aplicación** y de las **interfaces** se seguirá la metodología ordinaria (GPF-OCEX 5340), teniendo muy en cuenta los riesgos derivados de su gestión en la nube.

7.5. Consideraciones adicionales en relación con la utilización de servicios compartidos o nubes comunitarias realizadas por la *Guía de Seguridad CCN-CERT IC-01/19 ENS: Criterios adicionales de Auditoría y Certificación*

Con relativa frecuencia encontraremos situaciones en las fiscalizaciones de los OCEX, por ejemplo, cuando se audita el presupuesto de ingresos de un ayuntamiento de menos de 20.000 habitantes cuya gestión tributaria y recaudatoria es realizada por la nube de una diputación provincial, la cual no dispone del certificado de conformidad con el ENS. Si se trata de un área significativa deberíamos disponer de dicha certificación (o alternativamente de un informe tipo 2, lo que en general será menos probable. La referida guía del CCN señala lo siguiente:

16 Apartado 10 de la NIA-ES-SP 1402.

"3.8 EN RELACIÓN CON LA UTILIZACIÓN DE SERVICIOS COMPARTIDOS

35. En tanto los Servicios Compartidos ofrecidos por la AGE o, en su caso, por las Administraciones Territoriales competentes, que pudieran estar comprendidos en el alcance de la auditoría no dispongan de la preceptiva Certificación de Conformidad con el ENS, la Auditoría de Conformidad con el ENS deberá concentrarse solo en los servicios que puedan satisfacerse a través de los propios sistemas de información de la organización auditada (o en sistemas de información externos que posean la Certificación de Conformidad con el ENS o puedan ser auditados y certificados en tal sentido).

36. De no ser posible lo anterior, y cuando se trate de la utilización de Servicios Compartidos suministrados por la AGE o, en su caso, por las Administraciones Territoriales competentes, el alcance de la Certificación de Conformidad (y la subsiguiente Certificación de Conformidad) **habrá de señalar la parte que ha sido auditada, mencionando, expresamente, que la porción no auditada** (ACCEDA o GEISER, por ejemplo) **no se encuentra comprendida en tal alcance**.

37. No obstante, cuanto tales servicios compartidos logren la Certificación de Conformidad, la Entidad de Certificación podrá generar un nuevo Certificado de Conformidad, eliminando la precisión anterior."

Trasladado a nuestras fiscalizaciones, esta circunstancia implica una limitación al alcance en una auditoría financiera, tal como se señala en el apartado 9.2 siguiente o un párrafo aclaratorio del alcance en los informes mencionados en el apartado 9.4 sobre revisión del control interno.

8. Obtención de evidencia electrónica, uso de herramientas ADA[17] y de especialistas en ASI[18]

Las evidencias de auditoría comprenden toda la información utilizada por el auditor para alcanzar las conclusiones a partir de las cuales emite su informe, e incluyen tanto la información contenida en los registros contables de los que se obtienen los estados financieros, como otra información. A través de ellas, el profesional pretende determinar si la información auditada se presenta de acuerdo con el criterio establecido y si los estados financieros representan la imagen fiel.

Además, cuando se audite en un entorno en la nube **la práctica totalidad de la evidencia disponible será electrónica**. Se deberán aplicar los criterios de actuación en relación con este tipo de evidencia señalados en las guías prácticas de fiscalización de los OCEX.

No es posible la estandarización de procedimientos para la obtención, análisis y presentación de evidencias, debido a la diversidad de las arquitecturas de la nube y a que cada servicio es distinto a los demás, debiéndose adaptar los programas y procesos de obtención de evidencias a cada caso en particular

Aunque con carácter general es aplicable la NIA-ES-SP 1500 y la *GPF-OCEX 1503 La evidencia electrónica de auditoría*, hay diversos factores que afectan a la cantidad y detalle de las evidencias que podrán obtenerse durante la ejecución de una auditoría:

