CAPÍTULO VI

El cumplimiento del Esquema Nacional de Seguridad (ENS) en las entidades locales

Miguel Á. Lubián Rueda
Ingeniero en Informática.
Director General de CIES (Grupo Seresco)

SUMARIO. 1. Introducción. 2. El marco de certificación del ENS para entidades locales: grandes y pequeños municipios. 2.1. Cómo abordar una implantación. 2.2. Categorización del sistema y declaración de aplicabilidad. **3. El perfil de cumplimiento específico del ENS para entidades locales: grandes municipios y pequeños municipios.** 3.1. ¿Qué es un PCE? Regulación, ejemplos de principales perfiles publicados. 3.2. ¿Por qué un PCE para las entidades locales? 3.3. PCE 890. 3.4. PCE 883. **4. Los Gobiernos intermedios como organismos de certificación del ENS. 5. Implicaciones de la Directiva relativa a las medidas para un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS2) en las entidades locales. 6. Bibliografía.**

1. Introducción

En el presente capítulo se analizan diferentes modelos desarrollados por el Centro Criptológico Nacional (en adelante, CCN) para ayudar a las entidades locales a la mejora de la seguridad de los sistemas de información, incluyendo las especialidades de los Perfiles de Cumplimiento Específicos de gobernanza en seguridad (en adelante, PCE).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Se analizará, también, la relevancia que adquieren las diputaciones provinciales, los cabildos y consejos insulares y las comunidades autónomas uniprovinciales en la mejora de la seguridad de la información de los ayuntamientos de menor tamaño, un papel desarrollado en el marco de sus competencias.

Por último, sin perjuicio de las adaptaciones de la transposición de la Directiva NIS2, que a fecha de elaboración de este capítulo aún no se ha aprobado, se analizará su impacto en las entidades locales, abordando la clasificación de determinados servicios que prestan como esenciales o importantes y la necesidad de definir nuevas estrategias para la gestión de los riesgos en ciberseguridad.

2. El marco de certificación del ENS para entidades locales: grandes y pequeños municipios

Para poder abordar las peculiaridades de los PCE, es necesario primero analizar aspectos clave de la conformidad con el ENS en el modelo estándar o tradicional.

Si bien a lo largo de este libro ya se han ido exponiendo las implicaciones del nuevo ENS y su afección a las entidades locales, pasaremos ahora a comentar, desde un punto de vista más práctico, los detalles de cómo abordar la conformidad con el ENS, bien porque la entidad desee iniciar el camino de la adecuación a la norma con este modelo, o bien porque ya disponga de una declaración de aplicabilidad en categoría básica o se haya adaptado con un PCE, que explicaremos en el siguiente apartado de este capítulo, para entidades locales, y quiera continuar evolucionando hacia un sistema de gestión más completo.

Es importante destacar que la seguridad de la información es trasversal a toda la organización y afecta no solo a los sistemas de información, sino también a los tradicionales expedientes en formato papel, por lo que la complejidad de abordar un proyecto de implantación en el modelo estándar debe iniciarse en aquellos sistemas de información más críticos para la organización. La identificación de los sistemas más críticos se realizará previo análisis inicial de riesgos, teniendo siempre también presente que uno de los principios básicos tanto de la seguridad de la información como de otros sistemas, como el relacionado con el cumplimiento de la normativa de protección de datos, es el de mejora continua, es decir, nunca se debe mantener una actitud estática, sino proactiva, por lo que una entidad local debe continuar extendiendo las medidas del ENS a los distintos sistemas

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

de información, bien porque sirvan de forma directa para prestar servicios a las personas interesadas (servicios finalistas como, a modo de ejemplo, prestaciones sociales, subvenciones, urbanismo...) o bien porque sirvan de soporte a estos (a modo de ejemplo, gestión del personal, contratación, compras, contabilidad...).

La conformidad con el ENS supone evidenciar el cumplimiento de las medidas de la norma, si bien, a priori, podría verse como algo ajeno a las Administraciones públicas. El ENS, recordemos, es una obligación del art. 156 de la Ley 40/2015 que ha ido adquiriendo especial relevancia con la implantación de los procesos administrativos electrónicos y los nuevos riesgos a los que se exponen las entidades locales. Pensemos, por ejemplo, que palabras como ciberseguridad, *hacking*, *phishing* o *ransomware* no eran conocidas hasta hace pocos años; tampoco los incidentes se materializaban con la gravedad con la que ocurren en la actualidad (cifrado y secuestro de bases de datos, suplantaciones y estafas cibernéticas...). Es, por tanto, una necesidad prioritaria que las entidades locales pongan todos los medios para evitar que un incidente de seguridad se materialice, o, si esto ocurre, para que su gravedad sea mínima[1].

Cuando se produce un incidente de seguridad o una brecha de datos personales[2] y se debe comunicar a los organismos de control, una mane-

1. La Sentencia núm. 188/2022 de la Sección Tercera de la Sala de lo Contencioso-Administrativo del Tribunal Supremo, de 15 de febrero de 2022, en su Fundamento de Derecho Tercero, establece lo siguiente:

"La obligación de adoptar las medidas necesarias para garantizar la seguridad de los datos personales no puede considerarse una obligación de resultado, que implique que producida una filtración de datos personales a un tercero exista responsabilidad con independencia de las medidas adoptadas y de la actividad desplegada por el responsable del fichero o del tratamiento.

En las obligaciones de resultado existe un compromiso consistente en el cumplimiento de un determinado objetivo, asegurando el logro o resultado propuesto, en este caso garantizar la seguridad de los datos personales y la inexistencia de filtraciones o quiebras de seguridad.

En las obligaciones de medios el compromiso que se adquiere es el de adoptar los medios técnicos y organizativos, así como desplegar una actividad diligente en su implantación y utilización que tienda a conseguir el resultado esperado con medios que razonablemente puedan calificarse de idóneos y suficientes para su consecución, por ello se las denomina obligaciones 'de diligencia' o 'de comportamiento'".

2. Se incorpora también la referencia a las violaciones de seguridad o brechas de datos personales de la normativa de protección de datos, ya que la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales vincula las medidas del ENS con la protección de datos: "1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679".

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

ra de evidenciar el cumplimiento de la normativa es la conformidad con el ENS, pero siempre que se haya mantenido en el tiempo el despliegue de las medidas de forma proactiva, supervisando y mejorando aquellos aspectos que sean precisos para evitar o mitigar el impacto de un incidente, teniendo en cuenta que el riesgo 0 no existe.

A fecha de redacción de este capítulo, el número de entidades locales que contaban con la conformidad con el ENS en sus sistemas de información era de 31 ayuntamientos, 3 diputaciones y un consorcio, además de aquellas que certifican el sistema de información que soporta la tramitación de sus servicios conforme al PCE de requisitos esenciales, que, según anuncia el CCN, pasará a denominarse PCE de Requisitos Fundamentales de Seguridad. Es evidente que son pocas las entidades locales que han afrontado un proceso de conformidad con el ENS; esto puede deberse a múltiples factores (lejanía del mundo administrativo con la seguridad, escasez de medios o de personal con suficiente capacitación en la materia, costes del proceso, falta de sensibilización sobre la relevancia de la seguridad de la información...). Si bien el número de entidades locales que disponen de conformidad con el ENS es reducido, el número de empresas privadas que ha optado por certificar sus sistemas de información (aquellas que son proveedoras para las Administraciones públicas) se ha ido elevando paulatinamente hasta alcanzar a fecha actual las 1754, distribuyéndose en categoría alta 618, en media 1104 y en básica 32.

La ampliación del número de empresas se debe a una mayor concienciación, por parte de las Administraciones públicas, de exigir el cumplimiento del ENS en la contratación, tal y como ya se indicaba en la Resolución de 13 octubre 2016 que aprobaba la Instrucción *Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad*, y que ahora se recoge en el art. 2.3 del ENS:

> "Este real decreto también se aplica a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad a que se refiere el art.12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.
>
> La política de seguridad a que se refiere el art. 12 será aprobada en el caso de estas entidades por el órgano que ostente las máximas competencias ejecutivas.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

> Los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación de este Real Decreto contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las correspondientes declaraciones o certificaciones de conformidad con el ENS.
>
> Esta cautela se extenderá también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos".

El control de la cadena de proveedores, como se verá en el último apartado, es también uno de los aspectos más destacados de la Directiva NIS2. Las entidades locales en muchas ocasiones no disponen de sistemas de información propios, sino que son adquiridos a proveedores externos en diferentes modalidades de prestación de servicios y/o suministros que pueden instalarse en local o en la nube (PaaS[3], IaaS[4], SaaS[5]), por lo que deben reforzar su control para evitar que los medios no sean los adecuados a los riesgos de la información y/o los servicios que prestan.

Como puede observarse, reiteradamente se hace referencia a la necesidad de analizar los riesgos en relación con los servicios y la información (incluyendo los datos personales) que gestionan las entidades. El análisis de riesgos no solo va a permitir identificar áreas críticas, sino también implementar los medios de seguridad adecuados a las mismas, descritos en el Anexo II del ENS, preservando la debida confidencialidad, integridad, autenticidad o trazabilidad de la información, así como la disponibilidad de los servicios.

Si bien la confidencialidad y, ligadas a ella, la integridad y la autenticidad son dimensiones que se deben asegurar de forma reforzada, en ocasiones, como cuando se tratan datos personales de categorías especiales o cuando existe una norma con rango legal que obliga a ello (a modo de ejemplo, los datos tributarios), la disponibilidad debe ser interpretada de acuerdo, también, con la posibilidad de alargar los plazos administrativos en caso de ciberincidentes graves, según se dispone en la adición del apdo. 5 al art. 32 de la Ley 39/2015, por la disposición final 21.ª del Real Decreto-ley 6/2022, de 29 de marzo.

