

**Pliego de prescripciones técnicas para la contratación de los
servicios de consultoría para la adecuación al Esquema Nacional
de Seguridad y de auditoría en el ámbito de
protección de datos personales.**

Código seguro de verificación: B34BB0BFE2FE61134354992C59ED740357F1CE34.

Contenido

Introducción	2
Objeto del contrato	4
Plazo y lugar de ejecución del servicio	4
Desarrollo de los trabajos objeto del servicio	4
Fase 1.- Planificación y organización del proyecto	5
Entregables de esta fase.....	5
Fase 2.- Análisis del entorno y evaluación del cumplimiento	5
Auditoría PDCP	5
Consultoría de adecuamiento ENS	6
Entregables de la auditoría PDCP	7
Entregables de la consultoría de adecuamiento ENS.....	7
Fase 3- Análisis de riesgos.....	7
Entregables de la auditoría PDCP	8
Entregables de la consultoría adecuamiento ENS.....	8
Fase 4.- ENS, elaboración del Plan de mejora de la seguridad	8
Entregables de la consultoría adecuamiento ENS.....	9
Fase 5.- Informe de auditoría PDCP, recomendaciones de seguridad	9
Entregables de la auditoría PDCP	11
Fase 6.- Formación	11
Condiciones para la realización del servicio	11
Planificación, dirección y seguimiento de los trabajos	12
Aceptación del servicio objeto del contrato	13
De las ofertas	13
Anexo A – Cuestionarios: Modelos de documentos	15

INTRODUCCIÓN

1. PROTECCIÓN DE DATOS PERSONALES: El art. 96 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (PDCP),



acoge la necesidad de una auditoría bienal que verifique el cumplimiento de dicho reglamento y de los procedimientos e instrucciones vigentes en materia de seguridad de datos de carácter personal. Además, el día 25 de mayo de 2018 será de aplicación el nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 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. Dado que la última auditoría fue realizada en diciembre de 2016 y que comenzará en breve la aplicación del nuevo Reglamento UE, se hace necesaria realización de una nueva auditoría que compruebe el grado de cumplimiento por parte del Tribunal de los procedimientos y medidas de seguridad exigidos por la citada normativa.

2. ESQUEMA NACIONAL DE SEGURIDAD (ENS): El art. 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, estableció la necesidad de crear un Esquema Nacional de Seguridad, que fue desarrollado por el Real Decreto 2/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Aunque esa Ley 11/2007 ha sido derogada por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC), la importancia del cumplimiento del ENS sigue siendo una constante exigencia legal: por ejemplo, respecto del archivo de documentos (art. 17.3 LPAC), de la validez de las copias electrónicas o en papel (art. 27.3 LPAC), de la remisión el expediente electrónico (art. 70.2 LPAC) o del registro y archivo electrónico (disposición adicional segunda LPAC). Aunque ni la Ley 11/2007 (art. 2) ni la Ley 39/2015 (art. 2) incluyen al Tribunal Constitucional en su ámbito de aplicación, sin embargo, el Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI), viene requiriendo a lo largo de los últimos años de este Tribunal el suministro de una cantidad ingente de datos e informaciones relativas al nivel de cumplimiento del ENS. Como se cree conveniente disponer de los datos y las informaciones requeridas, se hace necesaria la realización de una consultoría que analice el grado de adecuamiento de los sistemas de información del Tribunal al ENS.

3. AUDITORÍA Y CONSULTORÍA: Dado que las tareas a realizar en materia de protección de datos personales y en materia de adecuación al ENS son en gran parte coincidentes, es imprescindible acumular la realización de ambos trabajos en un único proyecto.

OBJETO DEL CONTRATO

Según lo que antecede, el objeto del presente documento lo constituye la contratación de los servicios necesarios para la realización de una auditoría en el Tribunal Constitucional que verifique el nivel de cumplimiento de la legislación de protección de datos personales que comenzará a aplicarse el 25 de mayo de este año, así como de los procedimientos e instrucciones vigentes en materia de seguridad de datos que les afecte; que identifique sus deficiencias y proponga las medidas correctoras o complementarias necesarias.

