**Auditoría Pública nº 67** (2016), pp. 69 - 76



**Domingo A. Guerra París**
Funcionario de administración local
Auditor de sistemas de información (RASI-CGE, número 80)
Axudante de auditoría Consello de Contas de Galicia

# Esquema Nacional de Seguridad y auditoría

**RESUMEN/**ABSTRACT:

El Esquema Nacional de Seguridad (ENS) persigue crear condiciones de confianza en el uso de medios electrónicos. Actualmente, su nivel de implementación en las diferentes administraciones es muy reducido, sobre todo en municipios de menor dimensión en términos de presupuesto y habitantes. Uno de sus principales elementos es la auditoría de la seguridad, por lo que, en este trabajo, se presenta la documentación básica que se debe solicitar para su ejecución, se indican aspectos necesarios para evaluar la confianza del sistema auditado, y se especifican los capítulos mínimos que debe contener el informe de auditoría, armonizando lo previsto en la guía CCN-STIC-802, creada al efecto por el Centro Criptológico Nacional, con lo dispuesto en la ISSAI-ES 400 Principios fundamentales de la fiscalización de cumplimiento. De esta forma, las Instituciones Públicas de Control Externo (ICEX), pueden disponer de una herramienta que ayude a concluir sobre el estado de seguridad de la información del ente auditado, de acuerdo con criterios internacionales de fiscalización.

T e National Security Scheme (NSS) aims to create confidence conditions in the use of electronic media. Nowadays, his level of implementation in the dif erent administrations is very limited, especially in smaller municipalities in terms of budget and population. One of his main features is the security audit, so, in this paper, the basic documentation that must be requested for execution is presented, aspects necessary are indicated to evaluate the confidence of the audited system, and the minimum chapters must contain the audit report, harmonizing the provisions of CCN-STIC-802 guide, created by the National Cryptologic Centre, with the provisions of ISSAI-ES 400 fundamental principles of compliance audit. T us, the Public Institutions External Control (ICEX) may have a tool to help to conclude about the security status information of the audited entity, in accordance with international audit criteria.

**PALABRAS CLAVE/**KEYWORDS:

ESQUEMA NACIONAL DE SEGURIDAD, AUDITORÍA DE LA SEGURIDAD, ICEX, FISCALIZACIÓN DE CUMPLIMIENTO, E-ADMINISTRACIÓN
NATIONAL SECURITY SCHEME, SECURITY AUDIT, ICEX, AUDIT OF COMPLIANCE, E - ADMINISTRATION

## INTRODUCCIÓN

La utilización de medios tecnológicos en las comunicaciones entre ciudadanos, empresas y diferentes organismos del sector público, constituye una práctica muy extendida que tiende a generalizarse. Esta circunstancia, recomienda establecer mecanismos que respondan eficientemente a todo tipo de ciberamenazas.

Con el fin de proporcionar la confianza necesaria a los diversos usuarios de tecnologías de información y comunicación, se creó el Esquema Nacional de Seguridad, constituido por principios básicos y requisitos mínimos que permitan salvaguardar la información de entes públicos en actuaciones electrónicas.

Uno de sus elementos principales es la "auditoría de la seguridad", definida como revisión y examen independiente de los registros y actividades del sistema, para verificar la idoneidad de los controles, asegurar que se cumple la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.

En este artículo, se describe someramente en qué consiste el Esquema Nacional de Seguridad, se aportan datos sobre su implementación y algunas causas explicativas de su escaso cumplimiento en nuestras administraciones. También, además del apartado de conclusiones, se comentan tres aspectos substantivos de una fiscalización (documentación necesaria, actuaciones a realizar y elementos mínimos del informe), conjugando lo señalado en la guía de auditoría CCN-STIC-802 y lo dispuesto en la ISSAI-ES 400 *Principios fundamentales de la fiscalización de cumplimiento*.

