FUNDACIÓN FIASEP
GESTIÓN Y AUDITORÍA PARA LA TRANSPARENCIA EN EL SECTOR PÚBLICO

Serie ***OPINIONES FIASEP***

Nº 13/2022

"Auditoría de cuentas anuales y Ciberseguridad: la nueva NIA-ES 315 (Revisada) y el auditor público"

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

Abril, 2022

1. Introducción

La ciberseguridad se ha convertido en una preocupación cada vez más importante tanto para el sector privado como para las administraciones públicas, las instituciones de control y también para el público en general. Esta creciente preocupación es debida al significativo e imparable crecimiento en el número y la gravedad de los ciberataques a todo tipo de entidades.

En estas notas me voy a centrar en analizar cómo deben considerar los auditores públicos los riesgos de ciberseguridad en una auditoría de cuentas anuales realizada de conformidad con las NIA-ES/NIA-ES-SP y en especial de conformidad con los requerimientos establecidos al respecto por la nueva[1] *NIA-ES 315 (Revisada) Identificación y valoración del riesgo de incorrección material* o NIA-ES 315R.

En los últimos tiempos ha habido una amplia integración de la tecnología en el funcionamiento de las entidades públicas, incluida una mayor dependencia de las interconexiones a través de internet, que en gran medida se ha acelerado por la incorporación del teletrabajo en respuesta a la problemática que planteó el confinamiento por la pandemia COVID-19.

La realidad, en 2022, es que el auditor público audita en un **entorno de administración electrónica avanzada** en el que la gestión de las administraciones y entidades públicas se caracteriza, expuesto de forma telegráfica, por:

- Gestión totalmente digital con ausencia de papel físico.
- Uso intensivo de aplicaciones informáticas complejas, integradas e interconectadas a través de internet.
- Integración de controles internos automatizados o semiautomatizados en las aplicaciones de gestión.
- Uso creciente de la computación en la nube.
- Bases de datos masivas, con todo tipo de formatos.
- Uso creciente de tecnologías emergentes como el blockchain y la inteligencia artificial.
- Teletrabajo.
- Riesgos crecientes y preocupación por la ciberseguridad.

Si bien existen enormes oportunidades para las entidades públicas en la adopción de tecnologías avanzadas, el aumento de la conectividad y la dependencia de internet aumenta de forma paralela el riesgo de ciberataques y de accesos no autorizados a sus sistemas de información, lo que puede dar lugar a la pérdida de información confidencial, la manipulación y destrucción de datos y sistemas, e incluso el daño de los activos físicos. El impacto en las cuentas anuales de una entidad afectada por un ciberincidente puede llegar a ser muy significativo y por tanto es un riesgo que requiere la atención de los auditores.

Los acontecimientos internacionales recientes, como la guerra en Ucrania, no han hecho más que intensificar esta tendencia, incrementándose los ciberataques a nivel mundial de forma generalizada y la consiguiente preocupación a todos los niveles. Baste como botón de muestra de esa preocupación la reciente declaración del presidente de la nación más poderosa del mundo: *Statement by President Biden*

[1] Aprobada mediante resolución del ICAC de 14 de octubre de 2021.

on our Nation's Cybersecurity[2]*,* y los consejos emitidos por su administración: *FACT SHEET: Act Now to Protect Against Potential Cyberattacks*[3]*.* Las recomendaciones incluidas en este último documento son válidas para todos, no solo para los ciudadanos de ese país.

En España, el Consejo de Ministros aprobó el 29 de marzo de 2022 el Plan Nacional de ciberseguridad, dotado con un presupuesto de 1.000 millones de euros para reforzar en el conjunto de España las capacidades de planificación, preparación, detección y respuesta en el ciberespacio.