3. Plataforma como servicio, por sus siglas en inglés (*Platform as a Service*).
4. Infraestructura como servicio, por sus siglas en inglés (*Infrastructure as a Service*).
5. *Software* como servicio, por sus siglas en inglés (*Software as a Service*).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

2.1. Cómo abordar una implantación

A continuación, veremos de una forma más práctica lo que supone el proceso de adecuación al ENS, que, con carácter general, se estructura en las siguientes fases, independientemente de si se trata de una adecuación estándar o de si nos acogemos a un PCE.

Fuente: elaboración propia

A continuación, se describen brevemente estas fases:

- **Definición de la gobernanza de la seguridad**. Es muy conveniente iniciar el proceso de adecuación con esta tarea, pues, como norma general, el proceso de identificación de los roles de seguridad puede llevar su tiempo, e incluso se pueden identificar necesidades formativas que será necesario llevar a cabo. Además, durante el proceso de implantación de la seguridad habrá actuaciones (procedimientos, normas, declaración de aplicabilidad...) que deberán ser evaluadas y aprobadas por los roles de seguridad y/o el comité de seguridad de la información, si bien no es necesario haber finalizado esta tarea para que podamos seguir con la siguiente fase en la implantación del ENS.

- **Elaboración del plan de adecuación**, que requerirá las siguientes acciones:

    - Identificación del **alcance de la conformidad con el ENS**. Es importante, ya desde el principio del proceso de adecuación, concretar los servicios que se incluirán en el alcance.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- **Categorización del sistema**. Este proceso se realizará tal y como se ha definido en el Anexo I del ENS y en las guías del CCN. Se prestará especial atención al requisito necesario de que las soluciones proporcionadas por terceros que formen parte de la prestación del servicio (total o parcialmente) dispongan de la conformidad con el ENS para el servicio proporcionado y en la categoría requerida.

- Elaboración de la **declaración de aplicabilidad** provisional, análisis de riesgos y declaración de aplicabilidad definitiva; por su importancia se ampliarán estos conceptos más adelante.

- Realización del **diagnóstico** de cumplimiento de las medidas de seguridad recogidas en la declaración de aplicabilidad, y elaboración del **plan de implantación** con definición de tareas, responsables y plazos de ejecución. Es muy recomendable que este plan sea aprobado formalmente; esto hará que el proceso de implantación del ENS se interiorice en la entidad.

- **Implantación de la seguridad**, compuesta por las siguientes acciones:

  - **Seguimiento del plan de implantación** mediante revisiones regulares de su cumplimiento, y, llegado el caso, reprogramación de las tareas necesarias.

  - Despliegue de **medidas técnicas, organizativas y legales**, desarrollando a la par el marco normativo, políticas, normas, procedimientos, instrucciones técnicas que forman parte del Sistema de Gestión de Seguridad de la Información (SGSI).

  - **Aprobación por parte de la dirección** de la entidad (alcaldía/presidencia de la diputación) del **SGSI**.

- **Obtención de la conformidad**. Recordemos que, para sistemas de categoría básica, será suficiente que, cada dos años, se realice una declaración de conformidad mediante una autoevaluación de cumplimiento. No obstante, resulta altamente recomendable realizar una auditoría de certificación, ya que esto permitirá que la entidad local figure en la lista de entidades certificadas del portal web

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

del CCN[6]. Para sistemas de categoría media o alta, será necesario realizar una auditoría de conformidad bienal y auditorías internas todos los años, tal y como se refleja en la Guía CCN-STIC IC-01/19 ENS sobre Criterios Generales de Auditoría y Certificación[7], cuyo objeto es servir de referencia y establecer los criterios generales para la Auditoría y Certificación de los sistemas de información del ámbito del ENS. Una vez superado el proceso de auditoría de certificación o autoevaluación, la entidad local estará en condiciones de obtener la certificación de conformidad con el ENS en el primer caso, y la declaración de conformidad en el segundo.

- **Definición de métricas** (Encuesta INES): será necesario definir las métricas para conocer el grado de implantación de las medidas de seguridad y para dar respuesta al informe anual requerido por el art. 32 del ENS, relativo al Informe Nacional sobre el Estado de la Seguridad (denominado INES). Para cumplir con este mandato, el CCN ha desarrollado el proyecto INES, para recopilar los datos a través de la plataforma habilitada a tal fin. Además, para sistemas de categoría media y alta, se definirán las métricas necesarias para conocer la efectividad del sistema de gestión de incidentes de seguridad y la eficiencia del sistema de gestión de la seguridad.

- **Vigilancia y mejora continua**. La gestión de la seguridad conllevará como mínimo las siguientes acciones:

    - **Al menos anualmente** se revisarán (con actualización y aprobación en caso de que sea necesario):

        - Los roles de seguridad[8], los miembros del Comité y el texto de la Política de Seguridad. Si existen vacantes, o nuevas incorporaciones.

        - El alcance de la certificación y su categorización, si es necesario incorporar nuevos servicios o bien revisar alguno que haya cambiado.

6. Lista de entidades certificadas: https://gobernanza.ccn-cert.cni.es/certificados.
7. La disposición adicional segunda del ENS señala que el CCN, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación, que se incorporarán al conjunto documental utilizado para la realización de las auditorías de seguridad.
8. Para información más detallada, puede acudirse a la Guía CCN-STIC 801, *Responsabilidades y Funciones en el ENS*.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- El análisis de riesgos y el seguimiento del plan de tratamiento de riesgos. Será necesario identificar si hay nuevas amenazas que afecten al sistema, si se han realizado cambios sustanciales en el sistema de información o si se han incorporado nuevos servicios, además de realizar el seguimiento periódico de las actuaciones reflejadas en el plan.

- El análisis de impacto, como resultado de los puntos anteriores, por incorporación de nuevos servicios o variación de los existentes, o de los criterios para valorar el impacto de la interrupción de dichos servicios.

- La declaración de aplicabilidad. También como resultado de las revisiones anteriores y de otras tareas de seguimiento del sistema, puede ser necesario incorporar nuevas medidas, o desarrollar medidas compensatorias o complementarias de vigilancia.

o **Al menos anualmente** se realizarán:

- La cumplimentación de la encuesta INES.

- Auditorías internas opcionales para sistemas de categoría básica y obligatorias para media y alta.

- La actualización de la documentación que forma parte del SGSI, ya sea derivada de las tareas anteriores, o bien por corrección de errores o inconcreciones.

o **Cada dos años** se realizará la auditoría de certificación de conformidad con el ENS, obligatoria para sistemas de categoría media y alta, o bien para sistemas de categoría básica, si bien para estos es suficiente con la declaración de conformidad con el ENS mediante una autoevaluación realizada por la propia entidad.

2.2. Categorización del sistema y declaración de aplicabilidad

Antes de proseguir con las explicaciones relativas a los PCE para las entidades locales, creemos conveniente definir los conceptos de categorización del sistema y declaración de aplicabilidad.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

La determinación de la categoría de seguridad de un sistema de información, tal y como se define en el Anexo I del ENS, se basa en la valoración del impacto que tendría sobre las entidades un incidente de seguridad que afectase a la seguridad de la información o de los servicios prestados para alcanzar sus objetivos, proteger los activos a su cargo y garantizar la conformidad con el ordenamiento jurídico. Para la determinación del impacto se tendrán en cuenta las cinco dimensiones de seguridad ya citadas: Confidencialidad [C][9], Integridad [I][10], Trazabilidad [T][11], Autenticidad [A][12] y Disponibilidad [D][13]. Cada una de estas dimensiones se adscribirá a uno de los siguientes niveles de seguridad: bajo, medio o alto; y, en caso de no verse afectada, no se adscribirá a ningún nivel, según los criterios indicados en el mencionado anexo. De acuerdo con la valoración, tal y como se indica en el Anexo I del ENS:

"1. Se definen tres categorías de seguridad: básica, media y alta.

a) Un sistema de información será de categoría alta si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad alto.

b) Un sistema de información será de categoría media si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad medio, y ninguna alcanza un nivel de seguridad superior.

c) Un sistema de información será de categoría básica si alguna de sus dimensiones de seguridad alcanza el nivel bajo, y ninguna alcanza un nivel superior".

La valoración de los servicios y la información la realizarán los responsables de la información y los servicios, pudiendo contar con la opinión del responsable de seguridad y/o del responsable del sistema. Y deberá ser aprobada formalmente por los responsables de la información y los ser-

9. [C]: Se establecerá en función de las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.

10. [I]: Se establecerá en función de las consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información.

11. [T]: Se establecerá en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido a —o modificado— una cierta información.

12. [A]: Se establecerá en función de las consecuencias que tendría el hecho de que la información no fuera auténtica.

13. [D]: Se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera usar el servicio cuando lo necesitase.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

vicios, respectivamente. La Guía CCN-STIC 803 sobre la valoración de los sistemas ayuda a realizar el proceso de categorización.

Por otro lado, la declaración de aplicabilidad en el ámbito del ENS es un documento en el que se formalizarán las medidas de seguridad que resultan de aplicación al sistema de información. Este documento pasará por dos estados: uno inicial, denominado declaración de aplicabilidad inicial, que contendrá las medidas de seguridad del Anexo II del Real Decreto ENS, conforme a la categoría del sistema tal y como se ha definido anteriormente; y otro definitivo, aprobado por el responsable de seguridad, tras un análisis de riesgos. A la hora de seleccionar las medidas de seguridad hay que tener en cuenta los siguientes aspectos:

- Las medidas se seleccionarán en función de la valoración de cada una de las cinco dimensiones de seguridad. Por ejemplo, si las valoraciones por dimensiones son las siguientes ([C]: medio, [I]: medio, [T]: medio, [A]: medio, [D]: bajo), la categoría del sistema será media y las medidas de seguridad del Anexo II del ENS que se aplicarán al sistema serán solo 65, en lugar de las 68 que corresponden a un sistema de categoría media cuando las cinco dimensiones de seguridad tienen un valor medio. Pero ¿por qué son 65 medidas en vez de 68? Esto se debe a que la dimensión de Disponibilidad [D] se valora en nivel bajo, y por tanto no son aplicables las medidas de análisis de impacto [op.cont.1], protección frente a inundaciones [mp.if.6] y protección frente a la denegación de servicio [mp.s.4], que se corresponden con la Disponibilidad [D] en nivel medio.

