La importancia de los controles de ciberseguridad en las fiscalizaciones de los ICEX

Montserrat Olano Salvador
Auditora de la Sindicatura de Comptes de Catalunya

Revista Auditoría Pública nº 83
junio 2024. Páginas: 95-104

Resumen: Dada la gran importancia del uso de las tecnologías de la información y las comunicaciones (TIC), es necesario conocer los riesgos (ciberamenazas, ciberataques, vulneración de protección de datos, etc.) a las que está expuesta toda la información que utiliza la ciudadanía en general y, en particular, las administraciones públicas. Conociendo los riesgos se pueden aplicar sistemas de protección que las instituciones relacionadas con la ciberseguridad ya están estudiando. Para esto, se ha querido profundizar en el concepto de ciberseguridad en las Administraciones públicas y presentar alguna pincelada del Esquema Nacional de Seguridad vigente, aprobado en mayo del 2022.
Por ello, es importante examinar en nuestras fiscalizaciones qué análisis se ha llevado a cabo, así como las medidas de protección que están aplicando. Solo así podremos saber si se están adoptando las medidas necesarias para reducir el riesgo relacionado. Para conseguirlo, los ICEX disponemos de una metodología de auditoría de sistemas específica en forma de guías prácticas de fiscalización (GPF) que nos ayudan en esta tarea.

Palabras Clave: ciberseguridad, ciberataque, ENS, TIC, ciberincidente.

Abstract: Given the great importance of the use of information and communication technologies (ICT), it is necessary to know the risks (cyber threats, cyber attacks, data protection violations, etc.) to which all the information used by citizens in general and public administrations in particular is exposed. By knowing the risks, protection systems can be applied, which institutions related to cybersecurity are already studying. For this, we wanted to go deeper into the concept of cybersecurity in public administrations and present some brushstrokes of the National Security Scheme in force, approved in May 2022. Therefore, it is important to examine in our audits what analysis has been carried out, as well as the protection measures that are being implemented. This is the only way to know if the necessary measures are being taken to reduce the related risk. To achieve this, ICEX has a specific systems audit methodology in the form of practical audit guides (GPF) to assist us in this task.

Keywords: cybersecurity, cyberattack, ENS, ICT, cyberincident.

1. Introducción.

Nuestra sociedad y, en particular, las administraciones públicas están haciendo un uso cada vez más intenso de las tecnologías de la información y las comunicaciones (TIC), lo que ocasiona que la dependencia de los sistemas de información y las comunicaciones para la gestión pública y la prestación de servicios a los ciudadanos no cese de incrementarse cada vez más. La experiencia de la pandemia COVID-19 incrementó hasta puntos impensables la utilización del teletrabajo, aumentando más todavía la dependencia de las TIC. Esta 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.

Además de la implantación de la administración electrónica, durante los últimos años ha habido una gran expansión en la utilización de tecnologías emergentes (cloud computing, internet of things, ERPs, etc) y un aumento del uso de servicios a través de internet. Cada vez con más frecuencia realizamos actividades que se desarrollan en el ciberespacio.

Todo esto conlleva múltiples beneficios, pero también nuevos retos y muchos riesgos a los que hacer frente. Estos riesgos pueden consistir en ciberataques, vulneración de la protección de datos, pérdida de datos, etc. y se denominan genéricamente **ciberriesgos**.

Las ciberamenazas han ido evolucionando con el tiempo. Desde los virus, gusanos, troyanos, etc, a ataques de denegación de servicios (DoS), malware (softwares maliciosos), ramsomware, hasta llegar a los más complejos y peligrosos como las amenazas persistentes avanzadas (APTs) o ataques dirigidos. La entidad europea ENISA elabora periódicamente estudios sobre el universo de las ciberamenazas que acechan a los ciudadanos, empresas y entidades públicas europeas.

Las ciberamenazas.

Podemos definir una ciberamenaza como la ocurrencia de uno o más acontecimientos de los que se deriva una situación en la que la información puede sufrir una degradación de su seguridad en cualquiera de sus dimensiones: confidencialidad, integridad o disponibilidad. Esto puede producir daños materiales o pérdidas inmateriales en sus activos.

El inventario de ciberamenazas incluye numerosos tipos, pero las más utilizadas en el sector público son:

- **Software malicioso (malware).**
  Descargado en un ordenador o dispositivo, puede hacer cualquier cosa, desde robar datos para cifrar archivos y exigir un rescate. Puede incluir virus, troyanos, ransomware, gusanos, adware y spyware.

