Sección 5331 Guía básica de auditoría en entornos de computación en la nube

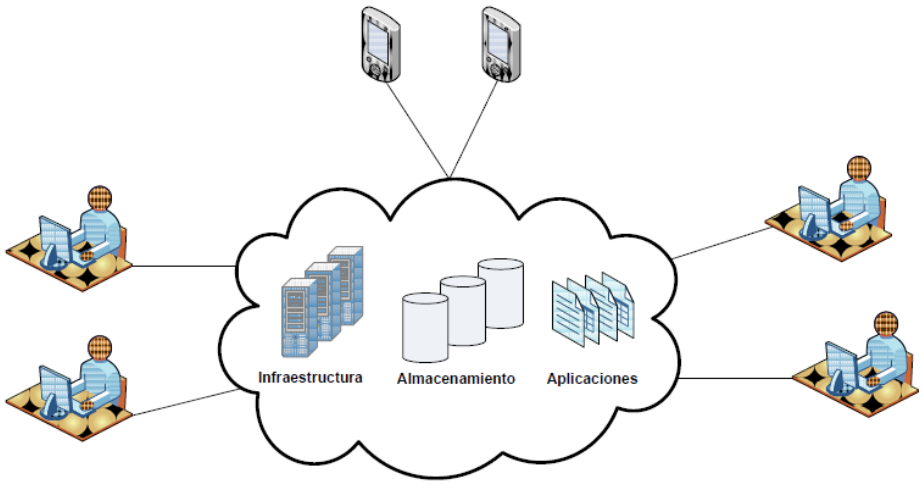
Referencia: GPF-OCEX 5330

Aprobada por el Consejo de la Sindicatura el 15/07/2019, a propuesta de la CTA de 05/07/2019

1. Introducción

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 a través de Internet desde diferentes dispositivos. Este hecho ha supuesto un importante auge en el uso de las tecnologías web como estándar, derivando también en la externalización de muchos sistemas de información.

Surge así el modelo de servicios en la nube[1], 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: CNN-STIC-823

Una de las definiciones de servicios en la nube con mayor aceptación es la propuesta por el NIST[2]: "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,

[1] De acuerdo al diccionario de términos y conceptos de la Administración Electrónica "la computación en la nube, conocida también como servicios en la nube, informática en la nube, nube de cómputo o nube de conceptos (del inglés 'Cloud Computing'), es un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet".

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

servidores, almacenamiento, aplicaciones y servicios) que pueden ser suministrados y desplegados rápidamente con una mínima gestión o interacción con el proveedor de servicio".

El modelo de computación en la nube o cloud computing se utiliza cada vez más. Ofrece a las organizaciones **grandes beneficios**[3], 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 usuarias y considerados en los trabajos de auditoría. Estos riesgos están relacionados fundamentalmente con la seguridad de la información procesada y almacenada en la nube.

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.

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 cloud**:

- Realizar una **auditoría específica** de uno o varios servicios cloud 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 cloud.
  - La evaluación del diseño, implementación y eficacia operativa de los controles que, en función de la categoría de servicio (IaaS/PaaS/SaaS), sean responsabilidad directa de la entidad auditada.

  Para realizar estas auditorías podrán utilizarse alguna de las guías señaladas en la bibliografía [4].
- Incluir la **revisión en el contexto de una auditoría financiera.** A nivel conceptual, dicha revisión 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 cloud. Así, se debe revisar los Controles Generales de Tecnologías de la Información aplicando la GPF-OCEX 5330, *Revisión de los CGTI en un entorno de administración electrónica*, relacionados con las áreas significativas para la auditoría.

  Cuando el ente auditado haga uso de servicios cloud, 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. Para más detalle ver el Anexo 1.
  - Se deberá prestar especial atención a la revisión del contrato del servicio cloud. En el Anexo 2 se incluye un programa de trabajo para facilitar esta revisión.

  La revisión del entorno de TI en el contexto de la auditoría financiera es el enfoque principal de esta guía.

A modo de aclaración cabe destacar que **los dos enfoques anteriores excluyen la revisión del control interno y de los controles aplicados por el proveedor del servicio cloud**, ya que éste no está sujeto a la fiscalización por parte de un OCEX.