- Como ya se ha señalado, las cláusulas incluidas en el contrato afectarán al desarrollo de la auditoría. Puede acordarse con el proveedor el envío de informes del servicio, reportes de incidencias, informes de auditoría llevados a cabo por el proveedor, etc.
- El modelo de servicio también es un factor clave a la hora de obtener evidencias. En un modelo SaaS, las evidencias accesibles al auditor externo son más limitadas, sin que llegue a obtenerse demasiada información sobre la infraestructura que soporta el servicio, pero sí sobre el acceso a

17 Análisis de Datos de Auditoría.

18 Auditoría de Sistemas de Información

ésta. Sin embargo, un modelo IaaS, permitirá la obtención de evidencias más ricas sobre dicha infraestructura y su funcionamiento.

- A medida que la madurez de la organización en relación con el uso de servicios cloud aumenta, y la gobernanza cloud mejora, habrá una mayor cantidad de evidencias disponibles como fruto del control que la organización ejerce sobre el servicio.

Una vez considerados estos factores, se debe evaluar la cantidad y tipología de evidencias (electrónicas) disponibles durante la auditoría.

Para obtener las evidencias que soporten las conclusiones del informe, deben diseñarse pruebas de auditoría (respuestas a riesgos de incorrección material), que en función de la valoración del riesgo puede tratarse de pruebas sustantivas, de pruebas sobre controles o ambas. La orientación general de las pruebas (más pruebas de controles o más procedimientos sustantivos, dependerá de la confianza depositada en el control interno de la usuaria y de la prestadora). Algunas pruebas podrían ser:

- El examen de los documentos mantenidos por la entidad usuaria y examen de los controles disponibles en ella.
- El acceso directo (físico o electrónico) a la organización de servicios para comprobar los registros de la entidad usuaria y controles establecidos sobre ellos.
- Examen de los documentos disponibles en la entidad prestadora del servicio sobre la actividad externalizada. Esta posibilidad de examen o acceso debería ponerse como obligación en el contrato del servicio.
- Obtención de confirmaciones de la organización de servicios sobre saldos y transacciones.
- Aplicación de procedimientos analíticos sobre la usuaria o a los informes recibidos de la organización de servicios.
- Uso de herramientas y técnicas ADA.
- Utilización de expertos, auditores de sistemas de información.
- Utilización de otros auditores terceros (no se modifica la responsabilidad del auditor de la entidad usuaria) mediante procedimientos acordados entre entidad usuaria (incluyendo a su auditor) y la entidad prestadora (incluyendo a su auditor).
- Obtención de un informe tipo 2 del auditor de la entidad prestadora del servicio y además aplicar procedimientos sustantivos.

Al planificar las pruebas a realizar, el auditor debe evaluar la **disponibilidad** de la información para los fines de la auditoría y los riesgos específicos de su uso. La misma puede verse afectada por características propias de la evidencia electrónica, como la falta de visibilidad de los registros de auditoría por la inexistencia de soporte documental material de los archivos electrónicos.

Asimismo, debe evaluarse, considerando cómo se haya obtenido cada evidencia, su nivel de **fiabilidad**. Aunque una evidencia no se haya manipulado de manera malintencionada, sigue existiendo la posibilidad de que ésta no sea relevante o que el proceso de obtención no haya sido apropiado. El auditor deberá hacerse, por ejemplo, las siguientes preguntas para asegurarse de la fiabilidad y exactitud de la información:

- ¿Qué datos son usados para elaborar el informe recibido?
- ¿Qué aplicación ha procesado los datos?
- ¿Son efectivos los CGTI de la aplicación que ha procesado los datos y generado el informe?

- ¿Hemos verificado específicamente algún control sobre la completitud y exactitud de los datos utilizados? ¿Son efectivos?
- ¿Los datos o informe que nos han proporcionado pueden ser susceptibles de cambios manuales?

