Expediente CF050-18-086

Pliego de Prescripciones Técnicas

Servicios de Oficina Técnica y de Soporte en Seguridad de la Información

INDICE

1. Objeto

2. Justificación de la no división en Lotes

3. Introducción y antecedentes

4. Descripción de los trabajos

5. Servicios de Oficina Técnica de Seguridad

5.1.1 Actividades de ejecución de acciones del Plan Director de Seguridad (documentación, formación, actualizaciones)

5.1.2 Servicio de asesoramiento

5.1.3 Auditorias

5.1.4 Otros servicios bajo necesidad o demanda

6. Servicios de soporte en Seguridad de la información.

6.1.1. Actividades de control, seguimiento y monitorización

6.1.2. Soporte al comité de seguridad.

6.1.3. Otros servicios bajo necesidad o demanda

7. Formación y Concienciación
8. Entregables
9. Metodología de prestación del servicio
10. Plazo de ejecución
11. Control de calidad de los trabajos
12. Transferencia tecnológica y soporte técnico
13. Documentación de los trabajos
14. Transición

1. Objeto

El objeto del presente pliego es la contratación, de los siguientes servicios:

- Oficina Técnica de Seguridad: responsable de la realización directa de actividades de seguridad o soporte técnico a la ejecución de las mismas por parte de VEIASA
- Soporte en Seguridad de la Información al Responsable de Seguridad de la Información (CISO) y/o Responsable de Protección de Datos Personales (DPO)

Ambos servicios se prestarán con carácter anual.

Se propone una asistencia que dé respuesta a las necesidades de seguridad tanto a nivel técnico como organizativo y estratégico, y alineada con el cumplimiento de las normas de seguridad aplicables y el estándar ISO 27001.

2. Justificación de la no división en Lotes

Veiasa requiere que la solución objeto del contrato sea integral, es decir, los Servicios Iniciales, Servicios Continuos y Servicios a Demanda deben funcionar de manera integrada y coordinada en la solución, además con un corto plazo de implantación. No es asumible una segmentación de dichas funciones en lotes diferenciados dada la estrecha interrelación entre las tareas, la alta especialidad de los perfiles técnicos necesarios, y los altos niveles de confidencialidad requeridos por la naturaleza de los trabajos. La realización independiente de las prestaciones objeto del contrato dificultaría la correcta ejecución del mismo desde el punto de vista técnico, comprometiendo igualmente los plazos asumibles para la puesta en marcha de los servicios objetos del contrato.

3. Introducción y antecedentes

Los procesos y los sistemas de información involucrados en la actividad de VEIASA están afectados por la siguiente legislación en materia de seguridad:

- Esquema Nacional de Seguridad (ENS): RD 3/2010, modificado por el RD 951/2015, para los sistemas de información afectados.
- Reglamento Europeo de Protección de Datos Personales (RGPD): (UE) 2016/679 del parlamento europeo y del Consejo Europeo. Y, hasta que no se aprueba la nueva ley orgánica española de protección de datos, siguen siendo de aplicación (en lo que no contradiga al RGPD) la siguiente legislación española relativa a la privacidad: Ley Orgánica de Protección de Datos y Reglamento de Desarrollo (LOPD, RDLOPD): Ley 15/1999 y RD 1720/2007.
- Por otro lado, todas las actuaciones en materia de seguridad deberán estar alineadas con el Decreto 1/2011 (modificado por el Decreto 70/2017), por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

A fin de aunar todas las necesidades en materia de seguridad y garantizar el cumplimiento normativo, con carácter reciente, VEIASA ha desarrollado un **Plan Director de Seguridad**, que es una Hoja de ruta en materia de Seguridad y cumplimiento normativo a un horizonte de tres años.

El siguiente paso consistirá en ejecutar y mantener las acciones de dicho plan para la cual es fundamental la figura del responsable de seguridad.