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

4 Existen guías que especifican los controles a tener en cuenta en auditorías del proveedor de servicios cloud, como el CIS Controls Cloud Companion Guide del CIS (Center for Internet Security) o la matriz de controles cloud (Cloud Controls Matrix) de CSA (Cloud Security Alliance) y la Guía CCN-STIC-823, Utilización de servicios en la nube, diciembre 2014

2. Objetivos de la guía

Esta *Guía básica de auditoría en entornos cloud* 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 en 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 identificados.

e) Considerar otros aspectos de la auditoría afectados cuando la entidad utiliza la nube en procesos significativos: evidencia, necesidad de expertos, utilización de ADA (análisis de datos de auditoría)[5], 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.

La presente guía se fundamenta 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 o soluciones de Administración Electrónica, 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 interna”. Cuando sea pertinente se seguirán criterios similares a los expuestos en esta guía.

3. Tipos y características de los 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 la categoría de servicio cloud que se ofrece[6].

En cuanto al **modelo de despliegue** podemos hablar de:

Nube pública

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

5 El análisis de datos de auditoría (ADA) hace referencia a metodología de auditoría basada en la utilización de programas informáticos que ayudan a los auditores en el tratamiento y análisis de la información en formato electrónico, con objeto de obtener evidencia que soporte las conclusiones de auditoría.

6 Clasificación establecida de acuerdo con diferentes guías y textos sobre cloud: CCN-STIC-823, de Utilización de servicios en la nube; The NIST Definition of Cloud Computing, etc.

Nube privada

Nube privada externa

Los recursos están disponibles a través de Internet únicamente para una empresa u organización, que contrata con un proveedor externo propietario de la infraestructura para que administre un entorno de forma exclusiva.

Nube privada interna

Cuando todos los recursos se alojen dentro de las dependencias y centros de datos de la organización, que asume los costes y recursos necesarios para construir y mantener la infraestructura. En estos casos la entidad dispone de un control total del entorno.

La nube privada interna, aunque está diseñada según un esquema cloud, solo es un caso particular de sistema de información al que hay que aplicar la metodología del enfoque de riesgo y la GPF-OCEX 5330 y al no ser un servicio cloud contratado con un CSP **no** lo consideraremos computación en la nube a los efectos de esta guía.

Nube comunitaria

Los recursos e infraestructura son compartidas entre varias organizaciones. Los recursos se pueden administrar internamente o por un tercero y se pueden alojar de forma local o externa. Las organizaciones comparten el coste y, a menudo, tienen requisitos de seguridad en la nube y objetivos comerciales similares.

Las soluciones de Administración Electrónica antes mencionadas pueden considerarse incluidas en esta clasificación.

Nube híbrida

Combina dos o más modelos de los anteriores.

En cuanto a las **categorías de servicios cloud** que se ofrecen, las principales son:

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

El proveedor se encarga de la administración de la infraestructura (hardware, redes de comunicaciones y almacenamiento) y el cliente tiene el control sobre los sistemas operativos, y todas las aplicaciones que instale en dichos recursos.

Como ejemplo tenemos máquinas virtuales o servidores como Amazon web services (AWS), por ejemplo, para instalar después una base de datos.

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

PaaS agrega una capa adicional a lo que facilita IaaS y añade utilidades para el desarrollo de aplicaciones, bases de datos, etc.

Siguiendo con el ejemplo de base de datos, en PaaS la base de datos se expandiría (o contraería) según sea necesario en función de su uso de forma transparente para el cliente, quien tampoco tendría que administrar los servidores individuales sobre los que esté la base de datos, las redes que la comuniquen, etc.