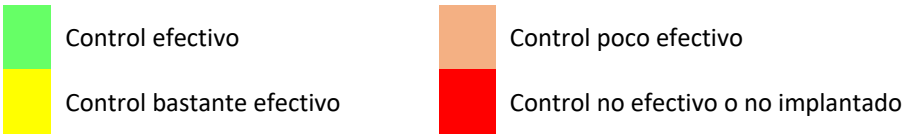
En la medida en que existe una cierta correlación entre el uso de computación en la nube y la existencia de cantidades masivas de datos, **se hace indispensable la utilización de herramientas ADA** para obtener, procesar y analizar la información disponible. Se aplicará la *GPF-OCEX 5370 Guía para la realización de pruebas de datos*. Además de hacer necesario el uso de estas técnicas y herramientas, la computación en la nube introduce dificultades adicionales para la utilización de ADA, ya que los **datos** están en posesión del CSP y el **modelo de datos**[19] puede que sea desconocido para la entidad auditada. No obstante, ambas cuestiones solo plantean dificultades transitorias, ya que el CSP está obligado a facilitarlas a la entidad y estos al OCEX. Esta circunstancia (la propiedad de los datos y el conocimiento del modelo de datos) debería estar prevista en los pliegos.

En general, dado el complejo entorno TIC, muchos de los procedimientos para revisar los controles y realizar las pruebas de datos (ADA) deberán ser llevados a cabo por personal especializado, idóneamente por **auditores de sistemas de información** que presten apoyo a los auditores. De no disponer de personal especializado en el OCEX se deberá estudiar la conveniencia de contratar a especialistas externos.

9. Evaluación de las deficiencias observadas e informe

9.1. Evaluación de las deficiencias de control interno

Cada control se evaluará en base a las evidencias obtenidas sobre su eficacia, pudiendo encontrarse cada uno de ellos en alguna de las siguientes situaciones, definidas en la GPF-OCEX 5330[20]:



Se seguirán los criterios de evaluación establecidos en el apartado *8. Evaluación de las deficiencias de control interno detectadas* de la GPF-OCEX 5330.

Dependiendo del tipo de auditoría (revisión de los controles como parte de una auditoría financiera o auditoría de los controles sobre el servicio cloud), el resultado del trabajo tendrá un reflejo distinto en el informe de auditoría.

9.2. Informe de auditoría financiera[21]

El auditor de la entidad usuaria expresará una opinión modificada en su informe de auditoría, de conformidad con la NIA-ES-SP 1705 R, si no puede obtener evidencia de auditoría suficiente y adecuada con respecto a los servicios prestados por el CSP que sean relevantes para la auditoría de estados financieros de la entidad usuaria (limitación al alcance). Esto puede deberse a:

- el auditor de la entidad usuaria no puede obtener conocimiento suficiente de los servicios prestados por la organización de servicios y no tiene una base suficiente y adecuada para identificar y valorar los riesgos de incorrección material;

19 Un modelo de datos consiste en una descripción de la estructura de una base de datos y de las relaciones existentes entre ellos.

20 Revisión de los Controles Generales de Tecnologías de la Información en el Anexo 4 apartado E

21 Apartado 20 de la NIA-ES-SP 1402.

- la valoración del riesgo por el auditor de la entidad usuaria parte del supuesto de que los controles de la organización de servicios funcionan eficazmente y el auditor de la entidad usuaria no puede obtener evidencia de auditoría suficiente y adecuada sobre la eficacia operativa de dichos controles; o
- la evidencia de auditoría suficiente y adecuada sólo está disponible en los registros mantenidos en la organización de servicios y el auditor de la entidad usuaria no puede obtener acceso directo a dichos registros.

La opinión será con salvedades o denegada dependiendo de la conclusión del auditor con respecto a si los posibles efectos sobre los estados financieros son materiales o generalizados.

9.3. Informe sobre el cumplimiento de la legalidad

Dada la relevancia creciente que están adquiriendo estos servicios y, en consecuencia, la dependencia cada vez mayor de los CSP, junto con los riesgos de ciberseguridad, la revisión de los contratos de servicios de computación en la nube, su licitación, adjudicación y ejecución, y los incumplimientos, en su caso, detectados deben reflejarse en los informes de fiscalización, considerando y evaluando cuidadosamente su significatividad.