## EL ESQUEMA NACIONAL DE SEGURIDAD (ENS)

Con la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (vigente hasta el 2 de octubre de 2016), se instituye el Esquema Nacional de Seguridad (artículo 42.2), con objeto de implantar una política de confianza en la utilización de medios electrónicos. Sin embargo, no es hasta la entrada en vigor del Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la administración electrónica (BOE número 25, del 29 de enero de 2010), cuando se sistematiza, regulando los principios básicos y requisitos mínimos requeridos para una adecuada protección de la información.

Coordinada directamente con estas normas, la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común, al regular prerrogativas de las personas en sus relaciones con la administración (artículo 13.h), establece derechos a la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de las informaciones que figuren en aplicaciones, ficheros y sistemas de entes públicos. Asimismo, en la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, se determina también que las administraciones se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes, a través de medios electrónicos que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizando la protección de datos de carácter personal, y facilitando preferentemente la prestación conjunta de servicios a los interesados. El Esquema Nacional de Seguridad se recoge, explícitamente, en su artículo 156.

Con estas disposiciones se pretende, en definitiva, generar normalidad en el uso de los medios electrónicos, para que los diferentes usuarios puedan ejercitar derechos y cumplir obligaciones con ciertas garantías de seguridad.

Por lo que respecta concretamente al ENS, su finalidad persigue asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de datos, informaciones y servicios, gestionados por las diferentes administraciones, en el ejercicio de sus respectivas competencias.

De esta manera, los responsables directos de la ejecución de la acción del gobierno (central, autonómico o local) deberán disponer formalmente de su política de seguridad, de acuerdo con los principios de seguridad integral; gestión de riesgos; prevención, reacción y recuperación; líneas de defensa; reevaluación periódica y función diferenciada; y aplicando los siguientes requisitos mínimos del Cuadro 1.

Pues bien, para dar cumplimiento a los objetivos del ENS, el reglamento que lo desarrolla especifica cinco dimensiones de seguridad (disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad), exigiendo que la información se clasifique en función de ellas, a fin de determinar el impacto que tendría sobre la organización un incidente que concerniera a la seguridad de los datos o de los sistemas, asignando la dimensión o dimensiones afectadas en uno de estos cuatro niveles: 1) nulo: irrelevante; 2) bajo: perjuicio limitado; 3) medio: grave; y 4) alto: perjuicio muy grave. En consecuencia, las diferentes administraciones deberán estudiar la información que manejan y deliberar sobre los niveles de seguridad exigidos para cada tipo de asunto en cada una de sus dimensiones.

Como las medidas de seguridad se aplican sobre los medios electrónicos existentes, es necesario identificar-

los para determinar su categoría en tres niveles (básico, medio y alto). Así, un sistema de información será de categoría alta cuando alguna de sus dimensiones de seguridad alcanza el mayor nivel; será de categoría media si cualquiera de sus dimensiones es de nivel medio y ninguna adquiere un nivel superior; y, por último, se considera de categoría básica cuando alguna de sus dimensiones es de nivel bajo, y ninguna logra un nivel superior.

Cuadro 1. Requisitos mínimos del ENS

| | |
|---|---|
| a) | Organización e implantación del proceso de seguridad. |
| b) | Análisis y gestión de los riesgos. |
| c) | Gestión de personal. |
| d) | Profesionalidad. |
| e) | Autorización y control de los accesos. |
| f) | Protección de las instalaciones. |
| g) | Adquisición de productos. |
| h) | Seguridad por defecto. |
| i) | Integridad y actualización del sistema. |
| j) | Protección de la información almacenada y en tránsito. |
| k) | Prevención ante otros sistemas de información interconectados. |
| l) | Registro de actividad. |
| m) | Incidentes de seguridad. |
| n) | Continuidad de la actividad. |
| o) | Mejora continua del proceso de seguridad. |

Fuente: artículo 11 RD 3/2010, de 8 de enero, que regula el ENS
Elaboración propia.

