GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
centro criptológico nacional

Guía de Seguridad CCN-STIC
CCN-CERT IC-02/20

Guía para la contratación de auditorías de certificación del Esquema Nacional de Seguridad (ENS)

Agosto 2020

MINISTERIO DE DEFENSA

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.08.29 03:56:31 +02'00'

Fecha de Edición: agosto de 2020

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. OBJETO

1. El objeto del presente documento es desarrollar unas recomendaciones básicas para ayudar a las entidades del ámbito de aplicación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS), y, muy especialmente, a las entidades públicas más pequeñas o con menos recursos, a acometer las actividades necesarias para la contratación de las Auditorías de Certificación del ENS.

2. LAS AUDITORÍAS DE CERTIFICACIÓN DEL ENS Y LAS EVIDENCIAS DE CONFORMIDAD

2. Como prescribe el art. 34 y el Anexo III del ENS, y desarrolla la Resolución, de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información (*ITS de Auditoría de la Seguridad*), los sistemas de información deberán ser objeto de una auditoría regular ordinaria, al menos cada dos (2) años, que verifique el cumplimiento de los requerimientos del ENS.

   Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas.

3. Por su parte, el art. 41 del ENS señala la obligatoriedad de publicitar en las sedes electrónicas (o equivalentes) de las entidades afectadas los distintivos y certificaciones de conformidad con el ENS, prescripción que se desarrolla en 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 (*ITS de Conformidad con el ENS*).

3. LA CERTIFICACIÓN DE CONFORMIDAD CON EL ENS

4. Trayendo causa de lo dispuesto en el art. 29.2 del ENS, la precitada *ITS de Conformidad con el ENS* señala que los sistemas de información de las entidades del ámbito de aplicación del ENS precisarán de una auditoría formal para su certificación de la conformidad, de carácter obligatorio para los sistemas de información de categoría MEDIA o ALTA y voluntaria para los de categoría BÁSICA.

5. La Certificación de la Conformidad con el ENS de los sistemas de información de su ámbito de aplicación se realizará mediante un procedimiento de auditoría

formal que, con carácter ordinario y obligatorio, verifique el cumplimiento de los requerimientos contemplados en el Esquema, al menos cada dos (2) años. Dicha auditoría se realizará según lo dispuesto en el artículo 34 y el Anexo III del ENS.

6. La Certificación de Conformidad con el ENS, tal y como está regulada en la antedicha ITS de Conformidad con el ENS, solo podrá ser expedida por una Entidad Certificadora, acreditada por la Entidad Nacional de Acreditación (ENAC), de las que se encuentran referenciadas en la página web del CCN-CERT y se completará mediante un Distintivo de Conformidad cuyo uso estará condicionado a la antedicha Certificación de Conformidad.

7. La evidencia pública de la conformidad con el ENS se realizará mediante la publicación en la sede electrónica de la entidad pública titular o usuaria del sistema de información en cuestión, del Distintivo de Certificación de Conformidad que incluirá un enlace al documento de Certificación de Conformidad correspondiente, que también permanecerá accesible a través de dicha sede electrónica

> **Nota importante:**
>
> *Solo aquellas Certificaciones de Conformidad con el ENS que se expidan cumpliendo los requisitos 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, podrán considerarse válidas y jurídicamente eficaces a efectos de exhibir la conformidad con el ENS.*

4. ENTIDADES DE CERTIFICACIÓN DEL ENS

8. La relación actualizada de Entidades de Certificación del ENS acreditadas se encuentra disponible en la dirección:

   https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/entidades-de-certificacion

5. EL PROCEDIMIENTO DE CONTRATACIÓN

9. La entidad que, de forma voluntaria para sistemas de categoría BAJA y obligatoria para sistemas de categoría MEDIA Y ALTA, vaya a someter sus sistemas de información a una Auditoría de Certificación del ENS, deberá desarrollar las actividades que se señalan seguidamente.

5.1 Actividades previas

10. Determinar con precisión el alcance de la Auditoría de Certificación, identificando el(los) sistema(s) de información afectado(s) y los servicios prestados a través de tales sistemas.

11. Hay que recordar que el ENS persigue, de forma originaria, la seguridad de los sistemas de información (garantizando, de forma derivada, los servicios soportados por tales sistemas de información).

12. Así pues, como una Certificación de Conformidad con el ENS tiene unos destinatarios últimos claros (los ciudadanos que confían en dicha Certificación como exhibición de la seguridad del sistema de información referenciado), es por lo que en el diseño de la Certificación de Conformidad deben mencionarse también los servicios comprendidos en la Certificación, sustentados en tal sistema de información (servicios declarados) y que se benefician de la seguridad del sistema de información sobre el que se apoyan.