Tal como se ha visto en apartados anteriores, los incumplimientos pueden referirse a la normativa de contratación, al ENS o a la LOPD.

9.4. Informe de control interno

Cuando se trate de una auditoría de los controles sobre el servicio cloud o sobre ciberseguridad, el informe deberá referirse a los hallazgos y conclusiones sobre la eficacia del control interno relacionado.

10. Bibliografía

Agencia Española de Protección de Datos

- Guía para clientes que contraten servicios de Cloud Computing

ASOCEX:

- GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa
- GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad
- GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica
- GPF-OCEX 1503 La evidencia electrónica de auditoría

Centro Criptológico Nacional:

- Guía de seguridad de las TIC CCN-STIC-801, Responsabilidades y funciones, mayo 2019
- Guía de seguridad de las TIC CCN-STIC-809 Declaración y certificación de conformidad con el ENS y distintivos de cumplimiento, junio 2019
- Guía de seguridad de las TIC CCN-STIC-823, Utilización de servicios en la nube, diciembre 2014
- Guía de seguridad de las TIC CCN-STIC-823, Utilización de servicios en la nube, septiembre 2020
- CCN-STIC-886 Perfil de cumplimiento específico para Sistemas Cloud Privados y Comunitarios, diciembre 2019

- Requisitos de seguridad adicionales para soluciones en la nube (SaaS) implementadas en modo local, enero 2020
- Guía de seguridad de las TIC CCN-STIC 858, Implantación de sistemas SaaS en modo local (on-premise), junio 2020
- Norma de Seguridad de las TIC CCN-STIC-220 Arquitecturas virtuales, julio2020
- Guía de Seguridad CCN-CERT IC-01/19 ENS: Criterios adicionales de Auditoría y Certificación

CIS Controls Cloud Companion Guide v7 (CIS, Center for Internet Security), 2019

Cloud Security Alliance (CSA, Spanish chapter)

- Guía de Seguridad de áreas críticas para computación en la nube, v4.0, 2018
- Cloud Audit & Forensics, 2018

Diccionario de términos y conceptos de la administración electrónica

RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Riesgos y amenazas en cloud computing, Instituto Nacional de Ciberseguridad de España (INCIBE)

National Institute of Standards and Technology

- The NIST Definition of Cloud Computing (NIST SP 800-145), septiembre de 2011
- Evaluation of Cloud Computing Services Based on NIST 800-145, (NIST SP 500-322), febrero 2018

NIA-ES-SP 1402 Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios

Cloud Service Level Agreement Standardisation Guidelines, 24 de junio de 2014, Comisión Europea

Anexo 1 Adaptación de los CGTI a entornos de computación en la nube

La siguiente tabla recoge un análisis general de la aplicabilidad de los CGTI a entornos en la nube, en función de la categoría del servicio (SaaS/PaaS/IaaS).

Para cada uno de los controles se indica si aplica (control marcado con "x") o bien si, por las características del control y del propio servicio cloud no se debe incluir en nuestro trabajo de revisión (controles señalados con "N/A"). Este último caso responde a aquellos controles que, por las propias características de la categoría del servicio, son realizados por el proveedor.

Este análisis, no obstante, constituye una base para realizar el trabajo de auditoría de los CGTI y los controles de ciberseguridad, pero deberá ser revisado y adaptado convenientemente al entorno TI del ente en función de sus características específicas, a partir del conocimiento de estas por parte del auditor.