- **Ransomware.**
  Cifra los datos de un ordenador, lo que evita que los usuarios accedan a sus archivos hasta que se paga un rescate.

- **Denegación de servicios (DoS).**
  Ataques que abruman un servidor, sistema o red con tráfico falso. Hacen no disponibles los servicios o recursos, al inundarlos con más solicitudes de las que pueden manejar.

- **Ataques basados en la web.**
  Son URL maliciosas o scripts maliciosos que se utilizan para dirigir al usuario al sitio web deseado o descargando contenido malicioso.

- **Correos electrónicos de phishing.**
  Diseñados para engañar a las víctimas para que den contraseñas y otras credenciales. Los usuarios pueden ser manipulados para que realicen una acción o divulguen información confidencial sin saberlo.

De acuerdo con los datos de julio de 2021 a julio de 2022 de la Agencia de la UE para la Ciberseguridad publicados por el Consejo de la Unión Europea[1] las principales ciberamenazas en la UE son:

1 https://www.consilium.europa.eu/es/infographics/cyber-threats-eu/#0

- **Ataques con programas de secuestro.**
  Son ataques en los que los ciberdelincuentes se apoderan de un activo de su víctima y exigen un rescate para su restitución.

- **Ataques distribuidos por denegación de servicio.**
  Consisten en ataques que impiden a los usuarios de una red o sistema acceder a información, servicios u otros recursos pertinentes.

- **Programas malignos.**
  Son programas informáticos malintencionados concebidos para dañar un dispositivo, perturbar su funcionamiento o acceder a él sin autorización.

- **Amenazas de ingeniería social.**
  Son amenazas que tratan de aprovechar un error o comportamiento humanos para obtener acceso a información o servicios.

- **Amenazas a los datos.**
  Consisten en ataques para obtener acceso no autorizado a los datos y manipularlos con el fin de interferir en el funcionamiento de un sistema.

- **Amenazas a internet.**
  Son ataques que afectan a la disponibilidad de internet. Por ejemplo, los secuestros del BGP (Border Gateway Protocol, o protocolo de pasarela fronteriza).

- **Desinformación e información errónea.**
  Consiste en un ataque intencionado consistente en crear o divulgar información falsa o engañosa para manipular la opinión pública.

- **Ataques a la cadena de suministro.**
  Son ataques dirigidos contra una organización a través de las vulnerabilidades de su cadena de suministro, capaces de producir efectos en cascada.

Son muchos los ejemplos de administraciones públicas que han sufrido robos de información en sus bases de datos, indisponibilidades en sus sistemas, daños reputacionales o sabotajes en sus servicios on line. Uno de los más importantes en Cataluña fue en el Hospital Clínic de Barcelona, en marzo del 2023, en el que los ciberatacantes pidieron un rescate de varios millones de dólares para liberar los datos y no publicarlos. El hospital tardó semanas en volver a la normalidad y meses después aún se publicaban datos en la dark web por parte de los atacantes.

Es muy importante identificar las amenazas. Todas las amenazas y riesgos, aunque improbables, deben ser considerados en la valoración de riesgos y en el diseño de los controles generales de las tecnologías de la información (CGTI). Por todo este entorno actual y por la obligación legal existente, las administraciones públicas deben disponer de un sistema de ciberseguridad que las proteja y/o les permita reaccionar y reestablecer sus servicios en el menor tiempo posible.

En conclusión, para el auditor externo es necesario conocer los controles de ciberseguridad que dispone la entidad con el fin de poder valorar los riesgos asociados a ellos y poder dar una opinión en su informe de auditoría lo más fiable posible. Si el auditor no conoce cómo se protege y la posible reacción de la entidad ante estos riesgos, no está realizando una valoración de todos los riesgos significativos de la entidad y, por tanto, estaría realizando un trabajo acorde con las NIA-Es-SP.

2. ¿Qué es la ciberseguridad?

Frente al amplio espectro de ciberamenazas existente en los entornos actuales de administración electrónica, las posibles consecuencias pueden ser muy variadas y potencialmente nefastas. De acuerdo con el informe de Cibernamenazas y tendencias del 2017 del CCN[2], las consecuencias de un incidente de ciberseguridad serían, entre otras:

- **Inactividad:** en muchos casos los atacados suelen necesitar un tiempo de inactividad para hacer frente a la infección. Esta inactividad puede afectar a millones de personas.

- **Costes económicos:** por extorsión (se piden rescates) o por el coste de reparación y restauración de las infraestructuras afectadas.