13. A partir de estas premisas, la entidad de que se trate debería identificar aquellos sistemas de información que deben o desean adecuar al ENS, y esto, habitualmente, se hace considerando los servicios sustentados en tales sistemas; distinguiendo los "servicios finalistas" (aquellos destinados directamente a satisfacer una necesidad de los ciudadanos o una competencia estatutaria de la institución), de "servicios instrumentales" (aquellos destinados a satisfacer una necesidad de la propia institución).

14. Obviamente, puestos a señalar prioridades, suele ser más prioritario garantizar la seguridad de los sistemas de información que sustentan los primeros, pero sin olvidar que, en algún momento, habrá que acometer igualmente los segundos, especialmente cuando esos servicios se desarrollan conforme al derecho público (la contratación, por ejemplo).

15. Finalmente, en un mismo sistema de información pueden existir elementos (hardware o software) que no participen en la prestación de ninguno de los servicios declarados en la Certificación de Conformidad y no presten servicio a los elementos que componen dichos servicios declarados.

    En este caso, si no se desea someterlos a auditoría, será necesario asegurar que un incidente de seguridad que se originara en alguno de tales elementos no puede trasladarse a aquellos otros que sí participan en la prestación de los servicios declarados, aseguramiento que exige adoptar las medidas oportunas, como, por ejemplo, una segregación física o lógica de aquellos elementos (por ejemplo, la

inclusión de los distintos elementos en redes diferenciadas, segregadas y protegidas), estableciendo filtros por usuario-aplicación, etc.

5.2 Redacción de Pliegos

16. En su caso, redactar los Pliegos de Prescripciones Técnicas y Administrativas correspondientes, de conformidad con la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público y sus normas de desarrollo.
17. Una Auditoría de Conformidad con el ENS se corresponde con un contrato de servicios, de los regulados en el art. 17 de la precitada Ley 9/2017, siendo habitual su instrumentación a través de una adjudicación directa ("contrato menor"), un procedimiento abierto o un procedimiento negociado.
18. La entidad contratante deberá tener en cuenta que los costes de una Auditoría de Certificación son directamente proporcionales al número de jornadas de auditor necesarias.
19. El coste por jornada/auditor es de libre elección por parte de las Entidades de Certificación para cada anualidad. Debe tenerse en cuenta que, aplicando el principio de condiciones no discriminatorias, **una entidad de certificación no puede alterar arbitrariamente las tarifas establecidas a principio de año**, durante el transcurso de éste, para ajustarlas a determinado pliego en concreto.

    Tampoco puede variar arbitrariamente el número de jornadas de auditoría, calculando éstas en función de determinados parámetros que se obtienen de las características y situación del cliente a ser auditado.
20. La Guía de Seguridad CCN-STIC CCN-CERT IC-01/19 *ENS: Criterios Generales de Auditoría y Certificación,* señala unos **tiempos mínimos** para el desarrollo de tales Auditorías, que se reproducen seguidamente:

Fase de estudio documental previo	Mínimo, entre 0,5 y 1 jornada.
Fase de auditoría modo remoto/in situ	· Categoría BÁSICA: mínimo, 1 jornada. · Categoría MEDIA: mínimo, 2 jornadas. · Categoría ALTA: mínimo, 3 jornadas.
Fase de redacción de informes	Cualquier Categoría: mínimo, 1 jornada que comprenderá la redacción del Informe de Auditoría completo y adecuadamente evidenciado (señalando cada medida auditada); en su caso, evaluación del Plan de Acciones Correctivas (PAC), revisión y decisión del Comité de Certificación.

21. Conviene que la **entidad contratante examine con detenimiento** cualquier oferta cuyos **tiempos de auditoría sean inferiores a los señalados en el cuadro anterior**, requiriendo del licitador la correspondiente justificación.
22. Se hace hincapié en que se tratan de tiempos mínimos que podrían incrementarse en función de determinados parámetros, como son el número de sedes a auditar, el número de CPD, etc.
23. Como se ha indicado, es necesario señalar con claridad en los antedichos Pliegos el alcance de la Auditoría de Conformidad, sabiendo que tal alcance será el que aparezca en la Certificación de Conformidad con el ENS, en caso de resultar satisfactoria la Auditoría de Certificación.
24. Para la enunciación del alcance se recomienda utilizar una expresión del tipo:

> ***"Los sistemas de información utilizados para prestar los servicios de _____".***

25. Sin olvidar incluir la categoría del (de los) sistema(s) de información objeto de la Auditoría de Conformidad.
26. Debe tenerse en cuenta que las entidades de certificación acreditadas pueden ayudar a determinar la conveniencia, o no, del alcance elegido para la certificación y asesorar, respecto a que éste sea certificable y cumpla con los requisitos exigidos en el apartado 3.1 EN RELACIÓN CON EL ALCANCE DE AUDITORÍA de la Guía de Seguridad CCN-STIC CCN-CERT IC-01/19 *ENS: Criterios Generales de Auditoría y Certificación*.