También, se fijan tres grupos de medidas de seguridad: a) marco organizativo, constituido por el conjunto de actuaciones relacionadas con la organización global de seguridad; b) marco operacional, formado por las gestiones realizadas para proteger la operación del sistema como conjunto integral de componentes para un fin; y c) medidas de protección, que se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

En resumen, el mencionado Real Decreto 3/2010[2], determina las dimensiones de seguridad y sus niveles, la categoría de los sistemas y medidas de prevención, e instituye la auditoría periódica de la seguridad, cuya realización, con carácter ordinario, deberá practicarse al menos cada dos años, sin perjuicio de que, de existir modificaciones significativas en el sistema de información que puedan afectar a las medidas de seguridad, se efectúe la consiguiente auditoría con carácter extraordinario.

La disposición transitoria del reglamento articula un mecanismo escalonado para la adecuación al ENS, de tal forma que a 30 de enero de 2014 los sistemas de las administraciones deberían estar acondicionados al esquema. Pero, con la entrada en vigor del RD 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, se dispone de un nuevo plazo de veinticuatro meses contados a partir del 5 de noviembre de 2015, para la adecuación de los sistemas al ENS.

## IMPLEMENTACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD

La vigente información publicada disponible, en espera de estadísticas oficiales que permitan conocer datos más actuales[3], evidencia que el grado de implantación del ENS es prácticamente inexistente.

El Ministerio de Hacienda y Administraciones Públicas, como responsable del esquema, ha desarrollado el seguimiento de su implementación a través de la Dirección General de Modernización Administrativa, procedimientos e impulso de la administración electrónica, y en colaboración con el Centro Criptológico Nacional del Centro Nacional de Inteligencia. Este seguimiento se ha realizado mediante sucesivos sondeos en febrero, mayo, septiembre y diciembre de 2013 y marzo de 2014, utilizando un cuestionario basado en una herramienta disponible en el Portal CCN-CERTi, cuyos resultados se presentan en el siguiente Cuadro 2.

[2]Con las modificaciones introducidas por el RD 951/2015.
[3]En el portal del CCN-CERT (www.ccn-cert.cni.es) se habilitó una plataforma de recogida de datos (Informe Nacional del Estado de Seguridad-INES), para que las distintas Administraciones pudiesen cumplimentar, antes del 18 de diciembre de 2015, la información sobre su estado de seguridad.

Cuadro 2. Resultados de la implementación del ENS

| ENTIDADES | 2013 | | | | 2014 |
|---|---|---|---|---|---|
| | FEBRERO | MAYO | SEPTIEMBRE | DICIEMBRE | MARZO |
| Admon. Central | 64 | 69 | 77 | 78 | 80 |
| Admon. Autonómica | 5 | 26 | 28 | 30 | 30 |
| Admon. Provincial | - | 5 | 6 | 6 | 9 |
| Ayuntamientos | 2 | 12 | 13 | 14 | 22 |
| TOTAL | 71 | 112 | 124 | 128 | 149 |

Fuente: Observatorio de Administración Electrónica, junio 2014.
Elaboración propia.

De acuerdo con esta información, el estado de cumplimiento del ENS en nuestras administraciones (central, autonómica, provincial y municipal) es muy reducido. Los datos son concluyentes: en diciembre de 2013, tan sólo 128 administraciones lo habían implantado; y en marzo de 2014, el número es de 149 entidades.

Ciertamente, existen determinados factores que no ayudan a su articulación, a pesar de tratarse de una provechosa herramienta para proteger la información y los servicios. Razones de tipo económico, factores tecnológicos, de falta de medios materiales y recursos humanos, de concienciación de su necesidad, entre otros, conforman algunos de los principales impedimentos de su puesta en práctica, sobre todo, en municipios menores de 5.000 habitantes, como se subraya en el epígrafe siguiente.