- Conforme a lo establecido en el ENS, las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras denominadas compensatorias, siempre y cuando se justifique documentalmente que los activos se protegen igual o mejor frente al riesgo, y que también se satisfacen los principios básicos y los requisitos mínimos previstos en los Capítulos II y III del ENS. Para documentar las medidas compensatorias se podrá tomar como referencia la Guía CCN-STIC 819 *Medidas Compensatorias*, y se incluirán en la declaración de aplicabilidad.

En base a lo mencionado anteriormente tendremos la declaración de aplicabilidad inicial, y posteriormente se procederá a la realización del análisis de riesgos. Tras realizar el análisis, si el resultado (el riesgo residual) no es aceptado por la entidad será necesario aplicar nuevas medidas para mitigar el riesgo, medidas que serán de aplicación al sistema y por tanto for-

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

marán parte de la declaración de aplicabilidad, considerándose entonces como la definitiva.

En este punto también es cuando la entidad podrá acogerse a un PCE que sea de aplicación, tras la aceptación del riesgo residual.

La declaración de aplicabilidad es uno de los documentos más importantes, ya que nos servirá para identificar las medidas de seguridad que debamos implementar sobre el sistema y, a su vez, en un proceso de auditoría tanto interna como externa, será el documento de apoyo para su revisión. Por tanto, es importante que la declaración de aplicabilidad contemple lo siguiente:

- Para cada una de las 73 medidas de seguridad del Anexo II del ENS, se indicará no solo si aplica o no al sistema de información, sino también, de forma muy resumida, cómo aplica y/o la documentación donde se detalla y, en su caso, por qué no aplica.

- En el caso de medidas de seguridad que planteen la opción de aplicabilidad con refuerzos elegibles, se deberá indicar cuál se ha aplicado.

- Si la medida se sustituye por una compensatoria, deberá indicarse y referenciarse la ubicación de la descripción de la medida compensatoria.

- Si en la medida indicada se ha aplicado una medida complementaria de vigilancia[14].

- Para cada medida de aplicación, se indicará el nivel de madurez y el grado de implementación, conforme a lo establecido en la Guía CCN-STIC-808 *Verificación del cumplimiento de las medidas en el ENS*.

14. Esta medida complementa y equilibra los requisitos exigibles que se han implementado para una determinada medida de seguridad, ya sean base o de refuerzo, cuando estos no son suficientes, a juicio de la entidad, para poder alcanzar el cumplimiento del ENS para dicha medida. También puede complementar a una medida compensatoria que no consigue igualar o mejorar el riesgo de la medida original. En ocasiones, dichas medidas serán transitorias (limitadas en el tiempo) hasta que se consiga la efectividad plena en la implantación de una medida. Conforme a lo establecido en la Guía CCN-STIC-808 "Verificación del cumplimiento de las medidas en el ENS".

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

La declaración de aplicabilidad será aprobada formalmente por el responsable de supervisión/vigilancia (responsable de la seguridad). Para su elaboración, podemos tomar como referencia la Guía y su Anexo CCN-CERT_BP_14_Declaración de Aplicabilidad ENS.

Como ya se ha señalado, se pueden integrar otras medidas, y aquí es relevante destacar, por la propia conexión que hace el texto del ENS, el plan de tratamiento del riesgo derivado de un análisis de riesgos y/o evaluación de impacto en protección de datos.

En relación con la normativa de protección de datos, el propio ENS indica que deberán tenerse en cuenta las medidas recogidas en el análisis de riesgos en privacidad y, en su caso, una evaluación de impacto, debiendo consultarse al delegado de protección de datos, tal y como se recoge, entre otros, en el art. 3.2 del ENS.

Asimismo, se indica en el apdo. 3.3 del ENS que resultarán de aplicación las medidas derivadas del análisis de riesgos en privacidad o de las evaluaciones de impacto cuando estas sean más exigentes que las derivadas del análisis de riesgos del ENS.

Atendiendo a la definición que el propio ENS da de análisis de riesgos [15], la valoración de la información (donde se incluyen los datos personales), como ya se ha venido comentando, se hace sobre cuatro dimensiones: confidencialidad [C], integridad [I], autenticidad [A] y trazabilidad [T], siendo la dimensión que afecta a los servicios la de disponibilidad [D].

Como puede observarse, las dimensiones del ENS para la información son similares a las analizadas por la normativa de protección de datos, a excepción de la autenticidad y la trazabilidad. Por ello, en los análisis de riesgos se deberán tener en cuenta aquellas especificaciones propias relacionadas con los datos personales, como pueden ser las normativas sectoriales que los afectan[16] o la calificación de los datos como "categorías especiales"[17].

15. En el Anexo IV se define como "estudio de las consecuencias previsibles de un posible incidente de seguridad, considerando su impacto en la organización (en la protección de sus activos, en su misión, en su imagen o reputación, o en sus funciones) y la probabilidad de que ocurra".

16. Véase, a modo de ejemplo, la especial confidencialidad sobre los datos de índole tributaria que se regula en el art. 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria.

17. El Reglamento General de Protección de Datos define las categorías especiales de datos, sujetas a una especial protección, en su art. 9.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Teniendo en cuenta los conceptos básicos y cómo abordar una adecuación estándar, procederemos ahora a exponer los PCE que el CCN ha aprobado específicamente para las entidades locales, como sector con características singulares.

3. El perfil de cumplimiento específico del ENS para entidades locales: grandes municipios y pequeños municipios

3.1. ¿Qué es un PCE? Regulación, ejemplos de principales perfiles publicados

Para dar comienzo a este apartado, en sintonía con lo que se ha ido comentando en los capítulos precedentes, es necesario señalar que, entre los diferentes cambios introducidos por el Real Decreto 311/2022 (ENS), se encuentra la posibilidad de crear perfiles de cumplimiento específicos (en adelante PCE), tal y como se indica en su art. 30.

Un PCE, como una postura de seguridad adaptada a unas circunstancias concretas, tal como se indica en el preámbulo del Real Decreto, es un reajuste de las medidas del ENS adaptadas a un sector o sistema[18] concreto que cuenta con unas peculiaridades propias; en concreto, se señala que entre los tres grandes objetivos del ENS se encuentra el siguiente:

> "[...] introducir la capacidad de ajustar los requisitos del ENS, para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y sus servicios. Ello aconseja la inclusión en el ENS del concepto de 'perfil de cumplimiento específico' que, aprobado por el Centro Criptológico Nacional, permita alcanzar una adaptación del ENS más eficaz y eficiente, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible".

18. El nuevo ENS modifica en el glosario el concepto de sistema de información, que ahora incluye cualquiera de los elementos siguientes:
1.º- Las redes de comunicaciones electrónicas que utilice la entidad del ámbito de aplicación de este real decreto sobre las que posea capacidad de gestión.
2.º- Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales.
3.º- Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Es interesante reseñar que el legislador ha entendido la necesidad de realizar adaptaciones de las medidas estándar definidas en el Anexo II del ENS, teniendo en cuenta los recursos —en muchas ocasiones escasos— con los que cuentan las diferentes entidades incluidas en el ámbito de aplicación del ENS, en aras de una mayor eficacia y eficiencia, principios que —recordemos— rigen la actuación de las Administraciones públicas, tal y como se señala en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

El glosario del ENS define al PCE como "conjunto de medidas de seguridad, comprendidas o no en el anexo II de este real decreto, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad, y que haya sido habilitado por el CCN".

Por su parte, el art. 30 del ENS regula los PCE en los siguientes términos:

> "1. En virtud del principio de proporcionalidad y buscando una eficaz y eficiente aplicación del ENS a determinadas entidades o sectores de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten idóneas para una concreta categoría de seguridad. [...]
>
> 3. El CCN, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento específicos que se definan y los antedichos esquemas de acreditación y validación, de acuerdo con las instrucciones técnicas de seguridad y guías de seguridad aprobadas conforme a lo previsto en la disposición adicional segunda. [...]".

De lo hasta aquí comentado sobre la regulación del ENS, se pueden extraer las principales características de los PCE:

- Se crean para entidades, sectores de actividad específicos o sistemas de información con características comunes.
- Pueden aplicarse tanto a entidades públicas como privadas, ya que debe tenerse en cuenta que el art. 2 del ENS abarca tanto a las Administraciones y su sector público como a las entidades privadas que prestan servicios a estas.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- Suponen una adaptación de las medidas del ENS para racionalizar su cumplimiento, en atención a las características peculiares del sector, atendiendo a los riesgos.

- Pueden incluir las medidas del Anexo II o bien otras no previstas que se recogen en la declaración de aplicabilidad.

- Dichas medidas siempre parten de un análisis de riesgos necesario para la redacción del PCE.

- Las entidades incluidas en el alcance del PCE podrán acogerse a este tras realizar el preceptivo análisis de riesgos, e implementar las medidas recogidas en la declaración de aplicabilidad, adaptadas a sus características peculiares, solicitando la acreditación de conformidad con el ENS respecto al PCE.

- Los PCE son aprobados y publicados por el CCN, lo que permite una actualización común y ágil de los riesgos y medidas a adoptar por las entidades ante nuevas amenazas en materia de seguridad.