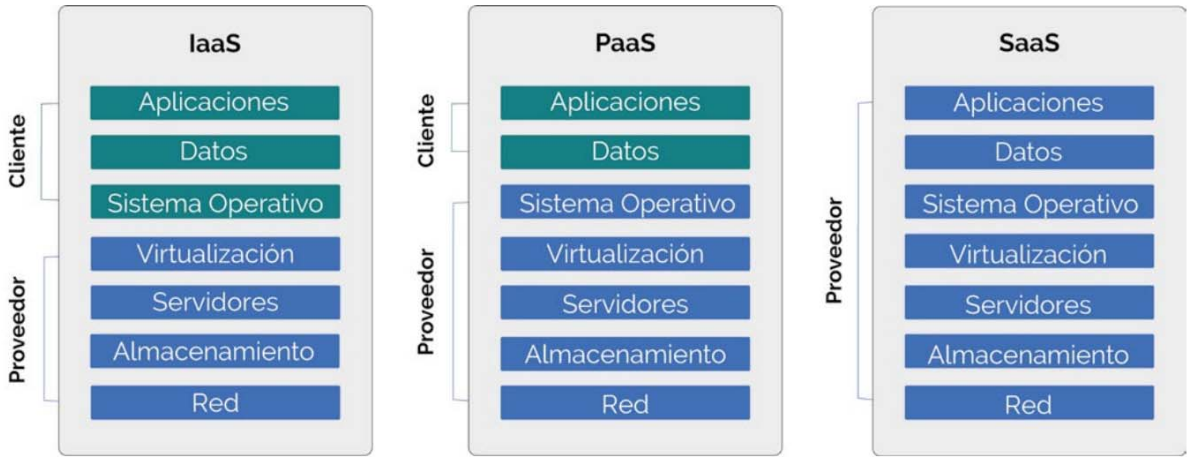
Google app engine para el desarrollo de aplicaciones es un ejemplo de esta categoría.

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

El proveedor ofrece al cliente aplicaciones como un servicio. 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.

Ejemplo: suites ofimáticas online, Gmail, TeamMate (versión web), FACE, etc.

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 cloud en cuanto a la responsabilidad y capacidad de supervisar cada uno de sus componentes son:



Fuente: CSA, Cloud Audit & Forensics

Según Cloud Security Alliance[7] las **características esenciales**, establecidas en el marco NIST, que hacen que **una nube sea una nube** son:

- **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 puede delimitar ubicaciones a un cierto nivel de abstracción (país, estado, etc.).
- **Autoservicio bajo demanda**. El cliente puede ajustar la capacidad necesaria de forma unilateral, sin necesidad de involucrar al personal del proveedor.
- El **amplio acceso a la red** significa que todos los recursos están disponibles en una red, sin necesidad del acceso físico directo; la red no es necesariamente parte del servicio.
- Adaptación inmediata. La **elasticidad rápida** permite a los usuarios ampliar o contraer los recursos que utilizan del grupo (aprovisionamiento y desaprovisionamiento), a menudo de forma completamente automática. Esto les permite relacionar más estrechamente el consumo de recursos con la demanda (por ejemplo, agregar servidores virtuales cuando la demanda aumenta y luego apagarlos cuando baja la demanda). Desde el punto de vista del consumidor, los recursos parecen ilimitados, pudiendo disponer de cualquier volumen en cualquier momento.
- **Servicio consumido.** El proveedor puede controlar el servicio prestado efectivo en cada momento, al nivel de abstracción 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.

Según la publicación de CSA citada, si falta alguna de estas características, probablemente no sea una nube.

[7] Véase *Guía de Seguridad de áreas críticas para computación en la nube*.

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 que han de ser identificados y controlados. La identificación de riesgos asociados al servicio cloud contratado es una actividad que debe desarrollar cada organización, puesto que el tipo, las características de los y el uso de los servicios contratados determinará 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 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 que pueden destacarse son:

Pérdida de gobernanza

El uso de un entorno cloud 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 adhoc en los pliegos y en el contrato. En este sentido, aclarar que la responsabilidad final sobre los datos sigue siendo de la entidad.

Riesgos legales

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

Si por cumplimiento regulatorio o legal 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 cloud por parte de los OCEX se prestará siempre atención a la normativa vigente, en especial al cumplimiento con el ENS, ENI[8], LOPDP y GDD[9] y el RGPD[10].

Normalmente un CSP se convertirá en un encargado del tratamiento respecto a los datos personales del cliente. La DA 1ª de la LOPDP y GDD 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.

---

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

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

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

Brechas/Fuga de datos

Al igual que los entornos tradicionales, las tecnologías cloud pueden verse afectadas por las amenazas clásicas presentes en aplicaciones, sistemas y redes. Sin embargo, la superficie de exposición en un servicio cloud es mayor (ya que dicho servicio es utilizado por varias organizaciones y, además, en el caso de nube pública, está accesible desde Internet) y el 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 en cloud, suele ser alto (entornos cloud para uso de big data).