## PROBLEMAS PARA SU APLICACIÓN PRÁCTICA

No es necesario advertir que, el esfuerzo, para que las distintas administraciones se adecúen al ENS, se enmarca en unas coordenadas concretas, donde la actividad financiera del sector público ha estado limitada por restricciones presupuestarias y de reposición de efectivos.

Especialmente significativa es la situación de los ayuntamientos, donde la fuerte presión sobre el gasto contrasta con la escasez de ingresos, provocando debilidades en adquisición y mantenimiento de estructuras relacionadas con las nuevas tecnologías de la información y comunicación, sobre todo en los municipios de menor dimensión en términos de presupuesto y habitantes.

La realidad municipal atestigua que, en materia de administración electrónica, todavía queda un largo camino por recorrer. Según datos de la *Encuesta sobre el grado de implantación de la Ley 11/2007, en las administraciones locales, a los cinco años de su entrada en vigor (FEMP, 2014),* se concluye que "los municipios menores de 5.000 habitantes no cuentan, en la mayoría de los casos, con los recursos técnicos y medios humanos suficientes, para la prestación de servicios de e-Administración a los ciudadanos". Algunos datos de la encuesta se presentan en este Cuadro 3.

Cuadro 3. Algunos datos de la Encuesta, referidos a municipios menores de 5.000 habitantes

| DESCRIPCIÓN | PORCENTAJE |
|---|---|
| Acceso a internet a través de banda ancha | 11,1 % |
| Disponen de red *wifi* | 21,2 % |
| Personal dedicado a soporte informático | 11,8% |

Fuente: Elaboración propia a partir de la Encuesta sobre el grado de implantación de la Ley 11/2007.

Los resultados de esta encuesta informan que, solamente, el 11,1% de municipios menores de 5.000 habitantes disponen de acceso a internet a través de banda ancha. Y que sólo el 21,2% del conjunto de estos municipios cuentan con red wifi en sus instalaciones. En el estudio no se citan otros porcentajes para municipios pequeños, pero se indica que, en general, no existen planes estratégicos para la e-Administración y que el nivel de implantación de los sistemas de gestión electrónica de documentos es bajísimo. En cuanto a sede electrónica, registro electrónico, comunicaciones electrónicas y tablón de anuncios virtual, los resultados –se afirma– son muy bajos también[4].

El índice de ayuntamientos pequeños que disponen de personal dedicado en exclusiva a soporte informático se sitúa en el 11,8%, confirmando de esta manera la

[4] En este informe, publicado por la FEMP en febrero de 2014 y que ha sido elaborado por Carmen Cubero y Eugenio Villareal, se concluye expresamente, además, que "existe una gran fractura digital" entre municipios pequeños (menores de 5.000 habitantes) y el resto (pág. 36).

carencia de personal especializado en la implantación y adaptación de medidas para garantizar la seguridad según el ENS.

Otro de los motivos por los que, tal vez, esta iniciativa no ha terminado de cuajar, tiene que ver con la escasa importancia que determinadas administraciones otorgan a la seguridad de la información, y a la ausencia de un régimen disciplinario que sancione el incumplimiento de sus prescripciones (Enjuto Gozalo, 2013).

Porque, la seguridad de la información, en muchos casos, no se considera un aspecto prioritario y, en general, no es tenida en cuenta como un elemento preocupante a la hora de jerarquizar los proyectos que definitivamente se deben acometer. Por otro lado, la falta de medidas sancionadoras asociadas al incumplimiento de las exigencias del ENS, independientemente de las responsabilidades genéricas derivadas de infringir lo determinado en un Real Decreto, provoca cierta laxitud en comparación con otro tipo de disposiciones normativas, donde las multas pueden ser coercitivas y de elevada cuantía.

En cualquier caso, la realidad de los datos exhibe claramente el reducido nivel de compromiso de nuestras administraciones con el ENS.