Área	Control	SaaS	PaaS	IaaS	Comentarios
A. Marco Organizativo	A1 CLCS 8 Cumplimiento de Legalidad	x	x	x	Los controles del área A, al ser de naturaleza organizativa, se revisarán de igual forma tanto para entornos cloud como para entornos TI propios.
	A2 Estrategia de Seguridad	x	x	x	
	A3 Organización y Personal de TI	x	x	x	
	A4 Marco Normativo y Procedimental de Seguridad	x	x	x	
B. Gestión de Cambios en Aplicaciones y Sistemas	B1 Adquisición de Aplicaciones y Sistemas	x	x	x	El control B1, al ser un control más estratégico que operativo, aplica igual que en entornos en los que no se utilicen servicios cloud.
	B2 Desarrollo de Aplicaciones	N/A	x	x	
	B3 Gestión de Cambios	N/A	x	x	
C. Operaciones de los Sistemas de Información	C1 CBCS 1 Inventario y control de dispositivos físicos	N/A	x	x	
	C1 CBCS 2: Inventario y control de software autorizado	x	x	x	
	C2 CBCS 3 Proceso continuo de identificación y remediación de vulnerabilidades	N/A	x	x	En modo IaaS, la gestión de vulnerabilidades incluirá todos los componentes de la infraestructura salvo los específicos del HW. En modo PaaS, la entidad auditada será responsable de la gestión de vulnerabilidades del SW que instale en la plataforma proporcionada por el CSP.
	C3 CBCS 5 Configuraciones seguras del software y hardware	N/A	x	x	En modo IaaS, el proporcionar una configuración segura de la plataforma es responsabilidad del CSP (no la revisaremos) pero el configurar el SW de forma segura (tanto de aplicaciones como ciertas características del sistema operativo, bases de datos y otro middleware) sí se revisará, pues depende del ente auditado.

	C4 CBCS 6 Registro de la actividad de los usuarios	x	x	x	Aplica en todos los casos, pero con diferentes niveles de profundidad. En SaaS el ente auditado sólo será responsable de la gestión de los logs de actividad de los usuarios dentro de la aplicación, en PaaS se incluirá toda la gestión de los logs de todos los componentes que el cliente instale en la plataforma contratada al CSP e IaaS incluirá la gestión de los logs de todos los componentes (salvo los elementos de comunicaciones que facilite el CSP para dar conectividad a la infraestructura).
	C5 Servicios Externos	**x**	**x**	**x**	**La revisión de los subcontroles de este punto es FUNDAMENTAL cuando la entidad auditada haga uso de un entorno cloud, con independencia de la categoría del servicio (SaaS, PaaS e IaaS).**
	C6 Protección Frente a Malware	N/A	N/A	x	
	C7 Protección de Instalaciones e Infraestructuras	N/A	N/A	N/A	
	C8 Gestión de Incidentes	x	x	x	La gestión de incidentes que realice el CSP para garantizar el servicio contratado es responsabilidad del CSP y queda fuera del alcance del trabajo. Sin embargo, sí es crítico revisar que la entidad auditada tenga un procedimiento de gestión de incidentes y que éste contemple la coordinación con el CSP en modo bidireccional, es decir, para los incidentes que afecten al entorno cloud con independencia de que estos sean detectados por la entidad auditada o por el CSP.
	C9 Monitorización	N/A	x	x	En el caso de PaaS, la entidad auditada sólo será responsable de la monitorización a nivel de aplicación (si es que la tiene).
D. Controles de Acceso a Datos y Programas	D1 CBCS 4 Uso controlado de privilegios administrativos	x	x	x	Todos los controles del área D son de aplicación a un entorno cloud, con la única particularidad de que se debe circunscribir la revisión a los componentes que administre total o parcialmente el cliente. De esta forma, si el servicio cloud es un SaaS, la revisión se realizará sobre la gestión de usuarios y privilegios a nivel de aplicación que sea responsabilidad del cliente (es decir, el CSP siempre dispondrá de usuarios administradores de la aplicación, por ejemplo, para la realización de actualizaciones de la aplicación o cambios de configuración que no estarán disponibles para la entidad auditada y, por tanto, quedarán excluidas de nuestro trabajo de revisión). En caso de PaaS, se debe realizar la revisión completa a nivel de aplicación y de las opciones (autenticación, configuración de seguridad, etc.) que sean administradas por la entidad auditada. En caso de servicio de tipo IaaS, se revisarán todos los controles a todos los niveles, salvo en lo concerniente a aquellos asociados al hardware propiamente y las comunicaciones del CSP.
	D2 Mecanismos de Identificación y Autenticación	x	x	x	
	D3 Gestión de Derechos de Acceso	x	x	x	
	D4 Gestión de Usuarios	x	x	x	
	D5 Protección de Redes y Comunicaciones	x	x	x	
E. Continuidad del Servicio	E1 CBCS 7 Copia de seguridad de datos y sistemas	N/A	x	x	En modo SaaS, la continuidad del servicio deberá ser garantizada por el CSP y será responsabilidad del ente auditado el que esté adecuadamente reflejado por contrato y se realice seguimiento del cumplimiento de los SLAs definidos. En modo PaaS, el cliente deberá garantizar la continuidad del software que instale por encima de la infraestructura facilitada por el CSP. En modo IaaS, el cliente deberá garantizar la continuidad de todos los componentes de la pila tecnológica que instale en la infraestructura facilitada por el CSP, siendo éste únicamente responsable de la continuidad en lo que respecta al HW y las comunicaciones.
	E2 Plan de Continuidad	N/A	x	x	
	E3 Alta Disponibilidad	N/A	x	x	