Hasta la fecha, el CCN ha aprobado los siguientes PCE, incluidos en las guías CCN-STIC 800:

- 852 PCE Organismos pagadores
- 881 PCE Universidades
- 883 PCE Entidades Locales
- 884 PCE para Azure de Servicios Cloud Corporativo
- 885 PCE para Office 365 Servicio de Cloud Corporativo
- 886 PCE para LORETO NG Base
- 887 PCE para AWS Servicio de Cloud Corporativo
- 888 PCE para Google Servicio de Cloud Corporativo
- 889 PCE para Oracle Cloud Servicio de Cloud Corporativo
- 890 PCE Requisitos Fundamentales de Seguridad

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- 891 PCE Prestaciones Sanitarias a Pacientes (atención primaria y especializada)

- 892 PCE para organizaciones en el ámbito de aplicación de la Directiva NIS2 (PCE NIS2). A fecha de redacción de este artículo, este PCE se había despublicado, pendiente de la aprobación de una versión modificada tras los cambios introducidos por el anteproyecto de transposición.

Volviendo a los PCE, es interesante resaltar que, para cada uno, se realiza un análisis de riesgos, lo que facilita en gran medida la labor de implantación por parte de las entidades incluidas en su ámbito. Esto se debe a que se parte de una selección de medidas adaptadas a las amenazas específicas del ecosistema en cuestión (infraestructura, recursos, tecnología, etc.), lo que puede derivar en la inclusión de medidas propias del ENS o de otras no previstas, desarrolladas en la detallada declaración de aplicabilidad que acompaña a cada PCE. Esta última opción permite, entre otras cosas, adaptar el sistema a nuevas obligaciones derivadas de modificaciones legislativas, tanto a nivel estatal como europeo. A modo de ejemplo, cabe mencionar la legislación relativa a la protección de datos o a la ciberseguridad (como la Directiva NIS2).

Si bien el PCE proporciona una declaración de aplicabilidad, la entidad incluida en su ámbito —o que desee acogerse a uno concreto, motivando así el inicio del camino hacia la adecuación al ENS mediante dicho PCE— deberá, en todo caso, valorar sus propios riesgos y asumir el riesgo residual.

Otro ejemplo que ilustra la capacidad de los PCE para adaptarse a nuevas obligaciones se encuentra en el perfil elaborado para los Organismos Pagadores. Este fue diseñado con el objetivo de que dichas entidades pudieran cumplir no solo con los requisitos establecidos por el ENS, sino también con los exigidos por el legislador europeo[19] en materia de seguridad de los sistemas de información.

19. Reglamento Delegado (UE) 2022/127 de la Comisión de 7 de diciembre de 2021 que completa el Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo con normas relativas a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro (en adelante, Reglamento Delegado (UE) n.º 2022/127), Anexo I, 3 INFORMACIÓN Y COMUNICACIÓN, letra B): "La seguridad de los sistemas de información deberá estar certificada de conformidad con la norma ISO 27001: Information Security management systems – Requirements (ISO) (Sistemas de gestión de la seguridad de la información-Requisitos) (ISO)".

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

3.2. ¿Por qué un PCE para las entidades locales?

Las entidades locales tienen unas características especiales en relación con el resto de las Administraciones territoriales del Estado, tanto desde el punto de vista organizativo como económico o competencial, sin olvidarnos de su gran volumen.

A fecha actual, según los datos publicados por el INE, el número de ayuntamientos alcanza los 8132, a los que deberíamos añadir otras entidades locales como diputaciones, mancomunidades, consorcios y entidades dependientes (fundaciones, empresas municipales). Sin embargo, el número de entidades locales que cuentan con una certificación acreditativa de conformidad con el ENS (con 185 ayuntamientos y un consorcio conforme al PCE, y en certificación tradicional del ENS en torno a 31 ayuntamientos, 3 diputaciones y 1 consorcio, como ya se ha señalado) es significativamente inferior. Es decir, han sido relativamente pocas las que han logrado un nivel de seguridad adecuado a los riesgos que presentan la información y los servicios que proporcionan.

No podemos obviar que las entidades locales, tradicionalmente, vienen reclamando una mayor capacidad de financiación para hacer frente a un ingente volumen de gastos derivados de las competencias propias que les atribuye la legislación básica del Estado, como aquellas otras que, calificadas como impropias, son asumidas sin tener una competencia específica, o las que son delegadas por otras Administraciones.

Además, la población (envejecida) en aquellas provincias con una amplia dispersión territorial se distribuye en ayuntamientos de pequeño tamaño. Según datos del INE, el número de municipios por debajo de los 5000 habitantes supera los 6000.

Esta situación compleja, junto con la competencial, es a la que pretenden dar solución los PCE para entidades locales en el ámbito de la seguridad de la información.

A modo de ejemplo, el análisis realizado por el Tribunal de Cuentas en 2022 en su informe *de fiscalización de la asistencia a municipios por las diputaciones provinciales o entidades equivalentes en materia de administración electrónica y el estado de implantación en los ayuntamientos de municipios de población entre 10 000 y 20 000 habitantes*, en relación con esta competencia de las diputaciones, en el apartado referido al cumplimiento del ENS, señala:

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

> "El 43 % de las entidades que prestaron asistencia, veinte de ellas, lo hicieron en relación con el cumplimiento del ENS. El número total de ayuntamientos que recibieron asistencia ascendió a 2489, el 32 % del total de los de población inferior a 20 000 habitantes del territorio nacional. No desarrollaron asistencia veintiséis entidades, ascendiendo a 3768 el número de ayuntamientos de población inferior a 20 000 habitantes en dichos territorios. [...] El contenido de la asistencia fue heterogéneo y consistió, entre otras cuestiones, en la realización de talleres formativos, servicios de atención a usuarios, apoyo en materia normativa y resolución de dudas. Las especiales características de los ayuntamientos de menor población y sus recursos limitados hacen que la adecuación al ENS y su ulterior certificación constituyan obligaciones de difícil cumplimiento de manera individualizada. Por ello, se hace necesario medidas para su implementación en grupos homogéneos de entidades, así como un Marco de Certificación Específico que contemple un procedimiento de auditoría y certificación que optimice los recursos. No obstante, únicamente el 33 % de las entidades que desarrollaron asistencia en ENS, siete de ellas, habían llevado a cabo actuaciones relacionadas con dicho Marco de Certificación para entidades locales del Centro Criptológico Nacional, al objeto de cubrir transversalmente las necesidades de seguridad de todas las entidades adheridas, mediante la implantación conjunta del ENS en ayuntamientos de características similares de la misma provincia, con el objetivo de alcanzar la Certificación de Conformidad para sus sistemas de información".

3.3. PCE 890

Pasaremos ahora a describir las principales características de los PCE que afectan a las entidades locales.

En primer lugar, abordaremos el PCE de la Guía CCN-STIC 890, que pasará a denominarse de Requisitos Fundamentales de Seguridad, en adelante PCE-RFS.

Este PCE se desarrolla para aquellas entidades que, por la falta de recursos (económicos, organizativos o de personal), tienen serias dificultades para abordar un proceso de certificación ordinario, por lo que, además de analizar los riesgos y describir las medidas aplicadas, es, obviamente, un primer acercamiento a la implementación de una Política de Seguridad vinculada al ENS en categoría básica en los sistemas de información que soportan la tramitación de los servicios prestados en estas entidades.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

El PCE proporciona un catálogo de servicios conforme a lo establecido en el art. 25 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (LBRL), y cuenta con medidas de seguridad básicas y fáciles de asumir, teniendo a su disposición herramientas adaptadas a los requisitos del PCE (herramientas ABS - Análisis Básico de Seguridad), que son proporcionadas por el CCN para apoyar la implementación y obtener así la certificación de conformidad en el ENS, en base a una metodología específica del CCN denominada μCeENS, automatizada en las herramientas de Gobernanza de la Ciberseguridad del CCN.

Es importante destacar la relevancia que adquiere la diputación provincial en la implementación del PCE. Tal como se indica en el art. 36.1.g) de la LBRL, tiene entre sus competencias: "La prestación de los servicios de administración electrónica y la contratación centralizada en los municipios con población inferior a 20 000 habitantes", regulándose en el art. 30 del Texto Refundido de 1986 los distintos tipos de cooperación con los ayuntamientos. En desarrollo de las competencias, especialmente para los ayuntamientos de una población inferior a los 1000 habitantes, con una escasa capacidad de financiación de sus servicios, las diputaciones, con carácter general, han provisto a los municipios de menos de 20 000 habitantes que así lo necesitasen de los medios electrónicos necesarios para abordar los retos de la gestión electrónica de los procedimientos ya con la Ley 11/2007 y, especialmente, con las leyes 39 y 40 de 2015, apoyando con medios técnicos y humanos el despliegue de la administración electrónica.

Pasaremos ahora a abordar de forma sucinta las diferentes fases del proceso, desde un punto de vista práctico, y las medidas de seguridad que se deben implementar, si bien, en primer lugar, se debe señalar que el PCE, a fecha actual, cuenta con dos variantes: una para entidades locales de escasos recursos, y otra para el resto de entidades de la Administración General o las comunidades autónomas de reducido tamaño, recursos limitados y que presten un número limitado de servicios, obviamente no esenciales, o bien como un primer acercamiento al sistema de gestión del ENS.

Modelo de gobernanza simplificado

El tipo de entidades al que se dirige este PCE tiene, como ya se ha comentado, una estructura organizativa de pequeño tamaño y un número reducido de personal. Esto supone que desde el CCN se haya propuesto una adaptación del modelo de gobernanza estándar.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

El modelo de gobernanza propuesto, por bloques de responsabilidad, unifica y simplifica funciones, pero respetando las obligaciones impuestas por la normativa:

1.- Bloque de Gobierno o Responsable de Gobierno, que en un ayuntamiento se corresponderá con la alcaldía o concejalía delegada. Incluye las funciones clásicas de:

- Comité de Seguridad de la Información.
- Responsable de la Información.
- Responsable del Servicio.

