Auditoría Pública nº 70 (2017), pp. 27 - 38

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

La ciberseguridad, el auditor externo y los OCEX

RESUMEN/ABSTRACT:

La creciente omnipresencia y dependencia de las tecnologías de la información y las comunicaciones a todos los niveles, tanto en el ámbito individual como en el empresarial y en el sector público, ha originado que en los últimos años hayamos asistido a un crecimiento sin precedentes de ataques de muy distinto tipo, procedencia y objetivos a los sistemas de información y a los datos en ellos procesados y almacenados en cualquiera de los tres ámbitos señalados.

En un mundo interconectado en el que las distintas redes de las administraciones públicas no son sino elementos integrantes de una red global, los ciberriesgos se multiplican en el sector público.

Los OCEX no son ajenos a esta problemática y deben realizar un ejercicio profundo de reflexión, tanto colectivamente puesto que es un tema que afecta a todos de forma profunda, como a nivel de cada institución, analizando el potencial impacto de las ciberamenazas, valorando los ciberriesgos generales y determinando cuáles son las medidas más adecuadas a adoptar tanto en materia de recursos humanos especializados en seguridad que deben incorporarse a los equipos de auditoría, como en materia de metodología de auditoría, formación específica para su personal y en recursos tecnológicos.

En el presente artículo se ofrece una visión general de esta problemática.

The growing omnipresence and dependence upon information and communication technologies at all levels, on the individual level as well as businesses and the public sector, has meant that over the last few years, we have witnessed an unprecedented increase in attacks of very different types, origin and objectives on information systems and the data in them processed and stored in any of the three areas mentioned.

In an inter-connected world in which the different networks of the public administrations are merely integrating elements of a global network, cyber risks are multiplied in the public sector.

The external control bodies are not excluded from this issue and they should carry out an exercise of deep reflection, collectively, since it is an issue that affects everyone deeply, as well as on the level of every institution, analysing the potential impact of cyber threats, assessing the general cyber risks and determining which are the most appropriate measures to adopt in terms of human resources specialising in security that should be incorporated into the audit teams, as well as in terms of audit methodology, specific training for their staff and technological resources.

This article offers an overall view of this issue.

PALABRAS CLAVE/KEYWORDS:

AUDITORÍA DE SISTEMAS, CIBERSEGURIDAD, SEGURIDAD DE LA INFORMACIÓN, CONTROLES GENERALES TI, ADMINISTRACIÓN ELECTRÓNICA
SYSTEMS AUDIT, CYBER SECURITY, INFORMATION SECURITY, IT GENERAL INSPECTIONS, E-ADMINISTRATION

INTRODUCCIÓN

La creciente omnipresencia y dependencia de las tecnologías de la información y las comunicaciones (TIC) a todos los niveles, tanto en el ámbito individual como en el empresarial y en el sector público, ha originado que en los últimos años hayamos asistido a un crecimiento sin precedentes de ataques de muy distinto tipo, procedencia y objetivos a los sistemas de información y a los datos en ellos procesados y almacenados en cualquiera de los tres ámbitos señalados[1].

En un mundo interconectado en el que las distintas redes de las administraciones públicas no son sino elementos integrantes de una RED global, los ciberriesgos se multiplican. En palabras del Director del Centro Criptológico Nacional: "*El uso masivo de las tecnologías de la información y las telecomunicaciones, en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas*[2]**".**

Así, la ciberseguridad se ha convertido en uno de los temas más relevantes tanto para los gobiernos, como para los gestores públicos y privados, y por supuesto para los auditores, dada la potencial repercusión que las amenazas a la seguridad de los sistemas de información representan sobre los entes públicos y su efecto sobre las cuentas que se auditan.

La magnitud del problema a nivel global queda reflejada en el esfuerzo presupuestario previsto por el gobierno federal de los EEUU para apoyar la estrategia de ciberseguridad en el ejercicio fiscal 2016: 14.000 millones de dólares[3]. Más recientemente, el 11 de mayo de 2017, la Casa Blanca ha emitido una Orden Ejecutiva en la que se declara como una política general de la administración federal gestionar los ciberriesgos y ordena a todas las agencias públicas que emprendan una serie de iniciativas para reforzar la ciberseguridad de las redes e infraestructuras críticas federales.

Como respuesta de la Unión Europea a los retos planteados por la ciberseguridad en 2004 se creó la *European Union Agency for Network and Information Security* (ENISA), agencia que coordina e impulsa actividades relacionadas con dicha materia[4].

Conscientes de la magnitud del problema la Comisión Europea publicó el 7 de febrero de 2013 la *Estrategia de ciberseguridad de la UE: Un ciberespacio abierto, protegido y seguro*, acompañada de una propuesta de Directiva de la Comisión sobre la seguridad de las redes y de la información. Esta estrategia de ciberseguridad representa la visión de conjunto de la UE sobre cómo prevenir y resolver las perturbaciones de la red y los ciberataques. En dicho documento se señala que la ciberseguridad vela por la preservación de la disponibilidad e integridad de las redes e infraestructuras de información, y por la preservación de la confidencialidad de la información contenida en éstas.

[1] Baste citar el reciente caso del troyano Wannacry que ha provocado el cierre temporal de sistemas enteros de entes públicos y privados. Una vulnerabilidad de ciberseguridad como la conocida en julio de 2017 sobre el servicio LEXNET provocó el cierre temporal de ese servicio esencial para la Administración de Justicia. Además, se vulneró la confidencialidad de miles de datos personales de especial protección.

[2] Prólogo a la Guía de implantación del ENS, CCN-STIC 804, junio de 2017.

[3] *The President Budget, Fiscal Year 2016, Cybersecurity*, 7/8/2015.