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.

Portabilidad

Los servicios cloud 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 cloud 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 cloud.

Disponibilidad

Dependiendo de la criticidad de la información que esté alojada en cloud, 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 cloud deben tener definida una política de recuperación de datos y servicio en caso de desastre.

Uso inadecuado de usuarios administradores

La revisión de los superusuarios es un aspecto muy relevante en cualquier auditoría. Cuando se audita un entorno cloud 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.

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 implica 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 robustecerlas 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 cloud frente a la centralización de las mismas en un repositorio único. En el caso de optar por el cloud, el auditor debe analizar si la organización ha revisado los controles de seguridad que dicho proveedor ofrece para proteger los accesos.

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 a la nube

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

De todos los riesgos existentes a nivel operativo, 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 cloud y del auditado

En función de la propiedad y de la administración de la infraestructura cloud, el cumplimiento legal y normativo recaerá sobre la organización usuaria o el proveedor de servicios. 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 sea de aplicación en lo que respecta a prestadores de servicios.

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 (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 la Seguridad de la entidad pública destinataria de los servicios.

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 y GDD en materia de seguridad de la información. En la *Guía de seguridad de las TIC CCN-STIC-823 Utilización de servicios en la nube*, también se regula esta materia de forma específica.

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, incluyendo instalaciones y personal, y pudiendo ser reemplazadas por otras siempre y cuando se justifique que protegen igual o mejor el riesgo sobre los activos, y se satisfacen los principios básicos recogidos en el Capítulo II del ENS.

Asimismo, siempre que la prestación de servicios cloud albergue datos de carácter personal, deberán cumplirse, además de los requisitos establecidos por el ENS (DA 1ª LOPDP y GDD), todos aquellos desarrollados en materia de protección de datos. Para más detalle sobre esta materia puede consultarse el apartado 3 de la CCN-STIC-823.

6. Contratación del servicio

La primera medida a implantar al contratar servicios en la nube es la que recoge el apartado *[op.ext.1] Contratación y acuerdos de nivel de servicio* del Anexo II del ENS y recogido en el apartado *C.5 Servicios Externos* de la GPF-OCEX 5330: 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.

El contrato debe recoger con claridad las responsabilidades del proveedor y los niveles de seguridad de la información y los servicios afectados, de forma que el proveedor cuente con 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 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, de cumplimiento del ENS, de adecuación a la LOPD, la auditoría de PCI/DSS[11], ISO 27000 de Gestión de Seguridad de la Información, etc.).

Cuando no se recoja esta exigencia en los PCAP 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.

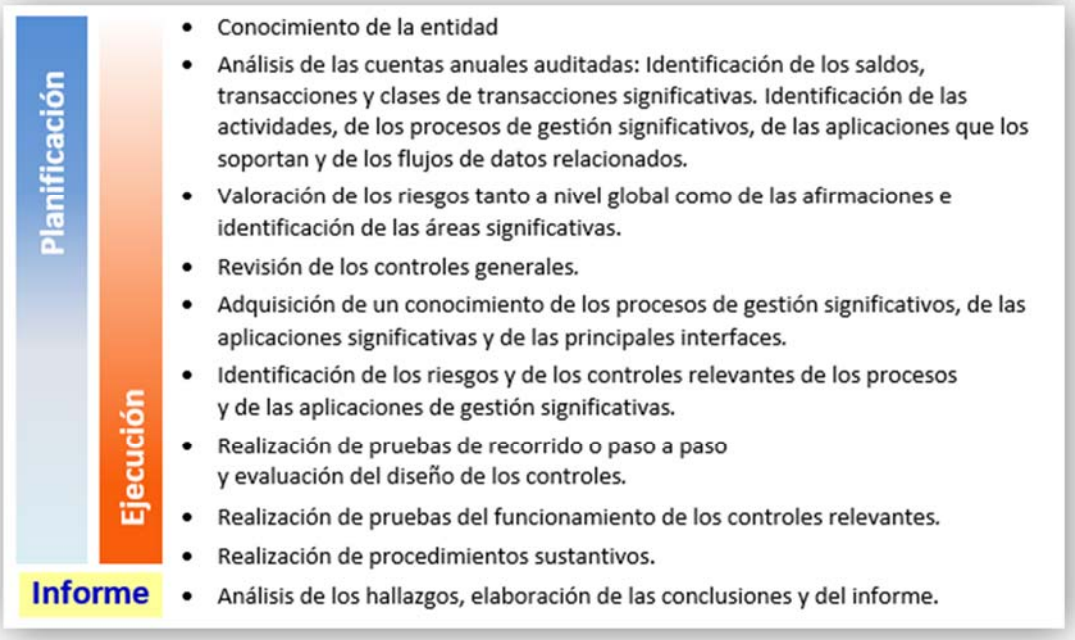
Por tanto, dado que en la contratación de un servicio cloud muchos de los aspectos que determinarán la seguridad de la información y el cumplimiento legal y regulatorio vendrán determinados por lo recogido en el contrato del servicio, la revisión de éste es un punto fundamental en el trabajo de auditoría. En el **Anexo 2** se incluye una guía para realizar dicha revisión.

