Marco de Certificación ENS para Entidades Locales

Abstract: *las especiales características que enmarcan la actuación administrativa de las Entidades Locales más pequeñas y los limitados recursos de los que suelen disponer, hacen que, frecuentemente, la adecuación al Esquema Nacional del Seguridad (ENS) y su ulterior Certificación constituyan obligaciones de difícil cumplimiento de manera individualizada. Por este motivo, parece necesario desarrollar acciones concretas, que contemplen mecanismos de adecuación e implantación multi-organismo, dirigidas a grupos homogéneos de dichas entidades, así como un Marco de Certificación Específico que contemple un procedimiento de auditoría y certificación que optimice los antedichos recursos.*

Contenido:

1. OBJETO

El objeto del presente documento es posibilitar el cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS), señalando unos criterios generales para la creación de un Marco de Certificación Específico con el ENS (MCE-ENS) para un conjunto determinado de entidades locales.

El modelo persigue la implantación conjunta del ENS en ayuntamientos de la misma provincia, de 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 sus entidades locales dependientes, adheridas o conveniadas, con el objetivo de alcanzar la Certificación de Conformidad con el ENS para los sistemas de información de tales ayuntamientos que, en principio, soporten los servicios municipales que se ofrezcan a través de Sede Electrónica.

Si bien, para el caso de sistemas de información de categoría BÁSICA, de conformidad con la normativa vigente, resulta suficiente una autoevaluación satisfactoria para exhibir la Declaración de Conformidad, no siendo necesario el concurso de una Entidad de Certificación, el objetivo de la presente iniciativa es conseguir que muchas entidades locales, de recursos reducidos, puedan exhibir una Certificación de Conformidad con el ENS, aprovechando los medios dispuestos por la Diputación Provincial, Cabildo, Consejo

Insular o entidad competente en materia de administración electrónica o informatización de sus entidades locales dependientes, adheridas o conveniadas.

2. CRITERIOS GENERALES

La materialización de la presente iniciativa busca, en primera instancia, que tanto el Plan de Adecuación al ENS como las Políticas de Seguridad, Normativas de Seguridad y Procedimientos de Seguridad de las entidades adheridas al MCE-ENS se aborden de manera conjunta y unificada, cubriendo transversalmente las necesidades de seguridad de todas las entidades locales concernidas por el citado Marco.

2.1 PLAN DE ADECUACIÓN CONJUNTO

El MCE-ENS contemplará la redacción y aprobación conjunta del Plan de Adecuación al ENS y sus componentes: Categorización de los sistemas de información, Análisis de Riesgos, Declaración de Aplicabilidad y Plan de Adecuación con objetivos y plazos, así como los documentos necesarios para la constitución del Comité de Seguridad y las figuras que se describan en él, recogiendo y dando respuesta a las necesidades de seguridad y adecuación al ENS de todos los ayuntamientos adheridos.

Los ayuntamientos susceptibles de adherirse al citado MCE-ENS deberán poseer unas características administrativas y técnicas similares que permitan la realización conjunta de una Valoración de Activos y Análisis de Riesgos que abarque las necesidades de todos ellos, así como una la adecuada estructura funcional que posibilite la asunción de las responsabilidades derivadas, bajo la dirección del Comité de Seguridad Conjunto que se constituya a tales efectos.

Una guía CCN-STIC determinará las características técnicas y los requisitos mínimos de seguridad para que los ayuntamientos que pueden adherirse al MCE-ENS y cuya adscripción se analizará y determinará caso por caso.

2.2 MARCO NORMATIVO CONJUNTO

Los ayuntamientos finalmente adheridos al MCE-ENS podrán disponer de una Política de Seguridad común elaborada por la entidad administrativa, vinculada o dependiente con competencias en la materia, que asuma la responsabilidad de la seguridad de la información de los sistemas municipales afectados por el MCE-ENS.

A tales efectos, se constituirá un Comité de Seguridad conjunto, compuesto por miembros de las antedichas entidades y de los ayuntamientos concernidos, y entre cuyas funciones principales estarán la dirección y seguimiento de las actividades de implantación de la seguridad contempladas en el MCE-ENS, la responsabilidad de su correcta ejecución y la elaboración, aprobación y mantenimiento del Marco Normativo conjunto: Plan de Adecuación conjunto, Política de Seguridad conjunta, Normativa de Seguridad conjunta y Procedimientos de Seguridad conjuntos, contando siempre con la aprobación de los responsables de los ayuntamientos concernidos, cuando ello sea preceptivo.