[4] Actualmente hay una propuesta de la Comisión para transformar ENISA en la Agencia de Ciberseguridad de la UE, con muchas más competencias en la materia.

Más recientemente, el 6 de julio de 2016 se aprobó la Directiva 2016/1148 del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, también conocida como Directiva de Ciberseguridad o Directiva NIS.

El presidente de la Comisión Europea J.C. Juncker señaló, el 13 de septiembre de 2017, en su discurso del Estado de la Unión que la cuarta prioridad de la Comisión para el próximo año es "proteger mejor a los europeos en la era digital". Continuaba señalando que "los ciberataques pueden ser más peligrosos para la estabilidad de las democracias y las economías que las armas y los tanques. … Los ciberataques no conocen fronteras y nadie es inmune a ellos."

Las ciberamenazas también han forzado a los gobiernos nacionales a diseñar estrategias frente a ellas, como la elaborada en 2013 por el Gobierno de España y recogida en la "Estrategia de Ciberseguridad Nacional".

En noviembre de 2016 entraron en vigor en nuestro país las leyes 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas y la 40/2015, de Régimen Jurídico del Sector Público, ambas de 1 de octubre de 2015. Estas leyes constituyen el eje vertebrador de las relaciones de los ciudadanos y sus Administraciones Públicas y de estas entre sí, consagrándose el uso de las herramientas electrónicas basadas en sistemas de información interconectados, como el medio habitual para encauzar tales relaciones y el principio de "digital por defecto" en el funcionamiento de la administración. También suponen el impulso definitivo para la transformación digital del sector público, transformación para la que los OCEX deben prepararse sin demora.

Según la Ley 40/2015, el Esquema Nacional de Seguridad (ENS) tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de dicha Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

En España el Centro Criptológico Nacional (CCN) es la entidad que tiene encomendada las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada. También elabora y difunde normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas TIC de las administraciones públicas.

El Instituto Nacional de Ciberseguridad (INCIBE) es la entidad de referencia para el desarrollo de la ciberseguridad e impulsar el uso seguro del ciberespacio en España.

En resumen, la importancia máxima de la ciberseguridad en los actuales entornos de administración electrónica está en estos momentos fuera de toda discusión. El crecimiento y extensión de los ciberataques padecidos en los últimos tiempos ha fortalecido la concienciación de los gestores públicos para implantar controles robustos que hagan frente a las ciberamenazas y mitiguen su impacto en las administraciones públicas.

1. QUÉ ES LA CIBERSEGURIDAD

Aunque el término "ciberseguridad" sea posiblemente uno de los más utilizados en los últimos años, tanto en ámbitos profesionales como generales, no existe una definición o significado preciso de general aceptación. Para abordar esta cuestión ENISA publicó en 2015 un estudio titulado "*Definition of Cybersecurity*" que analizaba las distintas acepciones del término.

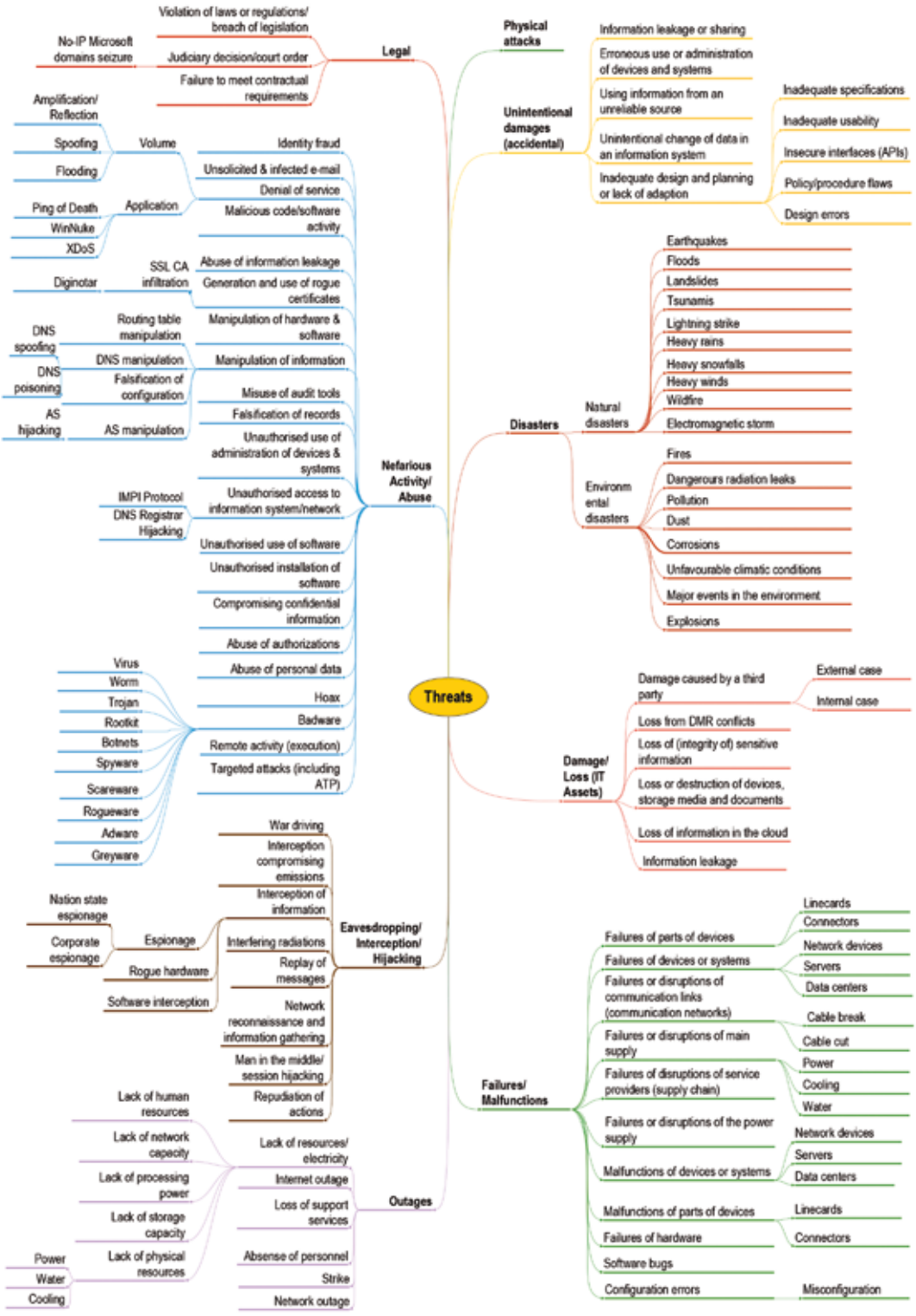
ISACA, una organización de referencia en materia de auditoría de sistemas de información considera (ISACA, 2013) que el término "ciber" en el contexto de la seguridad de la información es utilizado a menudo en un sentido demasiado amplio y ciñen el término ciberseguridad a todo lo que protege a entidades públicas, privadas e individuos de ataques intencionados e incidentes graves y de sus consecuencias. Según ISACA la ciberseguridad hace frente principalmente a los ataques e incidentes que están focalizados, son sofisticados, difíciles de detectar y controlar, hace frente básicamente a las denominadas amenazas avanzadas persistentes (APT en inglés).

