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)

Junio, 2023

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.06.18 09:16:46 +02'00'

Fecha de Edición: junio de 2023

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 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), muy especialmente, a las entidades públicas más pequeñas o con menos recursos, a acometer las actividades necesarias para la contratación de las Auditorías de la Seguridad que persigan la expedición de una Certificación de Conformidad con el ENS, a las que llamaremos **Auditorías de Certificación**.

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

2. Como prescribe el art. 31 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 del ámbito de aplicación del ENS deberán ser objeto de una auditoría regular ordinaria, al menos cada dos (2) años, que verifique el cumplimiento de los requerimientos del ENS.

   Sin perjuicio de lo anterior, con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en el sistema de información en cuestión que puedan repercutir en las medidas de seguridad requeridas.

   La auditoría se realizará atendiendo a la categoría de seguridad del sistema de información -o, en su caso, al Perfil de Cumplimiento Específico que corresponda-, según lo dispuesto en los Anexos I y III del ENS, y de conformidad con lo regulado en la antedicha Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los sistemas de información.

   Como señala el precitado art. 31, en la realización de las auditorías de la seguridad se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de actividades.

   El resultado final de una Auditoría es el denominado *Informe de Auditoría*, que deberá dictaminar sobre el grado de cumplimiento del sistema o sistemas auditados en relación con los criterios de auditoría (referencial) señalados en el ENS, identificando los hallazgos de cumplimiento e incumplimiento detectados, incluyendo igualmente los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas, todo ello de conformidad con la citada ITS de Auditoría de la Seguridad.

   El Informe de Auditoría, que se presentará al Responsable del Sistema y al Responsable de Seguridad, deberá ser cuidadosamente analizado por el Responsable de Seguridad,

quién señalará los hallazgos (desviaciones) sobre las que deberán adoptarse las medidas correctoras oportunas.

En el caso de los sistemas de categoría ALTA, visto el Informe de Auditoría y su correspondiente dictamen, y atendiendo a la eventual gravedad de las deficiencias encontradas, el Responsable del Sistema podrá suspender temporalmente el tratamiento de informaciones, la prestación de servicios o la total operación del sistema, hasta su adecuada subsanación o mitigación. Naturalmente, una suspensión que pudiera dilatarse en el tiempo requerirá la preceptiva aprobación de la autoridad competente de la organización titular de los sistemas afectados.

Los Informes de Auditoría podrán ser requeridos por los responsables de cada organización con competencias sobre seguridad de las TIC y por el Centro Criptológico Nacional (CCN).

3. Por su parte, el art. 38 del ENS señala la obligatoriedad de las entidades afectadas de publicitar en sus sedes electrónicas (o portales de internet) las Declaraciones y/o 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 la Disposición adicional segunda 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 y ALTA y voluntaria para los de categoría BÁSICA.

5. Los sistemas de categoría BÁSICA que no se certifiquen voluntariamente del ENS, deberán cumplir asimismo con las disposiciones del RD 311/2022 para su categoría, evidenciándolo asimismo mediante un Distintivo específico de Conformidad tras superar la autoevaluación correspondiente.

6. La Certificación de Conformidad con el ENS solo podrá ser expedida por una Entidad de Certificación acreditada por la Entidad Nacional de Acreditación (ENAC) o por un Órgano de Auditoría Técnica del Sector Público, reconocido por el CCN, que se encuentren referenciados en la página web del CCN-CERT y se completará mediante un Distintivo de Conformidad cuyo uso estará condicionado a los requisitos señalados en la antedicha *ITS de Conformidad con el ENS*.

7. La evidencia pública de la Certificación de 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 con el ENS, que

incluirá un enlace al documento de Certificación de Conformidad correspondiente, que también permanecerá accesible a través de dicha sede electrónica o página web.

8. La relación actualizada de organizaciones que tengan certificada la conformidad respecto al ENS de alguno de sus sistemas de información, se encuentra disponible en la siguiente dirección del portal web del CCN-CERT:

   https://gobernanza.ccn-cert.cni.es/certificados

> **Nota importante:** *solo aquellas Certificaciones de Conformidad con el ENS que se expidan por Órganos de Auditoría Técnica del sector Público reconocidos por el CCN o aquellas otras expedidas 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. ORGANISMOS DE CERTIFICACIÓN DEL ENS

9. La relación actualizada de Entidades de Certificación (EC) del ENS acreditadas, así como los Órganos de Auditoría Técnica del Sector Público (OAT) reconocidos, se encuentra disponible en la dirección:

   https://ens.ccn.cni.es/es/certificacion/entidades-de-certificacion

5. EL PROCEDIMIENTO DE CONTRATACIÓN

10. Aun habiendo en este apartado actividades comunes entre una Entidad de Certificación del sector privado y un OAT del sector público, está especialmente orientado a la contratación de una Entidad de Certificación (EC).

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

5.1 Actividades previas

12. Determinar con precisión el alcance de la Auditoría de Certificación, identificando el(los) sistema(s) de información afectado(s) y los servicios soportados por medio de tales sistemas. En este sentido, 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).

