Auditoría Pública nº 74 (2019), pp. 33 - 44

Enrique Benítez Palma
Consejero
Carlos Vaz Calderón
Auditor
Cámara de Cuentas de Andalucía

La ciberseguridad en las entidades locales: cómo enfocar una fiscalización externa de cumplimiento de legalidad

RESUMEN/ABSTRACT:

El aumento exponencial de los ataques informáticos sufridos por las administraciones públicas españolas, y muy especialmente por las entidades locales, supone un sólido argumento para incorporar la fiscalización del cumplimiento de legalidad en materia de ciberseguridad en los planes de actuación de los Organismos de Control Externo (OCEx). El presente artículo describe los controles incorporados en la normativa que desarrolla el Esquema Nacional de Seguridad (ENS) y su relación con los contenidos de las Guías Prácticas de Fiscalización (GPF) en materia de ciberseguridad, acreditando su adecuada complementación.

The exponential increase in the number of cyber attacks suffered by Spanish public administrations, and especially by local authorities, provides a solid argument for include legal compliance audits regarding cybersecurity into Bodies of External Control (OCEx, in Spanish) action plans. This article describes the controls added in regulations developed by the National Security Scheme (ENS, in Spanish) and their relationship with the contents of the Practical Guidelines for Examination (GPF, in Spanish) on cybersecurity, accrediting their suitable complementarity.

PALABRAS CLAVE/KEYWORDS:

CIBERSEGURIDAD, ENTIDADES LOCALES, ESQUEMA NACIONAL DE SEGURIDAD (ENS), GUÍAS PRÁCTICAS DE FISCALIZACIÓN (GPF), CUMPLIMIENTO DE LEGALIDAD
CYBERSECURITY, LOCAL AUTHORITIES, NATIONAL SECURITY SCHEME (ENS), PRACTICAL GUIDELINES FOR EXAMINATION (GPF), LEGAL COMPLIANCE

INTRODUCCIÓN

Cualquier actividad formativa o de sensibilización en materia de ciberseguridad o seguridad de los sistemas de información de las entidades locales celebrada durante el año 2018 habría tenido que recurrir a ejemplos foráneos, sobre todo de los Estados Unidos, para ilustrar la problemática enfrentada. Sin embargo, a lo largo del ejercicio 2019 se han producido, ya en España, diversos ejemplos concretos que han tenido su correspondiente repercusión mediática.

Si en junio los medios de comunicación comentaban que un hacker mantenía paralizada la administración municipal de Baltimore, solicitando un rescate para desencriptar el acceso a sus sistemas de información, en estos últimos meses podemos hacer ya un breve pero intenso balance de ataques informáticos sufridos por diversas entidades locales españolas:

- En los primeros días de julio, un hacker logró penetrar en la red local del Ayuntamiento de Roquetas (Almería), un municipio de casi 100.000 habitantes, y realizar dos transferencias a una cuenta alemana por importe de 700.000 euros, destinados al pago de la nómina municipal. Distintas fuentes confirman que la Guardia Civil y el CNI lograron recuperar el dinero, sin realizar detenciones.
- A mediados de agosto, el pequeño municipio valenciano de Albuixech, de casi 4.000 habitantes, se vio obligado a formatear todos sus ordenadores tras sufrir un ataque externo que "secuestró" el acceso a los mismos, solicitando un rescate para permitir de nuevo el acceso a los sistemas de información de la entidad local.
- A finales de septiembre, la Empresa Municipal de Transportes de la ciudad de Valencia sufrió la llamada "estafa del CEO": una bien urdida madeja de correos falsificados permitió a los atacantes conseguir que desde su dirección financiera se transfirieran nada menos que 4 millones de euros a Hong Kong para financiar una operación ficticia.
- En la mañana del 2 de octubre, el Ayuntamiento de Jerez (en la provincia de Cádiz), un municipio de más de 200.000 habitantes, sufrió la paralización de sus ordenadores víctima de un ataque informático similar al de Baltimore o Albuixec. La ayuda del Centro Criptográfico Nacional (CCN) permitió recuperar la normalidad en dos semanas y detectar que se trataba de un ataque con el virus Ryuk.
- En la primera quincena de noviembre se produjo una detención en las islas Canarias relacionada con el hackeo a las cuentas de la Diputación de Orense, un ataque que logró realizar una primera transferencia de 170.000 euros a una cuenta en Alemania, procedente de los pagos de subvenciones, y que estaba a punto de ser repetido con otra partida de 500.000 euros destinados al mismo fin.
- Finalmente, a mediados de noviembre el Instituto de Empleo del Ayuntamiento de Zaragoza ha sufrido un ataque y el secuestro de sus sistemas de información, exigiéndose un rescate de 30.000 euros para, de nuevo, permitir el acceso a ellos. La entidad local se ha negado a pagar y asegura que no se han producido pérdidas de información.