Igualmente, también es objetivo la contratación de los trabajos necesarios para la realización de una consultoría en el Tribunal Constitucional para la adecuación de todos sus sistemas de información al Esquema Nacional de Seguridad, estableciendo la política de seguridad en la utilización de los medios electrónicos así como los principios básicos y requisitos mínimos que permitan una protección adecuada de la información en el ámbito de la administración electrónica del Tribunal. Como resultado final deberán elaborarse los documentos necesarios, como el Plan de Implantación, la categorización de los Sistemas de Información, Declaración de Aplicabilidad y el Análisis de Riesgos.

PLAZO Y LUGAR DE EJECUCIÓN DEL SERVICIO

El plazo máximo de ejecución del servicio objeto de este contrato será de **dieciséis semanas** desde la reunión de arranque del proyecto tras la comunicación de adjudicación.

El servicio se desarrollará en Madrid, en los locales de la sede del Tribunal Constitucional, calle Doménico Scarlatti, 6 (28003 – Madrid).

DESARROLLO DE LOS TRABAJOS OBJETO DEL SERVICIO

A modo de resumen (más adelante se detallan las fases que se deben contemplar), deberá realizarse un análisis de la situación actual en materia de seguridad de los sistemas de información del Tribunal Constitucional. Aquellos sistemas que traten ficheros automatizados o no, que contengan datos de carácter personal, se analizarán también desde los puntos de vista de la actual normativa en materia de protección de datos con carácter personal incluido el nuevo Reglamento General de Protección de Datos que comenzará a aplicarse el 25 de mayo de este año.

Se deben proponer las medidas correctoras que se estimen oportunas ante situaciones de incumplimiento de la normativa referenciada y/o mejoras que se consideren convenientes.



El personal de la empresa adjudicataria que desarrolle el servicio objeto de esta contratación, actuará, junto con los recursos humanos designados por el Servicio de Informática del Tribunal Constitucional, en cada una de las fases que a continuación se especifican.

Fase 1.- Planificación y organización del proyecto

La planificación, detallada por funcionalidad a realizar, será responsabilidad de la empresa adjudicataria del servicio de forma que se garantice el cumplimiento de los objetivos globales del proyecto. La planificación deberá ser aprobada por el comité de seguimiento del Tribunal Constitucional constituido al efecto y del que formará parte una persona designada por la empresa adjudicataria.

En el plazo de diez días tras la adjudicación, la empresa adjudicataria del servicio deberá entregar un documento en el que se refleje una descripción funcional detallada de los trabajos a desarrollar, que se plasmará en un documento redactado de forma que se interprete con facilidad por usuarios ajenos al sistema, y que será aprobado por el comité de seguimiento del Tribunal Constitucional.

La empresa adjudicataria del servicio entregará, con la documentación anterior, un calendario de detalle de la ejecución del proyecto, sin que en el mismo se puedan establecer plazos que supongan incumplimiento de los plazos previstos en este documento para el desarrollo del conjunto del proyecto ni, en su caso, del posible plazo menor ofrecido por la empresa adjudicataria en la oferta correspondiente.

El Tribunal Constitucional garantizará a la empresa adjudicataria las vías de comunicación con usuarios y actores del sistema, cuando resulte necesario, de tal modo que pueda disponer de la información necesaria para la ejecución del servicio.

Entregables de esta fase.

- Documento con la enumeración y descripción de los trabajos a desarrollar.
- Cronograma de la ejecución del proyecto.

Fase 2.- Análisis del entorno y evaluación del cumplimiento

Auditoría PDCP

Se partirá de los resultados de las anteriores auditorías de seguridad informática realizadas en el Tribunal Constitucional durante los años anteriores con carácter bienal. De forma resumida, a continuación se enumeran los documentos que conforman el marco normativo interno del Tribunal Constitucional en materia de seguridad informática y protección de datos personales:

- Acuerdo de 21 de diciembre de 2006, del Pleno del Tribunal Constitucional, por el que se regulan los ficheros automatizados de datos de carácter personal existentes en el Tribunal (BOE núm. 1, de 1 de enero de 2007).