13. Así pues, puesto que 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 el sistema de información auditado (servicios declarados) y que se benefician de la seguridad del sistema de información sobre el que se prestan materialmente.

14. A partir de estas premisas, la entidad de que se trate debería identificar aquellos sistemas de información que deben adecuarse 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 legal o estatutaria de la institución) de los "servicios instrumentales" (aquellos destinados a satisfacer una necesidad de la propia institución).

15. Obviamente, puestos a señalar una ordenación para el acometimiento, suele ser más prioritario garantizar la seguridad de los sistemas de información que sustentan los primeros (servicios finalistas), pero sin olvidar que, en algún momento, habrá que acometer también los segundos (servicios instrumentales), especialmente cuando esos servicios se desarrollan conforme al derecho público (la contratación, por ejemplo).

16. 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 los 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

17. Una vez realizada la actividad anterior, será necesario 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 (LCSP) y sus normas de desarrollo.

18. La realización de una Auditoría de la Seguridad que persiga la expedición de una Certificación 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.

19. 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. El coste por jornada/auditor es de libre determinación por parte de las Entidades de Certificación, siendo frecuente que fijen unos precios concretos al comienzo de cada anualidad, precios que no podrán ser alterados de forma arbitraria o no justificada, menos aún para ajustarlos a un determinado Pliego salvo excepciones (Los contratos de las Administraciones Públicas podrán modificarse durante su vigencia hasta un máximo del veinte por ciento del precio inicial cuando en los pliegos de cláusulas administrativas particulares se hubiere advertido expresamente de esta posibilidad)

Además de ello, tampoco se puede variar arbitrariamente el número de jornadas de auditoría cuando esas jornadas se han calculado en función de determinados parámetros que reflejan las características y situación del cliente y el sistema a auditar.

20. La versión vigente (publicada) de 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.

21. En este sentido, hay que recalcar que conviene que la **entidad contratante examine con detenimiento** cualquier oferta cuyos **tiempos de auditoría sean inferiores a los señalados** en la Guía de Seguridad CCN-STIC *CCN-CERT IC-01/19 ENS: Criterios Generales de Auditoría y Certificación*, requiriendo del licitador la correspondiente justificación.

22. Se hace hincapié en que se trata de tiempos mínimos que podrían incrementarse hasta un determinado porcentaje en función de determinados parámetros, tales como el número de sedes a auditar, el número de CPDs, la complejidad o diversidad tecnológica presenta, etc. tal y como está descrito en la precitada Guía *CCN-CERT IC-01/19*.

23. Si la entidad contratante desconoce el precio medio por jornada de las entidades de certificación, se sugiere contactar previamente a lanzar la licitación pública con alguna de ellas para que hagan una oferta aproximada en base a su precio por jornada de auditoría y el número de éstas que determinen son requeridas, de modo que la licitación no quede desierta por haber indicado un importe por debajo del cálculo resultante en función de diversos parámetros por parte de quienes oferten.

24. Como se ha indicado, es necesario señalar con claridad en los Pliegos de Prescripciones el alcance de la Auditoría de la Seguridad que persiga la expedición de una Certificación de Conformidad con el ENS, sabiendo que tal alcance será, en caso de resultar satisfactoria dicha auditoría, el que aparezca en la Certificación de Conformidad correspondiente.

25. Para la enunciación del alcance se recomienda utilizar una expresión del tipo:

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

26. Sin olvidar incluir las dimensiones de seguridad afectadas y la categoría del (de los) sistema(s) de información objeto de la auditoría, todo ello de conformidad con lo

señalado en la Instrucción Técnica de Seguridad de Conformidad con el ENS y en lo recogido en las Guías *CCN-CERT IC-01/19* y *CCN-STIC 809*.

27. Debe tenerse en cuenta que las Entidades de Certificación acreditadas -y, en su caso, los Órganos de Auditoría Técnica del Sector Público reconocidos- pueden ayudar a determinar la conveniencia, o no, del alcance elegido para la certificación y asesorar, respecto a su certificación y cumplimiento, de los requisitos exigidos en la versión vigente de la antedicha Guía de Seguridad CCN-STIC *CCN-CERT IC-01/19 ENS: Criterios Generales de Auditoría y Certificación*.

5.3 Evaluación de las Propuestas/Ofertas

28. Una vez recibida(s) la(s) propuesta(s) del (de los) oferente(s), la entidad contratante deberá verificar:

    - Que el oferente (licitador) se corresponde con una de las Entidades de Certificación del ENS acreditadas, relacionadas en la antedicha página web del CCN o, en su caso, un Órgano de Auditoría Técnica del Sector Público reconocido.
    - Que el alcance de la Auditoría ofrecido por el oferente (licitador) se corresponde efectivamente con el deseado por la entidad contratante, incluyendo los sistemas de información auditados y los servicios soportados.
    - Que los tiempos de auditoría están debidamente fundamentados y, en todo caso, no son inferiores a los señalados en la Guía de Seguridad CCN-STIC *CCN-CERT IC-01/19 ENS: Criterios Generales de Auditoría y Certificación*. En caso de duda, se sugiere consultar al Centro Criptológico Nacional en la dirección de correo cocens@ccn.cni.es.
    - Como se ha señalado, los tiempos de auditoría podrán ser, no obstante, mayores de los reflejados en la Guía CCN-STIC *CCN-CERT IC-01/19 ENS: Criterios Generales de Auditoría y Certificación* cuando concurren circunstancias que exigen un incremento justificado de los tiempos de auditoría, hasta un determinado porcentaje.

