Auditoría Pública nº 75 (2020), pp. 35 - 44

Antonio Minguillón Roy
Auditor director del Gabinete Técnico de la SCCV
Esperanza Pinar Lorente
Técnico de auditoría de sistemas de información de la SCCV

Auditando en la nube (no en las nubes)

RESUMEN/ABSTRACT:

La utilización de la computación en la nube es una forma de provisión de servicios tecnológicos utilizada desde hace muchos años por las grandes empresas y las administraciones públicas que en los últimos años ha experimentado un fuerte crecimiento.

La crisis provocada por el Covid-19 ha puesto de manifiesto el mayor nivel de resiliencia de las entidades que tenían un mayor despliegue de sus sistemas información en la nube respecto de aquellas con unos sistemas de información tradicionales.

La computación en la nube aporta notables ventajas a las entidades usuarias, pero también tiene riesgos importantes y afecta de forma significativa al sistema de control interno y a la seguridad, y por consiguiente al trabajo de los auditores públicos. Al igual que la sociedad y las administraciones se están adaptando a marchas forzadas a una nueva realidad, los auditores debemos apretar el paso y adaptarnos. Para ayudar a los auditores en esta tarea, la Conferencia de Presidentes de los OCEX aprobó el 20 de mayo pasado la GPF-OCEX 1403 Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios de computación en la nube.

Una de las cosas más importantes sobre la que todos los auditores y las instituciones de control deben reflexionar es que, en general, dado el complejo entorno TIC, muchos de los procedimientos para revisar los controles internos y realizar las pruebas de auditoría deberán ser llevados a cabo por personal especializado, idóneamente por auditores de sistemas de información que presten apoyo a los auditores integrados en los equipos de fiscalización.

The use of cloud computing is a technology service provision that has long been used by large companies and public administrations and has grown consistently in recent years.

The Covid-19 crisis has shown that entities with a greater deployment of their information systems in the cloud have greater levels of resilience than those with traditional information systems.

Cloud computing provides considerable advantages to user entities, but it also has major risks and significantly affects the internal control system and security, and therefore, the work of public auditors. Just as society and administrations are rapidly adapting to a new reality, we, the auditors, have to keep up the pace and adapt. To assist the auditors in this task, on 20 May the Conference of Presidents of OCEX (Regional External Control Bodies) approved the Practical Guide for (GPF-OCEX 1403) Audit Considerations for an entity using a cloud computing services organisation.

One of the most important things for all auditors and control institutions to reflect upon is that, in general, given the complex ICT environment, many procedures for reviewing internal controls and performing audit tests will need to be carried out by specialised personnel, ideally by information systems auditors supporting the auditors on the audit teams.

PALABRAS CLAVE/KEYWORDS:

COVID-19, COMPUTACIÓN EN LA NUBE, CLOUD COMPUTING, CONTROL INTERNO, FUTURO, RIESGO DE AUDITORÍA, NIA-ES-SP, GPF-OCEX
COVID-19, CLOUD COMPUTING, INTERNAL CONTROL, FUTURE, AUDIT RISK, NIA-ES-SP, GPF-OCEX

1. LA NUBE EN 2020

Aunque la utilización de la computación en la nube o cloud computing es una forma de provisión de servicios tecnológicos utilizada desde hace muchos años por las grandes empresas y las administraciones públicas, en los últimos años ha experimentado un fuerte crecimiento de forma paralela a la expansión de la digitalización en todos los niveles de la gestión pública. La creciente implantación de la administración electrónica ha llevado aparejada en muchos casos la externalización de numerosos sistemas de información y la utilización de internet para acceder a los sistemas de gestión públicos.

La grave crisis sanitaria, social y económica provocada por el Covid-19, entre otras cuestiones de no menor importancia, ha puesto de manifiesto la necesidad de profundizar en esta tendencia ya que las entidades que tenían un mayor despliegue de sus sistemas información en la nube han sido más resilientes y han respondido mejor a la necesidad de operar durante el confinamiento y de acceder de forma ubicua a los sistemas de gestión que aquellas otras entidades con unos sistemas de información tradicionales, que se han visto desbordadas y con poca capacidad de reacción para mantener unos niveles aceptables de operatividad.

Esta expansión de los sistemas de información en la modalidad de computación en la nube aporta notables ventajas a las entidades usuarias, pero también tiene riesgos importantes y afecta de forma radical al sistema de control interno y a la seguridad. Considerando que importantes entidades públicas tienen o van a tener a corto y medio plazo aplicaciones de gestión económica significativas desplegadas en la nube, los auditores de los OCEX debemos preguntarnos si este nuevo escenario afecta en algo a nuestra forma de fiscalizar. Debemos preguntarnos: ¿sabemos qué es eso del cloud computing? ¿sabemos qué riesgos de auditoría nos crea? ¿sabemos cómo deben enfocarse las auditorías? ¿sabemos hacerlo? ¿podemos hacerlo?