2. Qué es la ciberseguridad

De acuerdo con la guía *GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa* entenderemos por ciberseguridad la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad 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 es coherente con el Esquema Nacional de Seguridad (ENS) y contempla las **características fundamentales de la información y de los sistemas de información** que la ciberseguridad debe garantizar y que forman las cinco dimensiones de seguridad de la información:

- La **disponibilidad** 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 **confidencialidad** es la propiedad de la información, por la que se garantiza que está accesible únicamente al personal autorizado a acceder a dicha información.
- 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.
- 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 **trazabilidad** es la propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

En síntesis, podemos decir que la finalidad de la ciberseguridad es proteger los activos de información procesada, almacenada y transportada por redes y sistemas de información interconectados.

Los controles que tienen por finalidad proteger los activos de información y garantizar el cumplimiento de estas características o dimensiones de la seguridad de la información forman parte de los controles generales de tecnologías de la información (CGTI).

3. Qué es un incidente de ciberseguridad

En la Guía práctica de fiscalización *GPF-OCEX 5312 Glosario de Ciberseguridad* se define incidente de seguridad como **todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información**. También puede definirse como cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la entidad, por ejemplo: el acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

A fin de determinar la importancia de los efectos de un incidente, se tendrán en cuenta los siguientes

[2] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/, 21 de marzo de 2022.

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/, 21 de marzo de 2022.

parámetros:

a) el número de usuarios afectados por la perturbación del servicio;

b) la duración del incidente;

c) la extensión geográfica de la zona afectada por el incidente;

d) el impacto (coste) económico.

Algunos ejemplos de incidentes de ciberseguridad con efectos **directos o indirectos en las cuentas anuales** incluyen, por ejemplo:

- Extracción o robo de información protegida o sensible.
- Paralización de la actividad por un ataque de *ramsomware*. Además de los costes de la no actividad, los costes de recuperación suelen ser muy elevados.
- Acceso a la información y aplicaciones financieras mediante la utilización de usuarios privilegiados, lo que permitiría manipular la información financiera.
- Robo de credenciales y fraude posterior.
- Fraude del CEO. En muchos casos este tipo de fraudes ascienden a millones de euros robados.
- Deterioro de los activos debido a la disminución de los flujos de efectivo operativos como resultado de un ciberataque.

4. La responsabilidad de los órganos de gobierno y dirección de la entidad, y la gobernanza de ciberseguridad

Los órganos de gobierno y dirección de la entidad son los responsables de preparar las cuentas anuales de conformidad con el marco de información financiera aplicable y de diseñar e implementar los controles internos necesarios para ello. También son los responsables de contar con un proceso de gestión de riesgos con objeto de identificar riesgos, incluidos los de ciberseguridad, valorarlos e implementar y supervisar los controles internos para responder a esos riesgos.

Reconocer y gestionar el riesgo es una parte crucial del papel de los órganos de gobierno y dirección. El crecimiento de la ciberdelincuencia significa que la ciberseguridad es un riesgo de negocio que las entidades públicas deben considerar y gestionar, incluyendo el diseño e implantación de los controles pertinentes para disponer de una protección adecuada frente a amenazas externas e internas.

Para las entidades cuyas operaciones puedan verse afectadas de forma significativa, es importante que los órganos de gobierno y dirección tengan en cuenta los riesgos relacionados con la ciberseguridad, que analicen cuándo puede producirse un incidente de este tipo que sea cuantitativa o cualitativamente importante y las implicaciones para las cuentas anuales.

En relación con las responsabilidades de la alta dirección, el párrafo A108 de la NIA-ES 315R señala que la evaluación del entorno de control en relación con la utilización de TI por parte de la entidad incluirá el conocimiento de si la **gobernanza de TI** de la entidad es acorde con la naturaleza y complejidad de las operaciones de negocio realizadas a través de TI, incluida la complejidad de la plataforma tecnológica de la entidad.