2.3 IMPLEMENTACIÓN DE LAS MEDIDAS TÉCNICAS DE SEGURIDAD

Una vez aprobado el Marco Normativo conjunto, se procederá a implantar los controles contemplados en el Marco Operacional y las Medidas de Protección determinados por el ENS, según se haya definido y así se desprenda de los documentos comprendidos en el citado Marco Normativo, en relación con la Declaración de Aplicabilidad correspondiente.

Para facilitar el proceso de implantación, se potenciará que los ayuntamientos adheridos utilicen los servicios y medios técnicos proporcionados por la Diputación Provincial, Cabildo, Consejo Insular o la entidad competente en materia de administración electrónica o informatización municipal de forma que gran parte de la implementación de estas medidas técnicas sea asumida por tal entidad en su condición de Entidad Proveedora de Servicios, para lo que los sistemas de información utilizados deberán estar en posesión de la correspondiente Certificación de Conformidad con el ENS.

2.4 PERFIL DE CUMPLIMIENTO ESPECÍFICO PARA ENTIDADES LOCALES

El Centro Criptológico Nacional publicará un Perfil de Cumplimiento Específico para Entidades Locales que permita la implantación del ENS en las mismas y donde, tras un estudio de las necesidades de seguridad y los recursos de los que disponen, un Análisis de Riesgos valide este perfil de cumplimiento para cada una de las entidades que se acojan al mismo.

Con el Perfil de Cumplimiento Específico, se podrá establecer un conjunto de medidas y el nivel o categoría de seguridad con el que se debe aplicar, de forma que se garantice que las medidas de seguridad implementadas sean las necesarias y proporcionadas en relación con el nivel de riesgo y los recursos disponibles.

3. PROCESO DE VERIFICACIÓN DE LA CONFORMIDAD

En primer lugar, será necesario habilitar a la Diputación Provincial, Cabildo, Consejo Insular o entidad competente en materia de administración electrónica o informatización de sus entidades locales dependientes, adheridas o conveniadas, como Entidad de Certificación del ENS y que el Centro Criptológico Nacional reconozca y acredite tal habilitación, de conformidad con lo señalado en la cláusula VI de la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, y preservando todas las garantías de capacidad técnica, imparcialidad y ausencia de conflicto de intereses.

El proceso de verificación de Conformidad con el ENS de los ayuntamientos adheridos se realizará en las fases descritas seguidamente.

3.1 FASE 1. AUDITORÍAS DE CERTIFICACIÓN DE CONFORMIDAD

Las Auditorías de Certificación de esta primera fase deberán ser realizadas por una Entidad de Certificación acreditada por la Entidad Nacional de Acreditación (ENAC). Para ello:

Se auditará una muestra representativa de los ayuntamientos adheridos al MCE-ENS, que se calculará en función del número de ayuntamientos adheridos atendiendo a los habituales procedimientos estadísticos usados para el cálculo de muestras representativas, con un Nivel de Confianza en torno al 80% y un Margen de Error en torno al 15%.

Dicho cálculo final se realizaría utilizando la ecuación ($y = \sqrt{x}$), donde "y" será el tamaño de la muestra (redondeado al entero superior) y "x" el total número de emplazamientos. Por ejemplo, si el número de ayuntamientos adheridos al MCE-ENS fuera de 300, el número de ayuntamientos que será necesario auditar sería de 18.

Ante la existencia de un Marco Normativo conjunto, un único análisis de esta documentación conjunta se considerará suficiente para establecer el grado de cumplimiento normativo en todos los ayuntamientos adheridos.

La Entidad de Certificación revisará individualmente, en cada uno de los ayuntamientos de la muestra representativa, las medidas técnicas de seguridad implementadas. Se podrá realizar también cualquier revisión documental que se estime oportuna para completar o validar la revisión conjunta señalada anteriormente.

Tras un informe de auditoría favorable, la Entidad de Certificación expedirá la correspondiente Certificación de Conformidad con el ENS a los sistemas de información de las entidades locales correspondientes.