5.3 Evaluación de las Propuestas/Ofertas

27. Una vez recibida(s) la(s) propuesta(s) del (de los) oferente(s), la entidad deberá verificar:
    - Que el oferente (licitador) se corresponde con una de las Entidades de Certificación del ENS acreditadas, relacionadas en la página web del CCN.
    - Que el alcance de la Auditoría ofrecido por el oferente (licitador) se corresponde efectivamente con el deseado por la entidad, incluyendo los sistemas de información auditados y los servicios soportados correspondientes.

- Que los tiempos de auditoría son fundamentados y, en todo caso, no son inferiores a los señalados en la tabla mostrada anteriormente sin que esté debidamente justificada tal reducción. En caso de duda, se sugiere consultar al Centro Criptológico Nacional en la cuenta de correo cocens@ccn.cni.es.
- Los tiempos de auditoría podrán ser, no obstante, mayores si, como señala la Guía de Seguridad CCN-STIC CCN-CERT IC-01/19 *ENS: Criterios Generales de Auditoría y Certificación,* concurren circunstancias que exigen un incremento justificado de los tiempos de auditoría.

6. TIPO DE CONTRATACIÓN

28. La contratación de la ejecución de una Auditoría de Conformidad con el ENS se corresponde con un **contrato de servicios**[1], de los regulados en el art. 17 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP).

29. Aunque existe una significativa variedad de procedimientos de contratación (ver Anexo), para la contratación de los servicios de Auditoría de Conformidad suelen utilizarse los siguientes:

    1. Por **adjudicación directa**, cuando se trate de **contratos menores**, determinados en la Ley 9/2017 por su cuantía; siendo contratos menores los de importe inferior a 15.000 €, cuando se trate de contratos de servicios, impuestos no incluidos (artículo 118 LCSP). Es poco frecuente que una auditoría de certificación supere dicha cifra.

    2. Por **procedimientos ordinarios**, de entre el que destacamos el **procedimiento abierto,** en el que todo licitador interesado puede presentar una proposición, siempre que acredite los requisitos de solvencia exigidos en el pliego de cláusulas administrativas particulares, quedando excluida toda negociación de los términos del contrato con los licitadores (artículos 156 a 159 LCSP), pudiéndose desarrollar bajo la forma de **procedimiento abierto simplificado**,

[1] Artículo 17. Contrato de servicios. Son contratos de servicios aquellos cuyo objeto son prestaciones de hacer consistentes en el desarrollo de una actividad o dirigidas a la obtención de un resultado distinto de una obra o suministro, incluyendo aquellos en que el adjudicatario se obligue a ejecutar el servicio de forma sucesiva y por precio unitario.
No podrán ser objeto de estos contratos los servicios que impliquen ejercicio de la autoridad inherente a los poderes públicos.

en los contratos de servicios cuyo valor estimado sea igual o inferior a 100.000 € cuando se cumplan las condiciones establecidas en el artículo 159 de la LCPS[2].

3. Por **procedimiento restringido,** en el que cualquier licitador interesado podrá presentar una solicitud de participación en respuesta a una convocatoria de licitación, pudiendo solo presentar proposiciones aquellos empresarios que, a su solicitud y en atención a su solvencia, sean seleccionados por el órgano de contratación, estando prohibida toda negociación de los términos del contrato con los solicitantes o candidatos (artículos 160 a 165 de la LCSP).

4. Por **procedimiento negociado,** en el que la adjudicación recaerá en el licitador justificadamente elegido por el órgano de contratación, tras negociar las condiciones del contrato con uno o varios candidatos (artículos 166 a 171 de la LCSP).

7. PLIEGO DE PRESCRIPCIONES ADMINISTRATIVAS

30. Cuando se usen procedimientos de contratación que exijan la publicidad de los Pliegos de Prescripciones Administrativas (o Condiciones Generales), deben explicitarse determinadas informaciones.