¿Qué supone en la práctica? Que la alcaldía o concejalía delegada será la encargada de aprobar los documentos que forman parte del sistema de gestión, comprometerse con la implantación del modelo, y determinar el riesgo de la información que gestiona o de los servicios.

2.- Bloque de Supervisión, que en un ayuntamiento de pequeño tamaño corresponde a la secretaría-intervención:

- Responsable de Supervisión/Vigilancia, cuyo rol ENS será el de responsable de la seguridad.
- Delegado de Protección de Datos, en apoyo al anterior en las materias que le son propias.

¿Qué supone en la práctica? Que realizan las funciones de supervisión (fiscalización) y asesoramiento propias de ambos puestos. Además, el Responsable de Supervisión deberá aprobar la declaración de aplicabilidad, tomando en cuenta las valoraciones realizadas por el Responsable de Gobierno.

3.- Bloque de Operación, que corresponde a un empleado del ayuntamiento, pudiendo ser, en caso de que exista, una persona con conocimientos en informática:

- Responsable de Operación, cuyo rol ENS será el de responsable del sistema.

¿Qué supone en la práctica? Qué realizará las funciones de solventar las pequeñas ineficiencias del sistema y comunicará los fallos que detecte

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

en los equipos bien a la diputación o bien a una entidad privada que gestione los servicios de soporte.

Si bien a *priori* puede causar cierta incertidumbre en relación con la complejidad de las funciones a desarrollar, máxime si observamos las competencias estándar en los diferentes roles del ENS, siempre se debe tener en cuenta que estos ayuntamientos cuentan con la cooperación de la diputación, que suministra los servicios de administración electrónica y asistencia jurídico-técnica, bien prestada de forma directa o indirecta mediante entidades públicas (a modo de ejemplo, CAST en Asturias o ANIMSA en Navarra) o privadas.

Análisis de riesgos y declaración de aplicabilidad

Como se indicó anteriormente, la declaración de aplicabilidad asociada a un PCE de cumplimiento se fundamenta en la realización del preceptivo análisis de riesgos. En el caso particular del PCE-RFS, que, como comentábamos, está dirigido a entidades que disponen de recursos limitados, para la realización de este análisis se han tenido en cuenta las principales situaciones que pueden propiciar que se materialicen diversas amenazas, comprometiendo así la seguridad de los sistemas de información. Entre otras, podemos citar la navegación por sitios inseguros, el uso indebido del correo electrónico, deficiencias en la configuración, inadecuado acceso a los recursos, etc.

En definitiva, el objetivo que persiguen estas medidas es proporcionar un *framework* de seguridad que se constituye como básico para proteger los sistemas de información, propiciando:

- El uso eficiente de los recursos mediante el desarrollo de normas que regulen el uso de los medios electrónicos (correo electrónico, internet, equipos de usuario, dispositivos portátiles, puestos de trabajo despejados, limpieza de metadatos, etc.) que se ponen a disposición de los usuarios y que incluyan la responsabilidad frente a los usos indebidos.

- El control y seguridad en la definición del sistema, estableciendo los requisitos para la adquisición de nuevos componentes y el posterior proceso de autorización para su entrada en el sistema. Disponiendo también la necesidad de su inventariado, la aplicación de una configuración de seguridad, el mantenimiento y el parcheado

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

de seguridad, evitando así los posibles errores y que los sistemas sean vulnerables.

- La trazabilidad de las actuaciones mediante la activación de los registros de actividad, al menos en los servidores.

- La prevención frente accesos no autorizados al sistema y a la información, estableciendo identificadores únicos para entidades, usuarios o procesos; políticas de control de acceso basadas en los principios de "mínimo privilegio", "necesidad de conocer", "responsabilidad de compartir y capacidad de compartir", y la implementación del doble factor de autenticación recomendado para el acceso local y necesario para el acceso remoto.

- La protección frente a la pérdida de datos y el aseguramiento de la continuidad de la actividad mediante el establecimiento de una completa política de copias de seguridad y el desarrollo de los procedimientos de operación del sistema necesarios.

- La concienciación en seguridad y profesionalidad, exigiendo la necesidad de disponer de planes de concienciación y formación que contemplen también la evaluación de la eficacia de las acciones realizadas.

- La reducción del impacto de los incidentes de seguridad, definiendo un proceso integral de gestión de los incidentes, que tenga en cuenta también la normativa de protección de datos y que detalle los organismos y autoridades de control a los que será necesario comunicar.

- La protección de la red interna frente a la red exterior (internet) mediante el despliegue de soluciones de seguridad perimetral, que, en el caso de sitios pequeños donde no exista red, se limitará a la activación del firewall del sistema operativo y a la utilización de VPN[20] cuando la comunicación discurra fuera del propio dominio de seguridad.

- El cumplimiento normativo, estableciendo que, cuando un sistema trate datos personales, se deberá atender a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de

20. Redes privadas virtuales, por sus siglas en inglés: *Virtual Private Networks*.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- La protección de la información cuando se aloja en soportes extraíbles, definiendo las medidas de seguridad a observar para su custodia y transporte, debiendo aplicarse mecanismos de cifrado en caso de que estos soportes alojen copias de seguridad. Para la reutilización de estos dispositivos deberá realizarse un borrado seguro. Medida que será de aplicación también a los discos duros de los equipos.

- La protección del sistema frente al código dañino y otras amenazas, mediante el despliegue de soluciones antivirus, de protección del correo electrónico y de la navegación web por parte de los usuarios.

- La protección de las claves criptográficas durante todo su ciclo de vida (generación, transporte, custodia, retirada y destrucción final) y de la firma electrónica mediante el empleo de cualquiera de los sistemas previstos en el vigente ordenamiento jurídico, entre ellos los sistemas de código seguro de verificación vinculados a la Administración pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre.

- La mejora continua del sistema mediante la definición de un sistema de métricas para recopilar los datos necesarios para conocer el grado de implantación de las medidas de seguridad y para dar respuesta a la encuesta INES (Informe Nacional del Estado de la Seguridad).

Proceso de Adecuación al PCE de Requisitos Fundamentales (PCE-RFS) en base a la metodología µCeENS

La metodología µCeENS desarrollada por el CCN, proporciona a las entidades un instrumento para abordar el proceso de adecuación al PCE-RFS, acompañándolas hasta la obtención de la certificación de conformidad

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

con el ENS conforme a dicho PCE. Este proceso se encuentra automatizado en la plataforma de Gobernanza del CCN, constituyendo un asistente para la adecuación que proporciona:

- Un modelo práctico de gobierno de la seguridad organizado por bloques de responsabilidad, tal y como se mencionó anteriormente. Ofrece los modelos de documentos necesarios para la designación de roles y la elaboración de la Política de Seguridad.

- Una categorización del sistema, básica, que incluye un catálogo de servicios contemplando las competencias de las entidades a las que va dirigido, conforme a lo establecido en el Anexo I del ENS, descargable y preparado para su aprobación.

- Una declaración de aplicabilidad definitiva, que incluye, a modo de ejemplo, una propuesta para la elaboración, en caso necesario, de medidas compensatorias relacionadas con la posible dependencia jerárquica que pueda existir entre el rol de Responsable de Supervisión (responsable de la seguridad) y el Responsable de Operación (responsable del sistema), la utilización de cuentas privilegiadas, sistemas operativos sin soporte de seguridad, política de contraseñas insuficientemente rigurosa o plan de formación-concienciación (si no es de aplicación el propuesto). Documentación descargable y lista para su aprobación.

- Un informe de riesgos y aceptación del riesgo residual disponible para su descarga, generado por el Módulo de Verificación de Perfiles de Cumplimiento en función de los riesgos (MVPCR) disponible en el asistente.

- Un plan de formación-concienciación listo para su descarga, de dos años de duración, con el objetivo de proporcionar los conocimientos necesarios para conseguir la concienciación adecuada, e impulsar el conocimiento de amenazas y vulnerabilidades. Está compuesto por seis módulos (introductorio µCeENS, concienciación en ciberseguridad y ENS, básico de ciberseguridad, seguridad en correo electrónico, navegación segura y seguridad en dispositivos móviles). Cada módulo va dirigido a un perfil concreto. Los módulos se ofrecen a través de la plataforma Ángeles.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- Un repositorio para descargar el marco normativo con modelos de documentación (políticas, normas, procedimientos y otros documentos del sistema) necesarios durante la implantación, tales como:

    - Normativas: de uso de medios electrónicos (incluyendo procedimiento de limpieza de metadatos y acuse de recibo para difundir a los usuarios), de gestión documental, de registros de actividad, de acceso remoto, y el modelo de adhesión a la política de firma electrónica de la Administración General del Estado (AGE).

    - Procedimientos: de gestión del mantenimiento y parcheado, de gestión de usuarios, de copias de seguridad, de requisitos legales, de soportes y registro de entrada y salida, de adquisición de nuevos componentes, de autorizaciones, de gestión de incidentes, y de soportes y dispositivos conectados a la red.

    - Otros documentos: lista de mantenimiento, acciones puntuales y registro de entrada y salida de soportes.

- Un apartado de implantación donde se irán subiendo las evidencias de cumplimiento de las 38 medidas de seguridad que forman parte del PCE-RFS.

Una vez subidas todas las evidencias, se podrá solicitar la auditoría de conformidad con el ENS, conforme al PCE-RFS. La entidad de certificación u Órgano de Auditoría Técnica (OAT), una vez tramitada la solicitud, procederá a iniciar el proceso de auditoría evaluando las evidencias aportadas. En caso de que se requiera aclaración o documentación adicional, estas entidades se pondrán en comunicación a través del foro de la plataforma. Una vez finalizado el proceso de auditoría, estas entidades emitirán de forma automática el correspondiente certificado de conformidad con el ENS o bien, en caso de que el dictamen no sea favorable (no conformidad), solicitarán que se les remita el Plan de Acciones Correctivas (PAC) en un plazo de un mes. Una vez analizado y considerado como correcto, emitirán el certificado de conformidad.

