EUSKO JAURLARITZA GOBIERNO VASCO

GOBERNANTZA PUBLIKO ETA AUTOGOBERNU SAILA
Informazioaren eta Komunikazioarean Teknologien Zuzendaritza

DEPARTAMENTO DE GOBERNANZA PÚBLICA Y AUTOGOBIERNO
Dirección de Tecnologías de la Información y la Comunicación

Expediente KM/2022/013

Asistencia técnica para la constitución de las Oficinas Técnicas de apoyo a la actividad de la DTIC en el ámbito de la seguridad

Pliego de Bases Técnicas

Donostia - San Sebastian, 1 – 01010 VITORIA-GASTEIZ
Tef. 945 01 85 22 – Fax 945 01 87 06

Índice

Objeto 3
Descripción de los lotes 5
Tareas específicas a realizar en cada lote 10
Entregables 18
Propiedad Intelectual 20
Seguridad y Confidencialidad 21
Calidad, Control y Seguimiento 22
Equipo de Trabajo 24
Estructura de las ofertas 27
Plazo de ejecución y presupuesto 28

Objeto

Este expediente tiene como objeto contratar los servicios de asistencia técnica necesaria para constituir las Oficinas Técnicas de apoyo a la actividad de la DTIC (Dirección de Tecnologías de la Información y la Comunicación) relacionadas con el ámbito de la seguridad de los sistemas de información. Este objeto se divide en varios lotes, en este caso, en TRES (3), uno por cada Oficina Técnica, necesaria para el desenvolvimiento de las tareas concretas descritas más adelante.

El presente Pliego de Bases Técnicas (PBT) describe, por tanto, el alcance, los objetivos y/o requisitos a cumplir por la/s empresa/s adjudicataria/s.

Las principales tareas o funciones que deberá realizar cada empresa adjudicataria serán las siguientes:

Común para todas las Oficinas Técnicas

Se trata de la activación de cada Secretaría Técnica, es decir, su creación, monitorización y mejora, en función del objeto específico de cada lote, según se explicará más adelante. Comprende las siguientes tareas generales:

#	Tareas generales
1	Activación de la Secretaría Técnica, definiendo un Plan de actuaciones
2	Revisar los temas a trabajar, sus objetivos y alcance
3	Medir la eficacia de las decisiones adoptadas
4	Registrar acciones y eventos
5	Establecer mecanismos de participación
6	Asegurar la adecuada coordinación
7	Garantizar que las reuniones sean productivas
8	Implantar mejoras y acciones correctivas, comprobando su eficacia
9	Asesoramiento multidisciplinar
10	Apoyo al desarrollo de políticas, guías y normativas
11	Formación que sea requerida para una adecuada transferencia del conocimiento
12	Asesoría para el cumplimiento legal y normativo

Las tareas a realizar, respecto a las **reuniones**, tanto periódicas como extraordinarias, serán las siguientes:

#	Tareas en reuniones
1	Preparación de las reuniones: proponer el Orden del Día, asesorar en aspectos técnicos respecto a dicho Orden del Día y aportar la visión organizativa
2	Participación activa en las mismas (salvo indicación en contrario)
3	A la finalización de las reuniones: asesorar en aspectos técnicos en función de lo acontecido en la reunión y realizar el Acta de la reunión
4	Otras tareas asociadas a las reuniones que se consideren oportunas
5	Realizar un análisis y estudio de los temas tratados en las reuniones y ver cómo se pueden interrelacionar con otros ámbitos, y el impacto que puedan suponer
6	Determinar indicadores de evaluación y seguimiento
7	Realizar informes y registros
8	Proponer Cuadros de Mando

Cada empresa adjudicataria deberá reportar a la DTIC, **según los hitos que se establezcan** o, al menos, **trimestralmente,** un resumen de las tareas realizadas para cada hito o durante los tres meses anteriores, así como de aquellos aspectos que se consideren significativos.

Los entregables son los relacionados con las tareas descritas anteriormente.

La gestión de la documentación asociada a los trabajos de este servicio por parte del adjudicatario se aportará a través de la herramienta colaborativa SharePoint, gestionada por la DTIC.

Toda la documentación que se genere como consecuencia de este trabajo (Actas de reuniones, documentos de trabajo, borradores…) deberá ser entregada a la DTIC en soporte ofimático, estando toda esa documentación en formato compatible con las herramientas y estándares establecidos.

Descripción de los lotes

Este expediente se divide en los siguientes LOTES:

1) Oficina Técnica de seguridad GureSeK
2) Oficina Técnica para realizar auditorías
3) Oficina Técnica para la certificación ENS

Los cuales pasamos a detallar a continuación.

Lote 1. Oficina Técnica de seguridad GureSeK

Como parte de la Administración Pública, la Administración General (Departamentos) y Organismos Autónomos del Gobierno Vasco están comprendidos dentro del ámbito de aplicación que se establece en el Real Decreto 3/2010 que regula el Esquema Nacional de Seguridad (ENS) para sus servicios de Administración Electrónica, por lo que todas las actividades y servicios comprendidos en el presente pliego, y para este lote, deberán estar orientadas a su cumplimiento, siendo la empresa adjudicataria consciente de este término, por lo que este Pliego tiene por objeto final el garantizar la adecuación y cumplimiento de los sistemas de información al ENS.

El objeto de la contratación de este Lote es, por un lado, proporcionar el servicio de **Asistencia Técnica** (soporte especializado, asesoramiento y apoyo instrumental) a los Comités y roles creados en la estructura organizativa y asignación de roles de seguridad para la Administración Electrónica del Gobierno Vasco en el Acuerdo de Consejo de Gobierno (ACG), esto es, el actual Comité de Seguridad y Privacidad Corporativa, Comité Técnico de Seguridad, y roles asociados, y, por otro lado, realizar las labores de gestión asociadas a la **Oficina Técnica** de Seguridad y el proceso GureSeK (implantación, monitorización y mejora).

a) Tareas de Auditoria interna para preparación de una auditoria externa para lograr certificación ENS.