- Acuerdo de 26 de marzo de 2009, del Pleno del Tribunal Constitucional, que modifica parcialmente el de 21 de diciembre de 2006, por el que se regulan los ficheros automatizados de datos de carácter personal (BOE núm. 86, de 8 de abril).
- Acuerdo de 28 de abril de 2010, del Pleno del Tribunal Constitucional, por el que se modifica parcialmente el de 21 de diciembre de 2006, por el que se regulan los ficheros automatizados de datos de carácter personal (BOE núm. 105, de 30 de abril).
- Acuerdo de 23 de julio de 2015, del Pleno del Tribunal Constitucional, por el que se regula la exclusión de los datos de identidad personal en la publicación de las resoluciones jurisdiccionales (BOE núm. 178, de 27 de julio).
- Instrucción de régimen interior de la Secretaría General del Tribunal Constitucional, de 30 de julio de 2013, sobre medidas de seguridad de los ficheros del Tribunal Constitucional que contienen datos de carácter personal.
- Directrices técnicas que desarrollan la anterior Instrucción de régimen interior.

Para la realización de las operaciones de diagnóstico que se juzguen necesarias podrán utilizarse técnicas, herramientas automáticas y manuales, así como otros medios de prueba, pero deberán ser expresamente autorizados por el Servicio de Informática.

Por evolución de los sistemas de información del Tribunal han podido surgir nuevos ficheros con datos personales para los que se precise su declaración (o registro, según nuevo RGPD), así como confección del documento de seguridad preceptivo y la definición de las medidas de seguridad que le correspondan en función del nivel de seguridad con el que se deba declarar.

Este trabajo de diagnóstico inicial se llevará a cabo, al menos, para los siguientes ámbitos:

- Cumplimiento de la legislación vigente¹ en materia de protección de datos.
- Cumplimiento del nuevo Reglamento General de Protección de Datos.
- Cumplimiento de procedimientos e instrucciones en esta misma materia.
- Análisis de la operativa de seguridad dentro del Servicio de Informática en lo referente a datos personales.

Consultoría de adecuamiento ENS

El inicio del análisis y evaluación del cumplimiento se organizará en las siguientes tareas:

- Análisis del entorno y documentación existente.
- Determinación del inventario de activos.

¹ A la fecha de realización de los trabajos objeto del contrato.

- Valoración de los activos y niveles de seguridad.
- Designación de interlocutores por áreas funcionales.
- Reuniones y requisitos mínimos de seguridad.

A través de un análisis diferencial se detectarán las no conformidades, menores o mayores, de tal forma que se pueda conocer las diferencias entre el modelo de seguridad actual en el Tribunal y el propuesto por el ENS.

Entregables de la auditoría PDCP

Como resultado de esta fase, se entregarán los siguientes documentos:

- Dictamen con la detección de nuevos ficheros o posibilidad de supresión de alguno de los existentes.
- Documento de seguridad de los nuevos ficheros.
- Informe detallado sobre las medidas de seguridad que les sea de aplicación según niveles de seguridad.

Deberá incluir, igualmente, los datos, hechos y/o observaciones en los que se basen los dictámenes y recomendaciones.

Entregables de la consultoría de adecuamiento ENS

- Informe de situación actual a partir de la información aportada por el Servicio de Informática y de la posible realización de entrevistas con el personal encargado de las diversas funciones asociadas a los sistemas de información implicados que determine:
 - Relación de activos
 - Infraestructura tecnológica existente
 - Nivel de criticidad de los Sistemas de Información
 - Identificación de las responsabilidades asociadas al ENS

Fase 3- Análisis de riesgos

Tras conocer el entorno y realizar el análisis diferencial, se realizará un proceso de Análisis de Impacto para cada uno de los sistemas de información identificados.

Este Análisis de riesgos servirá de base para decidir las medidas de protección a adoptar, enriquecidas o matizadas en función de las características del sistema, así como de las exigencias que se puedan derivar del tratamiento de datos de carácter personal de acuerdo a la normativa vigente en esta materia.