- **Pérdida de datos:** la mayoría de los ataques son robo de información sensible.

- **Pérdida de reputación:** cuando aparecen noticias con este tipo de ataques, la entidad sufre una pérdida de confianza.

2 https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2224-ccn-cert-ia-16-17-ciberamenzas-y-tendencias-edicion-2017/file.html

Por ello, es fácil deducir que, para prevenir y protegerse de los ciberataques, es necesario establecer una adecuada ciberseguridad en las entidades públicas.

No hay una definición concreta y única de qué es la ciberseguridad. Una definición podría ser la que establece la ISACA: «*la Ciberseguridad tiene como fin la protección de activos de información a través del tratamiento de amenazas que ponen en riesgo la información procesada, almacenada, transportada por los sistemas de información que se encuentran interconectados*»[3].

De acuerdo con la Directiva 2016/1148 de Ciberseguridad, se puede definir como 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 cuatro características fundamentales de los activos de información que debe salvaguardar la ciberseguridad, y que permitirá enlazar más adelante con el ENS y los objetivos del auditor público.

Como indican ambas definiciones la ciberseguridad pretende proteger los activos de información procesada, almacenada y transportada por redes y sistemas de información interconectados, es decir, la seguridad de las redes y sistemas de información. Por tanto, vemos que la ciberseguridad es la respuesta a las ciberamenazas y/o

3 https://www.tcu.es/repositorio/3e238319-7ade-4fac-bd5d-d2f16fd4f62a/Revista%2064.pdf
Revista Española de Control Externo | vol. XXII | n.º 64 (Enero 2020) | pp. 88-101

ciberataques que provienen del ciberespacio.

De acuerdo con el Instituto de Auditores Internos de España[4], la ciberseguridad conlleva el desarrollo de una estrategia global de seguridad, la monitorización y vigilancia de la seguridad, la gestión de amenazas de manera proactiva, la coordinación e intercambio de información, personal dedicado y experto y formación y concienciación de personal.

Para resumir y tal como se señala en el documento "La ciberseguridad en la UE y sus Estados miembros"[5], no existe ninguna definición normalizada y universal de la ciberseguridad. Por ciberseguridad entenderemos todas las actividades necesarias para la protección de las redes y los sistemas de información, los usuarios de tales sistemas y otras personas afectadas por ciberamenazas. Consiste en prevenir y detectar ciberincidentes, así como responder ante los mismos y recuperarse de ellos. Dichos incidentes pueden ser intencionados o no y oscilar entre una divulgación accidental de información y ataques a empresas e infraestructuras críticas, el robo de datos personales o incluso la injerencia en procesos democráticos y electorales, pasando por las campañas generales de desinformación para influir en el debate público.

Para los efectos de establecer una metodología de auditoría de ciberseguridad que sea compatible con la auditoría de sistemas integrada en una auditoría financiera o de cumplimiento, debemos destacar que de la definición vista anteriormente de ciberseguridad dada por la Directiva 2016/1148 se desprenden cuatro dimensiones, cualidades o criterios de los sistemas de información. A estas cuatro dimensiones el ENS (en su anexo 1) añade una quinta. Así, las cinco dimensiones de la seguridad, según el ENS, que es aplicable a todas las administraciones públicas, son:

- **Disponibilidad:** capacidad de un servicio, sistema o información, de ser accesible y utilizable.
- **Confidencialidad:** propiedad de la información por la que se garantiza que es accesible únicamente a personal autorizado.
- **Integridad:** propiedad de la información por la que se garantiza la exactitud de los datos.
- **Autenticidad:** propiedad en que una entidad es quien dice ser o se garantiza la fuente de la que proceden los datos.
- **Trazabilidad:** propiedad consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Por tanto, estas son las características de la información y los sistemas de información que la ciberseguridad debe garantizar mediante el establecimiento de medidas de seguridad (utilizando la terminología del ENS) o controles de ciberseguridad (en terminología de las guías prácticas de fiscalización de los OCEX), y, de esta forma, proteger los activos en redes y sistemas interconectados.

3. El esquema nacional de seguridad.

El ENS vigente está regulado en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Incluye una serie de principios básicos y requisitos mínimos que debe utilizar la administración pública para proteger los activos de información. Con estos principios y requisitos se pretende garantizar el acceso, disponibilidad, integridad, confidencialidad, autenticidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias. Como hemos visto anteriormente, se incluyen las características que definen a la ciberseguridad.