Se deberán de finalizar las tareas acometidas en un expediente anterior (expediente DTIC-03-2021 que tenía por objeto realizar las tareas de preparación para solventar una auditoria que consiga la certificación de los sistemas de información de EJ-GV y OOAA. Dichas tareas consistieron en:

- Actualización del Análisis de Riesgos de los Sistemas de Información de EJ-GV y OOAA:
- Reuniones de proceso sobre Global Suite para cada S. de I.
- Mapeo de aplicaciones. Proceso en Global Suite.
- Integrar el BIA (Business Impact Analysis) sobre el Análisis de Riesgos en la herramienta GlobalSuite, exigible para certificar el nivel medio de seguridad de los Servicios, y que permita determinar:
  - Los requisitos de disponibilidad de cada servicio medidos como el impacto de una interrupción durante un cierto periodo de tiempo.
  - Los elementos que son críticos para la prestación de cada servicio.

Tareas a realizar en este ámbito, se detallan en el apartado «Tareas a realizar».

b) Asistencia Técnica a los Comités

Las reuniones de los Comités de Seguridad son ordinarias (una reunión bianual para el Comité Técnico de Seguridad, y una reunión anual para el Comité de Seguridad y Privacidad Corporativa); asimismo, el presidente de ambos Comités puede convocar cuantas reuniones extraordinarias considere oportuno.

Las tareas a realizar en este ámbito, se detallan en el apartado *«Tareas a realizar»*.

c) Secretaría Técnica de Seguridad

Se debe tener en cuenta que esta parte es la que mayor peso tiene con respecto a la totalidad de las tareas asociadas a este lote.

Las tareas se corresponden con la activación (implantación, monitorización y mejora) del proceso de seguridad GureSeK, cuyo objetivo es tener un sistema gestionado y medible, teniendo como fin último el publicar la conformidad con el ENS. Las tareas concretas a realizar en este ámbito, se detallan en el apartado *«Tareas a realizar»*.

El alcance de la propuesta viene condicionado por los servicios electrónicos prestados por la Administración General (Departamentos) y Organismos Autónomos del Gobierno Vasco a la ciudadanía, esto es, los proporcionados por la Plataforma PLATEA, teniendo en cuenta que el Encargado del Tratamiento de esta plataforma tecnológica es la sociedad pública EJIE, que participa en el desarrollo y administración técnica de los servicios y los sistemas que integran dicha plataforma.

Lote 2. Oficina Técnica para realizar auditorías

Esta Oficina Técnica tiene como objetivo realizar auditorías relacionadas con el cumplimiento de la normativa sobre protección de datos personales (LOPD-GDD, RGPD…) y aspectos relacionados con la Seguridad.

La Unión Europea ha promovido un Reglamento General de Protección de Datos (RGPD) realizada con el objetivo de garantizar unos estándares de protección de datos elevados y adaptados a la realidad digital del mundo actual y que se aplica en todos los países miembros de la Unión Europea desde el pasado 25 de mayo de 2018 —Reglamento (UE) 2016/679—.

En alineamiento con dicho RGPD, el Gobierno Vasco ha ejecutado acciones para adecuarse a la nueva situación creada, y para ello se ha dotado de una norma jurídica que organiza la seguridad de los datos personales de la Comunidad Autónoma del País Vasco: «*Acuerdo de Consejo de Gobierno, de 19 de junio de 2018, por el que se aprueba la estructura organizativa y asignación de roles para la protección de datos personales tratados por la Administración Pública de la Comunidad Autónoma de Euskadi*».

Por ello, y a fin de garantizar que todos los Departamentos y Organismos Autónomos del Gobierno Vasco cumplan con lo establecido en el RGPD y LOPD-GDD, se pretende la activación de una Oficina Técnica encargada de realizar, a petición de los Responsables de las Medidas de Privacidad de los Departamentos y OO.AA., las auditorias en los tratamientos que estimen oportunos.

La Oficina Técnica será la responsable de realizar las gestiones con los Responsables de las Medidas de Privacidad de los distintos Departamentos y OO.AA. a fin de ofrecer sus servicios para realizar auditorías de cumplimiento del RGPD y LOPD-GDD, y favorecer así que dichos Responsables puedan demandar las auditorias que interese realizar.

Lote 3. Oficina Técnica para la certificación ENS

El Objetivo de esta contratación es una empresa **acreditada por el el Esquema Nacional de Seguridad (ENS)** para certificar los sistemas de Información de EJ-GV y OOAA, categorizados en **nivel Medio**. En definitiva, el objeto del contrato es la realización de una Auditoría de Certificación de los sistemas de información de EJ-GV y OOAA, conforme a lo dispuesto en el RD 3/2010, de 8 de enero, por el que se regula el ENS y normativa de desarrollo, para dar cobertura a los requisitos normativos referentes a la auditoría de seguridad recogidos en el art. 34 y Anexo III del ENS.

El alcance que se deberá auditar:

1. Sistemas de información: 71 sistemas
2. Servicios: 730 servicios (dato aproximado). El catálogo de servicios esta publicado en la Dirección de atención a la Ciudadanía y Servicios Digitales.
3. Número de sedes o ubicaciones donde se encuentran los sistemas a certificar: 3

Los medios para lograr la certificación del ENS son los especificados en:

https://ens.ccn.cni.es/es/docman/documentos-publicos/informes-cocens/372-ccn-cert-ic-02-20-guia-contratacion-auditorias/file

Tareas específicas a realizar en cada lote

A continuación, se definen las tareas y/o funciones que deberá asumir la empresa que resulte adjudicataria del expediente (en función del lote o lotes a los que le haya sido adjudicado), así como los recursos que serían necesarios, la dedicación estimada y los productos finales a entregar. La empresa que lleve a cabo dichas tareas actuará en todo momento bajo la supervisión directa de la Dirección de Tecnologías de la Información y la Comunicación (DTIC), o de aquellas personas que ésta establezca.