## AUDITORÍA DE LA SEGURIDAD

El ENS prescribe la necesidad de realizar auditorías de seguridad periódicas. Para ello, dependiendo del nivel de categoría, se comprobará, con mayor o menor calado, la seguridad implementada en cada organización. De esta manera, en los sistemas de información de categoría básica no será necesario efectuar auditoría en sentido estricto. Bastará con una autoevaluación practicada por el personal administrador del sistema. Para niveles de categoría media o alta, se auditará el grado de cumplimiento del ENS, identificando deficiencias y contemplando las medidas correctoras o complementarias que se juzguen pertinentes.

Con el propósito de facilitar la ejecución de auditorías, el Centro Criptológico Nacional publicó en junio de 2010 la guía CCN-STIC-802, en la que se establecen pautas de carácter general para encauzar su realización. Sin embargo, su contenido no se adapta a lo dispuesto en las Normas Internacionales de Entidades Fiscalizadoras Superiores (NIEFS, más conocidas por sus siglas en inglés-ISSAI), desarrolladas por la Organización Internacional de Entidades Fiscalizadoras Superiores (*International Organization of Supreme Audit Institution-INTOSAI).* Con todo, en la guía se concretan unas premisas mínimas de ejecución que, una vez adaptadas, podrían utilizarse perfectamente como referencia en fiscalizaciones de cumplimiento, realizadas por Instituciones Públicas de Control Externo (ICEX)[5] En las páginas siguientes, precisamente, se concreta el trabajo de refundición y homogeneización realizado en este sentido, para que se pueda disponer de una herramienta que permita diagnosticar y concluir sobre el estado de seguridad de la información del ente auditado, de conformidad con criterios internacionales de fiscalización. Porque, consideramos que los distintos órganos de control externo no pueden soslayar, por más tiempo, el análisis de la política de seguridad, y estamos convencidos de que se debería incluir este asunto, como uno de los objetivos de fiscalización en sus trabajos.

Para ello, en la planificación de las actuaciones, si con carácter previo se deduce que no se han realizado auditorías de seguridad, convendría plantear la realización de una auditoría de acuerdo con lo dispuesto en la ISSAI-ES 400 Principios fundamentales de la fiscalización de cumplimiento. Y si ya se efectuó este tipo de control, procedería revisar la auditoría y concluir sobre la observancia de la legislación aplicable –Real Decreto 3/2010– emitiendo el informe correspondiente según lo previsto en el parágrafo 10 ISSAI-ES 400.

En ambos casos, existe una perfecta conexión con el marco de fiscalización de cumplimiento que presenta la ISSAI-ES 400. Puesto que, esta norma internacional, especifica en su parágrafo 12, que la auditoría de cumplimiento puede tener un objeto más o menos amplio y proporcionará un grado de seguridad razonable o limitada, en función de los objetivos definidos, los procedimientos de obtención de evidencia y el formato de informe. Y, en el parágrafo 21, se indica que la fiscalización de cumplimiento podrá planificarse, ejecutarse y recogerse en informes independientes de las fiscalizaciones operativas y de estados financieros, constituyendo auditorías concretas y claramente definidas. Por último, y como es lógico, el parágrafo 44 de la ISSAI-ES 400 ordena que la auditoría esté adecuadamente documentada y dirigida a la obtención de pruebas suficientes, pertinentes y fiables para fundamentar los resultados.

En el mismo contexto que las observaciones anteriores, la guía CCN-STIC-802 destaca que, para lograr los objetivos de fiscalización, el equipo auditor comprobará que las medidas de seguridad del sistema auditado se ajustan a los principios básicos del RD 3/2010, y satisfacen los requisitos mínimos de seguridad. Y particulariza también la documentación mínima a requerir en la fase de planificación de los trabajos.

Con el propósito de facilitar el detalle de esos documentos imprescindibles de la guía, en el siguiente Cuadro 4 se relacionan pormenorizadamente

[5]ICEX es la denominación utilizada para designar conjuntamente al Tribunal de Cuentas y a los órganos de control externo de las comunidades autónomas.