6. TIPO DE CONTRATACIÓN

29. La contratación de la ejecución de una Auditoría de la Seguridad que persiga la expedición de una Certificación 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).

[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.

30. Aunque la legislación de Contratos del Sector Público, desde su promulgación, ha venido regulando una significativa variedad de tipos contractuales y procedimientos de contratación para la contratación de los citados servicios de Auditoría 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).

    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**, en los contratos de servicios cuyo valor estimado sea igual o inferior al señalado en el art. 22 de la LCSP y 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.

[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.

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 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) y normativa de desarrollo, para dar cobertura a los requisitos normativos referentes a la auditoría de seguridad recogidos en el art. 31 y Anexo III del ENS. (Ver el 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: _____ [día(s), semana(s), mes(es)], una vez alcanzado el acuerdo para la realización de la auditoría *in-situ* o remota. 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 de la entidad contratante o en las instalaciones de proveedores de servicios a la entidad, en aquellas actuaciones que se hayan previsto para su realización *in situ*. Realizadas de forma remota mediante soluciones de videoconferencia en aquellas otras actuaciones que a juicio del Organismo de Certificación no entrañen riesgo en relación a la calidad de la auditoría, siempre tomando en consideración lo señalado en la Guía CCN-STIC *CCN-CERT IC-01/19*. El resto de las actuaciones, como pudieran ser el estudio documental previo, la redacción del Informe de Auditoría o el análisis de las propuestas contempladas en el Plan de Acciones Correctivas o en documentación complementaria, podrán determinarse que se lleven a cabo en las instalaciones del adjudicatario.
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 60 puntos).	Oferta económica.
		Criterios valorables mediante juicio de valor (0 a 40 puntos).	· Número de Auditorías de Certificación del ENS realizadas por la entidad (a determinar la puntuación) · Metodología usada (a determinar la puntuación).
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 (5) 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: **Transcurrido un año desde la fecha de terminación del contrato**, y vencido el plazo de garantía, sin que la recepción formal y la liquidación hubiesen tenido lugar por causas no imputables al contratista, se procederá, sin más demora, a la devolución o cancelación de las garantías una vez depuradas las responsabilidades a que se refiere el artículo 110.
		Certificado de AEAT: - Certificación positiva, expedida dentro de los seis (6) 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 (6) 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 personales: 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 PRESCRIPCIONES 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*/remota) 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 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 de auditoría, el informe de auditoría documental, el informe de auditoría presencial y, en el caso de hallarse desviaciones, el informe de evaluación del Plan de Acciones Correctivas (PAC), todo ello según se detalla en la ITS de Auditoría, en la Guía *CCN-CERT IC-01/19* 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 ACTIVIDADES DE CONSULTORÍA Y AUDITORÍA

34. De cara a alcanzar la Certificación de Conformidad con el ENS, una organización del sector público, en función de los recursos propios de que disponga, puede redactar el plan de adecuación y ejecutar su implantación usando sus propios medios o bien contratando los servicios de una empresa externa de consultoría.

35. En este último caso, **no es admisible que la redacción de los Pliegos de Prescripciones que señalen las condiciones de selección de la empresa consultora recoja asimismo que dicha empresa será la que subcontrate a su vez a la Entidad de Certificación que finalmente realice la Auditoría de Certificación;** y ello por dos (2) razones:

    - Por requerimientos de la norma ISO/IEC 17065:2012, norma que obliga a todas las Entidades de Certificación del ENS, y en virtud de la cual debe poder evidenciarse una aceptación de la oferta por parte de la persona jurídica que finalmente habrá de ser auditada, no contemplándose la posibilidad de intermediación.

      Existiría un claro 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.

    - 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 correspondiente a la consultoría. Esto podría llegar a materializarse en base a dos (2) lotes separados, uno para consultoría y otro para la Auditoría de Certificación, o dos (2) 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 la Seguridad que persiga la expedición de una Certificación de Conformidad con el ENS.

    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 auditor de la Entidad de Certificación.

38. Seguidamente, se 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) y niveles de seguridad (Bajo, Medio o Alto) en cada dimensión (Disponibilidad, Confidencialidad, Integridad, Autenticidad y Trazabilidad).
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, del servicio que presta y de los recursos tecnológicos (sistemas de información) usados para tal prestación.
13. Relación de entidades que han prestado consultoría de seguridad o 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 CPDs de la organización y localización, indicando si se trata de CPDs propios o se encuentran externalizados, tanto para los CPDs 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).