Las principales tareas o funciones específicas que deberá realizar la empresa adjudicataria en cada uno de los lotes que le hayan sido asignados serán las siguientes:

Lote 1: Oficina Técnica de seguridad GureSeK

Las tareas a realizar, respecto al **Comité de Seguridad y Privacidad Corporativa**, son el apoyo y asesoramiento al Comité en las siguientes áreas:

#	Áreas
1	Las funciones de los roles de Responsable de la Seguridad y Responsable de los Sistemas (Director de la DTIC en ambos casos) en las cuestiones relacionadas con la seguridad de la Administración Electrónica
2	La resolución de conflictos que puedan aparecer en torno a la seguridad entre los diferentes afectados por la Administración Electrónica (Departamentos, Organismo Autónomos y EJIE)
3	Los niveles de seguridad aplicables
4	La creación de los órganos de trabajo apropiados para impulsar el desarrollo de la seguridad en la Administración Electrónica
5	Documentos que se deberán aprobar asociados a los entregables obtenidos en los procesos de los planes de adecuación y ejecución
6	Otras tareas asociadas al apoyo al Comité de Seguridad y Privacidad Corporativa que se consideren oportunas

De forma análoga, las tareas a realizar, respecto al **Comité Técnico de Seguridad**, son las siguientes:

#	Áreas	
1	Realizar un análisis y estudio de los temas tratados en las reuniones y ver cómo se pueden interrelacionar los dos comités y el impacto en el ámbito de la seguridad de la Administración Electrónica	
2	Apoyo y asistencia en los siguientes temas:	La información sobre el estado de la seguridad que el Comité Técnico debe proporcionar al Comité Corporativo
		La promoción de la mejora del proceso GureSeK
		La elaboración de la estrategia de evolución de la seguridad en el Gobierno Vasco
		La coordinación de los esfuerzos de todos los participantes e implicados en la Administración Electrónica en materia de seguridad de la información
		La revisión periódica y promoción de la actualización de la Política de Seguridad y las Normativas de Seguridad definidas por el Gobierno Vasco
		La definición de los requisitos de formación y cualificación de administradores, operadores y usuarios de la Administración Electrónica desde el punto de vista de la seguridad
		El análisis y gestión de riesgos de seguridad de la Administración Electrónica
		La monitorización del desempeño de los procesos de gestión de incidentes de seguridad
		La realización del programa de auditorías
		Priorización de las actuaciones en materia de seguridad
		La aplicación de las medidas de carácter no técnico que se definan
		Los conflictos en materia de seguridad que puedan aparecer entre los diferentes responsables y departamentos u organismos autónomos
		Documentos que se deberán aprobar asociados a los entregables obtenidos en los procesos de los planes de adecuación y ejecución
		Puesta en marcha de los mecanismos de automatización de GureSeK
3	Realizar tareas para dinamizar el Comité GureSeK, que sea participativo y asignarle tareas (involucrar al Comité GureSeK en la seguridad de una manera activa)	
4	Otras tareas asociadas al apoyo al Comité Técnico de Seguridad que se consideren oportunas	

Otras tareas para ambos Comités:

#	Áreas
1	Realización de acciones de formación avanzada, si se considerase oportuno, a las personas componentes de ambos Comités, así como el apoyo y asesoramiento en la realización de los planes de formación y difusión, si bien, **la articulación del programa de formación en materia de seguridad de la información en los departamentos y organismos autónomos del Gobierno Vasco se debe de llevar a cabo a través del Instituto Vasco de Administración Pública (IVAP), y debe formar parte del programa de formación transversal de dicho Organismo, por lo que la impartición de formación reglada no forma parte de las tareas de este Pliego**
2	Apoyar y asesorar respecto a los cambios normativos relacionados con la seguridad de la Administración Electrónica
3	**Apoyo y asesoramiento** para cumplir con el artículo 35 del ENS, que dice que «*El Comité Sectorial de Administración Electrónica articulará los procedimientos necesarios para conocer regularmente el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere el presente real decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las Administraciones públicas*», en la cumplimentación de los indicadores solicitados a la Administraciones Públicas para evaluar el estado de la seguridad a través del **proyecto INES** (Informe Nacional del Estado de Seguridad), al objeto de realizar la notificación legal sobre el grado de adecuación
4	Apoyo y asesoramiento en el cumplimiento de las instrucciones técnicas de seguridad asociadas al ENS (presentes y futuras)
5	Apoyo y asesoramiento en el **proceso de certificación (declaración y certificación de conformidad con el ENS)**
6	Apoyo y asesoramiento en la adecuación a las modificaciones, si las hubiera, sobre el ENS. Cumplir con las obligaciones marcadas por el ENS**. Y entre otras, la Auditoría correspondiente al 2022**
7	Apoyo en la implantación de la herramienta de automatización, con capacidad multi-organización, del proceso GureSeK

En referencia al SGSI GureSeK, las tareas previstas que deberán llevarse a cabo son las siguientes:

#	Tareas
1	Monitorización y mejora: revisar el SGSI, medir eficacia de los controles, revisar riesgos residuales, realizar auditorías internas del SGSI, registrar acciones y eventos, e implantar mejoras y acciones correctivas, comprobando su eficacia
2	Revisar GureSeK, sus objetivos y alcance (realización de las tareas propias de GureSeK en función de la definición realizada)
3	Revisar los roles y responsabilidades que intervienen en dicho Sistema de Gestión (GureSeK)
4	Describir los principales componentes de GureSeK (tarea implícita dentro de la activación del proceso GureSeK)
5	Establecer los mecanismos de participación en GureSeK de los diferentes actores tanto del Gobierno Vasco como de EJIE
6	Garantizar que el proceso de gestión de la seguridad GureSeK se aplica en todos los ámbitos en los que sea necesario
7	Asegurar la adecuada coordinación entre el proceso GureSeK y el SGSI de EJIE, de modo que la participación de más de una organización no provoque mermas en la eficacia y eficiencia de las medidas de seguridad, es decir, existencia de un SGSI multi-organización
8	Revisión y control del programa de mantenimiento de GureSeK