Se revisará si las amenazas o vulnerabilidades a los que están expuestos los activos se encuentra mitigadas o no con las medidas de seguridad sobre los servicios que el

Tribunal pueda tener ya implementadas y si es aceptable, o no, el nivel de riesgo residual.

En el análisis se evaluarán las dimensiones de seguridad relevantes en cada Sistema de Información, el nivel de seguridad de cada dimensión identificada, la categoría del Sistema de Información y las medidas de seguridad en los sistemas, tanto organizativa, operativa como técnicamente.

Para los Sistemas de Información que traten datos de carácter personal se matizarán también con respecto a las amenazas o vulnerabilidades que pueden afectar a este ámbito de protección de datos con carácter personal en función del tipo de datos personales contenidos en los ficheros.

La realización del análisis de riesgos se realizará necesariamente mediante la herramienta PILAR, disponible de forma gratuita para las administraciones públicas, para, desde ella, gestionar en el futuro la base de activos del Tribunal. El uso de esta herramienta aportará al Tribunal la ventaja de automatizar parte de la generación de información que se debe facilitar anualmente al Informe del Estado de la Seguridad del Sector Público.

Entregables de la auditoría PDCP

- Informe exhaustivo con los resultados del diagnóstico de la situación actual, con el dictamen sobre la adecuación de las medidas y controles al Reglamento General, identificando sus deficiencias para, en la siguiente fase, proponer las medidas correctoras o complementarias necesarias.

Entregables de la consultoría adecuamiento ENS

- Informe de amenazas, vulnerabilidades e impactos.
- Informe de recomendaciones para la gestión del riesgo, con inclusión de los activos sensibles y actuaciones para delimitar los riesgos asociados a ellos.

Fase 4.- ENS, elaboración del Plan de mejora de la seguridad

Una vez se conozca el nivel de cumplimiento de los principios básicos y los requisitos exigidos por el ENS, se estará en disposición de realizar la selección de las medidas de seguridad que permita alcanzar el adecuado nivel de cumplimiento:

- Marco Organizativo.
- Marco Operacional.
- Medidas de Protección.

Se realizará en esta fase un análisis diferencial con el fin de determinar qué controles, de los existentes en el ENS, ya se encuentran implantados y cuáles no. Como resultado

final se redactará el borrador de la **Declaración de aplicabilidad**, o documento de selección de controles, con los controles ya implementados y aquellos que se consideren necesarios para minimizar el riesgo de los activos para cumplir con el nivel de seguridad deseado.

Esta Declaración de aplicabilidad será revisada por los responsables del Tribunal para dar, como resultado final, el Plan de mejora de la seguridad que se seguirá como objetivo final del proyecto.

Se definirá la **Política de seguridad** de la organización, así como se desarrollarán las normativas de seguridad, que deberán establecer:

- El reparto de responsabilidades para realizar las distintas tareas asociadas a la seguridad.
- Los mecanismos a establecer para la identificación de anomalías.
- Los sistemas de resolución de las anomalías detectadas.
- La redacción de instrucciones específicas para los usuarios y responsables de los sistemas de información.
- La redacción de documentos tipo para el registro y control de las incidencias de seguridad y los procedimientos asociados.

Entregables de la consultoría adecuamiento ENS

- Política de seguridad de la organización
- Normativas de seguridad que desarrollen esa política; es decir, puntos ya enumerados en el anterior apartado.
- Borrador de la Declaración de aplicabilidad

Fase 5.- Informe de auditoría PDCP, recomendaciones de seguridad

En esta fase se expondrán las medidas que deberá adoptar el Tribunal Constitucional para mantener una adecuada protección de los datos de carácter personal y su tratamiento, siempre con cumplimiento de la legislación y la normativa vigente así como del nuevo Reglamento General de Protección de Datos.

Esta fase se compondrá de varios apartados, entre los que se detallan los siguientes:

Adecuación al nuevo Reglamento General de Protección de Datos (UE).

El objetivo es que el Tribunal Constitucional cumpla, en la mayor medida posible, lo exigido en el nuevo Reglamento General desde el inicio de su aplicación.