ANEXO 2 Cuestiones a revisar en los contratos de servicios de computación en la nube

En el contrato se deben definir con precisión las características del servicio y las responsabilidades de las partes, además de establecer acuerdos de nivel de servicio para definir la calidad del servicio contratado. También recogerá los niveles de seguridad de la información y los servicios afectados, de forma que el proveedor aplique las medidas de seguridad oportunas.

Los pliegos (PCA/PPT) deben contener:

- Tipo de servicio: dependiendo de las necesidades de la organización se optará por un servicio IaaS, PaaS o SaaS.
- Tipo de infraestructura requerida por la organización, en función del nivel de seguridad requerido.
- Dimensionado del servicio: recursos que conformarán el servicio, sea cual sea el baremo para determinar la capacidad del servicio contratado (número de instancias software, de registros, usuarios concurrentes, cpu, datos…) que deberá figurar expresamente en el acuerdo, así como la capacidad de aumentar o disminuir la demanda y las herramientas para medir dicha capacidad de servicio y rendimiento.
- Subcontratación: cuando el proveedor contrata con un tercero los servicios. Las obligaciones del proveedor en materia de seguridad se transmiten de forma transitiva a las partes subcontratadas, en particular los niveles de seguridad de la información y servicios y deberá atender a los requisitos derivados del ENS.
- Protección de la información: el contrato debe determinar la propiedad de la información a la que va a tener acceso el proveedor, quien se comprometerá por contrato a mantener confidencialidad y a no divulgar o acceder de manera indebida y sin autorización expresa a dicha información. El proveedor queda obligado a no acceder ni utilizar la información a la que tenga acceso para fin alguno que no esté explicitado en el contrato o se autorice expresamente por escrito. El contrato deberá incluir una cláusula de encargado del tratamiento adecuada a la RGPD.
- En los pliegos correspondientes a los contratos cuya ejecución implique la cesión de datos por las entidades del sector público al contratista será obligatorio el establecimiento de una condición especial de ejecución que haga referencia a la obligación del contratista de someterse a la normativa nacional y de la Unión Europea en materia de protección de datos, advirtiéndose además al contratista de que esta obligación tiene el carácter de obligación contractual esencial de conformidad con lo dispuesto en la letra f) del apartado 1 del artículo 211 de la Ley 9/2017.
- En aquellos contratos cuya ejecución requiera el tratamiento de datos personales por cuenta del responsable del tratamiento (la entidad contratante), adicionalmente en el pliego se hará constar, entre otras cuestiones:
    - La obligación del futuro contratista de someterse en todo caso a la normativa nacional y de la Unión Europea en materia de protección de datos.
    - La obligación de la empresa adjudicataria de presentar antes de la formalización del contrato una declaración en la que ponga de manifiesto dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos. Y la obligación de comunicar cualquier cambio que se produzca al respecto, a lo largo de la vida del contrato.
    - La obligación de los licitadores de indicar en su oferta, si tienen previsto subcontratar los servidores o los servicios asociados a los mismos, el nombre o el perfil empresarial, definido por referencia a las condiciones de solvencia profesional o técnica, de los subcontratistas a los que se vaya a encomendar su realización.