El ENS surge de la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos y debe aplicarse a todos los sistemas de las Administraciones Públicas (general del Estado, autonómica y local).

El artículo 46.3 de la Ley 40/2015 indica que los medios o soportes en que se almacenen los documentos deberán contar con medidas de Seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos

4 Ciberseguridad. Una guía de supervisión. La Fábrica de pensamiento. Instituto de auditores internos de España. Octubre 2016.

5 https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_ES.pdf

almacenados. Así mismo, el artículo 156 indica que el ENS tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley.

Como se ha citado anteriormente, el ENS está formado por unos principios básicos para proteger adecuadamente la información. En el capítulo II del ENS se establecen los principios básicos, éstos son:

a) Seguridad como proceso integral.

b) Gestión de la seguridad basada en los riesgos.

c) Prevención, detección, respuesta y conservación.

d) Existencia de líneas de defensa.

e) Vigilancia continua.

f) Reevaluación periódica.

g) Diferenciación de responsabilidades.

El artículo 31 del capítulo IV establece la obligatoriedad de una **auditoría de seguridad** regular, como mínimo **cada dos años** que verifique el cumplimiento de los requerimientos del ENS. Así, el informe de auditoría deberá dictaminar sobre el grado de cumplimiento de este real decreto, identificar sus deficiencias y sugerir las posibles medidas correctoras o complementarias necesarias, así como las recomendaciones que se consideren oportunas. Además, en el anexo III se establece el objeto, niveles e interpretación de esta auditoría.

En desarrollo de esta norma se aprobó la *Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información*, que es de obligado cumplimiento para las entidades locales, y establece las condiciones para la realización de la preceptiva auditoría a la que deben someterse los sistemas de información del ámbito de aplicación del ENS.

Además, el Centro Criptológico Nacional (CCN) aprobó en abril de 2017 la *Guía de Seguridad de las TIC CCN-STIC 802 Guía de auditoría del ENS*, para orientar en la realización de forma homogénea de este tipo de auditorías. Más recientemente en agosto de 2020 se publicó la *Guía CCN-CERT IC-01/19 Criterios generales de auditoría y certificación*.

Además de los principios, el ENS dispone de los siguientes elementos: los mecanismos para lograr el cumplimiento de los principios y requisitos mínimos mediante la adopción de medidas de seguridad proporcionadas a la naturaleza de la información y los servicios a proteger; el uso de infraestructuras y servicios comunes; las guías de seguridad; las instrucciones de seguridad; las comunicaciones electrónicas; la respuesta ante incidentes de seguridad; el uso de productos certificados; la conformidad; y la formación y concienciación.

Las responsabilidades derivadas del incumplimiento del ENS serían las que correspondieren a cada caso concreto, en virtud de lo dispuesto en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Para aplicar el ENS, en cumplimiento de su artículo 34, el Centro Criptológico Nacional ha elaborado y publicado una serie de guías.

4. Metodología de auditoría de sistemas.

Actualmente encontramos normas técnicas y guías que ayudan a fiscalizar esta área. Como de todos es conocido, las guías que sirven de referencia para las fiscalizaciones de los OCEX son las GPF-OCEX. Son las guías prácticas de fiscalización que utilizan los órganos de control externo de España para la elaboración de sus informes. Las guías específicas utilizadas en el ámbito de la ciberseguridad son las siguientes:

GPF-OCEX 5300 Directrices de auditoría de tecnologías de la información

Basándose en la ISSAI 5300[6] define las auditorías de TI como "*Un examen y revisión de los sistemas de TI y controles relacionados que busca obtener seguridad o identificar violaciones a los principios de legalidad, eficiencia, economía y eficacia del sistema de TI y sus controles relacionados*". Además, indica los requerimientos generales relacionados con las auditorías de TI (enfoque de riesgos, materialidad, documentación, competencia, planificación, objetivos de auditoría, alcance, capacidad, asignación de recursos, contratación de recursos externos, vinculación con la entidad auditada, evidencia de auditoría, recopilación de evidencia de auditoría, supervisión y revisión, casos de fraude, corrupción y otras irregularidades, limitaciones y seguimiento). La guía finaliza con la explicación de técnicas y herramientas de auditoría de TI.

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

Esta guía define la ciberseguridad y especifica las características de la información digital y de la evidencia electrónica. Así, de acuerdo con la GPF-OCEX 1500, los criterios que permiten valorar la fiabilidad de la información y tenerla como evidencia en los entornos informáticos son: autenticación, autorización, confidencialidad, integridad, disponibilidad, trazabilidad y no repudio.