A fecha de redacción de este capítulo, el CCN había anunciado la modificación del PCE para su actualización y mejora, reforzando además las medidas de seguridad conforme a la criticidad de los servicios afectados por la Directiva NIS2.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

3.4. PCE 883

Una vez analizado el PCE-RFS como un primer paso en la implantación del ENS en entidades locales de pequeño tamaño, procederemos a analizar el PCE 883. Al igual que en el PCE anterior, debe tenerse en cuenta que el CCN ha anunciado recientemente su modificación, así como la actualización de sus rangos poblacionales en un proceso de mejora continua.

Este PCE se subdivide según las especialidades de las entidades locales y los riesgos derivados de los servicios e información que gestionan; es decir, cuantas más competencias y habitantes, mayor riesgo, pero también mayor capacidad económica y de personal para implementar las medidas. Por ello, las declaraciones de aplicabilidad correspondientes a los subtipos del PCE 883 son diferentes. Así:

- Tiene en cuenta la escasez de medios de los ayuntamientos con menos de 5000 habitantes, así como sus menores competencias y su organización más sencilla.

- También contempla las peculiaridades de los ayuntamientos con menos de 20 000 habitantes y el apoyo que reciben de las diputaciones provinciales.

- Considera que los ayuntamientos con más de 20 000 habitantes, pese a disponer de más competencias, recursos económicos y estructura organizativa, no siempre tienen la suficiente madurez en el sistema de gestión de seguridad, y requieren las adaptaciones que facilita el PCE.

- Recoge las peculiaridades de diputaciones, comunidades autónomas uniprovinciales, cabildos y consejos insulares respecto a sus sistemas de información.

Si bien, al tratarse de un capítulo, no es posible detallar las peculiaridades de cada subtipo del PCE, se abordan algunos aspectos destacados y la forma de implementación global del PCE.

Modelo de gobernanza

En el PCE no existe un modelo de gobernanza adaptado, como ocurre con los bloques de gobierno del PCE 890, debiéndose acudir al modelo estándar descrito en la Guía CCN-STIC 801.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Es importante destacar que, aunque no forma parte de la organización interna de las entidades, uno de los aspectos que regula el PCE 883 es la aplicación de medidas en función de si existe externalización en la nube. En esos casos, se debe exigir a los prestadores de servicios TIC (incluidos los de la nube, incluso si el contrato es un suministro, tal y como ha declarado la Junta Consultiva de Contratación) que dispongan de un punto de contacto (POC). Esta figura es una de las novedades introducidas por el Real Decreto 311/2022 y tiene importancia crucial en la gestión de la seguridad, ya que es el contacto de la entidad con el prestador del servicio y debe ser quien comunique y gestione los incidentes de seguridad.

El POC, que será el responsable de la seguridad o alguien en quien este delegue, debe ser identificado por el adjudicatario comunicando un medio de contacto. Como recomendación, se debería exigir su designación o comunicación bien en los pliegos del contrato, en la resolución de adjudicación o —cuando sea un prestador con condición de encargado del tratamiento— incluso en el contrato de encargado del tratamiento, al igual que se exige un POC en materia de protección de datos, cargo que será ejercido en ese caso por el delegado de protección de datos de la entidad adjudicataria en el apartado correspondiente a las comunicaciones en dicha materia.

Análisis de riesgos y declaración de aplicabilidad

El PCE sigue el modelo de gobernanza estándar, pero modifica y adecúa la declaración de aplicabilidad según los rangos poblacionales y los servicios prestados por las entidades locales, dependiendo también de si cuentan o no con el apoyo de las diputaciones para la prestación de esos servicios.

En esta declaración de aplicabilidad se recogen las medidas conforme a los riesgos y a las características propias de las entidades locales —según sus peculiaridades como servicios prestados o información tratada—, aunque la adecuación es igual a la estándar. Gracias a esta declaración, no es necesario justificar las medidas de seguridad que no se aplican; siempre será necesario disponer de un análisis de riesgos y asumir el riesgo residual resultante, planificando actuaciones que permitan cumplir con el principio de mejora continua del art. 27 del ENS.

Es interesante, de cara a facilitar la implementación del sistema de gestión del ENS, que el CCN ha facilitado un asistente, al igual que ya se ha comentado en el apartado del PCE de Requisitos Fundamentales de Seguridad.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

El asistente, que sirve como repositorio documental en la generación de evidencias, comunicándose con el auditor, permite la concreción del alcance del sistema, disponiendo de un catálogo de servicios e información ya predefinido al que se podrán incorporar otros nuevos, así como un modelo de política, normativas y diferentes procedimientos. Además, tras la definición de la información y los servicios, se genera la declaración de aplicabilidad provisional que permite a la entidad valorar la adecuación de las medidas, procediendo después al paso a definitiva una vez realizado el correspondiente análisis de riesgos. Es decir, el CCN diseña un asistente que, paso tras paso, permite a la entidad llegar a la conformidad con el ENS, bien en el modelo estándar o bien mediante un PCE específico.

4. Los Gobiernos intermedios como organismos de certificación del ENS

A lo largo del presente capítulo se ha ido reiterando la importancia de que las diputaciones provinciales, cabildos, consejos insulares o comunidades uniprovinciales apoyen proactivamente a los ayuntamientos de menor tamaño para que puedan cumplir con el ENS. Dentro de esas labores de apoyo se encuentra, también, el Marco de Certificación ENS para Entidades Locales, en el cual el CCN propone un modelo de implantación conjunta en ayuntamientos con características tecnológicas y administrativas similares, contando con el soporte de la diputación provincial, cabildo, consejo insular o entidad competente en materia de administración electrónica o informatización de las entidades locales dependientes, adheridas o conveniadas, con el objetivo de alcanzar la certificación de conformidad con el ENS para los sistemas de información municipales, sobre todo los relacionados con Sede Electrónica.

Además, estas entidades pueden desempeñar una interesante función como órgano de auditoría técnica (en adelante OAT). La posibilidad de que las diputaciones actúen como OAT está dentro de las competencias que tienen atribuidas en materia de cooperación para el despliegue seguro de la administración electrónica y el soporte técnico-jurídico a los municipios dentro de su ámbito territorial.

Las entidades locales que, como las diputaciones, tienen competencias en la cooperación y colaboración con otras, pueden constituirse como un órgano de auditoría técnica que les permita realizar auditorías de conformidad con el ENS a las entidades incluidas en su territorio, siempre que cumplan determinados requisitos y puedan acreditarlos. A fecha actual, no existe ninguna entidad local acreditada como OAT; sí lo están algunos or-

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

ganismos públicos, como el CESTIC (Centro de Sistemas y Tecnologías de la Información y las Comunicaciones) o la *Agència de Ciberseguretat de Catalunya*.

Para constituirse como OAT, la entidad debe disponer de un área diferenciada con personal cualificado que incluya un responsable del área, un responsable técnico y un equipo de auditores especializados en ENS (senior, junior), encabezado por un auditor jefe y el comité o persona que aprueba la certificación de conformidad.

El proceso de acreditación como OAT requiere cumplir varios requisitos:

- Que la entidad disponga de roles diferenciados y autónomos que garanticen la debida imparcialidad y ausencia de conflicto de intereses entre el área de auditoría y otras, como las que prestan apoyo a la implantación en los ayuntamientos o los servicios técnicos. Esta independencia debe mantenerse también respecto de los propios auditados.

- Que el área tenga independencia funcional y no reciba instrucciones externas relacionadas con sus funciones.

- La Guía CCN STIC 122, que describe el procedimiento para ser un OAT, establece, entre otros requisitos, la confidencialidad del personal y el cumplimiento de las siguientes condiciones:

    - Competencia profesional: experiencia de al menos 3 años en auditorías o inspecciones de sistemas de información y su seguridad.

    - Competencia técnica del personal del área especializada en auditorías y ENS.

    - Disponer de procedimientos y metodologías que permitan llevar a cabo las auditorías.

La consideración de la entidad como OAT será realizada por el CCN, que además de verificar los requisitos citados, exigirá una parte práctica: los integrantes del OAT deberán asistir a dos auditorías realizadas por el CCN, y el CCN participará en dos auditorías realizadas por el OAT.

El reconocimiento como OAT tendrá una validez de dos años, y deberá ir renovándose por el mismo periodo.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

5. Implicaciones de la Directiva relativa a las medidas para un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS2) en las entidades locales

Para finalizar el capítulo, abordaremos las implicaciones de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS2), en relación con las entidades locales, si bien los términos de este apartado pueden sufrir modificaciones tras la transposición de dicha directiva, que, a fecha de redacción, estaba aún sin completarse.

La Directiva NIS2 afronta los nuevos retos en la ciberseguridad a nivel de la Unión Europea, ampliando el alcance de la anterior directiva y mejorando la coordinación entre los distintos actores implicados. Así, la Directiva NIS2 indica lo siguiente:

> "Los sistemas de redes y de información se han convertido en un aspecto crucial del día a día gracias a la velocidad de la transformación digital y la interconexión de la sociedad, también en los intercambios transfronterizos. Esta evolución ha causado una expansión del panorama de las ciberamenazas, con la consiguiente aparición de nuevos desafíos que requieren respuestas adaptadas, coordinadas e innovadoras en todos los Estados miembros. El número, la magnitud, la sofisticación, la frecuencia y los efectos de los incidentes van en aumento y representan una grave amenaza para el funcionamiento de los sistemas de redes y de información. Como consecuencia de ello, los incidentes pueden interrumpir las actividades económicas en el mercado interior, generar pérdidas financieras, mermar la confianza de los usuarios y ocasionar grandes daños a la economía y la sociedad de la Unión. Por consiguiente, la preparación y la eficacia en materia de ciberseguridad son más esenciales que nunca para que el mercado interior funcione correctamente. Además, la ciberseguridad es un factor facilitador esencial para que muchos sectores críticos se sumen con éxito a la transformación digital y aprovechen plenamente las ventajas económicas, sociales y sostenibles de la digitalización".