Este amplio abanico de ejemplos permite plantear diversas consideraciones. En primer lugar, la multiplicación de los intentos de ataques en tan corto período, lo que pone de manifiesto la vulnerabilidad del sector local en su conjunto y la necesidad de abordar la prevención del riesgo de sufrir un ataque de este tipo. Es importante señalar que, por una parte, el pasado 16 de octubre se publicó en el BOE la Resolución de 4 de octubre de la Secretaría de Estado para el Avance Digital, por la que se atribuye el número telefónico 017 al servicio de línea de ayuda en ciberseguridad. Y también que la Ponencia para el estudio de diversas cuestiones relativas a la ciberseguridad en España, elaborada en el Congreso de los Diputados en marzo de 2019, afirmaba en su recomendación 23 que "se considera necesario alcanzar un acuerdo amplio que permita incrementar la ciberseguridad de las entidades locales, especialmente de las más pequeñas, con la colaboración de la FEMP y la cooperación de las Comunidades Autónomas. En este sentido, también se considera imprescindible lograr una progresiva adecuación de los esfuerzos presupuestarios del Estado, de las Comunidades Autónomas y las Entidades Locales para hacer frente, con las debidas garantías, a los retos que plantea la ciberseguridad".

En segundo lugar, ha quedado acreditado que no importa el tamaño del municipio para estar en riesgo. Y en tercer lugar, si bien la mayoría de los ataques responden a la modalidad de encriptación externa de los activos para impedir el acceso a los mismos, también se han detectado otras vulnerabilidades en el acceso a las cuentas bancarias municipales que revelan los puntos débiles de la planta municipal en su conjunto.

Para proteger los sistemas de información de las entidades locales se hace necesario conocer la normativa es-

pañola promulgada a tal fin, verificar su cumplimiento y proteger los activos en riesgo. A continuación se detalla dicha normativa, se desarrolla el contenido del Esquema Nacional de Seguridad (ENS) y se vincula el control externo de cumplimiento de legalidad de esta normativa con las Guías Prácticas de Fiscalización (GPF) en materia de ciberseguridad.

1.- RESPUESTAS NORMATIVAS A LOS RIESGOS CIBERNÉTICOS

El uso de las TIC, que se ha implantado exponencialmente en los últimos tiempos, tiene múltiples implicaciones y ha generado nuevas amenazas a las que el ordenamiento jurídico se ha visto obligado a responder. La generalización del uso de la computación y la tecnología de sistemas ha dado lugar a que los riesgos asociados a las mismas se hayan concebido desde un punto de vista normativo como auténticos problemas de seguridad nacional.

Así, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, considera de especial interés el ámbito de la ciberseguridad. Es el Consejo de Seguridad Nacional, órgano de asistencia al Presidente del Gobierno en las materias relacionadas con la política de Seguridad Nacional y el sistema de Seguridad Nacional[1], el responsable de aprobar la Estrategia Nacional de Ciberseguridad, actualmente regulada por la Orden PCI/487/2019, de 26 de abril[2]. Para el cumplimiento de sus fines en esta materia, el Consejo de Seguridad Nacional está asistido por el Consejo Nacional de Ciberseguridad, actualmente regulado por la Orden PARA/33/2018, de 22 de enero[3].

En el ámbito del sector público, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), atribuye a este organismo, entre otras funciones, la relativa a garantizar la seguridad de las tecnologías de la información en el ámbito de la Administración y velar por el cumplimiento de la normativa relativa a la protección de la información clasificada (artículo 4, apartados e y f). Esta función la desarrolla a través del Centro Criptológico Nacional (CCN), órgano adscrito al CNI y creado mediante Real Decreto 421/2004, de 12 de marzo, cuyo ámbito de actuación alcanza a la seguridad de los sistemas de información de la Administración que procesan, almacenan o transmiten información, incluidas la de carácter clasificado.

Además de la producción normativa reguladora de las políticas y los órganos competentes en materia de ciberseguridad, que por supuesto no se agota en la comentada, se ha aprobado una batería de disposiciones relativas a la protección de datos y a las medidas de seguridad aplicables a los sistemas de información. Sobre protección de datos, se puede destacar la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales o el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal; en materia de sistemas, se han aprobado en el ámbito de la administración electrónica disposiciones reglamentarias que regulan el Esquema Nacional de Interoperabilidad (RD 4/2012, de 4 de enero) y, en lo que constituye el objeto de este artículo, el Esquema Nacional de Seguridad -ENS- (RD 3/2010, de 4 de enero).

El CCN realiza un esfuerzo encomiable para contribuir a garantizar, a través de múltiples medidas, la seguridad de los sistemas. Entre otras, el CCN aporta herramientas informáticas con distinta finalidad (cuadro nº 1) y un conjunto de guías de mejora del grado de ciberseguridad de las organizaciones (cuadro nº 2).

[1]Artículo 17 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.
[2]Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad nacional.
[3]Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad.