En mi opinión, esta visión de la ciberseguridad es importante puesto que se centra en amenazas provenientes de estados, de grupos terroristas o de mafias internacionales, pero desde el punto de vista del auditor externo es excesivamente restringida[5] y debe abarcar un ámbito más amplio.

Basta echar un vistazo a la amplitud de las amenazas de ciberseguridad publicada por ENISA que se muestra en la figura 1 (ENISA, 2016), para llegar a la conclusión de que la ciberseguridad no solo se refiere a las APT, sino que es una cuestión mucho más común que debe ser abordada por todas las entidades públicas de forma integrada en sus políticas de seguridad de la información.

[5] Matthew Loeb, CEO de ISACA no solo compartía este mismo punto de vista el 22 de agosto de 2017 en csoonline.com, también defendía que la ciberseguridad debe ser una materia escolar:
"*For nations and governments, cyber security must be a prime concern across the breadth of government at all levels and in all functions of government…*
For individuals, the journey towards a cyberculture should begin as early as possible. We need to make cyber security and good 'online hygiene' part of core curricula at the pre-university level, to imbed the concept of security online at the earliest possible levels and ensure that tomorrow's digital (and eventually cognitive) natives don't make cyber security an afterthought. Much like many universities already include humanities or similar courses as graduation requirements, we need to give similar importance to cyber security courses at the university level."

Figura 1 ENISA Threat Taxonomy



Aunque frecuentemente se utilizan como si fueran sinónimos, ciberseguridad y seguridad de la información son conceptos que comparten muchos elementos comunes pero que tienen ciertos matices diferenciadores importantes. Una distinción[6] entre ambos conceptos sería:

- La seguridad de la información trata de la protección de la información, independientemente de su formato, dentro de la entidad.
- La ciberseguridad se ocupa específicamente de la protección de los activos de información procesada, almacenada y transportada por **redes y sistemas de información interconectados**.

Con toda probabilidad este último factor sea el elemento clave que ha originado que, dentro del dominio de la seguridad de la información, se haya producido un creciente auge de los temas relacionados con la ciberseguridad. Un subdominio que debido a la imparable tendencia hacia un mundo datacéntrico totalmente interconectado, con los sistemas de información cada vez más en la "nube", ha adquirido una importancia propia con características diferenciadoras, en paralelo con conceptos como ciberespacio, ciberamenazas, ciberriesgos, ciberfraude, ciberresiliencia, etc.

Para finalizar, me quedaré con la definición dada por la Directiva de Ciberseguridad o Directiva NIS de la *seguridad de las redes y sistemas de información* (es decir la ciberseguridad): la *capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la* ***disponibilidad***, ***autenticidad***, ***integridad*** *o* ***confidencialidad*** *de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos*.

Esta definición contempla las cuatro características fundamentales de los activos de información que debe salvaguardar la ciberseguridad y la seguridad de la información: la confidencialidad, la autenticidad, la integridad y la disponibilidad.

Centrándonos en el ámbito de actuación de los OCEX, e independientemente del alcance concreto que se quiera dar al concepto de ciberseguridad, las políticas de ciberseguridad de las organizaciones públicas deben estar, como ya he señalado, totalmente alineadas e integradas con sus políticas de seguridad de la información. **Por su trascendencia e impacto potencial, el auditor público debe incluir en su metodología ordinaria de trabajo la revisión de los controles de seguridad de la información, incluyendo la ciberseguridad.**

2. NORMATIVA LEGAL SOBRE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Aunque son numerosas las normas legales con incidencia en temas de ciberseguridad[7], destacaré tres de ellas.