  Estas obligaciones en todo caso deben ser calificadas como esenciales a los efectos de ser consideradas como causa de resolución del contrato.
- Acuerdos de nivel de servicio o SLA (Service Level Agreement): deberán acordarse unos niveles de servicio que reflejen aspectos referentes a capacidad (desviaciones de carga asumidas por el proveedor y tiempos de notificación cuando se detecte insuficiencia de recursos), disponibilidad (en función de la criticidad del servicio), continuidad (mediante la definición de tiempos de recuperación), gestión de incidentes y gestión de cambio. De cada SLA se definirán:
    - Parámetro: identificador del SLA.
    - Responsabilidades: quién recoge y facilita los datos necesarios para realizar los cálculos

  - Fórmula: descripción del cálculo para la obtención del SLA.
  - Periodicidad de la captura de datos, del cálculo de las métricas derivadas y de la verificación de umbrales de aviso y de alarma
  - Umbrales: valores mínimos en la prestación del servicio que disparan situaciones de aviso (hay que monitorizar) y de alarma (hay que corregir)
  - Penalización: procedimiento para determinar y cuantificar las consecuencias derivadas del incumplimiento de SLA.

- Mecanismos de acceso al servicio, que identifiquen el acceso de usuarios y administradores, y que garanticen la confidencialidad y la integridad de la información.
- Condicionantes geográficos, en función de la ubicación geográfica de los servidores y de la información.
- Responsabilidades y obligaciones: El contrato definirá los roles de las personas involucradas en la prestación del servicio, en el organismo y en el CSP. Ambas partes deberán considerar las siguientes responsabilidades mínimas:
  - Responsable de seguridad
  - Persona de contacto para incidentes de seguridad
  - Persona de contacto para cambios y mantenimiento de sistemas
  - Persona de contacto para incidencias relativas a los indicadores de servicio (SLA)
  - Persona de contacto para aspectos contractuales
  - Persona de contacto para temas jurídicos y regulatorios, en particular en lo relativo a datos de carácter personal
- Requisitos legales y cumplimiento del ENS: En los casos en que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración Pública de origen y se ajustarán al ENS.
- Derecho de auditoria: Para garantizar el cumplimiento de las medidas de seguridad aplicables, la entidad deberá disponer del **derecho de auditoría sobre el CSP** o exigir:
  - Declaración de aplicabilidad de medidas a aplicar.
  - Auditoría que verifique con evidencias el cumplimiento de las medidas del Anexo II del ENS que sean de aplicación de acuerdo con el nivel del sistema (el ENS es aplicable a una empresa privada contratada por un ente público).
  - Auditorías de cumplimiento normativo para satisfacer requisitos de seguridad de información.
  - Otras certificaciones o acreditaciones en materia de seguridad en función de la actividad de la entidad y de los datos almacenados (por ejemplo: PCI/PSS).
- Gestión de cambios: deberá definirse un procedimiento que coordine entre ambas partes el mantenimiento de los sistemas, para prevenir paradas o errores en el servicio. Dicho procedimiento incluirá aspectos como la notificación anticipada de paradas del servicio, así como notificaciones posteriores al mantenimiento. Siempre que el mantenimiento o actualización impliquen cambios de envergadura, el proveedor habilitará un entorno actualizado de preproducción, donde el cliente verificará el correcto funcionamiento de sus sistemas.
- Registro de actividad: la trazabilidad de las acciones es uno de los aspectos seguidos por el ENS. Se detallará el control de accesos a la información, autorizaciones y obligaciones del proveedor en cuanto al registro de la actividad sobre los servicios contratados.
- Gestión de incidentes: El proveedor deberá disponer de un procedimiento de gestión de incidentes [op.exp.7] que incluya la notificación de incidentes a la organización, tipos de incidentes, tiempos de respuesta y resolución, mantenimiento y gestión del registro de incidentes. Además, el proveedor deberá informar periódicamente de los incidentes que han afectado a los sistemas del cliente.
- Debe especificarse que el propietario de los datos es la entidad contratante, quien puede disponer de ellos solicitándolos al CSP.
- Debe especificarse que la entidad contratante tiene derecho a conocer el modelo de datos de la aplicación