Cuadro nº 1. Soluciones Ciberseguridad CCN

Solución informática	Finalidad
ANA	Automatización y normalización de auditorías
CARMEN	Defensa de ataques avanzados/APT
CCNdroid	Seguridad para Android
CLARA	Auditoría de Cumplimiento ENS/STIC en Sistemas Windows
CLAUDIA	Herramienta para la detección de amenazas complejas en el puesto de usuario
EMMA	Visibilidad y control sobre la red
GLORIA	Gestor de logs para responder ante incidentes y amenazas
INES	Informe de Estado de Seguridad en el ENS
LORETO	Almacenamiento en la nube
LUCÍA	Sistemas de Gestión Federada de Tickets
MARÍA	Plataforma multiantivirus en tiempo real
MARTA	Análisis avanzados de ficheros
PILAR	Análisis y Gestión de Riesgos
REYES	Intercambio de Información de ciberamenazas
ROCÍO	Inspección de Operación. Auditoría de configuraciones de dispositivos de red
VANESA	Grabaciones y emisiones de vídeo en streaming

Fuente: https://www.ccn-cert.cni.es

Cuadro nº 2. Guías CCN-STIC

Título-Series	Nº de guías
Serie CCN-STIC-000 Políticas	3
Serie CCN-STIC-100 Procedimientos	13
Serie CCN-STIC-200 Normas	8
Serie CCN-STIC-300 Instrucciones Técnicas	6
Serie CCN-STIC-400 Guías Generales	108
Serie CCN-STIC-500 Guías de entornos Windows	74
Serie CCN-STIC-600 Otros entornos	63
Serie CCN-STIC-800 Esquema Nacional de Seguridad	59
Serie CCN-STIC-900 Informes Técnicos	15
Serie CCN-STIC-1000 Procedimientos de empleo seguro	8

Fuente: https://www.ccn-cert.cni.es

2.- EL ESQUEMA NACIONAL DE SEGURIDAD

2.1.- El proceso de implantación del ENS en una organización

El ENS es el conjunto de principios básicos (cuadro nº 3) y requerimientos mínimos que han de verificarse en la seguridad de la información, para asegurar el cumplimiento de los fines de una entidad cuando emplea sistemas de información.

Cuadro nº 3. Principios básicos ENS. Artículo 4 RD 3/2010

Principios básicos	Contenido
Seguridad integral	El ENS debe abarcar medios técnicos, humanos, materiales y organizativos
Gestión de riesgos	El ENS descansa en el análisis y gestión de riesgos que afecten a los sistemas
Prevención, reacción, recuperación	Las medidas deben prevenir y detectar amenazas, y restaurar información
Líneas de defensa	Se deben contemplar distintas capas de seguridad que minimicen daños
Reevaluación periódica	La valoración de la seguridad es un proceso dinámico
Función diferenciada	El sistema debe contemplar la segregación de funciones y de responsables

Fuente: Elaboración propia

La implementación del ENS en las organizaciones se ha de realizar a través del establecimiento de una **política de seguridad**, que se adoptará conforme a estos principios básicos y aplicando una serie de requisitos mínimos, recogidos y detallados en los artículos 11 a 26 del RD 3/2010.

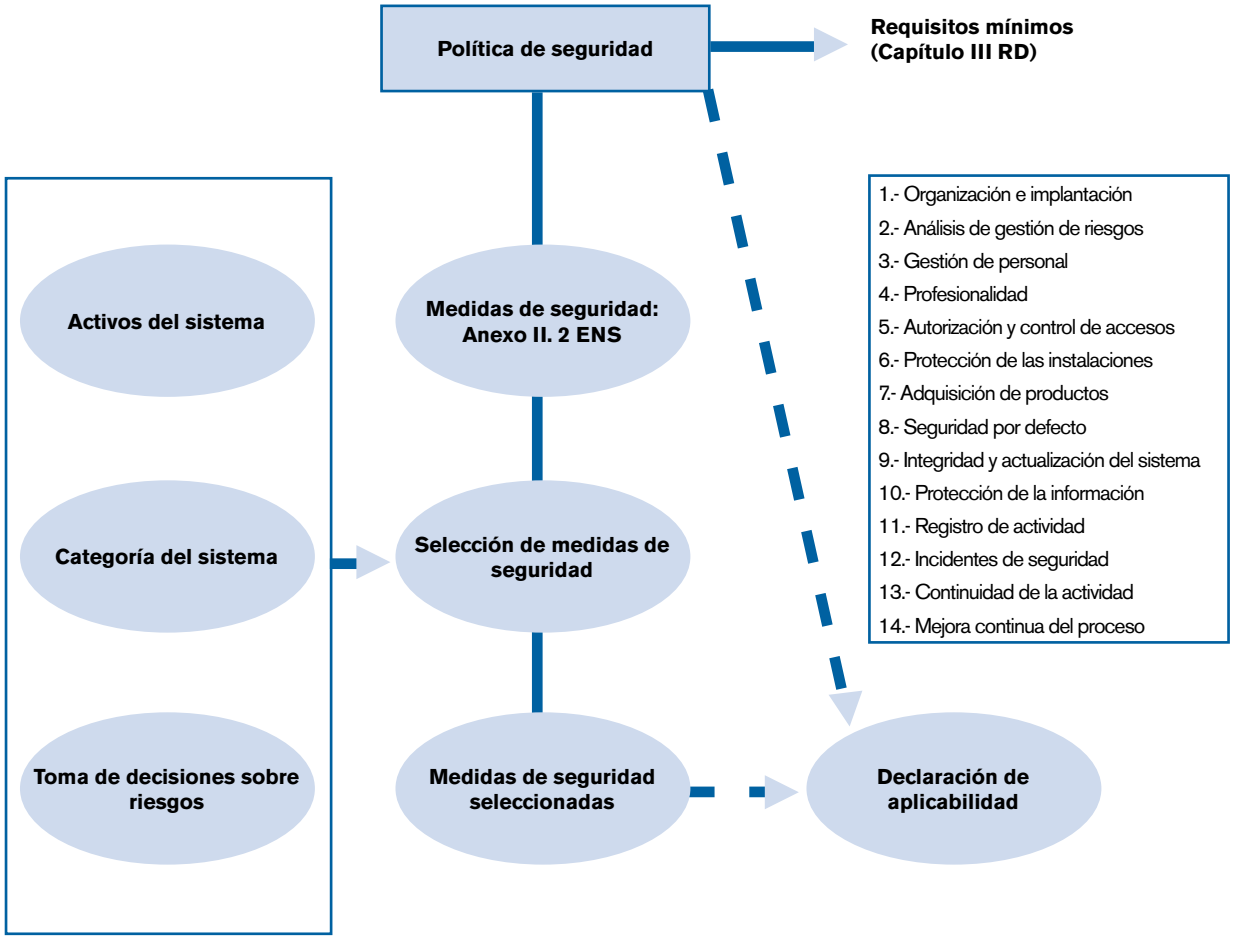
Según el artículo 11 del RD 3/2010, todos los órganos superiores de las Administraciones Públicas deben disponer formalmente de una política de seguridad aprobada por el responsable correspondiente. A tal efecto, se considerarán órganos superiores los responsables directos de la acción del gobierno central, autonómico o local.