En referencia a tareas de Auditoria de preparación de certificación ENS, son las siguientes:

#	Tareas
1	Actualización del Análisis de Riesgos
1.1	Completar las reuniones de identificación y valoración de servicios electrónicos con cada uno de los departamentos y organismos autónomos de Gobierno Vasco
1.2	Completar sobre la plataforma GlobalSuite el alta de todos los activos y las valoraciones no incorporadas hasta la fecha
1.3	Completar la identificación de las aplicaciones que soportan cada uno de los servicios electrónicos de cada uno de los departamentos y organismos autónomos de Gobierno Vasco
1.4	Completar el mapeo de las aplicaciones con los sistemas de información identificados en la plataforma GlobalSuite
2	Actualización del BIA
2.1	Completar las reuniones de valoración del impacto de los servicios electrónicos en función del tiempo con cada uno de los departamentos de EJ-GV y OOAA
2.2	Completar sobre la plataforma GlobalSuite las valoraciones no incorporadas hasta la fecha
3	Desarrollo final de las normas y procedimientos de seguridad de GureSeK aplicables a: • Análisis de riesgos (op.pl.1) • Adquisición de nuevos componentes (op.pl.3) • Análisis de impacto (op.cont.1) • Sistema de métricas (op.mon.2) • Deberes y obligaciones (mp.per.2) • Concienciación (mp.per.3) • Formación (mp.per.4) • Etiquetado de soportes de información (mp.si.1) • Limpieza de documentos (mp.info.6)
4	Revisión y ajuste final de todos los elementos que forman parte del proceso GureSeK
5	Despliegue del Proceso GureSeK:
5.1	Llevar a cabo una sesión con cada uno de los departamentos y organismos autónomos de Gobierno Vasco para la articulación de las normas y procedimientos de seguridad aplicables individualmente por cada departamento u organismo autónomo
5.2	Realizar el seguimiento de los mecanismos definidos para la articulación de las normas y procedimientos de seguridad aplicables individualmente por cada departamento u organismo autónomo
6	Auditoría interna del Proceso GureSeK
7	Soporte al desarrollo del Plan de Acciones Correctivas derivado de la auditoría interna
8	Soporte para la ejecución del Plan de Acciones Correctivas derivado de la auditoría interna
9	Asistencia durante la auditoría externa de certificación ENS
10	Soporte al desarrollo del Plan de Acciones Correctivas derivado de la auditoría externa
11	Soporte para la ejecución del Plan de Acciones Correctivas derivado de la auditoría externa

Otras tareas asociadas:

#	Otras tareas asociadas
1	Asesoramiento y apoyo en la ejecución de las medidas correctoras asociadas al Análisis de Riesgos realizado: (puntos 1.1, 1.2 y 1.3)
1.1	• Diseñar, elaborar e implantar un proceso formal de autorizaciones (medida organizativa [org.4] del anexo II del ENS) • Identificación de amenazas y vulnerabilidades (disponer de un catálogo de amenazas exacto) • Revisión de la arquitectura de seguridad; relación con respecto a la adquisición de nuevos componentes • Relación entre la adquisición de nuevos componentes y el análisis de riesgos • Revisión de la gestión de los derechos de acceso • Estudio de la utilización del doble factor de identificación en los mecanismos de autenticación y de la disponibilidad de la información sobre el último acceso válido establecido por la persona usuaria
1.2	• Revisión de la gestión de cambios y gestión de incidentes ([op.exp.5] y [op.exp.7] del anexo II del ENS) • Estudio del registro de actividad de las personas usuarias en el sistema y que se disponga de un sistema automático de recolección de registros y correlación de eventos • Revisión de la gestión diaria del sistema (medida [op.ext.2] del anexo II del ENS) • Revisión y mejora del sistema de métricas: datos como el tiempo empleado para cerrar el 50% de los incidentes y tiempo empleado para cerrar el 90% de los incidentes • Identificación de las personas: revisión del mecanismo de control • Caracterización del puesto de trabajo: normativa para definir responsabilidades y requisitos • Protección de equipos portátiles: cancelación de sesiones abiertas • Respecto a la autenticidad e integridad, establecer las exigencias altas para las claves concertadas en cuanto a su calidad respecto a ataques de adivinación, diccionario o fuerza bruta
1.3	• Estudio del empleo de dispositivos hardware en el establecimiento y utilización de la red privada virtual • Estudio etiquetado de los soportes de información (registros de entrada y salida) • Estudio del empleo de mecanismos de cifrado para los dispositivos removibles • Estudio de las medidas de protección [mp.sw.1] desarrollo de aplicaciones y [mp.sw.2] aceptación y puesta en servicio: uso de metodologías de desarrollo seguro, control y revisión del código fuente • Limpieza de documentos: establecer normativa, sobre todo respecto a la publicación de documentos en la web www.euskadi.eus • Estudio de la protección frente a los ataques por denegación de servicio
2	Asesoramiento y apoyo en la ejecución de las medidas correctoras asociadas a la auditoría ENS realizada
3	Formación que le sea requerida al adjudicatario para una adecuada transferencia del conocimiento
4	Servicios de asesoría para el cumplimiento legal y normativo (ENS, RGPD…) Implicaciones y valoración del nuevo Reglamento Europeo de Protección de Datos (RGPD) Implantar las relaciones que se puedan establecer entre el ENS y el RGPD

Lote 2: Oficina Técnica para realizar auditorías

El alcance de cada auditoría demandada por los Departamentos u Organismos Autónomos del Gobierno Vasco consistirá en la revisión y verificación del grado de cumplimiento de los principios legales de protección de datos durante su tratamiento, según el siguiente decálogo:

#	Principios legales de protección de datos
1	Licitud (base jurídica) de los tratamientos de datos
2	Lealtad y transparencia con las personas titulares de los datos
3	Limitación de la finalidad del tratamiento y usos ulteriores de los datos
4	Minimización de datos
5	Exactitud de los datos
6	Limitación del plazo de conservación de los datos
7	Seguridad de los datos (análisis de riesgos, medidas y política de seguridad)
8	Intervención de las personas titulares de los datos (ejercicio de los derechos de protección de datos)
9	Responsabilidad activa (registro de actividades de tratamiento, evaluación de impacto sobre la protección de datos, persona delegada de protección de datos, procedimiento de gestión y notificación de violaciones de la seguridad de los datos)
10	Protección de datos desde el diseño y por defecto

Las tareas a realizar en cada auditoría serán las siguientes:

#	Tareas
1	Presentar el plan de trabajo previsto: acción informativa para los interlocutores que vayan a participar en la auditoría, para explicarles los aspectos más relevantes del trabajo, qué es lo que se va a hacer y cómo, así como cuál será el carácter de su intervención
2	Obtener un conocimiento genérico de la organización que permita la preparación del programa de trabajo en el que se detallen las cuestiones relativas al desarrollo de la auditoría
3	Contactar con la oficina de la Delegada de Protección de Datos para planificar el trabajo y acordar la asistencia a todas las reuniones de auditoría.
4	Efectuar la revisión de los aspectos incluidos en el programa de trabajo
5	Analizar las deficiencias, obtener las conclusiones y proponer las mejoras correspondientes
6	Examinar en detalle con la persona Responsable de Tratamiento y con la Delegada de Protección de Datos el borrador del Informe de Auditoria
7	Redactar el Informe de Diagnóstico, incluyendo las Recomendaciones (Plan de Acción), y presentarlo a sus destinatarios

En la redacción del Informe de Evaluación de cumplimiento del RGPD y el plan de acción, se detallarán las deficiencias encontradas, así como las propuestas de mejora o recomendaciones técnicas, organizativas, procedimentales y jurídicas para minimizar o evitar los riesgos asociados con dichos defectos. El informe pasará por una fase provisional y se remitirá a los auditados y a la

Delegada de Protección de Datos, por si existieran desajustes o inexactitudes o informaciones erróneas, de modo que con el estudio de las alegaciones que aquellos pudieran formular se subsanasen, dando paso a la realización del informe definitivo.

Los aspectos a revisar serán los siguientes (para los tratamientos de datos que sean objeto de cada auditoría):

#	Aspectos a revisar
1	**Designación** del Delegado de Protección de Datos y su notificación al órgano de control competente
2	**Adecuación** del contenido del Registro de Actividades de Tratamiento: Se revisarán las Actividades de Tratamiento, las bases de legitimación, realizando las propuestas necesarias para su adecuación, en caso de ser necesarias.
3	**Revisión de Cláusulas Informativas y de Consentimiento**: Se comprobará que se cumple con el deber de información y se utiliza el modelo de cláusulas proporcionado por la oficina de la Delegada de Protección de datos. Comprobar formularios, aplicaciones, teléfonos de atención al público, etc.
4	**Revisión de los Contratos con Acceso a datos por Terceros**: Revisión de los contratos (mayores y menores), encargos, convenios y el cumplimiento del artículo 28 del RGPD de conformidad con los modelos proporcionados por la oficina de la Delegada de Protección de Datos.
5	**Revisar, en su caso, el Análisis de Riesgos realizado**: evaluar si han sido analizados y gestionados los riesgos para los derechos y libertades de las personas interesadas en relación con las operaciones de tratamiento de datos, teniendo en cuenta la naturaleza, el alcance, el contexto y fines de dicho tratamiento.
6	**Revisar, si se dispone de las Evaluaciones de Impacto necesarias previstas en el RGPD** según la naturaleza, alcance, contexto o fines, entraña un alto riesgo para los derechos y libertades de las personas físicas.
7	**Revisar si se conoce y se utiliza el Procedimiento de Notificación de violaciones de seguridad de los datos** establecido por la oficina de la Delegada de Protección de Datos.
8	**Comprobar si se conoce y se utiliza el Procedimiento de ejercicio de derechos de protección de datos** establecido por la oficina de la Delegada de Protección de Datos.

Lote 3: Oficina Técnica para la certificación ENS

Las tareas a realizar en la auditoría, entre otros serán:

#	Tareas
1	Trabajos necesarios para la obtención de la Certificación del ENS, mediante la correspondiente ejecución de una Auditoría (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 los sistemas de información concernidos y servicios prestados
2	Reevaluación de las *No Conformidades*, si las hubiera, más allá del plazo de 30 días prescrito. El licitador deberá junto con la DTIC establecer el calendario para la reevaluación de la Auditoria

Entregables

Si bien cada lote definido tendrá sus propios entregables (que se definirán más adelante), a continuación, se detallan los documentos (entregables) que son comunes a todos ellos:

- ✓ **Actas**: por cada reunión que se organice con los distintos interlocutores (con la DTIC, Departamentos/Organismos Autónomos o cualquier otro ente), la empresa adjudicataria deberá elaborar un acta de las mismas que resuman lo acontecido en ellas. [nota: el contenido de las actas podrá ser redactado en castellano o en euskera]

Los documentos que se elaboren deberán ser entregados a la DTIC en soporte ofimático, estando toda esa documentación en formato compatible con las propias herramientas y estándares establecidos en el Gobierno Vasco. En caso de que así se establezca, la documentación se aportará a través de las herramientas colaborativas gestionadas por la DTIC (SharePoint, etc.).

Asimismo, en caso de que así lo establezca la DTIC, todos estos documentos (salvo las ofertas) se deberán ajustar a las señas de identidad o imagen corporativa del Gobierno Vasco.