La **gobernanza de ciberseguridad**, como parte del concepto más amplio de gobernanza de TI, se refiere al conjunto de responsabilidades y actividades realizadas por la alta dirección con el objetivo de proporcionar una dirección estratégica en esta materia, garantizar que se logren los objetivos, verificar que el riesgo se gestione adecuadamente y comprobar que se utilicen los recursos de la entidad de una

forma responsable.[4]

Los principales elementos de una adecuada gobernanza de ciberseguridad están implícitos en el Esquema Nacional de Seguridad y la normativa relativa a la protección de datos de carácter personal. La responsabilidad sobre dicho proceso es de la alta dirección u órganos superiores. En el caso de las entidades locales son el presidente o la presidenta y la Junta de Gobierno los responsables de que existan unos controles adecuados sobre los sistemas de información y las comunicaciones. De acuerdo con sus competencias, deben garantizar que el funcionamiento de la entidad resulte conforme con las normas aplicables y que los controles internos proporcionen una garantía razonable de que la información, los servicios y los sistemas de información que les dan soporte cumplan con las cinco dimensiones de la seguridad de la información que establece el Esquema Nacional de Seguridad: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

La implicación de los órganos superiores es, tal vez, el factor más importante para la implantación con éxito de un sistema de gestión de la seguridad de la información o de ciberseguridad[5]. La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información[6] que debe materializarse en aspectos tales como[7]:

- De acuerdo con el artículo 11 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, debe formularse la **política de seguridad de la información (PSI) que debe ser aprobada por el titular del órgano superior** de la entidad.
- Asignar los roles y responsabilidades en materia de seguridad de la información. Los órganos superiores de la entidad deben nombrar al **responsable de la información**, al **responsable del servicio**, al **responsable de la seguridad** y al **responsable del sistema**.
- Autorizar la implementación y operación de un **Comité de Seguridad TIC.** La gobernanza de la seguridad de la información en una organización se articula a través de un comité de seguridad TIC[8], que se constituye como un órgano colegiado. Su composición debe constar en la PSI.
- **Proporcionar los recursos materiales y humanos** necesarios y asegurar que se implantan programas de concienciación, formación y capacitación.
- Decidir los criterios de aceptación del **riesgo** y los niveles aceptables de riesgo.
- Dirigir las revisiones periódicas de la PSI y velar por la realización de las **auditorías de seguridad**.

[4] Véase el glosario de la Information Systems Audit and Control Association (ISACA).

[5] *Guía de iniciación a actividad profesional implantación de sistemas de gestión de la seguridad de la información (SGSI) según la norma ISO 27001*, Colegio Oficial de Ingenieros de Telecomunicación.

[6] *UNE-EN ISO/IEC 27001 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información*, apartado 3.4.

[7] Véase el *Informe de auditoría de los controles básicos de ciberseguridad de la Diputación de Alicante del ejercicio 2021*.

[8] *Guía de seguridad de las TIC, CCN-STIC 201. Organización y gestión para la seguridad de las TIC*, CCN, enero de 2021.

El análisis de la gobernanza de la ciberseguridad tiene implicaciones muy relevantes tanto a efectos de la valoración de riesgos de incorrección material en una auditoría financiera por ser un **elemento esencial del *entorno de control* del sistema de control interno**, como a efectos del **cumplimiento de la legalidad**, de gran relevancia en la auditoría del sector público.

5. Responsabilidad del auditor

El objetivo del auditor en una auditoría de estados financieros es la obtención de una **seguridad razonable** de que los estados financieros en su conjunto están libres de incorrección material, debida a fraude o error, que le permita expresar una opinión sobre si los estados financieros están preparados, en todos los aspectos materiales, de conformidad con un marco de información financiera aplicable.

Para ello, de acuerdo con las NIA-ES-SP 1315 / NIA-ES 315R / GPF-OCEX 1315, el auditor **debe identificar y valorar los riesgos de incorrección material, debidos a fraude o error, tanto en los estados financieros como en las afirmaciones con la finalidad de proporcionar una base para el diseño y la implementación de procedimientos posteriores de auditoría en respuesta a los riesgos valorados de incorrección material** de conformidad con la NIA-ES-SP 1330.