El proceso de implantación del ENS tiene por objeto el cumplimiento de los requisitos mínimos contemplados en el RD 3/2010, conforme a los cuales se ha desarrollado la política de seguridad; para ello, la organización habrá de seleccionar las medidas de seguridad más adecuadas, de entre las contenidas en el Anexo II.2 del RD 3/2010. La selección de estas medidas ha de realizarse considerando tres aspectos:

- Los activos que constituyen el sistema de la organización.
- La categoría que la organización otorga a su sistema, según lo establecido en el Anexo I RD 3/2010.
- La toma de decisiones de la organización en materia de gestión de los riesgos identificados a que esté expuesto el sistema.

Las medidas seleccionadas conforme al procedimiento descrito se formalizarán en un documento denominado **"Declaración de Aplicabilidad"**, que deberá ir firmado por el responsable de seguridad (figura nº 1).

Figura 1. Herramientas de implementación ENS



Fuente: Elaboración propia

2.2.- La categorización del sistema

Para la selección de las medidas de seguridad, tras la identificación de los activos que conforman los sistemas de información, la organización ha de **clasificarlos por categorías**.

La categorización de los sistemas se ha de basar en el **principio de proporcionalidad**, considerando la información que el sistema maneja, los servicios que presta y los riesgos potenciales a los que queda expuesto. Teniendo en cuenta estas circunstancias, se deben valorar las consecuencias que tendría un incidente de seguridad sobre el sistema para que la organización (i) alcance sus objetivos, (ii) proteja sus activos, (iii) cumpla con sus obligaciones, (iv) respete la legalidad aplicable y (v) respete los derechos individuales.

Por otro lado, la valoración sobre el impacto que tendría un incidente de seguridad en un sistema ha de realizarse en función de **cinco aspectos o dimensiones de seguridad: la disponibilidad, la autenticidad, la integridad, la confidencialidad y la trazabilidad** (cuadro nº 4).

Cuadro nº 4 . Dimensiones de seguridad

Dimensiones	Significado
Disponibilidad (D)	Se ha de garantizar el acceso a la información en un determinado momento
Autenticidad (A)	Se ha de garantizar la fuente de la que proceden los datos
Integridad (I)	Se ha de garantizar que la información no ha sido alterada
Confidencialidad (C)	Se ha de garantizar que sólo acceden a la información las personas autorizadas
Trazabilidad (T)	Se ha de garantizar que una determinada acción se atribuya únicamente a una entidad

Fuente: Elaboración propia, a partir del ENS

En el proceso de categorización del sistema se atenderán a las siguientes reglas:

- Una información o servicio pueden verse afectados en una o más dimensiones de seguridad. De esta forma, si resultaran afectados en todas las dimensiones de seguridad, habría que realizar cinco valoraciones de la misma información o servicio.
- Una información o servicio puede no verse afectado en alguna dimensión, en cuyo caso, esa dimensión no se adscribirá a ningún nivel de calificación.
- Cada información y servicio se calificará como **BAJO, MEDIO O ALTO**, en cada una de las dimensiones afectadas (cuadro nº 5).
-

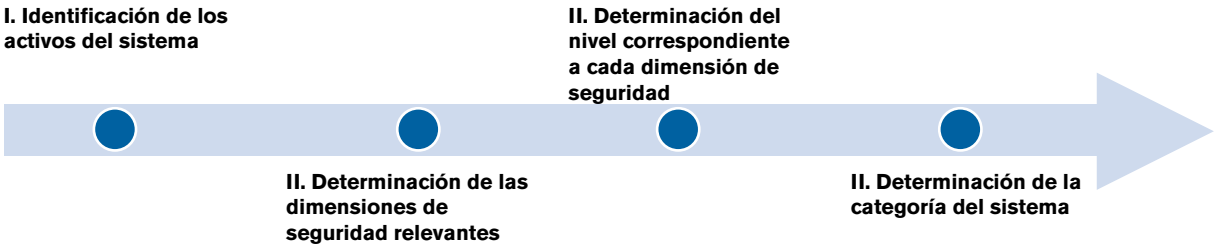
Cuadro nº 5. Calificación de los servicios o informaciones