7. Consideraciones que deben realizarse en una auditoría financiera

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 o la de 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 cloud no es sino una particularidad de un entorno TIC, con sus características y riesgos específicos.

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

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 debe seguir las siguientes etapas[12]:



De acuerdo con el enfoque de riesgo y lo previsto en la NIA-ES 315/GPF-OCEX 1315/1316, *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.

La auditoría en entornos cloud 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 y disponibilidad) brindado 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 cloud 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, incluyendo 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.

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

7.1 Conocimiento de la entidad auditada, incluyendo su sistema de información y de control interno (GPF-OCEX 1316)

Un primer paso fundamental en la etapa de planificación consiste en lograr un conocimiento profundo del negocio del ente auditado y 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 debe identificar y entender los sistemas de contabilidad y control interno afectados por el entorno TIC.

El auditor debe adquirir una clara comprensión del proceso de gestión auditado y conocer qué parte de este y qué actividades se realizan directamente por la entidad auditada, y cuáles son servicios prestados por un proveedor cloud, qué aplicaciones significativas hay en la nube e identificar las interfaces significativas.

Como de ordinario, el conocimiento adquirido se documentará mediante una narrativa y un flujograma. El conocimiento debe incluir dónde se almacenan los datos, los controles y cómo se puede acceder a ellos para realizar muestreos, análisis de datos y todo tipo de pruebas.

Se indagará sobre el tipo de servicio cloud y la relación contractual con el CSP. Una adecuada comprensión del modelo de servicio y de distribución de responsabilidad adoptado por el ente será fundamental, dado que no solo poseen características propias, sino que en principio pueden representar diferentes tipos de riesgos que pueden afectar la información financiera.

El equipo de auditoría debe conocer la diferencia entre las distintas formas de prestación del servicio TIC y de los riesgos asociados a cada una, que pueden ser muy diferentes, por eso es importante conocer el tipo de servicio contratado en cada caso.

El auditor debe considerar si el uso de la computación en la nube es significativo para los objetivos de la auditoría, deberá obtener una comprensión general de la organización de servicios (el proveedor), con el fin de identificar y analizar los riesgos de incorrección material y diseñar procedimientos de auditoría en respuesta a ellos.

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.

7.2 Identificación y valoración de riesgos (GPF-OCEX 1315)

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 cloud que se utilice.

A partir del conocimiento obtenido, el auditor estará en condiciones de valorar el riesgo de negocio 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 debe identificar únicamente aquellos que fueran relevantes para la auditoría financiera dentro del conjunto amplio de riesgos que representa la nube —algunos que le son propios y otros comunes a otras modalidades— pero que pueden verse potenciados en este entorno.

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.

El riesgo de auditoría es creciente conforme se incrementa la complejidad del entorno informatizado.

Al realizar la reunión del equipo para analizar riesgos y 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.

7.3 Revisión de los 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 los controles internos relevantes que sirven para prevenir, detectar o corregir los errores en la información financiera, definir 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 definirá 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 generales y los de aplicación, evaluándolos en ese orden, en la medida en que el mal funcionamiento de los primeros invalida los segundos, dando lugar a manifestaciones erróneas en los estados contables sin que sean detectadas.