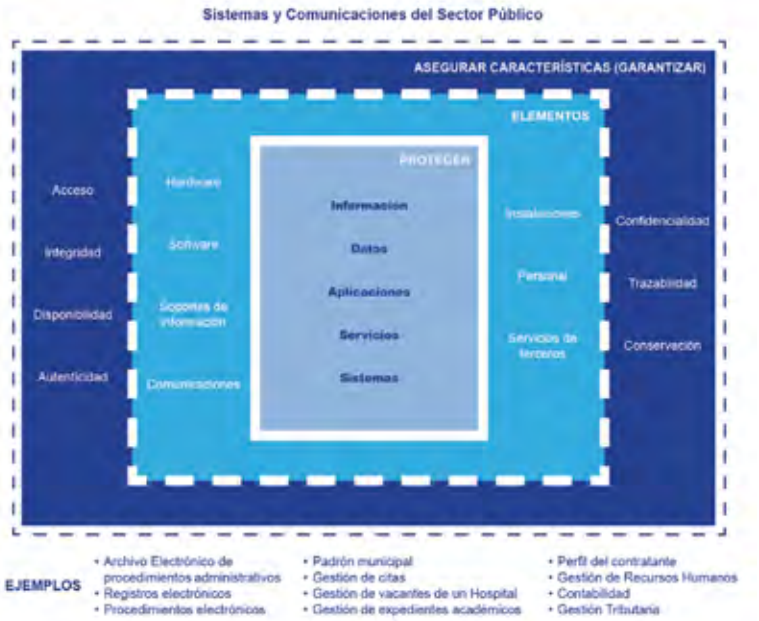
La primera es el Esquema Nacional de Seguridad (ENS), regulado en el Real Decreto 3/2010, de 8 de enero y actualizado por el Real Decreto 951/2015, de 23 de octubre. Es el elemento normativo que pretende garantizar la adecuada protección de la información tratada y los servicios electrónicos prestados por las entidades del sector público.

Su finalidad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, de forma que los sistemas de información presten sus servicios y custodien la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

El ámbito de aplicación objetivo o material del ENS puede representarse mediante el esquema de la figura 2[8], en el que se muestran las características de los sistemas de información que se deben garantizar, los elementos de los sistemas de información y los activos a proteger.

[6] Basada en las definiciones del ISACA Glossary.
[7] Para una visión completa de las normas relacionadas puede consultarse el Código de Derecho de la Ciberseguridad editado por el BOE y compilado por INCIBE.
[8] Guía de seguridad (CCN-STIC-830) - Ámbito de aplicación del ENS.

Figura 2 ENS: Sistemas y comunicaciones del Sector Público



Es importante destacar que en el artículo 34 del ENS se establece que todas las entidades públicas están obligadas a cumplir con el ENS y someter sus sistemas de información a una **auditoría** regular ordinaria, al menos cada dos años, que verifique el cumplimiento de sus requerimientos.

El objetivo final de esta auditoría de seguridad, realizada por expertos, es sustentar la confianza que merece el sistema auditado sobre el nivel de seguridad implantado, tanto internamente como frente a terceros, que pudieran estar relacionados; es decir, calibrar la capacidad del sistema para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los servicios prestados y la información tratada, almacenada o transmitida[9].

Para aplicar el ENS el CCN ha elaborado y publicado una serie de documentos guía que constituyen unos materiales esenciales, casi diría que inseparables del ENS, para todo aquel que quiera profundizar en estas cuestiones.

Lamentablemente, hoy en día el grado de cumplimiento del ENS por parte de las entidades públicas es, en general, bastante bajo y pocas entidades pueden acreditar que hayan realizado la citada auditoría de seguridad.

Por su gran importancia, los OCEX deberían verificar en todas las fiscalizaciones el cumplimiento de la legalidad en relación con el ENS y, si no se acredita, se deberá reflejar en el informe como un incumplimiento grave o muy significativo.

[9] Apartado 10 de la Guía de auditoría CCN-STIC-802.

Otra norma clave es la Directiva NIS, ya mencionada, que establece que los estados miembros adoptarán y publicarán, a más tardar el 9 de mayo de 2018, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a la misma. Actualmente España está en proceso de transponer esta directiva.

También interesa citar por su importante efecto sobre aspectos de la confidencialidad de la información, la aprobación por el Parlamento Europeo el 27 de abril de 2016 del nuevo Reglamento General de Protección de Datos de la UE, de plena aplicación para el sector público. Este RGPD será aplicable a partir del 25 de mayo de 2018, fecha a partir de la cual las políticas de seguridad de la información y los controles internos deberán contemplar sus requerimientos.

3. PROPIEDADES O CARACTERÍSTICAS DE LA INFORMACIÓN DIGITAL

La información y los datos que circulan, almacenan o se procesan en un sistema de información, deben tener una serie de características que los controles de seguridad deben garantizar, tal como requiere la Directiva de Ciberseguridad a nivel europeo o el ENS en España. Estas **características** son:

- La **autenticidad** es la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- La **confidencialidad** es la propiedad de la información, por la que se garantiza que está

accesible únicamente a personal autorizado a acceder a dicha información.

- La **disponibilidad** se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.
- La **integridad** es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.

El artículo 1.2 del ENS establece que será aplicado por las administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias. Es decir, debe garantizar que los medios o soportes en que se almacenen documentos cuenten con medidas de seguridad que garanticen las características señaladas. Vemos que además de las cuatro características fundamentales de la seguridad el ENS contempla alguna característica adicional.

Puesto que los OCEX trabajan en las fiscalizaciones, cada vez más, con evidencia electrónica, dichas características son esenciales para que la información y los datos en formato digital obtenidos por los auditores de los sistemas de información del ente auditado puedan constituir evidencia de calidad, es decir que sea pertinente y fiable.

Por esta razón los auditores externos deben revisar a fondo y verificar que los controles internos diseñados e implantados en los sistemas de información por la entidad funcionan eficazmente y garantizan que la información y los datos utilizados como fuente de evidencia electrónica tienen las características exigidas.

Así, en el ámbito de actuación de los OCEX, el apartado 37 de la GPF-OCEX 1500 establece y define los criterios, propiedades o características que permitirán valorar la fiabilidad de la información y garantizar la misma como evidencia electrónica de auditoría en entornos informatizados. Son las siguientes:

Autenticación[10]: Se refiere a la posibilidad de confirmar, de forma indubitada, la identidad de la persona o entidad que creó, originó o de la que procede la información.