Dimensiones	Significado
BAJO	Supone un perjuicio limitado sobre la organización, los activos o los individuos
MEDIO	Supone un perjuicio grave sobre la organización, los activos o los individuos
ALTO	Supone un perjuicio muy grave sobre la organización, los activos o los individuos

Fuente: Anexo I del RD 3/2010

- Si un sistema ofrece diferentes informaciones o presta distintos servicios, el nivel de cada dimensión (D, A, I, C, T) será el mayor de los establecidos para cada información ofrecida o servicio prestado.
- Una vez evaluado cada servicio e información que ofrezca un sistema, éste se calificará como **BAJO, MEDIO O ALTO**. Un sistema se calificará con el nivel superior con el que se haya calificado cualquiera de sus dimensiones; sin embargo, ello no implicará que, por este hecho, se altere el nivel de las dimensiones de seguridad que no hayan influido en la determinación de la categoría del mismo.
- Por lo tanto, el proceso de categorización de un sistema se puede representar de la siguiente forma:

Figura nº 2. Proceso de categorización de los sistemas



Fuente: Información CCN. https://www.ccn-cert.cni.es

2.3.- Las medidas de seguridad

El ENS contempla **75 medidas**, que habrán de aplicarse a cada una de las dimensiones, si las mismas resultan afectadas, en función de su categoría o calificación. Estas medidas se distribuyen en tres grandes grupos o marcos de actuación, que son el marco organizativo, el marco operacional y un grupo de medidas de protección (cuadro nº 6).

Cuadro nº 6. Medidas de seguridad

Grupos medidas de protección	Áreas	Nº Total	Categoría dimensiones		
			Baja	Media	Alta
Marco organizativo	1	4	4	+0	+0
Marco operacional	6	31	15	+10	+6
	Planificación	5	3	+1	+1
	Control de acceso	7	6	+1	+0
	Explotación	11	6	+4	+1
	Servicios Externos	3	0	+2	+1
	Continuidad del Servicio	3	0	+1	+2
	Monitorización del sistema	2	0	+1	+1
Medidas de Protección	8	40	25	+8	+7
	De las Instalaciones e infraestructuras	8	6	+1	+1
	Del personal	5	3	+1	+1
	De los equipos	4	2	+2	+0
	De las comunicaciones	5	2	+1	+2
	De los soportes de información	5	4	+1	+0
	De las aplicaciones informáticas	2	1	+1	+0
	De la información	7	5	+0	+2
	De los servicios	4	2	+1	+1
Total	15	75	44	+18	+13

Fuente: Anexo I del RD 3/2010

2.4.- Las pruebas a seleccionar

Dado que las 75 medidas contempladas en el ENS pueden aplicarse a una o varias dimensiones, finalmente se contemplan en la norma un total de 257 pruebas, según se detalla en el cuadro nº 7.

Cuadro nº 7. Pruebas de seguridad en el ENS

Marcos	Áreas	Nº de dimensiones a las que aplicar las medidas					Nº Pruebas
		1	2	4	5	Total	
Organizativo	1	0	0	0	4	4	20
Operacional	6	7	1	6	17	31	118
	Planificación	1	0	0	4	5	21
	Control de acceso	0	1	6	0	7	26
	Explotación	2	0	0	9	11	47
	Servicios Externos	1	0	0	2	3	11
	Continuidad del Servicio	3	0	0	0	3	3
	Monitorización del sistema	0	0	0	2	2	10
Medidas de Protección	8	18	3	0	19	40	119
	Instalaciones e infraestructuras	4	0	0	4	8	24
	Personal	1	0	0	4	5	21
	Equipos	2	0	0	2	4	12
	Comunicaciones	2	1	0	2	5	14
	Soportes de información	2	1	0	2	5	14
	Aplicaciones informáticas	0	0	0	2	2	10
	Información	5	1	0	1	7	12
	Servicios	2	0	0	2	4	12
Total Nº de Medidas		25	4	6	40	75	257
Peso relativo Nº de Medidas		33,33%	5,33%	8,00%	53,33%	100%	
Nº Pruebas (Medidas x Dimensión)		25	8	24	200	257	
Peso relativo Nº de Pruebas		9,73%	3,11%	9,34%	77,82%	100%	

Fuente: Anexo I del RD 3/2010

La CCN-STIC 804 es una guía de seguridad para la implantación del ENS, que establece unas pautas de carácter general aplicable a entidades de distinta naturaleza, sin valorar casuísticas particulares. Dicha guía explica y desarrolla cada una de las 257 medidas de seguridad contempladas en el Anexo II del RD 3/2010.

Para ello, recurre al empleo de **niveles de madurez**, que es un recurso habitual en la implementación de procesos. Según el apartado 6 de la CCN-STIC 804 "el modelo de madurez permite describir las características que hacen un proceso efectivo, midiendo el grado o nivel de profesionalización de la actividad. En la norma, se identifican hasta **seis niveles** de implementación de procesos y se exige un determinado umbral en proporción a la calificación de las dimensiones afectadas o a la categoría del sistema (figuras nº 3 y 4).