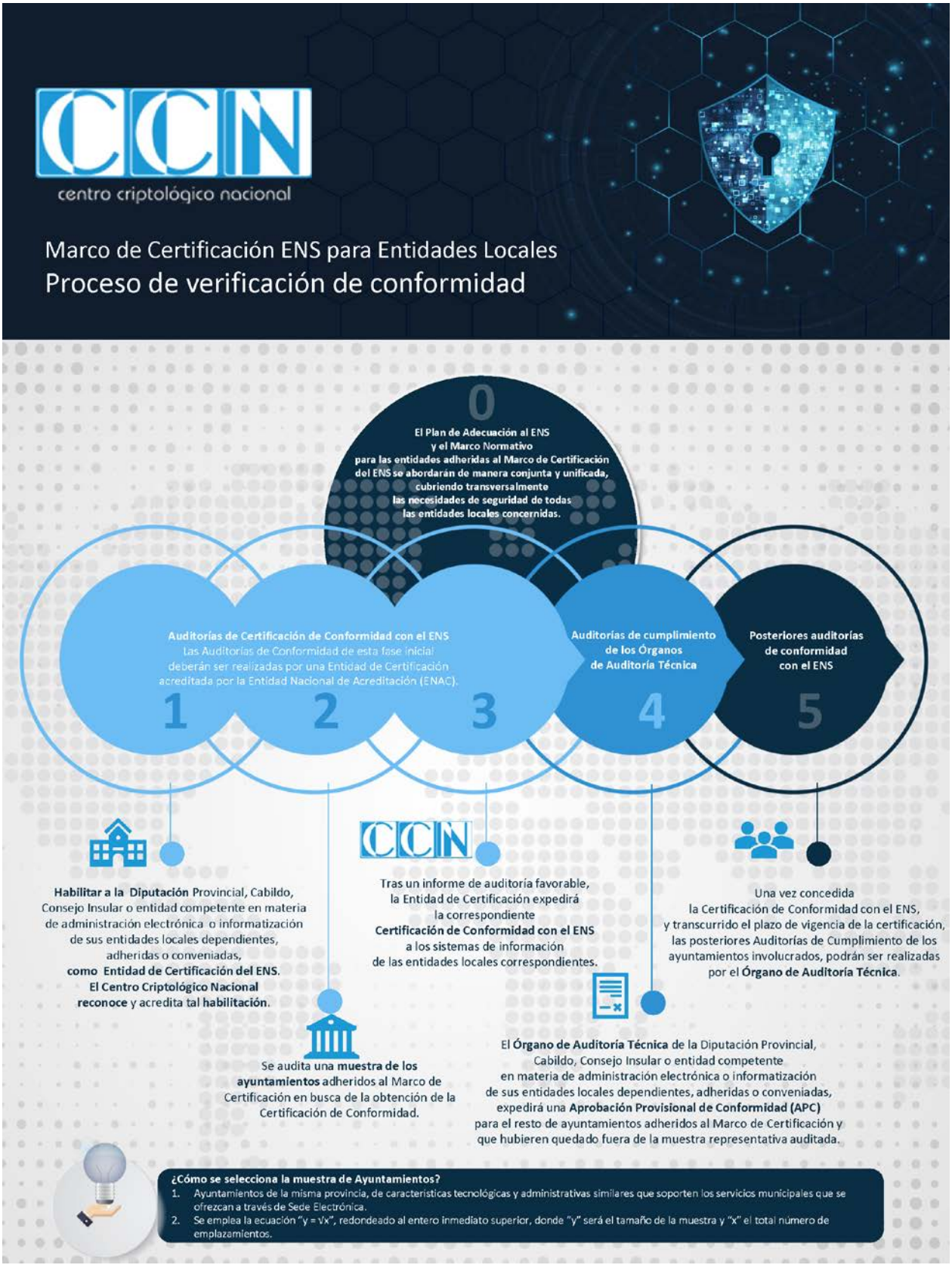
3.2 FASE 2. AUDITORÍAS DE CUMPLIMIENTO DE LOS ÓRGANOS DE AUDITORÍA TÉCNICA.

Una vez finalizada la primera fase, el Órgano de Auditoría Técnica de la Diputación Provincial, Cabildo, Consejo Insular o entidad competente en materia de administración electrónica o informatización de sus entidades locales dependientes, adheridas o conveniadas, expedirá una Aprobación Provisional de Conformidad (APC) para el resto de ayuntamientos adheridos al Marco de Certificación y que hubieren quedado fuera de la muestra representativa auditada.

Tras la emisión de la APC, dicho Órgano de Auditoría Técnica dispondrá de un período de dos (2) años para auditar a estas entidades y, en su caso, completar el proceso de certificación de las mismas y emitir el Certificado de Conformidad en el ENS.

3.3 FASE 3. POSTERIORES AUDITORÍAS DE CONFORMIDAD ENS

Una vez concedida la Certificación de Conformidad con el ENS y transcurrido el plazo de vigencia de la certificación, las posteriores Auditorías de Certificación de los ayuntamientos involucrados podrán ser realizadas por el Órgano de Auditoría Técnica de la Diputación Provincial, Cabildo, Consejo Insular u órgano competente, de forma similar al procedimiento para la certificación inicial.



centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.05.13 00:08:00 +02'00'