Autorización: Se refiere al hecho de que la información electrónica ha sido creada, procesada, grabada, corregida, enviada, archivada, ingresada y destruida solo por personas autorizadas y responsables.

Confidencialidad: La información únicamente será conocida por las personas o entidades autorizadas (quienes la originan y a quienes va dirigida).

Disponibilidad: La información ha de estar disponible para las personas o entidades autorizadas, evitándose las pérdidas de datos.

Integridad: Es la garantía de que los datos o información de origen han sido validados y estos no han sido alterados al ser creados, procesados, transmitidos y almacenados en los sistemas informáticos.

No repudio[11]: Imposibilidad de que una persona o entidad que haya originado, transmitido o recibido información pueda negar haber participado en ese origen o intercambio de datos.

Trazabilidad: Indica las acciones o procesos que se llevan a cabo en el sistema, así como quién y cuándo las realiza.

Esta exigencia de la GPF-OCEX 1500 está respaldada por lo previsto en los artículos 17 de la Ley 39/2015 y 46 de la Ley 40/2015 que establecen que los documentos administrativos se almacenarán por medios electrónicos y deberán conservarse en un formato que permita garantizar su autenticidad, integridad, conservación, disponibilidad y accesibilidad.

Vemos que las propiedades que el auditor público debe exigir a la evidencia electrónica son básicamente coincidentes con las características de la información que el ENS pretende garantizar.

Por tanto, una entidad que acredite el cumplimiento con el ENS mediante las auditorías de seguridad previstas en su artículo 34 proporcionará a los auditores de los OCEX una seguridad más elevada que la que proporcione una entidad que no acredite su conformidad con el ENS.

En estos últimos casos los auditores deberán realizar procedimientos adicionales para obtener un determinado nivel de seguridad respecto de la evidencia digital que soporte los informes de fiscalización (cualquiera que sea el tipo de fiscalización realizada: financiera, de legalidad u operativa). Esta seguridad se obtendrá mediante la revisión de los controles generales de tecnologías de la información CGTI que se comentan más adelante.

[10] O autenticidad.

[11] Según INCIBE *no repudio* es sinónimo de *autenticidad*. De una forma coloquial podría decirse que son las dos caras de una misma moneda.

4. LOS OCEX Y LA CIBERSEGURIDAD

Aunque la ciberseguridad es una cuestión de seguridad nacional, también es una materia que afecta a las empresas, a los individuos particulares y de forma directa a las entidades públicas, que tienen la responsabilidad de establecer medidas de protección y controles coherentes con sus políticas generales de seguridad de la información.

Los OCEX no son ajenos a la problemática provocada por los ciberriesgos y deben realizar un ejercicio profundo de reflexión, tanto colectivamente puesto que es un tema que afecta a todos de forma profunda, como a nivel de cada institución, analizando el potencial impacto de las ciberamenazas, valorando los ciberriesgos generales y determinando cuáles son las medidas más adecuadas a adoptar tanto en materia de nuevos recursos humanos especializados en sistemas de información y seguridad que deben incorporarse a los equipos de auditoría, como en materia de metodología de auditoría, en formación específica para su personal y en recursos tecnológicos.

En las fiscalizaciones individuales, los auditores responsables deben analizar cómo afectan las cuestiones relacionadas con la seguridad informática y la ciberseguridad a los objetivos de su auditoría y a la valoración de los riesgos.

Cuanto mayor sea la entidad auditada y más complejos sus sistemas de información, mayor impacto tendrán los aspectos tecnológicos y los riesgos tecnológicos, y mayores serán las consideraciones al respecto que deba hacerse el auditor.

La forma de abordar en una auditoría las cuestiones relacionadas con la ciberseguridad dependerá de cada caso concreto, del objetivo y alcance de cada fiscalización. Caben dos enfoques principales:

a) Auditorias operativas de ciberseguridad o específicas de sistemas de información.

Considerando que las redes de comunicaciones y sistemas de las administraciones públicas tienen interconexiones con otras entidades públicas y privadas, la descripción detallada del alcance de la auditoría es esencial. Generalmente todas las categorías de controles y todos los CGTI pueden ser relevantes excepto que expresamente se excluyan del alcance de la auditoría. Por tanto, se debe delimitar claramente la extensión y el límite de hasta dónde se audita. Podríamos estar hablando de:

- Auditorias de los controles de ciberseguridad y de ciberresiliencia.
- Auditoría de seguridad de la información.
- Auditoría de seguridad de los registros contables de facturas electrónicas.
- Auditoría de los sistemas de control interno automatizados.
- Auditoría de los controles de seguridad de la receta electrónica.
- Etc.

b) Auditorías de seguridad de la información en apoyo de auditorías financieras o de cumplimiento.

En cualquier auditoría, tanto si tiene un alcance limitado, como si se trata de auditorías financieras de cuentas anuales o de elementos de las cuentas anuales (por ejemplo: de la cuenta general de un ayuntamiento, de la liquidación del presupuesto, de los gastos de personal, de los ingresos tributarios) será necesario realizar una revisión de los CGTI (que básicamente incluyen los controles de seguridad de la información y ciberseguridad) con el alcance específico que se determine, en concordancia con el alcance y objetivos de la auditoría.

Los auditores de sistemas de información analizarán con los auditores financieros aquellos controles que son relevantes para los objetivos de la auditoría financiera, ya que no todos los riesgos son iguales, ni en probabilidad, ni en su materialidad. Se deberá adoptar un enfoque basado en el análisis del riesgo.