31. Se muestra un ejemplo de tales informaciones, para un procedimiento ordinario abierto simplificado.

1	**Número de expediente.**	(El que se trate)
2	**Entidad contratante:**	Con indicación del nombre o denominación, domicilio, teléfono y fax.
	Obtención de documentación, consultas e información:	Dirección de Internet del Perfil de Contratante de la entidad. Correo electrónico de consultas.
3	**Objeto del contrato:**	Tipo, según su finalidad y objeto: Servicios.
		Tipo, según su régimen aplicable: Administrativo o Privado.
		CPV: 79212200-3 Servicios de Auditoría.
		Descripción: el servicio objeto del contrato es la realización de una Auditoría de Certificación de los sistemas de información de la entidad, conforme a lo dispuesto en el RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) y normativa de desarrollo, para dar cobertura a los

[2] El denominado "procedimiento restringido**",** en el que sólo podrán presentar proposiciones aquellos empresarios que, a su solicitud y en atención a su solvencia, sean seleccionados por el órgano de contratación, quedando prohibida toda negociación de los términos del contrato con los solicitantes o candidatos (artículo 160 a 165 LCSP), no suele utilizarse en este tipo de contratación, toda vez que el número de posibles oferentes (Entidades de Certificación acreditadas) es muy limitado.

		requisitos normativos referentes a la auditoría de seguridad recogidos en el art. 34 y Anexo III del ENS. (Ver Pliego de Prescripciones Técnicas para más información).	
4	**Estructura del contrato:**	Número de lotes / Número de unidades: el servicio objeto de contrato constituye una unidad funcional (art. 99.3 Ley 9/2017 de Contratos Sector Público).	
5	**Duración total del contrato:**	Plazo total del contrato: _____ mes(es), una vez alcanzado el acuerdo para la realización de la auditoría *in-situ*. Prórrogas: no.	
6	**Presupuesto máximo:**	Importe neto: _____€ IVA 21%: _____€ Importe total (IVA incluido): _____ €	
7	**Presupuesto base de licitación (IVA excluido):**	_____ €	
8	**Revisión de precios:**	No.	
9	**Lugar de ejecución:**	En las instalaciones del adjudicatario, a excepción de las visitas asociadas a las auditorías *in-situ* en las instalaciones de la entidad o en las instalaciones de proveedores de servicios a la entidad. El resto de las actuaciones, como pudieran ser las auditorías documentales previas o los análisis y estudios de documentación complementaria, se llevarán a cabo en las instalaciones de la empresa adjudicataria.	
10	**Subcontratación y cesión:**	No permitida.	
11	**Modificación:**	Se permite la modificación del contrato en los siguientes supuestos: a. En el caso de que durante la ejecución del contrato se publiquen nuevas versiones de la legislación o normativa de referencia. b. En el caso de que durante la ejecución del contrato se adopte una decisión estratégica sobre la conveniencia y necesidad de implantar otros estándares de referencia y/o ampliar el alcance con nuevos servicios. Se prevé un presupuesto máximo de _____ €, IVA excluido, para cubrir estas necesidades sobrevenidas.	
12	**Tramitación y procedimiento:**	Tramitación: ordinaria. Tipo: abierto simplificado. Justificación: Art. 159 Ley 9/2017. Sujeto a regulación armonizada: no. Forma de publicidad: Perfil de Contratante.	
13	**Requisitos de los licitadores interesados y documentación a presentar:**	Capacidad jurídica y de obrar: (Detallar en el Pliego - Obligatoria en sobre 2) Solvencia económica y financiera: (Detallar en el Pliego – Obligatoria en sobre 2)	
14	**Criterios de adjudicación:**	Criterios cuantificables objetivos (0 a 80 puntos):	Oferta económica.
		Criterios valorables mediante juicio de valor (0 a 20 puntos).	· Número de Auditorías de Certificación del ENS realizadas por la entidad (10 puntos) · Metodología usada (10 puntos).