Expone las normas sobre seguridad de la información y ciberseguridad explicando qué es el ENS, su finalidad y las declaraciones o certificados de conformidad sobre el cumplimiento del ENS.

También explica las consecuencias de un incidente de seguridad como el tiempo de inactividad, costes económicos, pérdida de datos y pérdida de vidas. Y en su anexo 1 se exponen las amenazas más significativas.

Esta GPF define la ciberseguridad y las consideraciones sobre ciberseguridad en las fiscalizaciones de los OCEX. Éstos pueden realizar auditorías específicas de ciberseguridad, pueden integrar la ciberseguridad como un apartado de las auditorías financieras o de cumplimiento o una revisión de controles básicos de ciberseguridad.

En su anexo 4 se detallan los 20 controles de seguridad críticos del CIS con su objetivo y comentarios de cada uno de ellos.

GPF-OCEX 5312 Glosario de Ciberseguridad

Esta guía define diferentes conceptos relacionados con la ciberseguridad en concordancia con el ENS y/o el INCIBE (Instituto Nacional de Ciberseguridad).

GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad

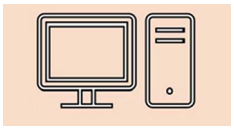
Derivada de la GPF-OCEX 5311, esta guía fue elaborada por la Comisión Técnica de los OCEX y aprobada por la conferencia de presidentes de ASOCEX el 12/11/208.

Esta guía detalla y define los ocho Controles básicos de ciberseguridad. Según el CIS[7] (*Center for Internet Security*) aplicando los cinco primeros controles se pueden reducir los ciberataques alrededor de un 85%. La versión siete de los controles CIS indica que los seis primeros controles son básicos y por ello la GPF-OCEX 5313 los ha establecido así también. A estos, añadió el décimo control CIS (copias de seguridad de datos y sistemas) y el octavo control de ciberseguridad (cumplimiento normativo) añadido por su importancia.

6 La ISSAI 5300 contiene principios generales sobre los fundamentos de la auditoria de Tecnologías de la Información (TI) y sirve de guía para que las EFS (entidades fiscalizadoras superiores) puedan llevar a cabo auditorias de TI.

7 El CIS establece un marco de ciberseguridad con una priorización de controles.

Cuadro 1. Controles básicos de ciberseguridad.

	Inventario y control de dispositivos físicos.	Gestionar activamente todos los dispositivos hardware en la red, de forma que sólo los dispositivos autorizados tengan acceso a la red.
	Inventario y control de software autorizado y no autorizado.	Gestionar activamente todo el software en los sistemas, de forma que sólo se pueda instalar y ejecutar software autorizado.
	Proceso continuo de identificación y remediación de vulnerabilidades.	Disponer de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.
	Uso controlado de privilegios administrativos.	Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir el uso y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.
	Configuraciones seguras del software y hardware de dispositivos móviles, portátiles, equipos de sobremesa y servidores.	Implementar la configuración de seguridad de dispositivos móviles, portátiles, equipos de sobremesa y servidores, y gestionarla activamente utilizando un proceso de gestión de cambios y conjuraciones riguroso, para prevenir que los atacantes exploten servicios y configuraciones vulnerables.
	Registro de la actividad de los usuarios.	Recoger, gestionar y analizar logs de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.
	Copias de seguridad de datos y sistemas.	Utilizar procesos y herramientas para realizar la copia de seguridad de la información crítica con una metodología probada que permita la recuperación de la información en tiempo oportuno.
	Cumplimiento del ENS (*).	-Política de seguridad y responsabilidades. -Declaración de aplicabilidad. -Informe de Auditoría (en nivel medio o alto). -Informe del estado de la seguridad. -Publicación de la declaración de conformidad y los distintivos de seguridad en la sede electrónica.
	Cumplimiento de la LOPD/RGPD.	-Nombramiento del DPD. -Registro de actividades de tratamiento. -Análisis de riesgos y evaluación de tratamiento (para los de riesgo alto). -Informe de auditoría de cumplimiento (cuando el responsable del tratamiento haya decidido realizarlo).
	Cumplimiento de la Ley 25/2013, de 27 de diciembre (impulso de la factura electrónica y creación del registro contable de facturas).	Informe de auditoría de sistemas anual del Registro Contable de Facturas.

Fuente: GPF-OCEX 5313.

(*) No actualizado con el nuevo ENS del 2022.