En el ámbito de los órganos de control interno, las normas de auditoría para las intervenciones tanto del Estado[12] como locales[13] establecen expresamente que en las auditorías públicas se podrá ***verificar la seguridad y fiabilidad de los sistemas informáticos*** *que soportan la información económico-financiera y contable.*

Los OCEX a través de ASOCEX y de su Comisión Técnica, están desarrollando sendas Guías Prácticas de Fiscalización (GPF-OCEX) relativas a la ciberseguridad, la seguridad de la información y los CGTI, que cubrirán el actual vacío existente en las normas técnicas de fiscalización en relación con la ciberseguridad.

5. AUDITORÍA DE ESTADOS FINANCIEROS, CONTROL INTERNO Y CIBERSEGURIDAD

Las auditorías específicas sobre ciberseguridad, que cabría clasificarlas dentro del amplio grupo de las auditorías operativas, tienen unas características propias que podrían dar lugar a más de un artículo sobre ellas. No obstante, en este apartado, por su interés más general, me centraré en las consideraciones que sobre ciberseguridad deben realizarse en las auditorías financieras.

[12] Resolución de 30 de julio de 2015, de la Intervención General de la Administración del Estado, por la que se dictan instrucciones para el ejercicio de la auditoría pública. Norma Duodécima.Dos e).

[13] Real Decreto 424/2017, de 28 de abril, por el que se regula el régimen jurídico del control interno en las entidades del Sector Público Local. Artículo 33.4.e).

En un reciente artículo publicado en la revista del Col.legi de Censors Jurats de Comptes de Catalunya, Joaquim Altafaja, presidente del capítulo de Barcelona de ISACA, señalaba que "la ciberseguridad se transforma en **un elemento material más de la auditoría de cuentas** por los efectos sobre el negocio, las posibles implicaciones legales y se postula como un indicador de la preparación de la organización para abordar el futuro" (Altafaja, 2017).

Por motivos que ya he comentado, esta afirmación relativa a las auditorías privadas es totalmente válida cuando hablamos de las auditorías públicas que realizan los OCEX.

Las normas de auditoría, en particular la GPF-OCEX 1316 y la NIA-ES 315, requieren al auditor que obtenga un conocimiento suficiente sobre cómo utiliza el ente auditado los sistemas de información, sobre los controles automatizados[14] y su impacto en los estados financieros.

Solo tras adquirir ese conocimiento se podrán valorar los riesgos de incorrección material en los estados financieros, por ejemplo, los riesgos de TI resultantes de un acceso no autorizado a una base de datos o de una disposición no autorizados de los fondos de banca electrónica de la entidad.

Los auditores deben conocer los controles automatizados que tienen impacto en el proceso de elaborar la **información financiera incluyendo los controles generales de tecnología de información (CGTI) que están formados principalmente por controles relacionados con la seguridad de la información, incluyendo los de ciberseguridad.**

Por ejemplo, si se audita el gasto correspondiente a la gestión de la receta electrónica, se deberá contar necesariamente con recursos humanos especializados para revisar los sistemas de información, los CGTI y la ciberseguridad. Este es un ejemplo muy claro de la problemática de la ciberseguridad, ya que el proceso está respaldado por un complejo conjunto de aplicaciones y sistemas de información interrelacionados a través de redes públicas y privadas, con múltiples actores, en el que los ciberriesgos son muy elevados. Hoy en día ciberdelincuentes podrían introducir recetas falsas en el sistema sin necesidad de acudir a un médico o una farmacia y cobrar el dinero fraudulentamente obtenido, cómodamente sentados en una ciudad de Asia o de América, suplantando las identidades electrónicas de facultativos, farmacias y funcionarios. Para evitar este tipo de fraude están los controles de ciberseguridad.

Siguiendo con este ejemplo, se puede afirmar que solo el **trabajo conjunto e integrado de auditores financieros y auditores de sistemas** de un OCEX, permite hoy día fiscalizar este componente muy significativo del gasto sanitario. Como en muchos otros ejemplos que se podrían poner, auditar de otra forma en el siglo XXI no es posible.

Por otra parte, debido al gran número de CGTI que existen en una entidad mediana o grande resulta materialmente imposible para un auditor revisarlos en su totalidad. Además, gran parte de ellos no tendrán interés para los objetivos de la auditoría ya que solo un pequeño subconjunto tendrá impacto en nuestro riesgo de auditoría y sólo sobre ellos se deberá centrar la atención y el trabajo del auditor.

Para seleccionar los controles a revisar el auditor de estados financieros utilizará un enfoque de riesgo, de arriba-abajo en la auditoría del control interno, siguiendo la metodología de la GPF-OCEX 1315, y para cada área o aplicación significativa identificada se requiere que:

a) Se valoren los riesgos de incorrección material relacionados.
b) Se revise la eficacia de los CGTI.
   La importancia de los CGTI es tal que del resultado de su revisión dependerá la naturaleza, extensión y momento de realización de las pruebas sobre los controles de procesos/aplicación y de las pruebas sustantivas.
c) Se revise la eficacia de los controles de aplicación.
d) Se realicen las pruebas sustantivas.

Este enfoque nos permitirá centrarnos solo en los controles que están relacionados con los sistemas y las aplicaciones significativas a efectos de la información contable, financiera o presupuestaria auditada, de acuerdo con los objetivos y alcance de la auditoría que se esté realizando. El resto carece de interés para la auditoría. Si se revisan los CGTI que no tiene relación con la información auditada se estará haciendo un trabajo innecesario y por tanto ineficiente.

[14] Véase el apartado 9.2 de la GPF-OCEX 1316 y apartados 21 y A95-A97 de la NIA-ES 315. De acuerdo con estas normas deben distinguirse dos tipos de controles:

- Los CGTI son políticas y procedimientos vinculados a muchas aplicaciones y favorecen un funcionamiento eficaz de los controles de las aplicaciones.
  Si los CGTI son débiles, disminuye la fiabilidad en los controles relacionados con aplicaciones individuales.
- Los controles de aplicación son procedimientos manuales o automatizados que normalmente operan a nivel de procesos de gestión y que se aplican al procesamiento de las transacciones mediante aplicaciones informáticas específicas.
  Tienen como finalidad asegurar la integridad de los registros contables, están relacionados con los procedimientos utilizados para iniciar y procesar transacciones y otros datos financieros, así como para informar sobre ellos.
  Estos controles ayudan a asegurar que las transacciones han ocurrido, están autorizadas y se han registrado y procesado íntegra y exactamente.