Figura 3. Niveles de madurez

Niveles de madurez identificados en la CCN-STIC 804

Nivel	**Descripción**
L0	**Inexistente** Esta medida no está siendo aplicada en este momento Inicial/ad hoc
L1	Cuando la organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas. Pese a su naturaleza caótica, es más que no tener nada; pero es difícil prever la reacción ante una situación de emergencia.
L2	**Repetible, pero intuitivo** Cuando existe un mínimo de planificación que, acompañada de la buena voluntad de las personas proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas.
L3	**Proceso definido** Se dispone de un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general. Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2, y que se gestiona en el nivel 3.
L4	**Gestionado y medible** Cuando se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida.
L5	**Optimizado** En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.

Fuente: CCN-STIC 804

Figura 4. Niveles de madurez

Niveles de madurez identificados en la CCN-STIC 804

	Categoría del sistema	Nivel de madurez mínimo
Nivel de la dimensión		
BAJO	BÁSICA	L2-Repetible pero intuitivo
MEDIO	MEDIA	L3-Proceso definido
ALTO	ALTA	L4-Gestionado y medible

Fuente: CCN-STIC 804

3.- El control externo y la auditoría del ENS

El artículo 34 del Real Decreto 3/2010 obliga a realizar una auditoría, al menos cada dos años, a los sistemas de información a los que les resulte de aplicación, para verificar el cumplimiento de los requerimientos establecidos en el ENS. No obstante, se exime de esta obligación a los de sistemas de categoría básica, respecto de los que bastará una autoevaluación realizada por el propio personal que administra el sistema.

Tal y como establece el artículo 34.4 RD 3/2010, en la ejecución de la auditoría "se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de auditorías de sistemas de información".

En la auditoría del artículo 34 se verificarán los siguientes extremos:

- Que la política de seguridad define los roles y funciones de los distintos responsables de la información, los servicios, los activos y la seguridad de la información.
- Que la designación de los responsables responde al principio de separación de funciones y que existen procedimientos de resolución de

conflictos que puedan surgir entre los distintos responsables.

- Que se ha realizado un análisis de riesgos, con revisión y aprobación anual, y se han implementado las recomendaciones de seguridad.
- Que existe un sistema de gestión de la seguridad.

Además de esta auditoría específica contemplada en el propio ENS, por situarnos en el entorno de las administraciones públicas, el cumplimiento del RD 3/2010 es materia de control por parte de los OCEX, en cuanto que órganos competentes para fiscalizar la actividad económico-financiera del sector público y la legalidad de todo acto que dé lugar al reconocimiento de derechos y obligaciones de contenido económico.

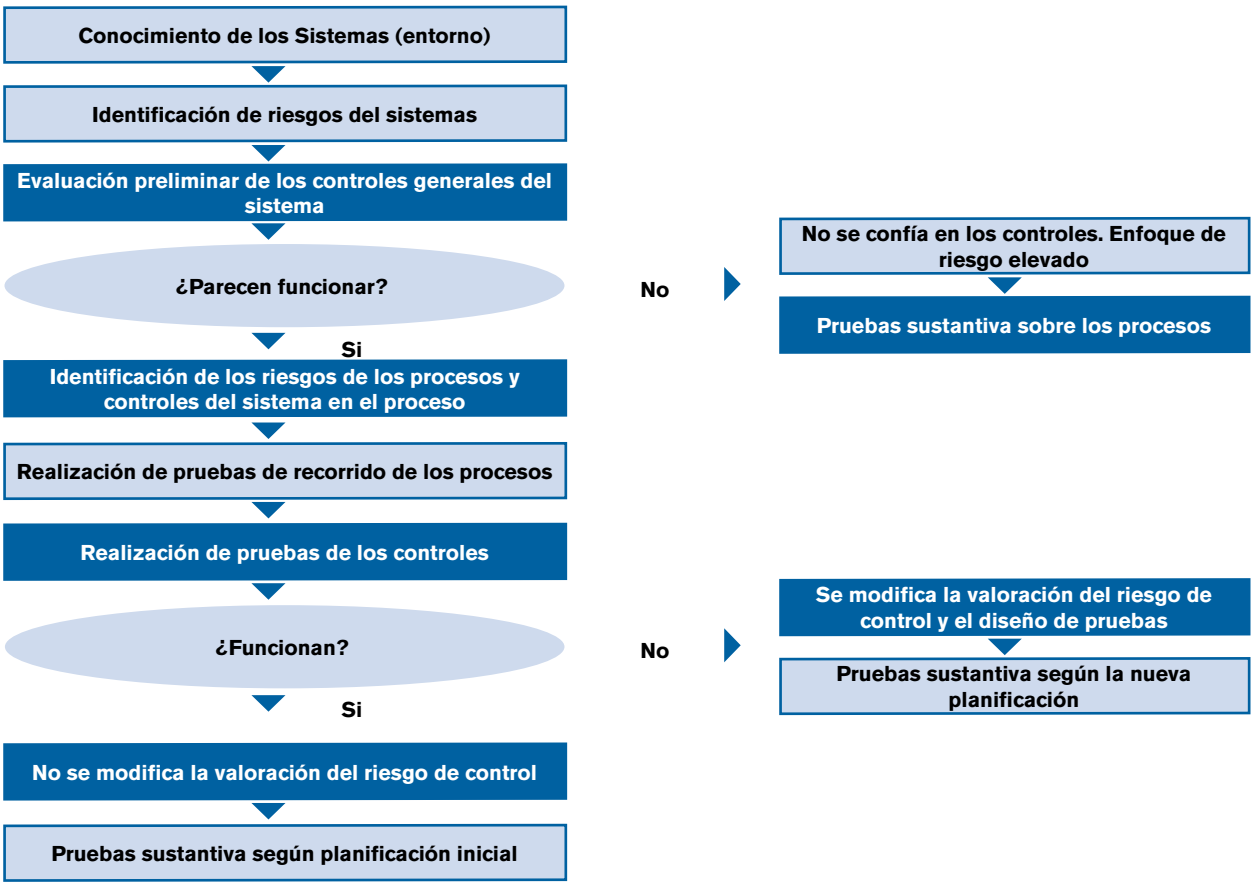
Según la GPF-OCEX-5300, las auditorías de la tecnología de la información se definen como "un examen revisión de los sistemas de TI y controles relacionados que busca obtener seguridad o identificar violaciones a los principios de legalidad, eficiencia, economía y eficacia del sistema de TI y sus controles relacionados".