En esta guía se establece el procedimiento de auditoría y el programa de trabajo que se debe seguir, así como la evaluación de los resultados obtenidos.

En los anexos están definidos cada uno de los controles de ciberseguridad con su concordancia con el anterior ENS y la guía CNN-STIC 804. También incorpora unas fichas de revisión con los subcontroles que se deben verificar.

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

Los objetivos de los CGTI 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 (y en cuatro con la definición de ciberseguridad): confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

La finalidad de la auditoría de los CGTI es verificar su eficacia, es decir que garantizan razonablemente estas propiedades.

5. ¿Cómo afecta la ciberseguridad a la auditoría financiera?

Para analizar cómo puede afectar la ciberseguridad a los estados financieros, debemos partir de la idea que los estados financieros son el resultado sintético de un conjunto de información y datos utilizados por las administraciones públicas, procesados por los sistemas de información que se utilizan para gestionar los servicios públicos. Estos sistemas y datos deben estar protegidos de cualquier amenaza relacionada con su disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad. La ciberseguridad debe de garantizar la protección de estas cinco características. Como he dicho, los incidentes cibernéticos pueden tener consecuencias financieras y tener un efecto significativo en los estados financieros. Para intentar protegerse, la entidad debe realizar una evaluación de los riesgos de ciberseguridad concretos de su entidad, hacer una valoración de éstos y poder determinar a qué activo afecta de los estados financieros. Una vez evaluado el riesgo se deberán establecer los controles pertinentes para mitigar estos riesgos de ciberseguridad. Por ello, el auditor público delimitará el alcance de las pruebas a realizar en función de los objetivos de la auditoría y los riesgos TIC relacionados.

No hay que olvidar que las entidades deben realizar una evaluación continua de los riesgos, ya que estos evolucionan constante y rápidamente.

Por el gran impacto potencial y su trascendencia, los riesgos de ciberseguridad deben ser incorporados a la valoración de riesgos durante la auditoría (como parte integrante de una auditoría financiera o como auditoría exclusiva de ciberseguridad). En un entorno de administración electrónica el auditor público debe incorporar en su metodología de trabajo, la revisión de los controles de seguridad de la información, entre ellos la ciberseguridad.

Durante los últimos años se han realizado auditorías de ciberseguridad en el ámbito internacional, europeo y en España a través de los OCEX.

6. Conclusiones.

1. El incremento de las tecnologías de la información aporta múltiples beneficios, pero también muchos riesgos (ciberriesgos) que deben ser considerados a la hora de hacer las auditorías públicas (ciberseguridad). Hemos visto los riesgos asociados y las consecuencias tan terribles que se desprenden (incluso algunos, hasta lo han vivido en sus instituciones).

2. Los auditores públicos debemos incluir en nuestra metodología de trabajo la revisión de los controles de seguridad de la información y la ciberseguridad, tanto en auditorías financieras como de legalidad. En

concreto, los OCEX deben verificar en todas las fiscalizaciones, entre otros puntos, el cumplimiento de la legalidad en relación con el ENS. Para ello disponemos de varias GPF-OCEX que integran los puntos a verificar de acuerdo con la normativa que es de aplicación.

3. Los perfiles de los futuros auditores deberían tener conocimientos de las tecnologías de la información. A su vez, el personal actual debería recibir más formación en relación con la administración electrónica, la seguridad de la información, la ciberseguridad y las TIC en general.

Todo evoluciona y los auditores públicos debemos adaptarnos a esta evolución.

7. Bibliografía.

- Ciberseguridad, Una guía de supervisión. La Fábrica de pensamiento. Instituto de auditores internos de España. Octubre 2016.
- Compendio de auditorías "La ciberseguridad en la UE y sus Estados miembros.
- Directiva 2016/1148 de Ciberseguridad.
- Guía CCN-STIC 802.
- Guía CCN-CERT IC-01/19.
- GPF-OCEX 5300 Directrices de auditoría de tecnologías de la información.
- GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa.
- GPF-OCEX 5312 Glosario de Ciberseguridad.
- GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad.
- GPF-OCEX 5330 Revisión de los controles generales de tecnología de información en un entorno de administración electrónica.
- Infografía de la Agencia de la UE para la Ciberseguridad publicados por el Consejo de la Unión Europea.
- Informe de Cibernamenazas y tendencias del 2017 del CCN.
- Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información aprobada por la Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública.
- ISSAI 5300.
- Revista Española de Control Externo | vol. XXII | n.º 64 (enero 2020) | pp. 88-101.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.