Por ejemplo, si se está revisando una aplicación de gestión de nóminas por ser los gastos de personal un área significativa, los procedimientos de revisión de los controles generales estarán focalizados en aquellos que afectan más directamente a esa aplicación. En este caso no tendría ningún interés revisar los controles relacionados con el desarrollo y mantenimiento de la aplicación de gestión del inventario del inmovilizado. Tampoco se revisarían los controles de acceso o la gestión de usuarios de la aplicación de ingresos, ya que esos trabajos no nos permitirían reducir el riesgo de auditoría del área de gastos de personal. Se deberían revisar los CGTI relacionados con la aplicación de recursos humanos, con la de nóminas, las bases de datos de ambas aplicaciones, y con los sistemas operativos y servidores que soportan dichas aplicaciones y bases de datos.

El interés principal de un auditor financiero y de los auditores de sistemas que le prestan apoyo está en los controles y sistemas más próximos a los datos y a las aplicaciones significativas para las cuentas auditadas, tales como las aplicaciones de contabilidad, compras, personal, inmovilizado, etc. Éstas son solo un subconjunto de la totalidad de los sistemas y datos utilizados por las entidades para gestionar todas las operaciones de su actividad.

En la figura 3[15] describe el típico camino de acceso a los datos en un sistema de información.

Es importante destacar que los ciberincidentes normalmente se inician a través de los niveles/capas de la red perimetral e interna, que tienden a estar cada vez más alejados de las aplicaciones, bases de datos y sistemas operativos que son los que se suelen incluir en las pruebas de controles de acceso a los sistemas que afectan a los estados financieros. La revisión de aspectos como por ejemplo, la protección perimetral de la red frente a intrusiones y los accesos a la intranet, la revisión de la configuración de los cortafuegos existentes en los puntos de acceso a las redes corporativas, requiere perfiles técnicos muy especializados en los equipos de auditoría de sistemas de información.

También será importante revisar los controles de acceso lógico (contraseñas, identificación y autenticación de usuarios), la gestión de usuarios de las aplicaciones significativas para la auditoría y de las bases de datos subyacentes. Una típica prueba de auditoría en esta área consiste en verificar que los denominados "superusuarios" o usuarios privilegiados están debidamente restringidos al mínimo estrictamente necesario y además que están debidamente controlados.

Adicionalmente, si el número de aplicaciones significativas es elevado, tal como sucede por ejemplo en la auditoría de las cuentas de una comunidad autónoma, será imposible revisar en una fiscalización todos los controles de aplicación y CGTI relacionados. En estos casos se diseñará un plan de auditoria plurianual que establezca un calendario para la revisión de los controles automatizados, tanto de aplicación cómo generales, que sea realizable con los recursos del OCEX.

6. RETOS EN MATERIA DE PERSONAL

Ante el reto que representa abordar las auditorías integrando cuestiones de ciberseguridad, los OCEX deben plantearse modificar sus plantillas e incorporar especialistas en auditoría de sistemas de información.

Estos especialistas en auditoría de sistemas de información prestarán apoyo a los auditores financieros y se formarán **equipos de auditoría integrados por ambas disciplinas, con metodología actualizada**, de forma que se haga un trabajo adaptado a las nuevas circunstancias de la administración electrónica mucho más efi-

[15] Gráfico inspirado en *Cybersecurity and the External Audit, Center for Audit Quality*.

caz y eficientemente. Esta integración de disciplinas es un aspecto clave para el futuro de los OCEX.

Descuidar esta materia, trabajar como se hacía hace 30 años, supone incrementar el riesgo de auditoría hasta niveles inadmisibles. Los OCEX deben estar perfectamente preparados para enfrentar el nuevo entorno y abordar los riesgos relacionados con la ciberseguridad, ya que no solo las actividades ordinarias se realizan a través de los sistemas de información interconectados, las actividades fraudulentas, corruptas y delictivas, también se realizan por medios electrónicos.

Hasta que se incorporen auditores de sistemas de información y expertos en ciberseguridad, los OCEX disponen del recurso de contratar expertos externos para cubrir ese déficit de conocimientos y de profesionales.

Por otra parte, hay que tener en cuenta que debido a que cada vez más organizaciones confían en las TIC para automatizar sus operaciones, la línea que separa el rol de los auditores de sistemas de información y el resto de auditores es cada vez más difusa[16]. El auditor financiero es responsable de valorar los riesgos de incorrección material en los estados financieros, incluyendo los derivados de accesos no autorizados a los sistemas TIC, por lo que cada vez se va a tener que relacionar más extensamente con el personal de sistemas de los entes fiscalizados y tener presente cuestiones relacionadas con la seguridad de la información.

De cara al futuro el perfil del auditor financiero va a requerir un mayor componente tecnológico, aspecto este que deberá incorporarse en los mecanismos de acceso a las plantillas de los OCEX.

Hasta que se incorporen las nuevas generaciones de auditores con perfiles actualizados, el personal actual debe recibir continuas actividades formativas relacionadas con la administración electrónica, la seguridad de la información, la ciberseguridad y las TIC en general.

7. CONCLUSIONES

Dada la potencial repercusión que las amenazas a la seguridad de los sistemas de información representan sobre la actividad de los entes públicos y su efecto sobre las cuentas que se auditan, la ciberseguridad se ha convertido en uno de los temas más relevantes tanto para los gobiernos, como para los gestores públicos y por supuesto para los OCEX.