15	**Presentación de ofertas:**	Fecha límite de presentación de ofertas: Hasta las _____ horas del día _____.
		Modalidad de presentación: Electrónica, usando _____
		Lugar de presentación (cuando se use la Plataforma de Contratos del Sector Público): las proposiciones para tomar parte en la licitación se presentarán únicamente por medios electrónicos a través de los servicios de licitación electrónica de la Plataforma de Contratación del Sector Público y mediante la herramienta de preparación y presentación de proposiciones que la Plataforma de Contratación del Sector Público pone a disposición de los licitadores a través de la cual se garantiza la integridad, no repudio, autenticidad y confidencialidad de las ofertas. Las ofertas deben ir firmadas por el licitador. Para la utilización de estos servicios, los licitadores interesados en la presentación de ofertas en este procedimiento deberán registrarse previamente en la Plataforma de Contratación del Sector Público, utilizando para ello las guías de ayuda disponibles, y en concreto, para este trámite, la Guía de Utilización de la Plataforma de Contratación del Sector Público para Empresas (Guía de Operador Económico), accesible a través de la siguiente página: www.contrataciondelestado.es
		Admisión de variantes y mejoras: No.
16	**Apertura de sobres:**	Composición de la Mesa/Comisión de Contratación: _____
		Sobre nº 1 Documentación relativa a los criterios de adjudicación sujetos a juicio de valor: De conformidad con lo dispuesto en el art. 157.4 LCSP, este acto de apertura se realizará por medios electrónicos y no será público.
		Sobre nº 2 Documentación relativa a los criterios de adjudicación objetivos y documentación general: De conformidad con lo dispuesto en el art. 157.4 LCSP, este acto de apertura se realizará por medios electrónicos y no será público.
		Lugar: entidad contratante. Fecha y hora: Serán las recogidas en el anuncio de licitación. En caso de modificación, serán publicadas en el Perfil de Contratante.
17	**Plazo de formalización del contrato:**	Tras la adjudicación, en un plazo no superior a cinco días desde el requerimiento para la formalización del contrato (art. 153 Ley 9/2017).
18	**Obligaciones oferta mejor valorada:**	Garantía: . Provisional: no. . Definitiva: sí. Importe: 5% del precio de adjudicación sin IVA. Plazo: 12 meses desde la recepción total de los servicios.
		Certificado de AEAT: - Certificación positiva, expedida dentro de los seis meses anteriores a la fecha de presentación, por el órgano competente de la Administración Tributaria, establecida en los términos y condiciones fijados en el Real Decreto 1098/2001, de 12 de octubre, por el que se aprueba el Reglamento General de la Ley de Contratos de las Administraciones Públicas. Certificado de TGSS:

		- Certificación positiva, expedida dentro de los seis meses anteriores a la fecha de presentación por el órgano competente de la Seguridad Social, establecida en los términos y condiciones fijados en el Real Decreto 1098/2001, de 12 de octubre, por el que se aprueba el Reglamento General de la Ley de Contratos de la Administraciones Públicas.
		Prevención de riesgos laborales (si/no) En caso afirmativo, antes de la formalización del contrato. Deberán presentarse: - Persona de contacto (nombre y nº de teléfono). - Modelo de organización preventiva adoptado por la empresa (si es propio, titulación del responsable y si es concertado con entidad ajena, documento del concierto). - Teléfono de urgencia en caso de accidente. - Evaluación de Riesgos Laborales y Planificación de la Actividad Preventiva de los trabajos a realizar. - Fotocopia del listado de aptitudes incluido en el informe de vigilancia de la salud de los trabajadores asignados al contrato efectuado por un especialista acreditado en Medicina del Trabajo.) - Documento acreditativo de la formación e información preventiva recibida por el trabajador asignado a este contrato, para el desempeño de su puesto de trabajo.
		Alta y Relación nominal de trabajadores: Sí.
		Acreditación declaración de adscripción de medios técnicos y personales: Para cada perfil adscrito al Equipo de Auditoría, deberá presentarse: - Vida laboral. - CV, que deberá recoger: ・ Perfil ・ Categoría profesional ・ Titulación / Formación ・ Actividad profesional (especificado como mínimo, empresa, duración del proyecto, descripción del mismo y actividades desarrolladas y cliente para el que se ejecuta) ・ Certificaciones (CISA, CISM, CGEIT, CRISC, etc.) ・ Número de auditorías ENS realizadas. ・ Número de auditorías de seguridad realizadas en el ámbito TIC. ・ Número auditorías a Sistemas de Gestión de Seguridad de la Información realizadas (v.g., 27001, 9001, etc.)
		Tratamiento de datos persónales: no.
		Confidencialidad: el contratista deberá respetar el carácter confidencial de aquella información a la que tenga acceso con ocasión de la ejecución del contrato, a la que se le hubiese dado el referido carácter en los pliegos o en el contrato, o que por su propia naturaleza deba ser tratada como tal. Este deber se mantendrá de manera indefinida desde el conocimiento de esa información.

		Penalizaciones: (sí/no) (Mencionar el apartado del Pliego en que se tratan).
19	**Obligaciones de la entidad contratante:**	Abono del precio: ver apartado correspondiente de los Pliegos.
		Devolución de la garantía: tras finalizar el plazo de garantía previsto en el apartado anterior.

8. PLIEGO DE PRESCIPCIONES TÉCNICAS

32. Cuando se usen procedimientos de contratación que exijan la publicidad de los Pliegos de Prescripciones Técnicas, deben explicitarse determinadas informaciones.