La ciberseguridad es un riesgo para cualquier entidad que utilice Internet, pero la probabilidad de que dé lugar a un riesgo de incorrección material para determinados saldos y revelaciones en las cuentas anuales es una consideración que se debe hacer en cada caso, ya que dependerá de los hechos y circunstancias de una entidad. Es decir, la ciberseguridad puede contribuir a la susceptibilidad a la incorrección en las cuentas de la entidad dependiendo de las circunstancias (como las que se verán más adelante en el ejemplo sobre las diferencias entre una agencia tributaria y un consorcio de bomberos).

Entre los riesgos que debe identificar y valorar el auditor se encuentran los riesgos derivados de la utilización de las TI[9]. Dentro de estos, los riesgos de ciberseguridad adquieren cada vez mayor importancia y deben ser, por tanto, objeto de mayor atención por el auditor.

En definitiva, la responsabilidad del auditor en relación con la ciberseguridad es, al igual que con el resto de riesgos, en primer lugar, valorar los riesgos inherentes derivados del uso de TI y los riesgos de control, considerar el impacto de un potencial ciberincidente y a continuación responder adecuadamente cuando se detecte un riesgo de incorrección material debido a este tipo de amenazas.

6. Conocimiento de los riesgos de negocio derivados del uso de las tecnologías de la información

Al realizar la valoración de riesgos, la NIA-ES 315R **requiere que los auditores obtengan un conocimiento de la entidad y su entorno, que incluya el modelo de negocio de la entidad y el modo en que ese modelo de negocio integra la utilización de TI en sus interacciones con clientes/usuarios/contribuyentes, proveedores, fuentes de financiación y otros interesados mediante intercomunicaciones de TI y otras tecnologías[10].**

Conocer el modelo de negocio y el uso de TI ayuda al auditor a entender los riesgos de negocio a los que se enfrenta una entidad, pero no todos los riesgos de negocio dan lugar a riesgos de incorrección material en las cuentas anuales.

El sector en el que opera la entidad es también una consideración relevante, ya que determinados sectores pueden tener un mayor riesgo debido a un historial de incidentes de seguridad y a la naturaleza

[9] Definidos en la NIA-ES 315R como la "exposición de los controles de procesamiento de la información a un diseño o un funcionamiento ineficaces, o riesgos para la integridad de la información (es decir, la completitud, exactitud y validez de las transacciones y demás información) en el sistema de información de la entidad, debido a un diseño o a un funcionamiento ineficaz de los procesos de TI de la entidad".

[10] Véase el *párrafo 19 y Anexo 1 Consideraciones para el conocimiento de la entidad y su modelo de negocio, de la NIA-ES 315R*

sensible de los datos que poseen. Según el informe "Ciberamenazas y tendencias Edición 2021" del Centro Criptológico Nacional los principales sectores de interés para los ciberatacantes han sido:

- **Gubernamental**
- Defensa
- Industria armamentística
- **Salud** e industria farmacéutica
- Centros de investigación
- Tecnologías de la información y las comunicaciones
- Energía
- Telecomunicaciones
- Inversión financiera
- Comercio internacional

Aunque la ciberseguridad es un riesgo para cualquier entidad, no todas las entidades se pueden ver afectadas de forma significativa por un incidente de ciberseguridad. Como he señalado, este riesgo no siempre da lugar a un riesgo de incorrección material en las cuentas anuales que exija que el auditor diseñe y aplique una respuesta (un procedimiento de auditoría posterior). Dependerá de su modelo de negocio y cómo se utilizan las TI.