Para ello, el adjudicatario deberá realizar las siguientes tareas:

- Revisión y adaptación de los procedimientos técnicos y organizativos. Se deberá evaluar el grado de adecuación de los procedimientos existentes relacionados con el Reglamento General desde el punto de vista organizativo. En especial, se revisarán, crearán y adaptarán aquellos procedimientos generales que

establece el marco para la aplicación de las medidas de seguridad descritas en el Reglamento.

- Revisión de las medidas de seguridad exigidas en el Reglamento y recomendaciones para su adaptación. Se deberá realizar una revisión de las medidas particulares de seguridad que se hayan implantado para llevar a cabo las políticas de seguridad, en cada sistema de información. En concreto, se analizarán aquellas medidas técnicas específicas que debieran estar implantadas sobre los ficheros de carácter personal y sistemas que los tratan, de acuerdo con el nivel de seguridad que le corresponde.
- Se procederá a realizar el informe de auditoría, que debe contemplar un plan de acción que defina las medidas correctoras necesarias, aún no realizadas, para la adecuación al Reglamento General.

Adecuación a la Ley Orgánica de Protección de Datos de Carácter Personal.

Se pretende que el Tribunal Constitucional siga cumpliendo con la legislación vigente en materia de protección de datos de carácter personal, principalmente la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre.

Para ello, el adjudicatario deberá realizar las siguientes tareas:

- Revisión, corrección y perfeccionamiento de los documentos de seguridad de cada uno de los ficheros inventariados, de acuerdo con lo establecido en el Reglamento de Medidas de Seguridad.
- Revisión y adaptación de los procedimientos técnicos y organizativos. Se deberá evaluar el grado de adecuación de los procedimientos existentes relacionados con el Reglamento de Medidas de Seguridad desde el punto de vista organizativo. En especial, se revisarán, crearán y adaptarán aquellos procedimientos generales que establece el marco para la aplicación de las medidas de seguridad descritas en el Reglamento de medidas de seguridad.
- Se procederá a realizar el informe de auditoría, que debe contemplar un plan de acción que defina las medidas correctoras necesarias, aún no realizadas, para la adecuación al Reglamento General UE.

Marco normativo de seguridad informática.

Análisis del marco normativo de seguridad informática vigente en el Tribunal y conclusiones sobre su nivel de cumplimiento; así como propuesta de mejora o actualización.

Entregables de la auditoría PDCP

Se generarán, al menos, los siguientes entregables referentes a los apartados hasta aquí enumerados:

- a) *Adecuación al nuevo Reglamento General de Protección de Datos (UE)*
 - Enumeración y descripción de todas las adaptaciones necesarias de los procedimientos técnicos y organizativos existentes, así como los de nueva creación, para cumplir el marco fijado por el Reglamento General.
- b) *Adecuación a la Ley Orgánica de protección de datos*
 - Revisión, y generación si procede, de normativa interna y guía de usuarios integrada con el marco normativo.
 - Revisión, y actualización si procede, del documento de seguridad.
 - Documento de mejora de los procesos internos del Tribunal Constitucional cuando los usuarios accedan, modifiquen y cancelen sus datos.
 - Propuesta de creación de nuevos ficheros o supresión de los existentes así como generación del documento de seguridad correspondiente.
- c) *Marco normativo de seguridad informática*
 - Políticas y directrices de seguridad de la información
 - Procedimientos de seguridad
 - Propuesta de modificaciones para mejora y/o actualización del marco.

Fase 6.- Formación

Se elaborará y realizará un plan de formación y sensibilización para el personal implicado en los procedimientos afectados por el ENS. Se tendrá en cuenta, de forma especial, la formación especializada a recibir por el personal técnico del Servicio de Informática que gestionará el Sistema de Gestión de la Seguridad y que velará, a partir de los resultados de esta consultoría, por el seguimiento de su cumplimiento y su actualización en el futuro.

CONDICIONES PARA LA REALIZACIÓN DEL SERVICIO



El personal de la empresa adjudicataria que desarrolle el servicio objeto de esta contratación, actuará, junto con los recursos humanos designados por el Servicio de Informática del Tribunal Constitucional, en cada una de las fases que a continuación se especifican.