33. Se muestra un ejemplo de tales informaciones, para un procedimiento ordinario abierto simplificado.

1	**Contexto, necesidad, objeto y alcance.**	Contexto. (Breve explicación de la situación actual de la entidad en materia de seguridad de la información)
		Necesidad, objeto y alcance. (Expresar la necesidad de la Certificación de Conformidad con el ENS en beneficio de la seguridad de la información tratada y los servicios prestados por la entidad).
2	**Requisitos técnicos del servicio.**	Descripción de los trabajos. (Concretar los trabajos necesarios para la ejecución de una Auditoría de Certificación del ENS (auditoría documental e *in-situ*) y expedición, en su caso, de la correspondiente Certificación de Conformidad con el ENS), para el alcance de que se trate, señalando el(los) sistema(s) de información concernido(s) y servicios prestados.
		Requisitos de cualificación y experiencia del Equipo Auditor adscrito al contrato. (Será necesaria la presencia, al menos, de un Auditor Jefe, que deberá satisfacer los requisitos personales expresados en la Guía de Seguridad CCN-STIC CCN-CERT IC-01/19, complementados con los expresados en la Guía CCN-STIC 802).
		Metodología y entregables. (La empresa licitadora deberá proponer de manera clara la metodología a seguir durante el desarrollo del proyecto, que deberá estar orientada a alcanzar los objetivos fijados en el Pliego. Asimismo, el licitador describirá en detalle el contenido y estructura de los entregables objeto del proceso de auditoría, entre ellos, el plan o programa de auditoría, el informe de auditoría documental, el informe de auditoría presencial y el informe PAC, todo ello según se detalla en la ITS de Auditoría y en la Guía CCN-STIC 802).
3	**Equipo Auditor.**	Perfiles técnicos requeridos. (Se requerirá, al menos, un Auditor Jefe)
		Dirección y seguimiento de los trabajos. (Determinación de la unidad encargada de la dirección y seguimiento del proyecto).
4	**Forma de ejecución.**	a. Lugar y horario de ejecución de los trabajos.

		b. Soporte técnico. c. Control de calidad. d. Obligaciones de información y documentación. e. Hitos de facturación.

9. INCOMPATIBILIDADES ENTRE CONSULTORÍA Y AUDITORÍA

34. Para certificar su(s) sistema(s) respecto al ENS, una organización perteneciente al Sector Público, en función de los recursos propios de que disponga, puede decidir realizar el necesario plan de adecuación, junto a la implantación del mismo, mediante sus propios medios, o bien contratando los servicios de una empresa de consultoría externa para que le ayude a adecuarse y poder así superar la preceptiva auditoría de certificación.

35. Un aspecto relevante que debe tenerse en cuenta es **la no conveniencia de destinar un pliego para seleccionar la empresa de consultoría** y que sea ésta la que subcontrate a su vez a la entidad de certificación.

    Esto es así por dos (2) razones:

    - Se daría la circunstancia de conflicto de interés si es la empresa consultora la que subcontrata a la entidad de certificación, ya que ésta última deberá auditar el trabajo realizado por la consultora.
    - Por requerimientos de la norma ISO/IEC 17065:2012, norma que obliga a todas las entidades de certificación del ENS, debe poder evidenciarse una aceptación de la oferta por parte de la persona jurídica que será auditada, no contemplándose la posibilidad de intermediación.

      Adicionalmente, en su apartado 4.1.2.1, dicha norma dispone que la entidad de certificación debe tener un acuerdo legalmente ejecutable con su cliente (no con un intermediario) para proporcionarle actividades de certificación, que deberán tener en cuenta sus respectivas responsabilidades: tanto de la entidad de certificación como del cliente.

36. En consecuencia, el procedimiento de contratación de la auditoría de certificación deberá ser independiente del de las labores de consultoría. Esto podría llegar a materializarse en base a dos lotes separados, uno para consultoría y otro para certificación, o dos licitaciones independientes en el tiempo, habida cuenta de que la certificación será siempre posterior a la consultoría.

10. SOLICITUD DE INFORMACIÓN

37. Habitualmente y de manera especial cuando se trata de procedimientos por adjudicación directa, las Entidades de Certificación requerirán de la entidad contratante, con anterioridad a la presentación de sus Ofertas o Propuestas, determinada información que utilizarán para dimensionar el esfuerzo y los recursos requeridos para llevar a cabo la Auditoría de Conformidad.

    Este dimensionamiento se traducirá en el número de jornadas de auditoría necesarias, las cuales tienen una incidencia directa en el importe de la misma, en base al precio por jornada de auditoría de la Entidad de Certificación.