En estas reflexiones andábamos cuando la Conferencia de Presidentes de los OCEX aprobó el 20 de mayo pasado la Guía Práctica de Fiscalización de los Órganos de Control Externo *GPF-OCEX 1403 Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios de computación en la nube.* Su finalidad es orientar sobre cómo se debe aplicar la *NIA-ES-SP 1402 Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios* cuando el ente que vamos a fiscalizar utiliza servicios de computación en la nube.

En este breve artículo pretendemos dar a conocer la GPF-OCEX 1403 y explicar sucintamente algunos conceptos básicos relacionados con el cloud computing y su impacto en las fiscalizaciones de los OCEX.

2. QUÉ ES EL *CLOUD COMPUTING* Y CUÁLES SON SUS CARACTERÍSTICAS ESENCIALES

La variedad de servicios prestados en la nube es amplísima, y a modo de ejemplo, puede comprobarse en la página web *Soluciones en cloud*[1] cómo la Administración General del Estado ofrece por esta vía diversas soluciones de administración electrónica a las Administraciones Públicas para dar respuesta a necesidades comunes.

Por su general aceptación, para su definición acudimos a la realizada en 2011 por el *National Institute of Standards and Technology*[2], que definió el cloud computing como "un modelo para permitir el acceso por red, de forma práctica y bajo demanda, a un conjunto compartido 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 del servicio".

Fuente: CCN-STIC-823

[1] https://www.administracionelectronica.gob.es/pae_Home/pae_Estrategias/Racionaliza_y_Comparte/soluciones_cloud.html
[2] *National Institute of Standards and Technology [NIST SP-800-145], 2011.*

En este tipo de servicios en la nube, unos agentes esenciales son las entidades o proveedores que ofrecen servicios en red (CSP, por sus siglas en inglés de *Cloud Service Provider*) con independencia de dónde se encuentren alojados los sistemas de información que soportan dichos servicios, y de forma transparente para el usuario final.

El *cloud computing* 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 relacionados con la seguridad de la información procesada y almacenada en la nube que deben ser previstos por las entidades usuarias y considerados en los trabajos de auditoría.

Según *Cloud Security Alliance*[4] son cinco las características esenciales que hacen que una nube sea una nube:

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 que intervenga el personal del proveedor.

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 medido.
El proveedor puede controlar en cada momento el servicio efectivamente prestado, 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.

3. MODELOS DE DESPLIEGUE Y TIPOS DE SERVICIOS CLOUD

Los servicios de cloud computing se pueden clasificar atendiendo a dos aspectos principales: el modelo de despliegue y el tipo de servicio que se ofrece. Podemos hablar de cuatro modelos de despliegue principales:

Nube pública
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 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.

Nube privada
Son aquellas que se basan en una infraestructura operada únicamente por una organización y que ofrecen servicios únicamente a esa misma organización. Puede ser propiedad de, administrada y operada por la organización, un tercero o alguna combinación de ellos, y puede existir dentro o fuera de las instalaciones de la organización. 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 estos, por ejemplo, administraciones públicas grandes.

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 servi-

[3] Guía de seguridad TIC CCN-STIC-823, Utilización de servicios en la nube.
[4] Guía de Seguridad de áreas críticas para computación en la nube.

cios compartidos). Los recursos informáticos y la infraestructura se comparten entre varias organizaciones para su uso exclusivo, y 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.

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 ambos.

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 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.

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,* y sus organismos públicos 2015-2020, se fijó como meta "la constitución de una nube híbrida (nube SARA) que ofrezca 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 proceso 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. Aunque inicialmente se centra en la infraestructura como servicio, proporcionará gradualmente servicios de mayor madurez, tales como plataforma como servicio y aplicación como servicio (por ejemplo, gestión de la nómina en la nube).

En cuanto a los tipos de servicios cloud que se ofrecen, los 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.

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

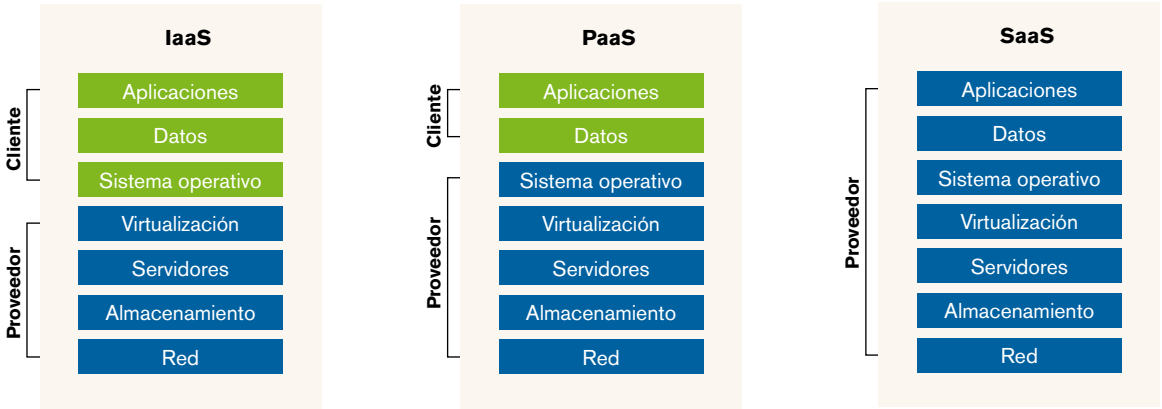
PaaS agrega una capa adicional a lo que facilita IaaS y añade utilidades para el desarrollo de aplicaciones, bases de datos, etc.