3.1- La auditoría de sistemas en las fiscalizaciones de los OCEX

La auditoría de sistemas debe estar presente, de manera más o menos intensa, en cualquier tipo de auditoría que relacen los OCEX, ya que la tecnología de la información debe formar parte del análisis del conocimiento general de la entidad auditada. Los sistemas de información y la tecnología empleados por las administraciones deben contar con controles, gran parte de los cuales son de seguridad, que permitan confiar en ellos.

En el análisis del control interno, se deberá comprobar la eficacia de los controles generales que afecten a los sistemas y planificar la auditoría en función de los resultados obtenidos, bien confiando en los controles y haciendo pruebas de su correcto funcionamiento, bien despreciándolos y realizando pruebas sustantivas basadas en un riesgo de control elevado. La comprobación de la eficacia de los controles significa verificar que los controles se han diseñado correctamente y que se han implementado de forma efectiva, lo que supone que el control exista y que efectivamente se utiliza (figura nº 5).

Figura 5. Control interno. Análisis de sistemas en un trabajo de auditoría



Fuente: GPF-OCEX 1315

La GPF-OCEX-1316, de control interno, identifica con carácter no exhaustivo una serie de riesgos específicos derivados del uso de las tecnologías de la información, como son: procesamiento de datos de forma inexacta, accesos no autorizados, accesos autorizados de un número excesivo de usuarios, accesos autorizados con capacidades superiores a las necesarias, cambios no autorizados, cambios no soportados documentalmente, cambios necesarios no realizados.

3.2- El control externo del ENS

La implantación del ENS también puede ser objeto de una auditoría de legalidad, al objeto de verificar si la entidad auditada cumple los requerimientos del RD 3/2010; en tales casos, de conformidad con la GPF-OCEX 5300, el mandato específico de la auditoría debe definir el alcance del trabajo.

En el ámbito de la ciberseguridad, la GPF-OCEX 5313 considera que un análisis de esta materia puede tener tres posibles enfoques:

Una auditoría cuya ejecución suponga la realización de un trabajo similar a la auditoría prevista en el ENS, o bien que siga la metodología de ISACA.

Una revisión de los controles generales de la tecnología de la información (gran parte de los cuales son controles de ciberseguridad) que estén relacionados únicamente con las áreas significativas de la auditoría financiera. Este sería un trabajo del tipo descrito en la figura nº 5, de carácter accesorio a la auditoría de los estados financieros y centrado en el conocimiento del entorno de la entidad y valoración de su control interno.

Una revisión limitada a una serie de controles básicos de ciberseguridad, que permitirá formarse una idea general de la situación en la entidad revisada en materia de sistemas y no requerirá la dedicación de excesivos recursos especializados ni del auditor externo ni del ente auditado

Los OCEX se han decantado por este último planteamiento a la hora de dictar sus propias guías de fiscalización, cuando la auditoría tenga por objeto verificar la existencia y eficacia de las medidas de ciberseguridad. La GPF-OCEX 5313 trata de establecer cuáles serían los controles básicos en materia de ciberseguridad que, por su relevancia frente a las ciberamenazas, deberían ser objeto de auditoría; en este diseño, se ha tenido especial cuidado en mantener la máxima coherencia con los postulados del ENS, por ser una norma **de obligado cumplimiento.**

En la selección de qué controles se consideran relevantes, la GPF-OCEX recurre al marco conceptual establecido por el CIS (Centro de Seguridad de Internet, Center for Internet Security), una organización de reconocido prestigio internacional en la materia. El CIS ha establecido **20 controles críticos**, y estima que aplicando *cinco* controles básicos es establece una efectiva defensa contra, aproximadamente, el 85% de los ataques; no obstante, el propio CIS califica como básicos a los *seis* primeros de esos 20 controles. Tales controles son:

- Administrar un inventario de dispositivos autorizados y no autorizados (hardware).
- Administrar un inventario de software autorizados y no autorizados. Lista blanca.
- Gestión de vulnerabilidades: Escaneo de vulnerabilidades mediante programas informáticos, gestión de parches de actualización.
- Uso controlado de privilegios.
- Configuraciones seguras para hardware y software en dispositivos móviles, portátiles, estaciones de trabajo y servidores.
- Registro de actividad: mantenimiento, monitoreo y análisis de logs de auditoría.

