FUNDACIÓN FIASEP
AUDITORÍA PARA LA TRANSPARENCIA EN EL SECTOR PÚBLICO

Serie OPINIONES FIASEP

Nº 2/2020

"NIAs, nubes y coronavirus"

Antonio Minguillón Roy
Auditor director del Gabinete Técnico
Sindicatura de Comptes de la Comunitat Valenciana

Mayo, 2020

1. Introducción

Los auditores públicos, y en general todos los auditores del sector público incluyendo los privados, hemos estado muy ocupados los primeros meses de 2020, entre otras muchas cosas, poniéndonos al día y estudiando cómo aplicar las nuevas NIA-ES-SP. Para algunos colegas quizá sea este su primer contacto con ellas y la tarea de asimilar todas a la vez será verdaderamente abrumadora. Para otros, que estamos acostumbrados a manejar y aplicar las NIA-ES desde hace años, tenemos la sensación de que realmente son viejas conocidas ya que, en general, no dejan de ser una suave adaptación de estas. Aun para estos últimos hay algunas que deben ser objeto de estudio detallado, bien porque los cambios son sustanciales respecto de la práctica anterior, por ejemplo todo lo referido a la estructura de los informes, bien porque hay alguna NIA que, en mi experiencia, no ha sido objeto de mucha atención hasta la fecha y sin embargo las circunstancias actuales, como la plena implantación de la administración electrónica, hace que adquieran una importancia muy relevante, me estoy refiriendo en concreto a la NIA-ES-SP 1402 *Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios,* que comentaré sucintamente en estas páginas.

Estábamos, como digo, bastante ocupados estudiando cómo iban a afectar las NIA-ES-SP a las auditorías de este año, cuando en marzo se ha desencadenado con gran virulencia (nunca mejor dicho) una crisis sin precedentes, que ha trastocado todos nuestros planes profesionales y personales.

Además de otras consideraciones de tipo más personal, social o económico, desde el punto de vista de auditor público, la grave crisis sanitaria, social y económica provocada por el COVID-19 me ha llevado a las siguientes reflexiones:

- Es un hecho incontestable que nuestra sociedad y en particular las administraciones públicas están haciendo un uso cada vez más extenso e intenso de las tecnologías de la información y las comunicaciones (TIC). La **dependencia** de los sistemas de información y las comunicaciones (SIC) para la gestión pública y la prestación de servicios a los ciudadanos no hace sino incrementarse cada vez más, hasta tal punto, que en estos momentos críticos los SIC han llegado a ser la espina dorsal sobre la que se han mantenido en funcionamiento muchos de los servicios públicos esenciales y no esenciales, y han respaldado el ingente esfuerzo personal realizado por los colectivos

que han debido estar en primera línea durante todo el transcurso de la crisis del COVID-19. Estoy convencido de que sin un adecuado funcionamiento de los SIC la catastrófica situación en la que nos ha dejado el virus hubiera sido todavía mucho peor en todos los aspectos.

- Esta circunstancia de total dependencia de las TIC para el funcionamiento de las administraciones ha ampliado de forma muy considerable su superficie de exposición frente a **ciberamenazas**. Cuanto mayor sea el uso y la dependencia de las TIC en la gestión pública mayor importancia debe concederse a las cuestiones relativas a la **ciberseguridad**, ya que los malos intentan aprovechar los momentos de confusión generalizada para sacar adelante sus actividades ciberdelictivas, sin importarles si sus víctimas son personas particulares, entidades hospitalarias o administraciones públicas.
- Las administraciones han tenido que exigir el máximo a sus SIC para mantenerse en funcionamiento, mientras se activaban mecanismos de **teletrabajo** en un tiempo récord para seguir cumpliendo con sus funciones de servicio a los ciudadanos. El avance en el desarrollo del teletrabajo por parte de todas las administraciones públicas, auditores públicos incluidos, sería mucho más fácil, desde mi punto de vista, si se dispusiera de sistemas y aplicaciones desplegados en la "**nube**" en mucha mayor medida.
- Las organizaciones que ya tenían desplegados gran parte de sus sistemas de información en la nube han sido capaces de responder mejor a la inesperada situación crítica provocada por la epidemia de COVID-19, han sido más **resilientes**. Las que no estaban preparadas deberían plantearse la conveniencia de **migrar a la nube,** total o parcialmente, sus sistemas críticos.

Pero estas reflexiones generales deben ir un poco más allá, ya que no solo debemos pensar en la ciberamenazas y en cómo pueden aprovechar las administraciones públicas la modalidad de servicio de computación en la nube en su operativa ordinaria, también debemos pensar en cómo afectan a la forma en que realizamos nuestras auditorías los ciberriesgos y el hecho de que la mayor parte de los entes que fiscalizamos están inmersos, ya, en una carrera imparable para migrar gran parte de sus sistemas de información al cloud computing.