Para cumplir con las funciones del responsable de seguridad, se requiere de personal dedicado, capacitado y con independencia suficiente de otras áreas involucradas en la gestión tecnológica. Para ello, se necesita una **estructura funcional** dedicada a la gestión de la seguridad que, por un lado realice las funciones de velar por la ejecución en tiempo y forma de las acciones de seguridad (responsable de seguridad/CISO), y por otro, se responsabilice directa o indirectamente de dicha ejecución (oficina técnica).

En este contexto se solicita una propuesta de colaboración por los servicios de Oficina de Seguridad y Soporte en la Seguridad de la Información a los Responsable de la seguridad de la Información (CISO) y de Protección de Datos Personales (DPO)

4. Descripción de los trabajos

La solución requerida consiste en proporcionar un conjunto de servicios especializados en seguridad que refuercen y completen los prestados por VEIASA en esta materia.

No consiste en una delegación de responsabilidad, sino en un servicio adjunto al responsable de seguridad propio de VEIASA.

Partiendo de la Hoja de Ruta (Plan Director de Seguridad) indicada en el punto anterior y la mencionada estructura de seguridad, los servicios que se precisan son los que se indican a continuación:

Servicios	Funciones
Actividades de control, seguimiento, monitorización y reporting del plan de seguridad.	Soporte en Seguridad de la Información
Soporte al comité de seguridad.	
Otros servicios bajo necesidad o demanda.	
Actividades de ejecución de acciones del plan de Seguridad.	Oficina Técnica de Seguridad.
Servicio de asesoramiento.	
Auditorias.	
Otros servicios bajo necesidad o demanda.	

En los siguientes apartados se describen de manera detallada estos servicios.

5. Servicios de Oficina Técnica de Seguridad

5.1.5 Actividades de ejecución de acciones del Plan Director de Seguridad (documentación, formación, actualizaciones)

Dentro de la Hoja de Ruta, se ejecutarán las acciones de carácter **documental** del plan, en concreto:

- Normativa de Seguridad
- Procedimientos de Seguridad
- Documentación de los procesos de autorización
- Catálogo de Indicadores

También se realizarán acciones relacionadas con la formación y concienciación, en concreto:

- Diseño del Plan de Formación y concienciación en materia de seguridad.
- La empresa adjudicataria ofrecerá algunas de las acciones de dicho plan de formación, fundamentalmente las relacionadas con la impartición de acciones presenciales de concienciación.

5.1.6 Servicio de asesoramiento

Para que el personal vinculado a este servicio pueda resolver cualquier tipo de duda, se prestará un asesoramiento experto permanente en materia de seguridad en general y en protección de datos en particular (soporte consultivo al DPO de VEIASA). Este asesoramiento será llevado a cabo tanto de forma **presencial** como de forma **remota**.

Para el asesoramiento en forma remota se requiere al adjudicatario disponer de un Centro de Atención a Usuarios para seguridad (CAU), que proporciona una atención experta personalizada para lanzar cualquier consulta relacionada con la ejecución de las acciones de la Hoja de Ruta.

Los niveles de servicio en la explotación de este CAU son:

Cobertura horaria	Tiempo máximo de respuesta a peticiones	Tiempo de solución a consultas
La misma de Veiasa	NBD	2 días laborables

NBD (Next Business Day): siguiente día laborable.

Además, gracias a este asesoramiento, Veiasa dispondrá del soporte adecuado para la adecuación de los procesos internos de seguridad a lo exigido por la normativa y procedimientos.

5.1.7 Auditorías

Con carácter anual se realizara una auditoria interna del ENS. La realización de la auditoria interna es un requisito del ENS conforme a la INSTRUCCIÓN TÉCNICA DE SEGURIDAD DE AUDITORÍA DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN para poder optar a una futura certificación.

Por lo tanto, no es objeto de esta auditoría la certificación del ENS, ya que el servicio está centrado en la implantación y preparación de la organización para poder optar a una futura certificación con garantías de éxito.

Esta auditoría interna, no obstante, servirá para recabar la información necesaria para el reporte del Informe Nacional de Estado de la Seguridad (INES) a nivel autonómico.

La información recabada será la que se utilice para rellenar la Encuesta del Estudio Estado de Seguridad JdA-20XX, la cual es enviada tal como se indica para su recopilación por parte de la Unidad de Seguridad TIC corporativa.