La importancia máxima de la ciberseguridad en los actuales entornos de administración electrónica está en estos momentos fuera de toda discusión. El crecimiento y extensión de los ciberincidentes padecidos en los últimos tiempos (por ejemplo los casos Wannacry y Lexnet) ha fortalecido la concienciación de los auditores públicos para incluir en su metodología ordinaria de trabajo la revisión de los controles de seguridad de la información y de ciberseguridad.

Puesto que en un futuro muy cercano los auditores sólo van a trabajar con evidencia electrónica es necesario realizar procedimientos de auditoría para obtener un determinado nivel de seguridad respecto de la evidencia digital que soporte los informes de fiscalización. Esta seguridad se obtendrá mediante la revisión de los CGTI y mediante la confianza que se deposite en el adecuado cumplimiento del ENS por parte de los entes fiscalizados.

Por su gran importancia, los OCEX deben verificar en todas las fiscalizaciones el cumplimiento de la legalidad en relación con el ENS, y si no se acredita se debería reflejar en el informe como un incumplimiento grave o muy significativo.

Los OCEX deben actualizar su metodología de trabajo de forma que contemple la importancia de las TIC y de la ciberseguridad, integrando la disciplina de auditoría de sistemas de información. Esta tarea a nivel general se está acometiendo con la elaboración de las Guías Prácticas de Fiscalización de los OCEX.

En las fiscalizaciones individuales, los auditores responsables deben analizar cómo afectan las cuestiones relacionadas con la seguridad informática y la ciberseguridad a los objetivos de su auditoría y a los riesgos.

Ante el reto que representa abordar las auditorías integrando cuestiones de ciberseguridad, los OCEX deben plantearse modificar sus plantillas y crear equipos de especialistas en auditoría de sistemas de información para que presten apoyo a los equipos que realizan auditorías financieras y se formen equipos de auditoría integrados por ambas disciplinas, con metodología actualizada, de forma que se haga un trabajo adaptado a las nuevas circunstancias de la administración electrónica mucho más eficaz y eficientemente.

Hasta que se incorporen auditores de sistemas de información y expertos en ciberseguridad, los OCEX disponen del recurso de contratar expertos externos para cubrir ese déficit de conocimientos y de profesionales.

De cara al futuro, el perfil del auditor financiero va a requerir un mayor componente tecnológico, aspecto este que deberá incorporarse en los mecanismos de acceso a las plantillas de los OCEX.

El personal actual debe recibir continuas actividades formativas relacionadas con la administración electrónica, la seguridad de la información, la ciberseguridad y las TIC en general.

La puesta en marcha de todas estas medidas, con total seguridad, no será ni fácil, ni rápida, ni barata, por eso

[16] Véase *Handbook on IT Audit*, apartado I.6.

es necesario el compromiso firme de los órganos de gobierno de los OCEX y de los directores de fiscalización, sin el cual las posibilidades de éxito en esta complicada empresa transformacional son prácticamente nulas.

Sin esa evolución o transformación tecnológica del núcleo de su actividad, las instituciones públicas de control externo solo podrán, como espectadores pasivos, ver agrandarse cada vez más la brecha digital que las separa del mundo de la administración electrónica y, en consecuencia, incrementarse el riesgo de auditoría. Solo es cuestión de tiempo que todos nos concienciemos plenamente y se tomen las decisiones adecuadas para que todos los OCEX se adentren con determinación en el futuro digital (Minguillón, 2016).

8. BIBLIOGRAFÍA

Altafaja, Joaquim (2017), "*La ciberseguretat, un nou component de risc rellevant en l'auditoria de Comptes*", *l'Auditor* número 79 de julio de 2017.

Center for Audit Quality (2017), "*The CPA's Role in Addressing Cybersecurity Risk*".

Center for Audit Quality (2016) "*Understanding Cybersecurity and the External Audit*".

Centro Criptológico Nacional (2017), "Guía de auditoría del ENS CCN-STIC-802".

Centro Criptológico Nacional (2017), "Ciberamenazas y Tendencias", CCN-CERT IA-16/17.

ENISA (2016), "*Threat Taxonomy*".

ENISA (2015), "*Definition of Cybersecurity*".

INCIBE (2017), "Glosario de términos de ciberseguridad". Versión 1.

INTOSAI, "WGITA-IDI Handbook on It Audits for Supreme Audit Institutions", 2014.

ISACA (2013), "Transforming Cybersecurity".

ISACA (2017), "Auditing Cyber Security: Evaluating Risk and Auditing Controls".

Loeb, Matthew (2017), "*Creating cyberculture*", csoonline.com, 22 de agosto.

Minguillón Roy, Antonio (2016), "El control externo y la auditoría de sistemas de información", *Revista Española de Control Externo*, nº 53.

Minguillón Roy, Antonio (2016), "La revisión de los controles generales en un entorno informatizado", *Auditoría Pública* nº 52.

Minguillón Roy, Antonio (2006) "La fiscalización en entornos informatizados", *Auditoría Pública* nº 40.

Minguillón Roy, Antonio (2014), "La importancia de los sistemas de información en la auditoría pública", ponencia presentada en el *VI Congreso de Auditoría Pública*.

Minguillón Roy, Antonio (2010),"La auditoría de sistemas de información integrada en la auditoría financiera. La perspectiva del sector público". Edición digital de la Sindicatura de Cuentas de la Comunidad Valenciana.

Sindicatura de Cuentas de la Comunidad Valenciana, Manual de fiscalización, Sección 2850-Los controles generales de TI.

OCEX, Guías prácticas de fiscalización de los OCEX 1315, 1316, 1317, 1500 y 5300.