38. El cuadro siguiente muestra un ejemplo de la información que suele solicitarse.

    1. Nombre de la Organización y URL (en su caso).
    2. NIF.
    3. Sector (Público / Privado).
    4. Actividad.
    5. Dirección postal y Teléfono.
    6. Persona de contacto (nombre, apellidos, cargo y e-mail).
    7. Categoría del sistema de información afectado por la Auditoría (BÁSICA, MEDIA o ALTA).
    8. Alcance de la Certificación solicitada.
    9. Personal relevante para el desarrollo de la auditoría.
    10. Empleados de la organización comprendidos en el alcance de la Certificación.
    11. Número total de empleados de la organización.
    12. Relación de Proveedores de Servicios externos, relevantes para la prestación de los servicios comprendidos en el alcance de la Certificación, con indicación del Proveedor y el servicio que presta.
    13. Relación de entidades que han prestado consultoría de adecuación al ENS a la organización.
    14. Relación de sedes administrativas de la organización, localización y la descripción de sus actividades concretas, especialmente las que se estima será necesario auditar.

15. Relación de CPD de la organización y localización, indicando si se trata de CPD propios o se encuentran externalizados, tanto para los CPD principales como para los de respaldo, de existir.
16. Indicación de los servicios de CPD externalizados: *hosting, housing, Cloud IaaS*, etc.
17. Servicios prestados a través de la Sede Electrónica de la entidad (en su caso).
18. Extensión y diversidad tecnológica usada en los sistemas de información sujetos al alcance de la Certificación.
19. ¿Hay sistemas industriales?
20. ¿Hay desarrollo de software? En caso afirmativo ¿Es interno o está externalizado?
21. Rango de fechas deseadas para realizar la Auditoría de Certificación.
22. Circunstancias que puedan limitar la actividad auditora (en su caso).
23. Exigencias específicas de confidencialidad (en su caso).
24. Otros requisitos legales aplicables (en su caso).

ANEXO: PROCEDIMIENTOS DE CONTRATACIÓN LEY 9/2017

1.- PROCEDIMIENTO ABIERTO (art. 156-158)

- General y preferente. No ha de justificarse. Con anuncio previo electrónico.

2.- PROCEDIMIENTO ABIERTO SIMPLIFICADO (PAS) Y SIMPLIFICADO ABREVIADO (PASS) (ART. 159) (Necesario estar inscrito en el ROLECE)

- Permite aligerar cargas administrativas.
- Plazo licitación: 20 días y 10 en el súper-simplificado, obras; 15 días y 10 (salvo adquisición bienes corrientes que son 5), servicios y suministros.
- Requisitos:
  a) De cuantía:
     - Contratos obras: valor estimado igual o inferior a 2.000.000 €.
     - Contratos servicios y suministros: igual o inferior a 100.000 €.
  b) De criterios de adjudicación: que no haya ninguno evaluable mediante juicio de valor y de haberlos su ponderación no supere el 25% del total salvo que el contrato tenga por objeto prestaciones de carácter intelectual en el que la ponderación no podrá superar el 45%.
- Para contratos de escasa cuantía: simplificados abreviados o súper-simplificados (art 159.6):
     - Obras: 80.000 €.
     - Servicios y Suministros: 35.000 € (Excepto que su objeto sean obras de carácter intelectual).
- Se exime en los súper-simplificados de la acreditación solvencia económica, financiera, técnica y profesional.
- No se puede utilizar esta modalidad de procedimiento abierto en contratos de concesión de servicios, de concesión de obra pública, y el contrato de asociación para la innovación.
- Tramitación de los abiertos:
     - Los licitadores deberán estar inscritos en el ROLECE (plazo: hasta el 9 de septiembre de 2018 para estar inscrito).
     - No procede garantía provisional.

3.- PROCEDIMIENTO RESTRINGIDO

- Adecuado para la contratación de servicios intelectuales de especial complejidad.
- Deben ser convocadas, al menos, 5 empresas, y sólo podrán presentar proposiciones las empresas seleccionadas.

4.- PROCEDIMIENTO CON NEGOCIACIÓN (ART. 166-171)

- De carácter extraordinario.
- Es aquel que recae en un solo licitador tras un proceso de negociación con uno o varios candidatos.
- No requiere necesariamente publicidad, pero se aconseja que sea comedida la ausencia de la misma. Se puede elegir sin publicidad cuando:
    - La licitación ha quedado desierta en un procedimiento abierto.
    - Circunstancias sobrevenidas excepcionales e imprevisibles, (ya que existen otros procedimientos como la tramitación de urgencia).
- Recomendaciones:
    1. Deben ser invitadas las empresas que, aunque no han sido llamadas a la negociación, así lo soliciten.
    2. Se deben establecer protocolos internos para la pre-selección en condiciones de igualdad.
    3. Los distintos aspectos de la negociación deben documentarse en el expediente.
    4. Si hay distintas fases, deberá asegurarse que el número de ofertas garantice la competencia efectiva.

5.- CONTRATOS MENORES (ART. 118)

1.- Por su valor:

- 40.000 € en obras.
- 15.000 € en servicios y suministros.