Lote 1. «*Oficina Técnica de seguridad GureSeK*»

El trabajo a realizar consistirá en las tareas recogidas en el apartado «*Tareas a realizar*», donde cada ámbito incluye sus correspondientes entregables (reuniones a realizar, redacción de las actas, etc.)

Lote 2. «*Oficina Técnica para realizar auditorías*»

La documentación a obtener, a la conclusión de cada auditoría es:

a) Actas de las reuniones realizadas con los interlocutores designados
b) Diagnóstico de evaluación de cumplimiento del RGPD y el plan de acción, que incluya
    i. deficiencias encontradas
    ii. propuestas de mejora o recomendaciones
c) Informe de la dedicación incurrida (tareas y horas dedicadas, por perfil profesional)

Estos entregables se presentarán formalmente con los siguientes documentos:

A. Informe completo de auditoría
B. Resumen ejecutivo para la Alta Dirección

Lote 3. «*Oficina Técnica para la certificación ENS*»

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).

Propiedad Intelectual

La empresa adjudicataria se compromete a aceptar las siguientes cláusulas:

- ✓ Los derechos de propiedad intelectual relacionados con el trabajo realizado pertenecerán a la Administración. Cualquier producto o subproducto derivado del mismo no podrá ser utilizado para otros fines fuera del ámbito que le corresponda, sin el permiso expreso por escrito de la Administración.
- ✓ La documentación generada durante la ejecución del trabajo es propiedad exclusiva de la Administración, sin que la empresa adjudicataria para llevar a cabo los trabajos correspondientes pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización escrita de la Administración, que la daría, en su caso, previa petición formal de la empresa con expresión del fin que pretende. Lo dispuesto en este párrafo se entiende salvo conservación a los efectos de prueba de realización del trabajo contratado. La Administración autoriza expresamente la utilización de los resultados del presente trabajo como referencia y como base de futuros trabajos a realizar.

Seguridad y Confidencialidad

Tanto la empresa adjudicataria como su equipo de trabajo quedarán expresamente obligados a mantener absoluta **confidencialidad** y reserva sobre cualquier dato que pudieran conocer con ocasión del cumplimiento del contrato, especialmente los de carácter personal, que no podrá copiar o utilizar con fin distinto al que figura en este Pliego de Bases Técnicas, ni tampoco ceder a otros ni siquiera a efectos de conservación.

La empresa deberá garantizar la confidencialidad de la información facilitada por la Administración quedando especialmente sujeta, en cuanto a datos de carácter personal se refiere, a la legislación vigente en la materia —es decir, cumplimiento de lo dispuesto en el RGPD y en la Ley Orgánica 3/2018, de 5 de diciembre, sobre Protección de Datos Personales y Garantía de los Derechos Digitales).

Todas las personas trabajadoras de la empresa adjudicataria se comprometen a mantener el más absoluto secreto profesional sobre aquellos datos, informaciones y documentos que pudieran conocer con motivo de la realización del trabajo, cualquiera que sea la forma bajo la que se representen (oral o escrita). Exclusivamente tendrán acceso a dichas informaciones los colaboradores que sean imprescindibles para el desarrollo de las tareas que les hayan sido asignadas dentro del ámbito al que nos estamos refiriendo. Todos ellos serán advertidos sobre el carácter estrictamente confidencial y reservado de la información a la que tendrán acceso.

A estos efectos, deberán establecerse las máximas cautelas en el acceso a los datos. Cualquier infracción en este sentido será calificada como grave y será causa de resolución del contrato, sin perjuicio de las responsabilidades penales, o de otro tipo, en que se puedan incurrir.

La empresa adjudicataria se compromete a no suministrar a terceros ni utilizar para sí ni para otros los datos facilitados por la Administración para fines distintos a los que contempla este trabajo.

Asimismo, la empresa queda obligada a informar a la Administración, de modo inmediato, sobre cualquier sospecha relacionada con fallos o fugas del sistema de seguridad y protección de la información, que pudiera ser detectada durante el desarrollo del trabajo correspondiente.

Calidad, Control y Seguimiento

Las empresas licitadoras deberán indicar en la oferta si utilizan algún método o plan para garantizar la calidad de los trabajos y su descripción, cuánto tiempo llevan utilizándolo y la experiencia en proyectos cuya calidad haya sido controlada con dicho método durante los últimos dos años (número de proyectos e importe total de los mismos).

En todo caso, la Administración se reserva el derecho de rescindir el contrato si se considera que la empresa adjudicataria no ofrece un servicio de la calidad precisa.

La empresa licitadora deberá establecer todos aquellos procedimientos de control (y describirlos en la oferta que presente) que permitan verificar de forma continuada el cumplimiento de los objetivos especificados, tanto en los plazos como en la calidad final.

Durante la ejecución del trabajo, se presentará un informe de las horas (unidades y %) imputadas a cada perfil profesional que se ejecuten cada trimestre (perfiles en concordancia con la información solicitada en el siguiente apartado «*Estructura de las ofertas*»). En cualquier momento, la Administración podrá solicitar a la empresa prestadora del servicio el total de horas dedicadas a la prestación del servicio asociadas a los perfiles profesionales y actividades realizadas.

Como se especifica dentro del apartado «*Tareas a realizar*» de este Pliego, una de las tareas a llevar a cabo es la «*realización de informes de seguimiento para la adecuada evaluación y mejora continua*».

Con objeto de realizar el seguimiento más adecuado de los trabajos que deben llevarse a cabo (y que se han detallado en los apartados anteriores), la DTIC realizará una serie de **reuniones** que se detallan a continuación:

- **Lanzamiento:**

  Se trata de la **primera reunión** que se celebrará al inicio del proyecto. En ella intervendrán tanto los interlocutores que designe la DTIC como las personas asignadas al proyecto por parte de la empresa adjudicataria. Y el objeto de la misma será establecer las principales líneas del proyecto.