Para la realización de las operaciones de diagnóstico y análisis que se juzguen necesarias podrán utilizarse técnicas, herramientas automáticas y manuales, así como otros medios de prueba, pero deberán ser expresamente autorizados por el Servicio de Informática. Recordar aquí la mención hecha, como de necesaria utilización, a la herramienta PILAR en el apartado de la “Fase 3- Análisis de riesgos”.

Para la realización de los trabajos propuestos se seguirán las pautas establecidas en las guías incluidas en la Serie CCN-STIC-800, en las que se establecen las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el ESN, y Guía CCN-STIC-410, “Análisis de riesgos en sistemas de la administración”.

Deberán incluirse los datos, hechos y/o observaciones en los que se basen los dictámenes y recomendaciones.

La empresa adjudicataria, antes de formalizar la recepción del servicio, entregará dos ejemplares en papel de toda la documentación generada, así como en versión electrónica (CD-ROM o pendrive) para su tratamiento en formatos Microsoft Office y en PDF.

Asimismo, como colofón de los trabajos a realizar se presentará un informe ejecutivo al personal directivo del Tribunal. En él se resumirán las acciones llevadas a cabo durante el desarrollo del proyecto y reflejará los principales aspectos a tener en cuenta en el desarrollo del Plan de mejora de la seguridad. En la presentación de los resultados se intentará diferenciar claramente los ámbitos del Esquema Nacional de Seguridad y del cumplimiento de normativa en materia de protección de datos de carácter personal.

PLANIFICACIÓN, DIRECCIÓN Y SEGUIMIENTO DE LOS TRABAJOS

Corresponde al Tribunal Constitucional la supervisión y dirección de los trabajos, proponer las modificaciones que convenga introducir o, en su caso, proponer la suspensión de los trabajos si existiese causa suficientemente motivada.

El Tribunal Constitucional designará un responsable de proyecto, cuya principal función será velar por el cumplimiento de los trabajos exigidos y ofertados, así como asegurar las vías de comunicación con los usuarios del Tribunal y los recursos materiales que se estimen necesarias por el adjudicatario.

El seguimiento y control de los trabajos se efectuará sobre las siguientes bases:

- Seguimiento continuo entre el responsable del equipo de trabajo por parte del adjudicatario y del responsable del proyecto por parte del Tribunal.



- El Tribunal Constitucional podrá determinar los procedimientos y herramientas a utilizar para poder llevar a cabo la planificación, seguimiento y control de los trabajos.
- Reuniones de seguimiento y revisiones técnicas, con la periodicidad oportuna, del responsable del equipo de trabajo por parte del adjudicatario, y del responsable del proyecto del Tribunal o persona en quien delegue, al objeto de revisar el grado de cumplimiento de los objetivos.
- Tras las revisiones técnicas, de las que el adjudicatario levantará acta, el responsable del proyecto del Tribunal podrá rechazar en todo o en parte los trabajos realizados, en la medida que no respondan a lo especificado en las reuniones de planificación o no superasen los controles de calidad acordados.

ACEPTACIÓN DEL SERVICIO OBJETO DEL CONTRATO

Para la aceptación por parte del Tribunal Constitucional de los documentos, pruebas y aprobación final del proyecto, se seguirá el siguiente procedimiento:

- *Documentos:* Los documentos de proyecto serán entregados al Servicio de Informática del Tribunal Constitucional para su revisión y posterior aprobación por el responsable del proyecto.
- *Aceptación final del proyecto:* El responsable del proyecto del Tribunal será el responsable de certificar la idoneidad de los trabajos entregados por la empresa adjudicataria y su adecuación a las necesidades de los gestores.

DE LAS OFERTAS

Se debe concretar en la oferta el equipo humano que desarrollará los trabajos; independientemente del desarrollo que en su descripción quiera realizar la empresa a través de su oferta, las empresas licitadoras deberán cumplimentar en su totalidad los cuestionarios que se adjuntan como Anexo A denominado "Cuestionarios".