Por ejemplo, en una entidad de gestión tributaria cuya gestión se realiza apoyándose totalmente en complejos sistemas y aplicaciones informáticas alojadas en la *nube*, el riesgo de negocio derivado del uso de TI y de ciberseguridad sería crítico. Sin embargo, para un consorcio de bomberos el riesgo de negocio derivado del uso de TI y de ciberseguridad sería mínimo. Por tanto, vemos como la valoración del riesgo inherente derivado de la actividad de la entidad auditada, del uso de TI y de la ciberseguridad en los dos casos del ejemplo sería muy distinto.

7. Conocimiento de la utilización de TI en los componentes del sistema de control interno de la entidad y la ciberseguridad

El apartado A94 de la NIA-ES 315R señala que **el objetivo global y el alcance de una auditoría no son diferentes si una entidad opera en un entorno mayoritariamente manual, un entorno totalmente automatizado o un entorno en el que se combinan elementos manuales y automatizados** (es decir, controles manuales y automatizados y otros recursos utilizados en el sistema de control interno de la entidad).

Aunque el objetivo y el alcance de una auditoría no sean diferentes, el grado de digitalización de la entidad, además de a los riesgos inherentes, afecta a la forma en que debe realizarse el conocimiento del sistema de control interno y sus componentes, la valoración de los riesgos de control y las pruebas de los controles automatizados.

Señalaré algunos apuntes sobre los componentes de un sistema de control interno:

- La evaluación por el auditor del **entorno de control**[11] en relación con la utilización de TI por la entidad puede incluir cuestiones tales como si la gobernanza sobre las TI es acorde con la naturaleza y complejidad de la entidad y de sus operaciones de negocio realizadas a través de TI, incluida la complejidad o madurez de la plataforma o arquitectura tecnológicas de la entidad y hasta qué punto confía la entidad en aplicaciones de TI para sustentar su información financiera. La gobernanza de ciberseguridad es un aspecto esencial para un buen sistema de control interno.

[11] Párrafo A108 de la NIA-ES 315R.

- El auditor también debe considerar el modo en que el **proceso de la entidad para el seguimiento del sistema de control interno**[12] trata el seguimiento de controles de procesamiento de la información (anteriormente denominados controles de aplicación) en el que interviene la utilización de TI. Esto puede incluir, por ejemplo: controles para el seguimiento de entornos de TI complejos o controles de segregación de funciones.

- El conocimiento que debe adquirir el auditor del **sistema de información**[13] incluye el entorno de TI relevante para los flujos de transacciones y el procesamiento de la información en el sistema de información de la entidad, porque la utilización de aplicaciones de TI u otros aspectos del entorno de TI pueden dar lugar a riesgos derivados de la utilización de TI. Este conocimiento se puede centrar en identificar y comprender la naturaleza y el número de las aplicaciones específicas de TI y otros aspectos del entorno de TI que son relevantes para los flujos de transacciones y el procesamiento de la información.

- Las **actividades de control**[14]. La NIA-ES 315R dedica un amplísimo espacio a las consideraciones que el auditor debe realizar sobre el conocimiento, identificación y valoración de riesgos, y la identificación de controles automatizados en un entorno TI, que resulta imposible reseñar en estas breves líneas. Se distingue claramente, como hasta ahora, entre controles de procesamiento de la información (antes denominados controles de aplicación) y controles generales de TI.

Como parte de la valoración de riesgos, la NIA-ES 315R requiere de forma explícita que el auditor obtenga un conocimiento de los sistemas de información relevantes para la preparación de las cuentas anuales y del sistema de control interno de la entidad con la finalidad de identificar y valorar los riesgos de incorrecciones materiales. Esto incluye comprender el uso de la tecnología de la información por parte de la entidad e identificar los riesgos derivados del uso de la tecnología de la información, entre los cuales los de ciberseguridad son cada vez más relevantes.