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. 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

4. FISCALIZACIÓN DE LA CONTRATACIÓN DE UN SERVICIO DE COMPUTACIÓN EN LA NUBE

Los contratos de servicios de computación en la nube suelen ser por regla general significativos por alguna de las siguientes razones: su elevado valor estimado, su larga duración o por afectar a alguna actividad o servicio clave para los objetivos de la fiscalización; por esas razones será bastante normal que debamos fiscalizar, cada vez con mayor frecuencia, este tipo de contrataciones. En estos casos deberemos conocer y tener en cuenta las peculiaridades especiales de los contratos de servicios de computación en la nube.

En primer lugar se deben definir con precisión las características del servicio a contratar y las responsabilidades de las partes, además de establecer acuerdos de nivel de servicio para definir la calidad del servicio contratado.

Es importante tener en cuenta que la responsabilidad del cumplimiento de las normas aplicables en materia de seguridad y de protección de datos 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.

En cuanto a las responsabilidades de las partes y el cumplimiento del ENS, el proveedor de servicios cloud está obligado a cumplir todas las medidas del ENS que sean pertinentes. Pero 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.

Los pliegos deben recoger con claridad las responsabilidades del proveedor, 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 en los pliegos se 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:

- Certificación de conformidad con el ENS.
- 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.
- Informes de auditoría tipo 1 o tipo 2 (requeridos por la NIA-ES-SP 1402).

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.

Asimismo, siempre que la prestación de servicios cloud albergue datos de carácter personal, deberán cumplirse, además de los requisitos establecidos por el ENS todos aquellos exigidos por la normativa en materia de protección de datos.

El artículo 122. 2 de la Ley de Contratos del Sector Público, exige que en aquellos contratos cuya ejecución requiera el tratamiento por el proveedor del servicio de datos personales por cuenta del responsable del tratamiento (la entidad contratante), que en el pliego se haga constar, entre otras cuestiones, las siguientes:

- 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.

Brevemente, 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

los pliegos, la revisión de estos es un punto fundamental en el trabajo de auditoría con efecto tanto en el control interno como en el cumplimiento legal.

5. CONSIDERACIONES GENERALES 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 basados en las TIC, y diseñar y ejecutar las pruebas pertinentes adaptadas a las circunstancias particulares. 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 ese entorno tecnológico. Un entorno cloud 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 1315/1316, *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 significativa de la gestión del ente auditado esté soportada mediante sistemas TIC y, si fuera el caso, mediante el procesamiento en la nube.

Por otra parte, los servicios de computación en la nube o cloud computing solo 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"*.

La NIA-ES-SP 1402 y la GPF-OCEX 1403 se aplican cuando una entidad auditada (usuaria) recibe servicios de cloud computing de otra entidad (organización de servicios o entidad prestadora o CSP) relacionados con aquellas áreas de la entidad (contabilidad, compras, personal, 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, que es lo que requiere la NIA-ES-SP/GPF-OCEX 1315 y la NIA-ES-SP/GPF-OCEX 1330.

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.

6. CONOCIMIENTO DE LA ENTIDAD AUDITADA, DE SUS SISTEMAS DE INFORMACIÓN Y DE CONTROL INTERNO

Un primer paso fundamental en la etapa de planificación, de acuerdo con los previsto en la *GPF-OCEX 1316 El conocimiento del control interno de la entidad,* consiste en lograr un conocimiento profundo de la actividad del ente auditado, de sus operaciones y de su entorno.

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 el proveedor cloud, qué aplicaciones significativas hay en la nube e identificar las interfaces significativas. El conocimiento debe incluir dónde se almacenan los datos, los controles existentes 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 cloud 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.

7. IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS CUANDO SE UTILIZA 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 varía en cada entidad, puesto que el tipo, las características y el uso de los servicios contratados determinará en gran medida los riesgos a los que está expuesta.

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, puede reducirse el riesgo; sin embargo, éste puede ser 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).