5.1.8 Otros servicios bajo necesidad o demanda

Además de las acciones asociadas al Plan Director de Seguridad, es posible que VEIASA tenga otras necesidades de asistencia relacionadas con la seguridad de la información y que sean susceptibles de ser realizados a través de la Oficina Técnica. A fin de dar respuesta a las mismas, se podrán pedir otros servicios bajo demanda, que podrán ser realizados en el marco del contrato.

A fin de acotar estos servicios, se ofrecerá un máximo de 10 jornadas (de 8 horas), de forma que, tras recibir una petición, la adjudicataria estudiará su viabilidad y el consumo de horas que supone y solo se procederá con la ejecución previa aprobación por VEIASA, tras valorar la viabilidad y el consumo de horas propuesto.

Para este servicio se establecerán unos SLAs mínimos que serán los mismos que los de la actividad de asesoramiento, a menos que se haya ofertado otro menor en la oferta presentada por los licitadores, en cuyo caso se entenderá éste como exigible.

6. Servicios de soporte en Seguridad de la Información

6.1.1. Actividades de control, seguimiento y monitorización

Sobre la Hoja de Ruta (Plan Director de Seguridad), se realizarán las siguientes actividades de control y asesoramiento:

- **Contacto directo con los responsables de cada acción**. Se mantendrá un contacto directo con los responsables de llevar a cabo las acciones de la hoja de ruta diseñada en el Plan Director de Seguridad realizado con anterioridad por parte de VEIASA..
- **Seguimiento de trabajos**. Como resultado de las actividades de seguimiento, se actualizará el estado de las diferentes acciones y se irá actualizando el grado de avance de cada acción y re-planificando, si procediese, las fechas dentro de la hoja de ruta.
- **Revisión de resultados de la ejecución.** Además del seguimiento para garantizar la ejecución en los plazos adecuados, también es preciso garantizar un satisfactorio resultado, para lo cual se realizará una revisión de los mismos.
- **Reporting del grado de avance**. Como resultado de la monitorización y revisión se irá completando un informe de seguimiento, reflejando el grado de avance.
- **Revisión de indicadores.** Sobre el cuadro de mandos que se habrá definido en otra actividad de la oficina técnica, se realizará el seguimiento para la adecuada actualización de los indicadores.
- **Comunicación y asesoramiento al CISO y al DPO.** A fin de que haya un alineamiento permanente entre la seguridad de la información y el cumplimiento de la protección de datos, reportando sobre cualquier aspecto que pudiera afectar a la privacidad y dando respuesta a las consultas que puedan ser planteadas

6.1.2. Soporte al comité de seguridad.

Se propondrá un modelo de funcionamiento de comités en el cual se contemplarán distintos niveles (estratégico, táctico y operacional).

Estos comités serán gestionados y dinamizados por el responsable de seguridad a través de una seria de actividades tales como propuesta de agenda, asistencia, acta de reunión y seguimiento de compromisos del comité.

6.1.3 Otros servicios bajo necesidad o demanda

Al igual que para el caso de la oficina técnica es posible que puedan surgir otras necesidades de participación del responsable de seguridad que no hayan sido previstas.

A fin de dar respuesta a las mismas, se podrán pedir otros servicios bajo demanda, que podrán ser realizados en el marco del contrato.

A fin de acotar estos servicios, la dedicación máxima estará incluida dentro de las 10 jornadas (de 8 horas) de forma que, tras recibir una petición, la adjudicataria estudiará su viabilidad y el consumo de horas que supone y solo se procederá con la ejecución previa aprobación por parte de VEIASA, tras valorar la viabilidad y el consumo de horas propuesto.

Para este servicio se establecerán unos SLAs mínimos que, serán los mismos que los de la actividad de asesoramiento, a menos que se haya ofertado otro menor en la oferta presentada por los licitadores, en cuyo caso se entenderá éste como exigible.