La nueva NIA-ES 315R concede un énfasis importante a la consideración de los riesgos tecnológicos y ofrece una amplia orientación sobre el conocimiento de las TI y la identificación de los riesgos derivados del uso de las TI en toda la norma y en especial en el *Anexo 5 Consideraciones para el conocimiento de las tecnologías de la información.* Este anexo incluye orientaciones sobre los casos en que puede haber un mayor riesgo relacionado con la ciberseguridad.

Finalmente, señalaré que independientemente de si se ha producido o no un ciberataque o un incidente de ciberseguridad, el auditor, como parte de sus procedimientos de valoración de riesgos, debe tener en cuenta las implicaciones de la ciberseguridad en las cuentas anuales y permanecer alerta durante toda la realización de la auditoría de los incidentes de ciberseguridad y su posible impacto en la valoración inicial del riesgo realizada.

8. Los Controles Generales de Tecnologías de la Información (CGTI)

La NIA-ES 315R requiere expresamente en su apartado 26 que los auditores obtengan un conocimiento del componente de actividades de control (los controles) del sistema de control interno mediante la aplicación de procedimientos de valoración del riesgo e identifique los CGTI de la entidad que responden directamente a los riesgos derivados de la utilización de TI, incluidos los de ciberseguridad. Para cada uno de los controles identificados evaluará si está diseñado eficazmente para responder al riesgo de incorrección material en las afirmaciones o si está diseñado eficazmente para sustentar el funcionamiento

[12] Párrafo A117 de la NIA-ES 315R.

[13] Párrafo A140 de la NIA-ES 315R.

[14] Párrafo A148 de la NIA-ES 315R.

de otros controles y determinará si el control ha sido implementado eficazmente.

Los auditores responsables de cada auditoría deben analizar cómo afectan las cuestiones relacionadas con la seguridad informática y la ciberseguridad a los objetivos de la auditoría. Cuanto mayor sea la entidad auditada y más complejos sus sistemas de información, mayor impacto tendrán los aspectos tecnológicos y los riesgos TI, y mayores serán las consideraciones al respecto que deba hacerse el auditor. El auditor obtendrá un conocimiento suficiente sobre cómo utiliza el ente auditado los sistemas de información, sobre el diseño y funcionamiento de los controles automatizados y su impacto en los estados financieros. Esto incluye revisar los CGTI (que en gran medida están formados por los controles de seguridad de la información y ciberseguridad) con el alcance específico que se determine en cada caso, en concordancia con el alcance y objetivos de la auditoría.

Solo tras adquirir ese conocimiento se podrán valorar los riesgos de incorrección material en los estados financieros, por ejemplo, los riesgos resultantes de un acceso no autorizado a los sistemas de información y de una utilización y disposición no autorizados de los activos de información de la entidad.

En el *Anexo 6 Consideraciones para el conocimiento de los controles generales de TI* de la NIA-ES 315R se proporcionan consideraciones adicionales que el auditor puede tener en cuenta para el conocimiento de los CGTI.

Los CGTI son las políticas y procedimientos que se aplican a la totalidad o a gran parte de los sistemas de información de una entidad, incluyendo la infraestructura y plataformas TI de la organización auditada y ayudan a asegurar su correcto funcionamiento. Son aquellos controles relacionados con el uso de las tecnologías de la información y las comunicaciones implantados en los distintos niveles de la estructura organizativa general de una institución y en sus sistemas de información.

Su **finalidad** en un entorno informatizado es establecer un marco general de control y confianza sobre las actividades del sistema informático y asegurar razonablemente la consecución de los objetivos generales de control interno y el correcto funcionamiento de los controles de procesamiento de la información (controles de aplicación).

Su importancia radica en que tienen un efecto generalizado, es decir, suelen afectar a más de una aplicación informática, y si los CGTI no funcionan adecuadamente se imposibilita que se pueda confiar en los controles de los procedimientos y aplicaciones de gestión.