Cuadro 4. Documentación necesaria

- Documentos firmados por el órgano correspondiente acreditativos de la aprobación formal de decisiones en materia de política de seguridad.
- Organigrama de los servicios y áreas, con descripción de funciones y responsabilidades.
- Identificación, en su caso, de responsables de la información, de los servicios, de la seguridad y del sistema, según se contempla en el RD 3/2010.
- Descripción detallada del sistema de información a auditar (software, hardware, comunicaciones, equipamiento auxiliar, ubicaciones).
- Identificación de la categoría del sistema según el Anexo I del RD 3/2010.
- Niveles de seguridad definidos.
- Política de seguridad.
- Política de firma electrónica y certificados.
- Descripción detallada del sistema de gestión de la seguridad y documentación que lo sustenta.
- Informes de análisis de riesgos.
- Declaración de aplicabilidad.
- Decisiones adoptadas para gestionar los riesgos.
- Relación de medidas de seguridad implantadas.
- Relación de registros de actividad en lo relativo a las medidas de seguridad implementadas.
- Informes de otras auditorías previas de seguridad relacionados con los sistemas y servicios incluidos en el alcance de la auditoría.
- Informes de seguimiento de deficiencias detectadas relacionadas con el sistema a auditar.

Fuente: Guía CCN-STIC-802 Planificación preliminar de la auditoría.
Elaboración propia

Con este reducido número de documentos e informes, los auditores disponen ya de material básico suficiente para valorar riesgos y efectuar una revisión con cierta profundidad. Sin perjuicio de que, si así se considera, se soliciten otros documentos, se realicen más averiguaciones y se ejecuten otros procedimientos que permitan valorar la existencia de otros incumplimientos, consecuencia de la obligatoria actitud de escepticismo profesional que se debe mantener durante todo el proceso de auditoría.

Sobre la base de las consideraciones anteriores, y siguiendo con otras particularidades de la auditoría de seguridad, consideramos que la metodología utilizada debería permitir identificar y formalizar los aspectos que figuran en el siguiente Cuadro 5.

Cuadro 5. Actuaciones a realizar

- El objetivo, alcance y enfoque de la auditoría.
- Los recursos necesarios y apropiados para realizar la auditoría, cronograma de actuaciones y calendario de ejecución.
- Las debidas comunicaciones con los responsables de la organización en todas las etapas de la fiscalización.
- La planificación documentada por escrito, requisitos de información previos al desarrollo del programa de auditoría, y a la ejecución de las pruebas que se consideren necesarias.
- El establecimiento de un programa detallado de auditoría con las revisiones y pruebas a realizar, fijando el umbral de importancia relativa en niveles bajos, de forma que se puedan poner de manifiesto irregularidades que, si bien en su cuantía podrían no ser elevadas, sin embargo, constituyen incumplimientos de la normativa.
- La evaluación global de los resultados de la auditoría en relación al objetivo y alcance definidos y a los requisitos del RD 3/2010, obteniendo evidencia de auditoría suficiente y adecuada para fundamentar conclusiones en las que basar la opinión.
- La presentación de los resultados para alegaciones.
- La confección y emisión formal del Informe de Auditoría definitivo.

Fuente: Elaboración propia a partir de la Guía CCN-STIC-802 Desarrollo y ejecución auditoría y de la ISSAI-ES 400 Principios fundamentales de la fiscalización de cumplimiento.

La elaboración y ejecución de estos aspectos servirá para sustentar la confianza que merece el sistema auditado en materia de seguridad; es decir, permitirá calibrar la capacidad para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los servicios prestados y la información tratada, almacenada o transmitida.

Una vez confirmados los hechos y deficiencias detectadas, como resultado del trabajo efectuado y de acuerdo con el último punto del anterior Cuadro 5, se deberá emitir un informe sobre la adecuación de las medidas exigidas por el RD 3/2010, identificando sus deficiencias y proponiendo las medidas correctoras o complementarias precisas, incluyendo los datos, hechos y observaciones en que se basen los dictámenes y las recomendaciones propuestas.