La auditoría deberá revisar los **Controles Generales de TI** (CGTI) de acuerdo con lo previsto en la GPF-OCEX 5330 particularizando la aplicabilidad de estos al tipo de servicio cloud y a las características específicas del entorno del ente auditado.
El Anexo 1 se incluye una guía **g**eneral para realizar esta tarea, si bien se debe señalar que ésta deberá ser modificada convenientemente en función de las características propias de los sistemas de TI y el entorno cloud presente en cada entidad.

En la verificación de los CGTI el auditor deberá hacer hincapié en la revisión del contrato y en el seguimiento del cumplimiento de los indicadores de nivel de servicio establecidos en éste, tal y como se ha indicado en el punto 6 de esta guía.

Por último, cabe señalar que determinadas comprobaciones de los CGTI podrán darse por cumplidas si las aplicaciones auditadas cumplen legalmente con auditorías de seguridad (ENS, protección de datos), tal como se señala en la GPF-OCEX 5330.

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.

7.4 Obtención de evidencia electrónica y uso de herramientas ADA.

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.

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.

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 las TI, como la falta de visibilidad de los registros de auditoría por la inexistencia de soporte documental material de los archivos electrónicos. 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** puede que sea desconocido para la entidad. 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 debería estar prevista en los pliegos.

Aunque con carácter general es aplicable la GPF-OCEX 1500, 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 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, así como el gobierno 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, es importante evaluar la cantidad y tipología de evidencias disponibles para analizar durante la auditoría. En la medida en la que el número de evidencias aumente y éstas contengan información más relevante o detallada, se podrán realizar auditorías de tipo más técnico.

Asimismo, debe evaluarse, dependiendo de cómo se haya obtenido cada evidencia, el nivel de fiabilidad de ésta. 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.

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”.

7.5 Uso de especialistas

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 o por informáticos que presten apoyo a los auditores. De no disponer de personal especializado en el OCEX, se deberá contratar a especialistas externos.

7.6 Análisis de los hallazgos, evaluación de las deficiencias observadas e informe

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[13]:

Control efectivo

Control bastante efectivo

Control poco efectivo

Control no efectivo o no implantado

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. En el primer caso podrán existir recomendaciones, o cuestiones clave de auditoría según los casos. En el segundo podrá emitirse un informe detallado con conclusiones sobre la eficacia del control interno relacionado.

8. Bibliografía

ASOCEX:

- GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa, 27/11/2017
- GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad, 12/11/2018
- GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica, 12/11/2018

Centro Criptológico Nacional:

- 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-801, Responsabilidades y funciones, mayo 2019

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

Cloud Security Alliance (CSA, Spanish chapter)

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

The NIST Definition of Cloud Computing (NIST SP 800-145, National Institute of Standards and Technology)

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)

[13] Revisión de los Controles Generales de Tecnologías de la Información en el Anexo 4 apartado E

Anexo 1 Adaptación de los CGTI a entornos cloud

La siguiente tabla recoge un análisis general de la aplicabilidad de los CGTI a entornos cloud, 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.
	E2 Plan de Continuidad	N/A	x	x	
	E3 Alta Disponibilidad	N/A	x	x	

					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.

ANEXO 2 Cuestiones a revisar en los contratos de servicios cloud

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…), ésta deberá figurara 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. Cláusula de encargado del tratamiento adecuada a la RGPD.
- 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. Además, de cada SLA, se definirán:
    - Identificador
    - Responsabilidades
    - Periodicidad de captura de datos e informes de cumplimiento
    - Umbrales que disparan situaciones de aviso y alarma
    - Consecuencias de incumplimiento
- Mecanismos de acceso al servicio, que identifiquen el acceso de usuarios y administradores, que garanticen la confidencialidad y la integridad de la información.
- Condicionantes geográficos, en función de la ubicación geográfica de los servidores y 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 la 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.
- Respaldo y recuperación de datos: el proveedor deberá disponer de un procedimiento de copias que garantice la restauración de la información como describe [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 y mecanismos que tardará el proveedor en realizar la destrucción efectiva de los datos.

En los apartados 5 y 6 de la guía CCN-823 se comentan con mayor detalle los aspectos a incluir en los contratos cloud.