Desde el punto de vista del auditor, los objetivos de los CGTI (ver GPF-OCEX 5330) son proporcionar una garantía razonable de que los datos, la información y los activos de los sistemas de información cumplen las siguientes propiedades, que coinciden con las cinco dimensiones de la seguridad de la información que establece el Esquema Nacional de Seguridad: Confidencialidad, Integridad, Disponibilidad, Autenticidad, y Trazabilidad.

Unos CGTI sólidos constituyen una buena línea de defensa para la ciberseguridad.

De acuerdo con la metodología establecida en la GPF-OCEX 5330, la revisión de los CGTI se estructura en las cinco categorías siguientes[15]:

A. Marco organizativo *(entorno de control)*

B. Gestión de cambios en aplicaciones y sistemas

C. Operaciones de los sistemas de información

D. Controles de acceso a datos y programas

E. Continuidad del servicio

[15] Esta estructura, establecida en el apartado 9.2 de la GPF-OCEX 1316, es totalmente coherente con el *Handbook on IT Audit* de INTOSAI y también con la NIA-ES 315R.

9. Los equipos de auditoría y la ciberseguridad

La NIA-ES 315R señala en el párrafo A55 que "la utilización de TI y la naturaleza y extensión de cambios en el entorno de las TI pueden afectar también a las **cualificaciones especializadas necesarias** para ayudar en la obtención del conocimiento requerido" de la entidad, de su entorno TI y del sistema de control interno. Y en el párrafo A171 se insiste en que "cuando el entorno de TI de una entidad es más complejo, es probable que la identificación de las aplicaciones de TI y otros aspectos del entorno de TI, la determinación de los riesgos relacionados derivados de la utilización de TI y la identificación de controles generales de TI requiera la participación de **miembros del equipo con cualificaciones especializadas en TI**. Es posible que esa participación sea **esencial** y **tenga que ser extensa en el caso de entornos de TI complejos**", como son los entornos de administración electrónica avanzada.

De acuerdo con esto, para auditar entidades medianas o grandes operando en un **entorno de administración electrónica avanzada** deben formarse equipos mixtos, integrados por auditores financieros y por especialistas en auditoría de sistemas de información y ciberseguridad, trabajando conjuntamente con metodología actualizada basada en las NIA-ES/NIA-ES-SP, de forma que se haga un trabajo adaptado a las nuevas circunstancias mucho más eficaz y eficientemente. Los expertos en seguridad TI analizarán juntamente con los auditores financieros aquellos riesgos y controles que son relevantes para los objetivos de la auditoría financiera, con un enfoque de riesgo según las necesidades de los auditores financieros, ya que no todos los riesgos que pretenden mitigar los CGTI son iguales, ni en probabilidad, ni en su materialidad.

No hacerlo de esta forma, no abordando los riesgos relacionados con la seguridad de la información y la ciberseguridad con personal especializado en TI integrado en los equipos de auditoría, supone asumir unos riesgos de auditoría hasta niveles muy elevados y, en muchos casos, inaceptables.

Si las plantillas no incorporan auditores de sistemas de información y expertos en ciberseguridad, se dispone del recurso de contratar expertos externos para cubrir ese déficit de conocimientos y de profesionales especializados.

10. Bibliografía

The Consideration of Cyber Security Risks in an Audit of a Financial Report, Australian Auditing and Assurance Standards Board, Boletín de mayo de 2021.

NIA-ES 315 (Revisada) Identificación y valoración del riesgo de incorrección material, 14 de octubre de 2021.

GPF-OCEX 1315 Identificación y valoración de los riesgos de incorrección material mediante el conocimiento de la entidad y de su entorno

GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa

GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad

GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica

Understanding Cybersecurity and the External Audit, The Center for Audit Quality, 2016.

Cyber Security: A Paradigm Shift in IT Auditing. How to Deal with Cyber Security Risks in the Financial Statement Audit, COMPACT, marzo de 2016.

Cybersecurity Risk Considerations in a Financial Statements Audit, ISCA, junio de 2018.