- **Seguimiento:**

  Mientras esté vigente el proyecto se realizará una reunión de seguimiento una vez al mes (preferiblemente la primera semana del mes).

  Durante la misma, la empresa adjudicataria, en primer lugar, hará un resumen de los trabajos realizados desde la última reunión de seguimiento, es decir, durante el periodo correspondiente al mes anterior (si ha lugar). De esta manera, la DTIC revisará los trabajos ya realizados y comprobará si se corresponden con las propuestas y tareas encargadas/planificadas en su momento. En caso de que todo sea conforme a lo planificado, la DTIC dará el visto bueno a los mismos. En caso contrario, las tareas que queden pendientes deberán ser replanificadas para llevarlas a cabo en el plazo más breve posible, ya que el pago correspondiente al mes en curso quedará supeditado al visto bueno de todas las tareas

definidas para ese mes, pudiéndose posponer dicho pago al periodo siguiente (una vez comprobado fehacientemente la finalización de las tareas pendientes).

En esta reunión la empresa entregará a la DTIC **un resumen** (incluyendo como mínimo, el **grado de avance de las tareas a realizar, horas dedicadas por cada perfil asignado al Equipo de Trabajo**) de los trabajos realizados y de los trabajos pendientes.

En segundo lugar, **la empresa propondrá a la DTIC** todas aquellas tareas que estime interesantes y que pretenda llevar a cabo durante ese mes, las cuales podrán ser aceptadas o rechazadas por la DTIC.

- **Extraordinaria:**

  Reunión que se llevará a cabo a petición de cualquiera de las partes (DTIC o empresa adjudicataria) en cualquier momento durante el proyecto, siendo su objetivo solventar cualquier **incidencia grave** que requiera una respuesta inmediata y que no pueda esperar a la reunión mensual de seguimiento.

- **Cierre:**

  Se trata de la **última reunión** del proyecto.

  Durante la misma se hará un repaso general de los objetivos planteados al comienzo del proyecto y cuáles han sido los trabajos realizados para alcanzar esos objetivos.

  La empresa adjudicataria entregará al comienzo de la misma un informe final con las tareas llevadas a cabo durante el proyecto.

Equipo de Trabajo

El programa de trabajo se circunscribe a la realización de las tareas descritas en el apartado OBJETO de este Pliego. La empresa adjudicataria coordinará las relaciones, supervisando la calidad de los trabajos y los productos a entregar mediante métodos de gestión de la calidad. Para ello deberá aportar su conocimiento y experiencia en trabajos similares.

La DTIC, por su parte, se encargará de:

- Ejercer la dirección de todos los trabajos. (La empresa que resulte adjudicataria realizará todas las tareas bajo la supervisión de la DTIC).
- Decidir sobre cualquier asunto que tenga influencia sobre el desarrollo del proyecto
- Aceptar (o rechazar en su caso) los productos intermedios y/o finales

El **equipo de trabajo** estará dirigido por un Responsable del Proyecto con dedicación estable, quien coordinará la realización de todas las tareas implicadas en el proyecto y actuará como interlocutor principal con la persona designada en la DTIC.

El equipo de trabajo, independientemente del Lote de que se trate, estará formado por personal con la categoría profesional y nivel de especialización adecuados a las necesidades planteadas, de acuerdo con las actividades que se vayan desarrollando.

En el caso del **Lote 1** (*«Oficina Técnica de seguridad GureSeK»*), por ejemplo, deberá contar con un **consultor sénior con una dilatada experiencia en la coordinación de proyectos de despliegue de la administración electrónica, que participará en las reuniones de seguimiento del proyecto (al menos con una periodicidad mensual)** y aportará su experiencia en la toma de decisiones. Además, el equipo de trabajo deberá reunir conocimientos en las siguientes materias:

a) Aplicación, en la práctica, de los fundamentos para la determinación de la categoría de un sistema, así como de la selección y aplicación de medidas de seguridad, de acuerdo a lo que establece el ENS.
b) Metodologías para el análisis de riesgos en el ámbito de la Seguridad de la información y de las TIC.
c) Herramientas de apoyo al análisis de riesgos.
d) Familia de normas ISO/IEC 27000, para la Gestión de la Seguridad de la información y las buenas prácticas en la materia, así como en la realización de auditorías técnicas, basadas en dichas normas.
e) Tecnologías y soluciones de firma electrónica.
f) Herramientas de integración y automatización de los procedimientos asociados al ENS.
g) Conocimientos generales en materia de Derecho aplicado a las TIC, y específicos en los siguientes apartados:

#	Norma	Fecha	Descripción
1	Ley 30/1992	26 de noviembre	de régimen jurídico de las administraciones públicas y del procedimiento administrativo común
2	Ley 15/1999	13 de diciembre	de Protección de Datos de carácter personal
3	Ley 34/2002	11 de julio	de servicios de la sociedad de la información y de comercio electrónico
4	Ley 59/2003	19 de diciembre	de Firma Electrónica
5	Ley 11/2007	22 de junio	de Acceso Electrónico de los Ciudadanos a los Servicios Públicos
6	Ley 25/2007	18 de octubre	de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones
7	Ley 37/2007	16 de noviembre	sobre reutilización de la información del sector público
8	Decreto 232/2007	18 de diciembre	por el que se regula la utilización de medios electrónicos, informáticos y telemáticos en los procedimientos administrativos
9	RD 1720/2007	21 de diciembre	por el que se aprueba el Reglamento de desarrollo de la LOPD
10	Ley 56/2007	28 de diciembre	de Medidas de Impulso de la Sociedad de la Información
11	RD 1671/2009	6 de noviembre	por el que se desarrolla parcialmente la Ley 11/2007
12	RD 3/2010	8 de enero	por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
13	RD 4/2010	8 de enero	por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica
14	Orden	26 de febrero	aprobando el Manual de Seguridad para el mantenimiento de la seguridad de la información de la Administración General de la CAPV y sus Organismos Autónomos
15	Decreto 21/2012	21 de febrero	de Administración Electrónica
16	Ley 9/2014	9 de mayo	General de Telecomunicaciones
17	Reglamento UE 910/2014 (eIDAS)	9 de julio	del Parlamento Europeo y del Consejo
18	Ley 39/2015	1 de octubre	del Procedimiento Administrativo Común de las AAPP
19	Ley 40/2015	1 de octubre	de Régimen Jurídico del Sector Público
20	RD 951/2015	23 de octubre	de modificación del ENS
21	(UE) 2016/679	27 de abril	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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
22	ACG	15 de junio 2018	Por el que se aprueba la estructura organizativa y asignación de roles para la protección de los datos personales tratados por la Administración Pública de la Comunidad Autónoma de Euskadi