Según la guía CCN-STIC-802 (punto 46, página 16), el informe contendrá una opinión sobre si la política de seguridad define los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema; si se cuenta con procedimientos para la resolución de conflictos entre responsables; si se han designado personas para dichos roles, respetando la adecuada segregación de funciones; si consta un sistema de gestión de la seguridad de la información documentado; si se ha realizado un análisis de riesgos, con revisión y aprobación regular; si se cumplen las medidas de seguridad y si existe un sistema de gestión de mejora continua.

La guía indica, igualmente, que el informe de auditoría podrá presentarse en formato audiovisual, pero siempre deberá entregarse en soporte papel y debidamente firmado o bien en soporte digital con firma electrónica. En cualquier caso, respetando un contenido mínimo que, como se especifica en el siguiente Cuadro 6, es absolutamente compatible con los elementos que deben incluir los informes de auditorías de cumplimiento reseñados en el parágrafo 55 de la ISSAI-ES 400.

Con independencia de su formato, el informe debe ser preciso, completo, objetivo, concluyente y tan claro y conciso como sea posible. Y debe manifestar, por supuesto también, la relevancia de los criterios utilizados, el nivel de seguridad proporcionado y todas las limitaciones al alcance existentes.

En el Cuadro 6, que figura a continuación, se presenta el índice que debe contener el informe. Procede recordar que se ha conjugado lo previsto en la guía CCN-STIC-802 con lo señalado en la ISSAI-ES 400, proporcionando así equivalencia y uniformidad.

Cuadro 6. Elementos mínimos del informe

| | |
|---|---|
| 1. | Título. |
| 2. | Destinatario. |
| 3. | Objetivos y razones de la auditoría, con breve descripción del proceso metodológico aplicado. |
| 4. | Alcance de la fiscalización, incluyendo el periodo de tiempo cubierto y limitaciones. |
| 5. | Descripción de la materia objeto de análisis, con la debida identificación del sistema auditado. |
| 6. | Enumeración de la legislación aplicable y normas de auditoría utilizadas al realizar el trabajo. |
| 7. | Un resumen del trabajo realizado y de los resultados, con identificación de la documentación revisada y tipología de pruebas efectuadas. |
| 8. | Conclusiones, con una sección de informe ejecutivo sintetizando los aspectos más relevantes o las áreas de acción más significativas, y resumen general del grado de cumplimiento. |
| 9. | Recomendaciones, que estarán sustentadas debidamente, y basadas en la existencia de un riesgo o relacionadas con un incumplimiento fehaciente y preciso de los requisitos básicos y mínimos del RD 3/2010. |
| 10. | Alegaciones de la entidad fiscalizada que se podrán incluir como anexo. En relación al contenido de las mismas, no se valorarán alegaciones que confirmen deficiencias o irregularidades señaladas, que ofrezcan criterios u opiniones sin soporte documental o normativo, o que sólo proporcionen explicaciones o justificaciones de la actividad sin rebatir el contenido del informe. |
| 11. | Fecha y firma del informe. |
| 12. | Anexos. |

Fuente: Elaboración propia combinando lo dispuesto en el apartado Presentación del informe de auditoría de la Guía CCN-STIC-802 y el parágrafo 55 de la ISSAI-ES 400 referido a Elaboración de informes

Las ICEX organizan y programan los trabajos de fiscalización considerando sus recursos disponibles. Esta circunstancia, provoca diversidad en el modo de diseñar y presentar informes. No obstante, somos de la opinión de que, al conjugar lo dispuesto en la guía con lo previsto en la norma internacional, se conseguirá dictaminar inequívocamente sobre el cumplimiento de las disposiciones del Real Decreto que regula el ENS, identificando deficiencias y sugiriendo las medidas correctoras o complementarias que se estimen oportunas, así como

las recomendaciones que procedan, con el fin último de que los entes fiscalizados mejoren sus procedimientos.