Los principales riesgos derivados o acentuados por el uso de soluciones cloud que se citan en la GPF-OCEX 1403 son:

- Pérdida de gobernanza.
- Riesgos legales.
- Brechas/Fuga de datos.
- Uso inadecuado de usuarios administradores.
- Inadecuada gestión de identidades, accesos y credenciales.
- Dependencia del proveedor.
- Portabilidad.
- Disponibilidad.
- Pérdida de trazabilidad.
- Otros riesgos o riesgos no vinculados solo a la nube.

De todos los riesgos existentes a nivel operativo, no solo los anteriores, 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.

Para poder valorar el riesgo de un entorno en la nube 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 cloud que se utilice.

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

La estrategia del auditor de la entidad usuaria para valorar el riesgo derivado del uso de cloud computing consistirá, según la NIA-ES-SP 1402 en:

- 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) de alguna de las siguientes formas:

a) Obteniendo informe tipo 1. Un **"informe tipo 1"** es un 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.

b) Obteniendo informe tipo 2. 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.

c) Obteniendo información específica, a través de la entidad usuaria, sobre la prestadora del servicio.

d) Visitando y aplicando directamente procedimientos de auditoría sobre la prestadora del servicio.

- Recurriendo a otro auditor a fin de que aplique determinados procedimientos.

8. 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 prestados por el

CSP, 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 la comprobación 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 cloud. 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 cloud, se adaptará este trabajo para incluir en el alcance de la revisión los controles que, en función de la categoría de servicio (IaaS/PaaS/SaaS), sean responsabilidad directa de la entidad auditada. También 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.

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.

9. OBTENCIÓN DE EVIDENCIA ELECTRÓNICA, UTILIZACIÓN DE TÉCNICAS Y DE HERRAMIENTAS INFORMÁTICAS PARA EL ANÁLISIS DE DATOS

Cuando se audite en un entorno cloud 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, en particular en la *GPF-OCEX 1503: La evidencia electrónica de auditoría***.**

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 y aplicación es distinta a los demás, debiéndose adaptar los programas y procesos de obtención de evidencias a cada caso en particular, si bien 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.

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 el nivel de **fiabilidad**, considerando cómo se haya obtenido cada evidencia. 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.

10. EFECTOS EN LOS INFORMES DE FISCALIZACIÓN

Si el auditor 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), deberá emitir un informe de auditoría que exprese una opinión modificada, de conformidad con la NIA-ES-SP 1705 R o la GPF-OCEX 1730. 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;
- 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.

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 cloud y las deficiencias, en su caso, detectadas deben reflejarse en los informes de fiscalización considerando y evaluando cuidadosamente su significatividad.

11. A MODO DE CONCLUSIÓN

Si a principios de año nuestra sociedad, nuestras administraciones públicas, nuestro entorno de trabajo en definitiva, se caracterizaba por un alto grado de desarrollo de las TIC, el mundo post-COVID-19 va a experimentar una aceleración notable del proceso de implantación de la administración electrónica. Y además con una característica diferencial muy relevante: se han roto las barreras sicológicas y culturales al trabajo en remoto y a la utilización de la computación en la nube. La computación en la nube ha pasado de verse por muchos como una fuente de riesgos y de pérdida de control, a considerarse una herramienta muy útil, sencilla de desplegar, que facilita la gestión en estos tiempos tan complicados.

Pero este cambio afecta de forma importante a nuestras auditorías. Igual que la sociedad y las administraciones se están adaptando a marchas forzadas a una nueva realidad, los auditores debemos apretar el paso y adaptarnos también, sin excusas y **sin demora**.

Los auditores debemos adquirir unos conocimientos mínimos suficientes que nos permitan entender cómo está estructurado el sistema de información y de control interno de los entes que fiscalizamos cuando está total o parcialmente desplegado en la nube, debemos entender cómo afecta a nuestras auditorías y debemos aprender a auditar en la nube **y evitar que los nuevos tiempos nos pillen en las nubes**.

En consecuencia, una de las cosas más importantes sobre la que todos los auditores y las instituciones deben mentalizarse es que, en general, dado el complejo entorno TIC, muchos de los procedimientos para revisar los controles internos y realizar las pruebas de auditoría deberán ser llevados a cabo por personal especializado, idóneamente por **auditores de sistemas de información** que presten apoyo a los auditores integrados en los equipos de fiscalización.

Aunque este tipo de perfiles profesionales se están incorporando poco a poco a las plantillas de los OCEX, es un proceso que sin duda debe acelerarse a corto plazo. La sociedad no espera.

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

GPF-OCEX 1403 Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios de computación en la nube, 20/05/2020

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

Centro Criptológico Nacional:

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

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

Cloud Security Alliance (CSA, Spanish chapter)

Guía de Seguridad de áreas críticas para computación en la nube, v4.0, 2018

Cloud Audit & Forensics, 2018

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.