La ampliación del alcance de la Directiva NIS2 incluye a las Administraciones públicas territoriales, tanto la Administración General del Estado, las autonómicas y las locales como su sector público, imponiendo nuevas

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

obligaciones. Si bien la Directiva incluye en su alcance a las Administraciones públicas, queda a la transposición de cada país la concreción del tipo de entidades locales a las que se aplica, según se indica en su art. 2.5.

El alcance de la Directiva se determina en función del tamaño de las entidades (gran, mediana o pequeña empresa), y las actividades incluidas en los anexos I y II se consideran esenciales o importantes. En dichos anexos se describen sectores estratégicos como el energético, transporte, investigación o sanitario.

Aunque la aplicación de la Directiva a las entidades locales puede variar según la transposición, en los anexos I y II se incluyen actividades que son competencias municipales según la LBRL, y que pueden considerarse servicios esenciales o importantes. A continuación, se enumeran los sectores incluidos en esos anexos cuyos servicios pueden ser prestados por las entidades locales (ya sea de forma directa o indirecta) mediante diputaciones, ayuntamientos, mancomunidades, consorcios, empresas públicas u otras figuras jurídicas:

ANEXO I

- Agua potable: suministradores y distribuidores de aguas destinadas al consumo humano, según la Directiva (UE) 2020/2184:

  "a) todas aquellas aguas, ya sea en su estado original, ya sea después del tratamiento, utilizadas para beber, cocinar, preparar alimentos y otros usos domésticos, en locales tanto públicos como privados, sea cual fuere su origen e independientemente de que se suministren a través de una red de distribución, de una cisterna o envasadas en botellas u otros recipientes, incluidas las aguas de manantial;

  b) todas las aguas utilizadas en empresas alimentarias para fines de fabricación, tratamiento, conservación o comercialización de productos o sustancias destinados al consumo humano".

- Aguas residuales: empresas dedicadas a la recogida, la eliminación o el tratamiento de aguas residuales urbanas, domésticas o industriales, conforme a la Directiva 91/271/CEE:

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

- o "Aguas residuales urbanas: las aguas residuales domésticas o la mezcla de las mismas con aguas residuales industriales y/o aguas de correntía pluvial".

- o "Aguas residuales domésticas: las aguas residuales procedentes de zonas de vivienda y de servicios y generadas principalmente por el metabolismo humano y las actividades domésticas".

- o "Aguas residuales industriales: todas las aguas residuales vertidas desde locales utilizados para efectuar cualquier actividad comercial o industrial, que no sean aguas residuales domésticas ni aguas de correntía pluvial".

Estos servicios están contemplados en el art. 25.2 c) de la LBRL: "c) Abastecimiento de agua potable a domicilio y evacuación y tratamiento de aguas residuales", sin perjuicio de las competencias de la diputación.

ANEXO II

- Gestión de residuos: según la Directiva 2008/98/CE, se define como "la recogida, el transporte, la valorización y la eliminación de los residuos, incluida la vigilancia de estas operaciones, así como el mantenimiento posterior al cierre de los vertederos, incluidas las actuaciones realizadas en calidad de negociante o agente".

Además, en los anexos se incluyen otras actividades que en ocasiones prestan las entidades locales, como servicios sanitarios o de investigación.

La prestación de estos servicios descritos en los anexos puede realizarse, según el art. 85 de la LBRL, de forma directa o indirecta, por lo que deberá prestarse especial atención tanto al sector público municipal (gestión directa) como a las empresas contratadas para la prestación de dichos servicios (gestión indirecta). Será, por lo tanto, tarea de la entidad local verificar si algunas de las empresas públicas o entidades de su sector público se encuentran en el ámbito de NIS2 para fortalecer sus medidas de seguridad y, si los servicios son prestados por empresas privadas, establecer mecanismos de control de la cadena de proveedores, como veremos más adelante.

Además, las entidades locales pueden estar bajo el alcance de NIS2 cuando hayan sido declaradas como operadores críticos, que son aquellas entidades u organismos responsables de las inversiones o del funcionamiento diario de una instalación, red, sistema o equipo físico o de tecno-

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

logía de la información designada como infraestructura crítica. Pueden incluirse las entidades cuando, según el art. 14 del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, al menos una de las infraestructuras por ellas gestionadas reúna la consideración de infraestructura crítica, existiendo en la ley los parámetros para la consideración como tal.

A fecha de redacción del presente capítulo, aún no se había aprobado la transposición de la Directiva, pero se había publicado un anteproyecto denominado "Ley de Coordinación y Gobernanza de la Ciberseguridad". Entre otras novedades relacionadas con las entidades locales, se puede destacar la inclusión de los ayuntamientos como entidades esenciales o importantes, así como de su sector público institucional.

- Son entidades esenciales la Administración General del Estado, las comunidades autónomas, las provincias, cabildos, islas y los ayuntamientos de gran población, más el sector público institucional de todas ellas.

- Se consideran entidades importantes los ayuntamientos de más de 20 000 habitantes y su sector público institucional.

- El ENS se configura como el *framework* de referencia que sirve, cuando exista certificación, como evidencia de cumplimiento de las obligaciones de esta normativa, pudiendo aprobarse por parte del CCN un PCE específico.

- Se destaca la importancia del Responsable de la Seguridad, que deberá ser interno, pero que contará con un equipo multidisciplinar de apoyo que puede ser interno o externo.

- Se regulan también las acciones de supervisión y las medidas a adoptar por las autoridades de control de los diferentes sectores.

- Se detalla el régimen de infracciones, así como la responsabilidad de los órganos de gobierno en caso de incumplimientos, quedando exoneradas las Administraciones públicas de la imposición de sanciones consistentes en una multa económica.

Como se ha explicado, la aplicación de NIS2 supone que las entidades bajo su alcance deban establecer medidas de seguridad reforzadas. La dirección adquiere nuevas responsabilidades en el cumplimiento de la seguridad, y el Responsable de la Seguridad en NIS2 adquiere un peso más

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

relevante dentro de la organización. También es preciso un control exhaustivo de la cadena de prestadores y los suministros, así como una adecuada gestión de los incidentes de seguridad.

En relación con las medidas de seguridad en NIS2, el CCN había aprobado un PCE —la Guía CCN-STIC 892— para organizaciones en el ámbito de aplicación de la Directiva NIS2 (PCE NIS2), que podrá ser objeto de adaptación una vez que se haya transpuesto dicha norma, si bien, a fecha actual, este perfil se ha despublicado para su actualización.

Todo apunta a que la nueva regulación que aprobará el CCN desarrollará, para España, el reglamento de ejecución de NIS2 relacionado con los sectores TIC[21], en el que se abordarán las medidas de seguridad aplicables a determinadas entidades y las especialidades en la comunicación de ciberincidentes.

Con carácter general, en una entidad local que no se encuentra en el ámbito de los PCE 890 u 883 antes señalados, las medidas de seguridad, tras el análisis de riesgos correspondiente, tienden a las correspondientes a la categoría media del ENS, por lo que aquellas entidades locales ya certificadas en el ENS que entren dentro del ámbito de aplicación de NIS2 (tanto del sector público como privadas) tendrán gran parte del camino ya recorrido de cara a la adaptación desde el punto de vista de la seguridad, sin perjuicio de cumplir con otras obligaciones, como el registro de la entidad como esencial o la comunicación de incidentes en ciberseguridad, que se analizarán, someramente, al final del capítulo.

Cuestión relevante en la Directiva NIS2 es, sin duda, el control de la cadena de prestadores/proveedores de las entidades en el ámbito de aplicación de la Directiva, algo que también ya recogía el ENS en la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, estando ahora recogido en el art. 2.3 del ENS, y existiendo también una alineación entre los requisitos exigidos por ambas normas en relación

21. El Reglamento de Ejecución (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024, por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555, regula las condiciones específicas en relación —entre otras— con las medidas de seguridad para los sectores tecnológicos de la Directiva, en concreto: los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en la nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, los motores de búsqueda en línea, las plataformas de servicios de redes sociales, y los proveedores de servicios de confianza.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

con la necesidad de controlar a las empresas proveedoras de servicios o suministros tecnológicos y a la cadena de subcontratistas.

La Directiva NIS2 aborda el control de los proveedores en su considerando 85:

> "Hacer frente a los riesgos de ciberseguridad provenientes de la cadena de suministro de una entidad y su relación con sus proveedores, como los proveedores de servicios de almacenamiento y tratamiento de datos o los proveedores de servicios de seguridad gestionados y editores de *software*, resulta especialmente importante habida cuenta de la prevalencia de incidentes en los que las entidades han sido víctimas de ciberataques y en que agentes malintencionados han podido comprometer la seguridad de los sistemas de redes y de información de una entidad aprovechándose de las vulnerabilidades que afectan a productos y servicios de terceros. Por ello, las entidades esenciales e importantes deben evaluar y tener en cuenta la calidad general y la resiliencia de los productos y los servicios, las medidas para la gestión de riesgos de ciberseguridad integradas en ellos y las prácticas en materia de ciberseguridad de sus proveedores y prestadores de servicios, incluidos sus procedimientos de desarrollo seguro. En particular, debe fomentarse que las entidades esenciales e importantes incorporen medidas para la gestión de riesgos de ciberseguridad en los acuerdos contractuales con sus proveedores y prestadores de servicios directos. Dichas entidades podrían tomar en consideración los riesgos provenientes de otros niveles de proveedores y prestadores de servicios".