*excepción en materia de Ciencia y Tecnología e Innovación que ha habido cambio del umbral y se ha subido a 50.000 € en suministros y servicios de esa índole.

**El Pleno del Congreso de los Diputados, en la sesión plenaria núm. 118, celebrada el miércoles 23 de mayo de 2018, ha aprobado el Proyecto de Ley de Presupuestos Generales del Estado para el año 2018, que incorpora una enmienda en la que se regula un nuevo régimen aplicable a los contratos menores*

celebrados por los agentes públicos del Sistema Español de Ciencia, Tecnología e Innovación. El contenido de la referida Disposición adicional es el siguiente:

"Disposición adicional quincuagésima cuarta. Régimen aplicable a los contratos celebrados por los agentes públicos del Sistema Español de Ciencia, Tecnología e Innovación.

Atendiendo a la singular naturaleza de su actividad, como excepción al límite previsto en el artículo 118 de esta Ley, tendrán en todo caso la consideración de contratos menores los contratos de suministro o de servicios de valor estimado inferior o igual a 50.000 € que se celebren por los agentes públicos del Sistema Español de Ciencia, Tecnología e Innovación, siempre que no vayan destinados a servicios generales y de infraestructuras del órgano de contratación.

A estos efectos, se entienden comprendidos entre los agentes públicos del Sistema Español de Ciencia, Tecnología e Innovación, en los términos establecidos en la Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación, las Universidades públicas, los Organismos Públicos de Investigación, fundaciones, consorcios, agentes de ejecución de la Administración General del Estado, los organismos y entidades de investigación similares a los anteriores dependientes de otras Administraciones Públicas, las Fundaciones de Investigación Biomédica y los centros, instituciones y consorcios del Sistema Nacional de Salud".

2.- Por duración:

- No superiores a 1 año. No prórroga.

3.- Por su justificación:

- Siempre el órgano de contratación los debe justificar, incluyendo la aprobación del gasto, la factura, y en obras también el presupuesto y el proyecto.

Cautelas:

1. En el expediente deberá justificarse que no se ha alterado el objeto del contrato para evitar las reglas generales de contratación.
2. El contratista no haya suscrito más contratos menores que individual o conjuntamente superen la cifra mencionada anteriormente.
3. Deberán ser objeto de publicación de manera agrupada y trimestral. Salvo los de menos de 5.000 € que se paguen a través de caja fija o similares.

6.- DIALOGO COMPETITIVO (art. 172 y ss.)

- Otro de los procedimientos extraordinarios.
- El ente público dirige un intercambio de opiniones con los candidatos seleccionados, previa solicitud de los mismos, con el fin de desarrollar una licitación que se ajuste a las necesidades de ambas partes.

- Similar al procedimiento con negociación, se reserva para contratos especialmente complejos (ej. Infraestructuras complejas).
- Requisitos:
    1. Debe ser flexible.
    2. Debe garantizar la libre competencia a través de un número mínimo de empresas a participar, no inferior a 3 siempre que sea posible.

7.- PROCEDIMIENTO DE ASOCIACIÓN PARA LA INNOVACIÓN (art. 177 y ss.)

- Cuando las obras, productos o servicios innovadores para el ente contratante no estén disponibles en el mercado.
- Se podrá crear una asociación con uno o varios socios que efectúen por separado las actividades de investigación y desarrollo necesarias.
- Fases:
    1. Selección de candidatos.
    2. Negociación con los licitadores.
    3. Asociación con los socios.
    4. Adquisición del producto resultante.
- Requisitos:
    1. Flexibilidad.
    2. No inferiores los socios a 3 siempre que sea posible.
    3. Garantizar la competencia con el nº de ofertas.

8.- TRAMITACIÓN DE URGENCIA

- Solo en aquellas situaciones en las que el plazo de tramitación ordinaria conlleve vulneración y detrimento del interés público. Los plazos se reducen a la mitad del ordinario.
- Requisito: justificación exhaustiva.

9.- ACUERDOS MARCO Y SISTEMAS DINÁMICOS DE CONTRATACIÓN (ART. 219-222)

- Adecuados a supuestos en que la contratación se extiende a lo largo de un período determinado, durante el cual existirán prestaciones continuadas.
- Con dichos acuerdos se busca la estabilidad en las condiciones contractuales.

- Una vez iniciados no se permite la incorporación de nuevas empresas durante el plazo de vigencia del contrato.
- Requisitos:
    1. Requiere justificación.
    2. Por cuatro (4) años ampliables excepcionalmente.
    3. Si se declara desierto o el número de empresas resulta reducido, deberá seleccionarse otro procedimiento de contratación.