En el caso del **Lote 2** (*«Oficina Técnica para realizar auditorías»*), por ejemplo, deberá contar con un consultor sénior con una dilatada experiencia en la coordinación de proyectos y disponer de algún título que certifique sus conocimientos, como puede ser el CISA (*«Certified Information Systems Auditor»*) o similar.

En el caso del **Lote 3** (*«Oficina Técnica para la certificación ENS»*), se deberá presentar la cualificación y experiencia del equipo Auditor. Deberá contar con al menos 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).

Para cada perfil adscrito al Equipo de Auditoría, deberá presentarse al menos: Categoría profesional; Titulación / Formación; 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.)

Independientemente del Lote asignado, la designación de los miembros del equipo de trabajo realizada por la empresa adjudicataria podrá ser modificada a simple petición de la DTIC, si ésta lo estimase conveniente. En este caso, la empresa adjudicataria quedará obligada a proponer otras personas con categoría y circunstancias personales y profesionales idénticas o similares a las inicialmente propuestas, sin que dicha circunstancia altere, en ningún caso, el precio ofertado ni cualquier otro concepto.

En las ofertas que se presenten, se deberá incluir en el capítulo «*Equipo de trabajo*» [ver apartado «*Estructura de las ofertas*»] la siguiente información:

El **organigrama** del equipo de trabajo (especificando las funciones y responsabilidades de cada una de las personas que lo integran por categoría profesional y sus *Curricula Vitae*). Detallando para cada miembro del equipo de trabajo, como mínimo, la siguiente información:

- Titulación
- Categoría profesional
- Trayectoria profesional
- Experiencia dentro de la empresa en la presente categoría profesional (meses)
- Experiencia en proyectos similares en los últimos años (indicar proyecto, duración, horas dedicadas, categoría profesional e importe)

Asimismo, se deberá aportar también un cuadro de horas similar al siguiente:

Perfil	Total Horas estimadas	% de horas dedicadas con respecto al total del proyecto
Responsable de Proyecto		
Técnico		
Especialista		
…		

(Nota: se podrán añadir cuantos perfiles se estimen necesarios)

Estructura de las ofertas

Toda aquella documentación técnica que se incluya en la oferta que aporte la empresa deberá adecuarse al siguiente esquema:

1. **Introducción**. Breve descripción de la estructura de la documentación aportada objeto de la misma.
2. **Propuesta técnica**
    a. **Planificación y Metodología**: descripción de las fases, actividades y tareas a realizar. Para cada una de las fases se detallarán los objetivos, actividades a realizar, herramientas y técnicas a emplear, productos a obtener, etc.
    b. **Total de horas** dedicadas a la prestación del servicio
    c. **Equipo de trabajo**
        i. La composición (perfiles profesionales y experiencia) del equipo de trabajo asignado a la realización de las actividades resultantes
        ii. Las horas (unidades y %) asignadas a cada perfil según las fases del proyecto, por meses (previsto)
        iii. Descripción, en cuanto a organización y funciones, que se realizarán para llevar a cabo el trabajo
3. **Seguridad y confidencialidad**: aceptación de las medidas de seguridad y confidencialidad descritas en el Pliego
4. **Calidad, Control y Seguimiento**. aceptación de las medidas de calidad descritas en el Pliego y descripción de los procedimientos que faciliten el control y seguimiento de los trabajos intermedios.

Cada empresa licitadora podrá aportar toda la **información adicional** que considere significativa y añadir en cualquiera de los apartados arriba señalados cualquier otra cuestión que se considere destacable.

La Administración se reserva la facultad de solicitar, en cualquier momento, antes o después de la adjudicación y durante el curso de los trabajos, cualquier otro documento complementario, en orden a la comprobación de cuantos datos haya ofrecido la empresa licitadora, tanto respecto a sí misma como con respecto al personal propuesto.

Plazo de ejecución y presupuesto

En referencia al plazo de ejecución máximo de las distintas tareas incluidas en este Pliego, éstas deberán realizarse en el plazo de **12 meses**.

El presupuesto máximo para la ejecución de todos los trabajos es de:

90.000,00 euros [IVA incluido]

[noventa mil euros)

Cantidad que será asignada de la siguiente forma:

Lote	Importe (euros)
1. Oficina Técnica de seguridad GureSeK	35.000,00
2. Oficina Técnica para realizar auditorías	20.000,00
3. Oficina Técnica para la certificación ENS	35.000,00
Total…	90.000,00

El abono de las tareas que se deben llevar a cabo se realizará de forma trimestral, y una vez que la DTIC haya comprobado y validado que las tareas correspondientes al trimestre anterior se han realizado de forma satisfactoria, o que se han alcanzado los hitos establecidos.

Se deberá utilizar el modelo de proposición económica del Anexo correspondiente para la realización de la oferta económica.

En Vitoria-Gasteiz, a 22 de noviembre de 2021

Vitoria-Gasteiz
2022.01.19 13:21:00 +01'00'

Patxi Sáez Ibáñez

Dirección de Tecnologías de la Información y la Comunicación