Todas estas guías y recomendaciones son muy útiles para el auditor a la hora de determinar qué aspectos de la ciberseguridad van a ser objeto fiscalización, pues son fruto de la experiencia obtenida por organizaciones profesionales y prestigiosas del sector. No obstante, no conviene olvidar que el ENS ofrece un marco general de referencia sobre medidas de ciberseguridad y que la entidad obligada a su implantación debe ajustarlo a las características propias de su organización; por tanto, puede ocurrir que en ocasiones no sea razonable o eficaz detenerse en analizar determinados controles propuestos con carácter general como básicos en las distintas normas y guías. Siguiendo la GPF-OCEX 5313, las auditorías de sistemas deben estar basadas en un enfoque de riesgo, lo que implica la identificación de aquellos elementos que supongan amenazas para la entidad auditada para, valorando potencial impacto que aquellos puedan tener, identificar las áreas prioritarias para ser auditadas.

A efectos de planificar una auditoría del ENS, es interesante considerar qué distribución de pruebas realiza el ENS, entre las distintas áreas; este análisis nos permitirá disponer de un conocimiento adicional importante para determinar qué áreas considera el RD 3/2010 más relevantes en materia de ciberseguridad. De esta forma, la planificación partirá de las orientaciones ofrecidas por las GPF-OCEX, pero podrán ser moduladas por el juicio profesional de auditor.

Realmente, la selección de los siete controles básicos de ciberseguridad que recoge la GPF-OCEX 5313 viene a responder a la distribución de medidas que establece el propio ENS. Estos siete controles están referenciados

a un total de 11 medidas del ENS, que se traducen en 40 pruebas; de estas 40 pruebas, únicamente 6 (las correspondientes a las medidas op.exp.3 y op.exp.10) no están previstas para servicios o informaciones de categoría baja (cuadro nº 8).

Cuadro nº 8. Controles básicos GPF-OCEX 5313

Control		Medida ENS	Nº dimensiones	Nivel de exigencia
CBCS 1	Inventario y control dispositivos físicos	op.exp.1	5	B = M = A
CBCS 2	Inventario y control software autorizado y no autorizado	op.exp.1	5	B = M = A
		op.exp.2	5	B = M = A
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades	mp.sw.2	5	B < M < A
		op.exp.4	5	B = M = A
CBSA 4	Uso controlado de privilegios administrativos	op.acc.4	4	B = M = A
		op.acc.5	4	B < M < A
CBCS 5	Configuraciones seguras del software y hardware de dispositivos móviles, portátiles, equipos de sobremesa y servidores	op.exp.2	5	B = M = A
		op.exp.3	5	M = A
CBCS 6	Registro de la actividad de los usuarios	op.exp.8	1	B < M < A
		op.exp.10	1	A
CBCS 7	Copias de seguridad de datos y sistemas	mp.info.9	1	B = M = A

Fuente: GPF-OCEX 5313

Esta constatación es una garantía de la orientación que adopta la GPF-OCEX 5313 respecto al ENS, de forma que el auditor, a partir del conocimiento de la distribución de pruebas que realiza el RD 3/2010, puede seguir estas pautas aún en el caso de tener que alterar el diseño de los controles de ciberseguridad cuando la entidad presente particularidades.

4.- CONCLUSIONES Y RECOMENDACIONES

Las entidades locales deben reforzar sus medidas de seguridad para la protección de sus sistemas de información. La amenaza es real y se conocen múltiples ejemplos, como se ha visto en la introducción. Al conocimiento de la normativa vigente, de los recursos disponibles y de la hoja de ruta a seguir en caso de que se produzca un incidente crítico, hay que añadir la necesidad de trabajar de manera transversal y la imprescindible formación del conjunto de empleados públicos que trabajan en el ámbito de la entidad local. La principal brecha de seguridad está en las personas.

Próximo a publicarse el Real Decreto por el que se desarrolla el RDL 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (del que ya existe un borrador), el presente artículo tiene como principal finalidad dar a conocer los contenidos del Esquema Nacional de Seguridad y de las Guías Prácticas de Fiscalización existentes en materia de ciberseguridad, además de proponer la inclusión de fiscalizaciones de cumplimiento de legalidad en materia de ciberseguridad en los diferentes planes de actuación de los OCEx previstos para 2020.

En un mundo interconectado, y donde la interoperabilidad es ya un mandato, un punto vulnerable debilita todo el sistema. La fragilidad de las entidades locales, sus escasos recursos humanos y presupuestarios y su heterogeneidad hacen de la administración local el eslabón más débil de la cadena. De ahí la importancia de cumplir con la normativa vigente y de verificar, desde el control externo, que así se está haciendo.