- Respaldo y recuperación de datos: el proveedor deberá disponer de un procedimiento de copias que garantice la restauración de la información como describe la medida [mp.info.9]. El proveedor deberá informar al cliente de:
    - Alcance de los respaldos.
    - Política de copias de seguridad.
    - Medidas de cifrado de información en respaldo.
    - Procedimiento de solicitud de restauraciones de respaldo.
    - Realización de pruebas de restauración.
    - Traslado de copias de seguridad (si aplica).
- Continuidad del servicio: De acuerdo con la medida [op.cont.2] del ENS, se deberá disponer de medidas de continuidad del servicio. Se deberá solicitar al proveedor evidencia de la existencia de un plan de continuidad de negocio que incluya:
    - Alcance con los servicios objeto de la prestación.
    - Tiempos de recuperación identificados en el análisis de impacto y alineados con los criterios definidos en los SLAs.
    - Procedimiento de coordinación ante incidentes y desastres, que defina los flujos e interacciones cliente-proveedor durante la gestión de incidentes o desastres. El proveedor también deberá informar periódicamente de los incidentes que han afectado a los sistemas que soportan los sistemas del cliente.
    - Pruebas periódicas para validar el funcionamiento de los planes, cumplimiento de plazos y servicios mínimos previstos.
- Finalización del servicio y eliminación de información: El contrato especificará condiciones, procedimientos y plazos para una terminación pactada o por incumplimiento de los supuestos contractuales, que deberá especificarse en una cláusula junto al tiempo que tardará el proveedor en migrar los datos. Se buscará "neutralidad tecnológica" para facilitar dicha migración. Por último, deberá recogerse una cláusula o establecer un procedimiento sobre el tiempo que tardará el proveedor en realizar la destrucción efectiva de los datos y mecanismos a utilizar.

En el ANEXO I – Clausulado y Acuerdos a Nivel de Servicio de la guía CCN-STIC-823 (2020) se especifican en detalle los aspectos a incluir en los contratos de computación en la nube.

Control de versiones

Versión	Cambios
22-05-2020	GPF-OCEX 1403 aprobada por la Conferencia de Presidentes de ASOCEX
20-10-2020	Se actualiza la GPF-OCEX 1403. En septiembre de 2020 el Centro Criptológico Nacional (CCN) ha actualizado la Guía de seguridad de las TIC, *CCN-STIC-823, Utilización de servicios en la nube*, cuya versión anterior de 2014 se utilizó como fuente importante en la elaboración de la GPF-OCEX 1403. En consecuencia, se ha considerado conveniente la actualización de las referencias a dicha *CCN-STIC-823.* Aunque con menor incidencia, el CCN también ha actualizado en junio la Guía de seguridad de las TIC, CCN-STIC 858, Implantación de sistemas SaaS en modo local (on-premise). De acuerdo con lo anterior se han actualizado los siguientes puntos de la GPF-OCEX 1403: • Se añade un segundo párrafo a la definición de "nube híbrida" en el apartado 3.1. • Se actualiza el último párrafo del apartado 5.1. • Se añaden dos nuevos apartados, el 5.4 y el 5.5. • Se actualizan los párrafos segundo y cuarto del apartado 6. • Se actualiza el antepenúltimo párrafo del apartado 7.4. • Se actualiza la bibliografía incluyendo las dos nuevas guías del CCN. • Se añade un último párrafo al Anexo 2. • Varios aspectos puntuales de terminología y actualización de referencias a las nuevas guías del CCN.