7. Formación y Concienciación

Se requerirán las siguientes acciones relacionadas con la formación y concienciación a realizar indistintamente por parte del CISO y/o la Oficina Técnica:

- **Cursos online**. Se requieren **cuatro** cursos online en formato scorm, que pueden cargarse en la plataforma Moodle. Estos cursos versarán sobre la siguiente temática
  - Esquema nacional de Seguridad.
  - Análisis de Riesgos con la herramienta PILAR.
  - Buenas prácticas en seguridad de la información.
  - Reglamento General de protección de Datos.

- **Acciones formativas presenciales sobre gestión de seguridad y privacidad**. Se requieren 10 jornadas formativas orientadas a proporcionar conocimientos al responsable de seguridad de la organización y al DPO. El contenido y la planificación de las mismas será proporcionado con antelación y acordado con VEIASA

- **Acciones formativas de ingeniería social**. Se requiere una acción de Ingeniería social basada en la simulación de un phishing a los empleados. Tras la realización del phishing se realizará un informe de conclusiones y una acción formativa orientada a concienciar sobre la amenaza de ingeniería social.

- **Acciones formativas técnicas**. Se requiere la realización de las siguientes acciones formativas técnicas:

  - **Herramientas de seguridad para administraciones públicas**. Versará sobre las diferentes herramientas gratuitas a disposición de la administración pública (PILAR, CLARA, CARMEN, LUCÍA...)

  - **Otras herramientas de seguridad.** Versará sobre otras herramientas de seguridad de interés para la seguridad de la información y su relación con el cumplimiento normativo, en particular del ENS y RGPD

8. Entregables

Los entregables mínimos del proyecto son los que se relacionan en la siguiente tabla:

Actividad	Entregables Mínimos
Actividades de control, seguimiento, reporting y monitorización	• Informes de avance del Plan Director • Cuadros de mandos actualizados

Actividades de ejecución de acciones del plan (documentación, formación, actualizaciones)	• Documentación:
	  ○ Normativa de Seguridad
	  ○ Procedimientos de Seguridad
	  ○ Documentación de los procesos de autorización
	  ○ Catálogo de Indicadores
	• Formación
	  ○ Plan de Formación y concienciación
	  ○ Material resultante de las acciones formativas

Servicio de asesoramiento	• Respuesta a consultas y peticiones
Auditorias	• Informe de auditoría del ENS ○ Informe INES (para la Consejería de Empleo, Empresa y Comercio)
Otros servicios bajo necesidad o demanda	• En función de la naturaleza de las peticiones

9. Metodología de prestación del servicio

Como se desprende del modelo propuesto, el servicio consiste en la realización de una serie de actividades programadas y no programadas (en este caso con unos SLAs).

Estas actividades serán realizadas por un equipo multidisciplinar con capacidad como para atender las necesidades del servicio.

Se nombrará un jefe de proyecto, que será el interlocutor con VEIASA y supervisor del resto de los integrantes, pero las actividades serán realizadas por quién corresponda, en función de su naturaleza.

Por otro lado, los trabajos podrán ser realizados de forma presencial o remota. Particularmente, al menos las siguientes tareas, por su naturaleza, deberán llevarse a cabo de forma presencial:

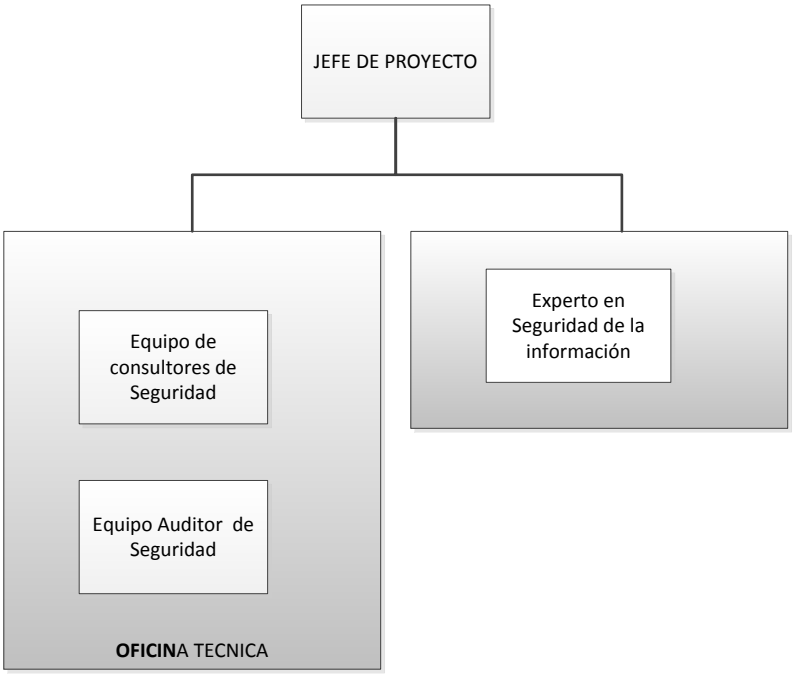
- Recogida de información para las auditorías (entrevistas).
- Presentación de resultados de auditoría.
- Reuniones presenciales para revisiones conjuntas de documentos (en caso de que fuese preciso).
- Seguimiento y control de cumplimiento de controles y medidas de seguridad (visitas periódicas programadas).
- Reuniones de seguimiento.
- Asistencia a los comités de seguridad (bajo demanda).
- Concienciación y sensibilización presencial en materia de seguridad de la información.

a. Estructura del Equipo de trabajo

El equipo de trabajo incluirá la siguiente estructura de roles y funciones:

- **Jefe de proyecto**. Su responsabilidad es garantizar la ejecución de los trabajos, velando para que éstos sean acometidos en tiempo y forma, a través de la coordinación del equipo de trabajo y ostentando la representación del equipo frente al Cliente.
- **Experto de Seguridad**. Su labor es la de prestar soporte experto al jefe de proyecto en los aspectos tácticos y operativos del proyecto y **realizar las funciones de asesoramiento al CISO y DPO.** A tal fin realizará una serie de funciones tales como la asistencia a las reuniones de los comités, asistencia consultiva, revisión de detalle del cumplimiento del plan de seguridad, realización de informes de avance del plan y presentaciones corporativas.
- **Equipo consultor de seguridad**. Se encargará de la ejecución de los trabajos bajo la coordinación del Jefe de Proyecto y soporte del Experto de Seguridad.
- **Equipo auditor de seguridad.** Se encargará de las actividades de auditoría de cumplimiento.

La siguiente figura ilustra gráficamente la organización del equipo de trabajo:



b. Requisitos del Equipo de Trabajo

El equipo de trabajo ofrecido debe reunir las características que se indican a continuación. A fin de poder demostrar el cumplimiento de las mismas se deberán entregar los CCVV del equipo de trabajo y presentar copias de los títulos universitarios y certificaciones de seguridad.

i. Titulaciones académicas

Todos los miembros del equipo de trabajo deberán tener titulación universitaria Nivel Meces 2 o equivalente como requisito de solvencia, según se indica en el Anexo 4 del Cuadro Resumen del Pliego del Cláusulas Administrativas Particulares.

Todos los miembros del equipo deberán contar con más de cinco años de experiencia en proyectos de seguridad de la información.

ii. Certificaciones

El equipo de trabajo en conjunto deberá contar con las siguientes certificaciones en vigor, como garantía de acreditación de las capacidades y conocimientos, según se exige como requisito de solvencia en el Anexo 4 del Cuadro Resumen del Pliego del Cláusulas Administrativas Particulares.

PMP (Project Management Professional)
CISA (Certified Information System Auditor)
CISM (Certified Information Security Manager)
CRISC (Certified Risk and Information Systems Control)
CDPP (Certified Data Privacy Proffessional) del ISMS Forum
ITIL Foundation
CISSP (Certified Information Systems Security Professional)
CHFI: Certified Hacking Forensic Investigation
CEH: Certified Ethical Hacking
Cobit 5 Foundation
CSX (Cibersecurity Nexus) Cybersecurity Fundamentals Certificate
ISO 27001 Implementer (expedido por algún organismo de certificación, como AENOR, SGS, Bureau Veritas, BSI...)
LEAD AUDITOR en Sistemas de Gestión de la Seguridad de la Información (expedido por algún organismo de certificación, como AENOR, SGS, Bureau Veritas, BSI...)
LEAD AUDITOR en Sistemas de Gestión de la Continuidad del Negocio –ISO 22301- (expedido por organismo de certificación como AENOR, SGS, Bureau Veritas, BSI...)