## CONCLUSIONES

En este trabajo se concluye que, gracias al vigente marco normativo, ciudadanos, empresas y administraciones públicas, en sus diferentes relaciones, pueden ejercitar derechos y cumplir obligaciones con garantías de seguridad en el uso de medios electrónicos. Precisamente, con la finalidad de asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de datos, informaciones y servicios, gestionados por la administración, surge el Esquema Nacional de Seguridad.

No obstante, su grado de implementación en nuestras administraciones es decepcionante. En marzo de 2014 tan sólo 149 entidades lo habían adoptado. Es verdad que existen determinados factores que no ayudan a su articulación, sobre todo en municipios pequeños, donde la ausencia de recursos técnicos y medios humanos, fundamentalmente, impiden el cumplimiento de sus prescripciones. A estas circunstancias, hay que añadir la escasa importancia que determinadas entidades públicas otorgan a la seguridad de la información, y a que en el Real Decreto que lo regula no existe un régimen disciplinario sancionador.

Al margen de estas consideraciones, el Centro Criptológico Nacional publicó la guía CCN-STIC-802, para facilitar la ejecución de auditorías. Pero su contenido no se adapta a las Normas Internacionales de Entidades Fiscalizadoras Superiores. Pues bien, con el propósito de armonizar algunos de los principales aspectos de la mencionada guía con lo dispuesto en la ISSAI-ES 400, en este trabajo se presenta la documentación básica que, a juicio del autor, se debe solicitar para realizar una fiscalización de cumplimiento (Cuadro 4); se formalizan aspectos que se considera de interés identificar, nítidamente, en dicha auditoría (Cuadro 5); y se proporciona una relación de elementos transcendentes que debe contener, como mínimo, el informe de fiscalización (Cuadro 6), siguiendo el criterio establecido en uno y otro documento.

Y, todo ello, porque consideramos que los distintos órganos de control externo no pueden soslayar, por más tiempo, el análisis de la política de seguridad, convencidos de que, esta cuestión, debe considerarse como uno de los objetivos de las fiscalizaciones que realicen las ICEX.

## BIBLIOGRAFÍA

**Enjuto Gozalo, J.** (2013). "Estudio del Esquema Nacional de Seguridad". http://www.criptored.upm.es/descarga/EstudioEsquemaNacionalSeguridadJosebaEnjuto.pdf.

**FEMP** (2014): "Encuesta sobre la implantación de la Ley 11/2007 de acceso electrónico, en las administraciones locales a los 5 años de su publicación, con referencias específicas a la participación del archivero. Informe de resultados", elaborado por Carmen Cubero y Eugenio Villareal, Madrid.

**Guerra París, Domingo A.** (2001): "Las operaciones de tesorería: una propuesta de fiscalización" *Auditoría Pública*, número 23, págs. 67-72.

**Guerra París, Domingo A.** (2007): "La rendición de cuentas de los municipios gallegos" *Auditoría Pública*, número 43, págs. 31-38.

**ISSAI-ES 100** – Principios fundamentales de auditoría del sector público http://www.tcu.es/export/sites/default/.content/pdf/NormasManuales/ISSAI-ES/01-ISSAI-ES-100.pdf

**ISSAI-ES 400** – Principios fundamentales de auditoría de cumplimiento http://www.tcu.es/export/sites/default/.content/pdf/NormasManuales/ISSAI-ES/04-ISSAI-ES-400.pdf

**López Hernández, A.M.** (2013). "Normas profesionales de la INTOSAI: directrices de auditoría. Aplicación a la actividad fiscalizadora de los Órganos Institucionales de Control Externo Autonómicos". *Auditoría Pública*, número 61, págs. 9-24.

**OBSAE** (2014): "Seguimiento de la adecuación a los ENS". http://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2014/Junio/Noticia-2014-06-11-nota-tecnica-ens-eni.html#.VsTMbeaYJzq