Dejando al margen por hoy la cuestión de las ciberamenazas, frente a la realidad como digo imparable del cloud computing, si somos auditores responsables debemos preguntarnos: ¿sabemos qué es eso del cloud computing? ¿sabemos qué riesgos de auditoría origina?

¿sabemos qué consecuencias tiene en nuestra metodología y métodos de trabajo? ¿sabemos hacerlo? ¿podemos hacerlo?

Para hacer frente a la situación comentada y responder a estas preguntas, señalaré algunos conceptos básicos sobre la computación en la nube y comentaré lo que la NIA-ES-SP 1402, que tenemos entre las manos estos días, requiere al auditor público.

2. Qué es el cloud computing

El cloud computing no es algo nuevo, lleva mucho tiempo entre nosotros, pero en los últimos años en paralelo a la expansión de la digitalización en todos los niveles de la gestión pública, se ha incrementado la externalización de muchos sistemas de información, la utilización de internet para acceder a los sistemas de gestión y a los servicios públicos desde diferentes dispositivos.

Internacionalmente es aceptada la definición realizada por el National Institute of Standards and Technology (NIST SP-800-145) 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.

Podemos observar en la sección ***Soluciones en cloud*** del Portal de Administración Electrónica cómo la Administración General del Estado ofrece soluciones de administración electrónica a las Administraciones Públicas mediante una serie de servicios prestados en la nube con los que da respuesta a necesidades comunes de distintas administraciones

En el modelo de servicios en la nube, son actores principales las entidades o proveedores que ofrecen servicios en red (CSP, *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.

Las cinco características esenciales que reúne el cloud computing según el NIST 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.
- **Autoservicio bajo demanda**: El cliente puede ajustar la capacidad necesaria de forma unilateral, sin necesidad de involucrar al personal del proveedor.

- **Amplio acceso a la red**: Todos los recursos están disponibles en una red (internet), 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 CSP, a menudo de forma completamente automática. Desde el punto de vista del consumidor, los recursos parecen ilimitados, pudiendo disponer de cualquier volumen en cualquier momento.
- **Servicio medido**: El CSP puede controlar en cada momento el servicio efectivamente prestado, al nivel de detalle que se especifique por contrato. 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.

Las diversas modalidades de servicios cloud se pueden clasificar atendiendo a dos aspectos principales: el modelo de despliegue y la categoría de servicio cloud que se ofrece. En cuanto al modelo de despliegue se puede distinguir entre:

- **Nube pública**: son aquellas cuya infraestructura, que es controlada por un CSP, es ofrecida al público general o a un gran grupo de usuarios. 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 y el software.
- **Nube privada**: son aquellas que se basan en una infraestructura operada únicamente para una organización y que ofrecen servicios únicamente a esa misma organización. Puede ser propiedad de la organización, administrada y operada por ella, por un tercero o alguna combinación de ellos, y puede existir dentro o fuera de las instalaciones de la organización.
- **Nube comunitaria o compartida:** son aquellas alojadas en infraestructuras compartidas por varias organizaciones relacionadas entre ellas, para su uso exclusivo, compartiendo requisitos de servicio (como los centros de servicios compartidos). Los recursos se pueden administrar internamente o por un tercero y se pueden hospedar en instalaciones propias de una o más de las organizaciones de la comunidad (modo local), externamente en una empresa de alojamiento, o alguna

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

- **Nube híbrida:** Combina dos o más modelos de los anteriores para que las organizaciones puedan aprovechar las ventajas de ambos. Los datos y las aplicaciones pueden moverse entre nubes privadas y públicas para una mayor flexibilidad y más opciones de implementación. Un ejemplo de nube híbrida es la Red SARA.

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 (sistemas operativos) 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 tipos de cloud implica diferentes niveles de responsabilidad del usuario y del proveedor sobre el control interno, la seguridad y la configuración del servicio. Por eso es importante en una auditoría conocer tanto el modelo de despliegue como el tipo de servicios cloud que recibe la entidad que estamos auditando.

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 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, es decir sobre el ente que estemos auditando, con independencia de la existencia de acuerdos, seguros u otras medidas compensatorias.

Por otra parte, el CSP queda obligado a cumplir todas las medidas del Anexo II del Esquema Nacional de Seguridad que correspondan. Es responsabilidad de las entidades

públicas contratantes notificar a los operadores del sector privado que presten servicios cloud, la obligación de que tales servicios sean conformes con lo dispuesto en el ENS y posean las correspondientes Declaraciones o Certificaciones de Conformidad. Esa exigencia, entre otras, se debe incluir en los **pliegos de contratación**.