Y en el art. 21.2, apdos. c) y d), cuando se detallan las medidas se seguridad: "d) la seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores o prestadores de servicios directos; e) la seguridad en la adquisición, el desarrollo y el mantenimiento de sistemas de redes y de información, incluida la gestión y divulgación de las vulnerabilidades". Incorporando el anteproyecto la obligación de los prestadores de servicios de comunicar el POC antes referido.

Estas obligaciones de control de la cadena de suministro que, desde un punto de vista jurídico, deben concretarse en los pliegos de condiciones técnicas y administrativas o, en contratos de menor cuantía (negociados, menores), en el contrato de encargado del tratamiento[22] o en la resolución

22. El contrato de encargado del tratamiento es un acto jurídico que vincula a las partes, como se indica en el art. 28 del RGPD, y en su contenido se pueden indicar las medidas técnicas y organizativas en el tratamiento de los datos personales.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

de adjudicación, podrán corresponderse con las siguientes medidas del Anexo II:

- [op.ext.3] Protección de la cadena de suministro (en categoría alta, como hemos señalado).
- [op.ext.1] Contratación y acuerdos de nivel de servicio.
- [op.ext.2] Gestión diaria.
- [op.ext.4] Interconexión de sistemas.
- Art. 19. Adquisición de productos de seguridad y contratación de servicios de seguridad. [op.pl.3] Adquisición de nuevos componentes.
- [op.pl.5] Componentes certificados.
- [mp.sw.1] Desarrollo de aplicaciones.
- [mp.sw.2] Aceptación y puesta en servicio.
- [op.exp.4] Mantenimiento y actualizaciones de seguridad.
- [op.mon.3] Vigilancia.

Otro de los puntos importantes que las entidades en el alcance de NIS2 deben abordar es la revisión de los procedimientos para la gestión de los incidentes en ciberseguridad. Si bien hasta la fecha las entidades locales ya deben disponer de un procedimiento para gestionar los incidentes de seguridad, que tendrá en cuenta los criterios de la Guía CCN-STIC 817, y de un procedimiento —integrado o no con el anterior— para la gestión de las violaciones de seguridad o brechas de datos personales, conforme a los arts. 33 y 34 del RGPD, sin perjuicio de otros a los que estén obligadas, como los relacionados con la posible consideración como infraestructura crítica, ahora deberán también canalizar los incidentes de ciberseguridad, detallándose en el anteproyecto que, para las entidades públicas, se deberán comunicar al CCN como organismo de control, como hasta la fecha, si bien se propone la creación de un organismo nuevo para coordinar las diferentes acciones y entidades que controlan los diferentes sectores.

El procedimiento de gestión de incidentes de ciberseguridad en NIS2, que para los sectores tecnológicos se detalla en el Reglamento de Ejecu-

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

ción[23], presenta similitudes en cuanto a plazos con el procedimiento de brechas de datos personales de los arts. 33 y 34 del RGPD, desarrollado en la *Guía para la notificación de violaciones de seguridad* de la Agencia Española de Protección de Datos. En NIS2, las notificaciones a la autoridad de control (pendiente de concretar en España en la transposición definitiva de la Directiva) deberán realizarse de forma paulatina, tal como recoge el considerando 101 de la Directiva:

> "La presente Directiva establece un enfoque en varias etapas respecto a la notificación de incidentes significativos a fin de alcanzar el equilibrio adecuado entre, por un lado, una notificación ágil que ayude a reducir la posible propagación de incidentes significativos y permita a las entidades esenciales e importantes buscar asistencia, y, por el otro, una notificación minuciosa que extraiga lecciones valiosas de cada incidente y mejore con el tiempo la ciberresiliencia de las entidades individualmente y de sectores completos. En este sentido, la presente Directiva debe incluir la notificación de incidentes que, según una evaluación inicial realizada por la entidad afectada podrían provocar perturbaciones operativas o perjuicios económicos graves para dicha entidad o podrían afectar a otras personas físicas o jurídicas causándoles perjuicios materiales o inmateriales considerables. Tal evaluación inicial debe tener en cuenta, entre otros aspectos, los sistemas de redes y de información afectados, y en particular su importancia para la prestación de los servicios de la entidad, la gravedad y las características técnicas de la ciberamenaza, así como las vulnerabilidades subyacentes que se estén aprovechando y la experiencia de la entidad con incidentes similares. Indicadores como la medida en que se ve afectado el funcionamiento del servicio, la duración de un incidente o el número de destinatarios de los servicios afectados podrían ser importantes a la hora de determinar si la perturbación operativa del servicio es grave".

23. Reglamento de Ejecución (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024, por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y en el que se detallan los casos en que un incidente se considera significativo con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, motores de búsqueda en línea y plataformas de servicios de redes sociales, y los proveedores de servicios de confianza ("DOUE" núm. 2690, de 18 de octubre de 2024).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

Las etapas para la comunicación del incidente significativo son las siguientes:

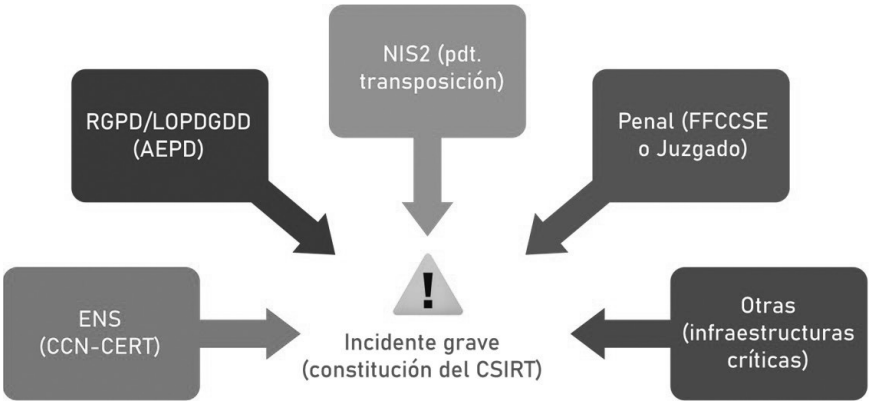
- Alerta temprana, en el plazo de 24 horas: se trata de una primera comunicación con los datos básicos del incidente —tipología, alcance dentro de la organización, si se produce por una actuación ilícita y si tiene implicaciones transfronterizas—.

- Dentro de las 72 horas desde que se conoce el incidente: se incluirá la información disponible y, cuando sea preciso, la actualización de los datos de la alerta temprana. Además, se realizará una evaluación inicial de la gravedad e impacto en la organización y, en caso de que ya sean conocidos, los indicadores de compromiso.

- El CSIRT al que se comunique el incidente podrá solicitar información adicional, debiendo la entidad emitir un informe sobre los puntos requeridos.

- Comunicación completa, en el plazo de 30 días desde la alerta: tras realizar el correspondiente informe forense, se detallará el vector de ataque, la causa raíz, el impacto y las medidas adoptadas para la mitigación y contención.

El modelo de gestión de incidentes debe tener en cuenta las distintas normas que puedan afectarle, debiendo coordinarse entre todos los actores implicados para su correcta gestión. A modo de ejemplo, en el siguiente gráfico se muestran las diferentes normativas aplicadas junto con la autoridad que las gestiona.



Fuente: elaboración propia

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6

6. Bibliografía

Guías y buenas prácticas CCN

CCN. Mar. 2024. Guía CCN-STIC IC-01/19 ENS sobre Criterios Generales de Auditoría y Certificación. (Categoría: Serie 100 Procedimientos).

CCN. Mar. 2019. Guía CCN-STIC 801 Responsabilidades y Funciones en el ENS. (Categoría: Serie 800 ENS).

CCN. May. 2020. Guía CCN-STIC 803 sobre la Valoración de los Sistemas. (Categoría: Serie 800 ENS).

CCN. Abr. 2024. Guía CCN-STIC-892 Perfil de Cumplimiento Específico para Organizaciones en el Ámbito de Aplicación de la Directiva NIS2 (PCE-NIS2). (Categoría: Serie 800 ENS).

CCN. Oct. 2018. Guía CCN-STIC 819 Medidas Compensatorias. (Categoría: Serie 800 ENS).

CCN. Oct. 2023. Guía CCN-STIC-808 Verificación del Cumplimiento de las Medidas en el ENS. (Categoría: Serie 800 ENS).

CCN. Feb. 2023. Informe de Buenas Prácticas CCN-CERT_BP_14 Declaración de Aplicabilidad ENS. (Categoría: Serie 800 ENS).

CCN. May. 2023. Guía CCN-STIC-852 Perfil de Cumplimiento Específico Organismos Pagadores. (Categoría: Serie 800 ENS).

CCN. May. 2022. Guía CCN-STIC-881A Perfil de Cumplimiento Específico Universidades. (Categoría: Serie 800 ENS).

CCN. May. 2020. Guía CCN-STIC-883 Guía de Implantación del ENS para Entidades Locales y Anexos. (Categoría: Serie 800 ENS).

CCN. Abr. 2020. Guía CCN-STIC-817 Gestión de Ciberincidentes. (Categoría: Serie 800 ENS).

CCN. Mar. 2023. Guía CCN-STIC-890A Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad - Entidades Locales. (Categoría: Serie 800 ENS).

CCN. Mar. 2023. Guía CCN-STIC-890C Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad. (Categoría: Serie 800 ENS).

CCN. Sep. 2023. Guía CCN-STIC-122 Procedimiento de Reconocimiento de Entidades de Certificación del ENS del Sector Público y Requisitos del Órgano de Auditoría Técnica. (Categoría: Serie 100 Procedimientos).

CCN. Abstract. Marco de Certificación ENS para Entidades Locales. (Categoría: Serie 800 ENS).

Otros documentos y normativa relacionada

AEPD. Jun. 2021. Guía para la Notificación de Brechas de Datos Personales.

Anteproyecto Ley de Coordinación y Gobernanza de la Ciberseguridad.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 48
ISBN: 978-84-128852-8-6