c. Certificaciones de Empresa

Certificaciones relevantes en materia de calidad/medio ambiente y gestión TI y de la seguridad o su equivalente europeo, según se exige como requisito de solvencia en el Anexo 4 del Cuadro Resumen del Pliego del Cláusulas Administrativas Particulares.

- Certificación ISO 27001 vigente (con el alcance de servicios de consultoría de seguridad)
- Certificación ISO 20000 vigente.
- Certificación ISO 14000 vigente.
- Certificación ISO 9001 vigente.

d. Experiencia de empresa

La empresa deberá acreditar haber ejecutado proyectos de seguridad en el ámbito del ENS, protección de datos e ISO 27001 en el sector público por valor de al menos 200.000 euros en los últimos 3 años, de conformidad con lo exigido como requisito de solvencia en el Anexo 4 del Cuadro Resumen del Pliego del Cláusulas Administrativas Particulares.

10. Plazo de ejecución

El plazo de ejecución de los trabajos será, como máximo, de 12 meses o 1.800 horas, a contar desde la fecha de la firma del contrato, con posibilidad de prorroga por otros 12 meses como máximo, pudiendo alcanzar una duración máxima total de 24 meses o de 3.600 horas.

11. Control de calidad de los trabajos.

La empresa adjudicataria deberá establecer un control de calidad sobre los trabajos que se desarrollen, certificando que se ajustan a las especificaciones técnicas exigidas.

Durante la duración del contrato los profesionales ofertados y admitidos no serán susceptibles de sustitución, salvo causa de fuerza mayor que justifique el cambio, o porque VEIASA lo requiera, en cuyo caso deberá ser sustituido adecuadamente en el plazo de 14 días naturales, sin que esto afecte ni a la planificación de trabajos prevista ni a la estimación de costes del proyecto.

Si a juicio de VEIASA alguno de los recursos propuestos no ejecutara los servicios descritos conforme a las exigencias del presente PPT, deberá ser sustituido adecuadamente por otro/s profesional/es, de igual o superior titulación en grado y experiencia, en el plazo máximo de 14 días naturales, quedando condicionada dicha sustitución a la validación por VEIASA para su incorporación al proyecto. Dicha sustitución no afectará ni a la planificación de los trabajos prevista ni a la estimación de costes del proyecto.

El periodo de garantía exigido sobre los trabajos realizados será de 12 meses.

El incumplimiento reiterado, entendiéndose como tal el que se produzca en dos o más ocasiones, en la calidad, tiempos y eficiencias en los trabajos, será razón suficiente para la imposición por VEIASA de las penalizaciones previstas, independientemente de la posibilidad de acordar la resolución del contrato con la empresa adjudicataria, de conformidad con lo estipulado en los Anexos 10 y 11 del Cuadro Resumen del Pliego de Cláusulas Administrativas Particulares.

12. Transferencia tecnológica y soporte técnico.

Durante la ejecución de los trabajos objeto del presente contrato el adjudicatario se compromete en todo momento a facilitar a las personas designadas por VEIASA la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

13. Documentos de los trabajos.

La documentación generada durante la ejecución del contrato será de propiedad exclusiva de Junta de Andalucía (VEIASA), sin que el adjudicatario pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización de VEIASA, que la daría, en su caso, previa petición formal del adjudicatario, con expresión del fin.

14. Transición.

El adjudicatario deberá colaborar con VEIASA en el proceso de finalización del contrato y transición de salida, asegurando el traspaso del servicio a VEIASA o la empresa que VEIASA determine, durante el tiempo que sea necesario para ello, colaborando activamente durante este proceso, para facilitar la transición de los servicios sin causar perjuicios.