3. 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 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 internos. Los servicios serán prestados a través de contratos y acuerdos de nivel de servicio incluidos en los pliegos de contratación, que deberán definir las responsabilidades y mecanismos para la gobernanza. Áreas no incluidas en el contrato (volvemos a la importancia de los pliegos) pueden provocar brechas de seguridad, que requerirán que el cliente ajuste sus propios procesos para gestionar los riesgos asociados.

Los principales riesgos derivados de o acentuados por el uso de soluciones cloud están relacionados con la **seguridad** y esquemáticamente 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 como desastres naturales, acceso no autorizado a instalaciones, robos o problemas en la red, etc.

De acuerdo con la metodología del enfoque de riesgo establecida en la NIA-ES-SP 1315, 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.

4. Consideraciones que deben realizarse en una auditoría financiera

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

Por otra parte, los servicios de computación en la nube o cloud computing son un caso particular de los servicios contemplados en la *NIA-ES-SP 1402 "Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios"*. Ésta debe aplicarse 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, en definitiva, aplicar lo previsto en las NIA-ES-SP 1315 y 1330.

Los principales aspectos de una auditoría financiera que se ven afectados por un entorno cloud y que deben ser considerados de acuerdo con la *NIA-ES-SP 1402* son:

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

   Se debe conocer y entender los sistemas de contabilidad y control interno afectados por el entorno cloud. 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.

Se indagará sobre el tipo de servicio cloud (de los que he comentado en el apartado 2 anterior) y la relación contractual con el CSP (análisis de los pliegos de contratación). 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.

b) La identificación y valoración de riesgos.

La auditoría en entornos cloud debe incluir la evaluación de riesgos y controles derivados del modelo de despliegue y tipo de servicio contratado y del grado de seguridad (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) brindado para la elaboración de la información financiera.

Aunque con carácter general el riesgo de auditoría es creciente conforme se incrementa la complejidad del entorno informatizado, 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 reducir el riesgo frente a ciberamenzas; sin embargo, éste puede aumentar 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).

La NIA-ES-SP 1402 establece una serie de orientaciones sobre la estrategia del auditor de la entidad usuaria para valorar el riesgo derivado del uso de cloud computing que no comento aquí por exceder la finalidad de este breve artículo.

c) La evaluación del sistema de control interno, tanto de los controles generales como los controles aplicación.

Una vez obtenido un adecuado conocimiento del ente a auditar e identificados y valorados los riesgos significativos, el auditor debe identificar y 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, incluidos los que se aplican a las transacciones procesadas por el CSP, valorar el riesgo de control y determinar el enfoque de auditoría a aplicar (de

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

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

En un entorno cloud la práctica totalidad de la evidencia disponible será electrónica, por tanto, al planificar las pruebas a realizar, el auditor debe evaluar la disponibilidad de la información, ya que los datos están en posesión del CSP y el modelo de datos (estructura de una base de datos y relaciones internas) necesario para planificar una prueba 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 estas a su auditor.

También debe evaluarse su nivel de fiabilidad. El auditor deberá hacerse, por ejemplo, las siguientes preguntas en relación con la fiabilidad y exactitud de la información: ¿Qué datos son usados para elaborar el informe recibido? ¿Qué aplicación ha procesado los datos? ¿Son efectivos los controles generales de la aplicación que ha procesado los datos y generado el informe? ¿Hemos verificado específicamente algún control sobre la completitud y exactitud de los datos utilizados? ¿Son efectivos? ¿Los datos o informe que nos han proporcionado pueden ser susceptibles de cambios manuales?

En la medida en que existe una cierta correlación entre el uso de computación en la nube y la existencia de cantidades masivas de datos, se hace indispensable la utilización de herramientas informáticas de auditoría para obtener, procesar y analizar la información disponible, lo que afecta positivamente a la cualidad de suficiencia de la evidencia por la posibilidad de hacer test sobre el 100% de la población en vez de sobre una muestra.

6. Las competencias del equipo auditor y el uso de especialistas.

En general, dado el complejo entorno TIC de los sistemas en la nube, muchos de los procedimientos para conocer, identificar y revisar los riesgos y los controles de ciberseguridad, controles generales y controles de aplicación y realizar las pruebas de datos, deberán ser llevados a cabo por auditores de sistemas de información que presten apoyo a los auditores. Por tanto, **todas las organizaciones auditoras públicas deben dotarse de auditores con este nuevo perfil tecnológico avanzado**.