La no cumplimentación de estos cuestionarios, la omisión de datos o la comprobación fehaciente de datos que desvirtúen la realidad, supondrá la exclusión de la oferta.

Se identificará claramente al Responsable-Coordenador de dicho equipo por parte del adjudicatario. Este Responsable deberá tener acreditada formación y experiencia en auditoría de sistemas de información, a través de certificaciones reconocidas a nivel nacional e internacional, o bien a través de experiencia verificable y evidenciada de al menos cuatro años en auditoría de tecnologías de la información; conocimientos de seguridad y gestión de riesgos (certificación y experiencia probada de al menos cuatro años); conocimientos de la legislación aplicable a la protección de datos de carácter personal.

El resto del equipo puede no cumplir en su totalidad con los requisitos para el Responsable-Coordinador; no obstante, deberá tener alguna preparación previa y acreditada tanto en seguridad como en auditoría de los sistemas de información, dependiendo de, y en consonancia, con las responsabilidades asignadas en el proyecto.

ANEXO A – CUESTIONARIOS: MODELOS DE DOCUMENTOS

A.1. Cuestionario de empresa

1. Identificación oferta:				
2. Empresa:				
3. Nacionalidad:				
4. Fecha Implantación España:				
5. Persona de contacto:				
Apellidos	Nombre	Cargo	Teléfono	Fax
6. Número empleados consultoría de seguridad:				
7. % empleados fijos:				
Categoría			Número	
8. Certificados de Garantía de Calidad:				

A.2. Cuestionario de personal²

1. Identificación oferta:	
2. Empresa licitante:	
3. Categoría ofertada:	
4. Apellidos y nombre:	

5. Antigüedad en empresa, antigüedad en categoría y experiencia TIC

Empresa	Categoría	Fecha alta	Fecha baja	Meses	Actividad Informática

6. Titulación Académica/Certificación

Título académico/Certificación	Centro	Años	Fecha	TIC
				(sí/no)
				(si/no)

A.3. Cuestionario de prestaciones superiores o complementarias a las solicitadas

Identificación oferta:		
Empresa licitante:		
Prestación superior	Descripción de la prestación	Valor estimado

² Una ficha “Cuestionario de personal” por cada integrante-categoría del equipo de trabajo propuesto.

Normas para cumplimentarlos

A.1.- Cuestionario de empresa

Generales

Cada empresa licitante cumplimentará un cuestionario de empresa según las instrucciones que se dan a continuación.

Específicas

- Nombre con el que se encuentra registrada la empresa.
- Plantilla total de la empresa a 31/12/2017.
- Número de empleados dedicados a funciones de consultoría de seguridad.
- Se indicarán los certificados de garantía de calidad que posee la empresa.

A.2.- Cuestionario de personal

Generales

La empresa licitante deberá aportar un cuestionario relleno para cada una de las personas que se proponen para prestar servicios en el Tribunal Constitucional.

Específicas

- Se ordenará cronológicamente el historial contractual y profesional de la persona, especificando la empresa, categoría profesional, fechas de alta y baja en formato dd/mm/aaaa, la permanencia en meses completos correspondientes a las fechas anteriores, así como una explicación sucinta de las actividades desarrolladas.
- Se relacionarán los cursos de formación informática recibidos por la persona siempre que la fecha de inicio del curso sea posterior al 01/1/2008. Se indicarán el nombre del curso, número de horas, la empresa o centro que lo impartió, así como la fecha de inicio en formato dd/mm/aaaa. Los cursos se desglosarán teniendo en cuenta si están relacionados o no con los trabajos a desarrollar y se detallarán en el apartado correspondiente.
- Se especificará la titulación académica, centro que la expidió, duración oficial en años de los estudios cursados para obtener dicha titulación, fecha en el que se expidió la titulación y si la misma está relacionada o no con las tecnologías de la información y las comunicaciones.

A.3.- Cuestionario de mejoras de prestaciones o complementarias a las solicitadas

La empresa licitante cumplimentará este cuestionario si la oferta contempla mejoras relacionadas con el objeto del contrato.