INFORME PARA LA VALORACIÓN DE CRITERIOS TÉCNICOS VALORADOS MEDIANTE JUICIOS DE VALOR

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

Expediente CF050-18-086

ÍNDICE

1. OBJETO 3

2. OFERTAS PRESENTADAS 3

4. CRITERIOS TÉCNICOS VALORADOS MEDIANTE JUICIOS DE VALOR 3

5. CONCLUSIONES 11

1. OBJETO

El objeto del presente informe es recoger el análisis de la documentación técnica presentada por las empresas que han acreditado todos los requisitos técnicos exigidos en el PPT en la licitación relativa a **Servicios de Oficina Técnica de Seguridad y de Soporte en Seguridad de la Información (Expediente CF050-18-086)**, con la finalidad de valorar las proposiciones técnicas de las mismas conforme a los criterios técnicos valorados mediante juicio de valor, que se establecen en el Anexo 8 del Cuadro Resumen.

2. OFERTAS PRESENTADAS

Tras la apertura de sobres el pasado 9 de abril de 2019, las empresas que han presentado oferta son las siguientes:

- Telefonica Soluciones de Informatica y Comunicaciones de España S.A.U.
- Ingenieria e Integración Avanzadas (INGENIA), S.A.
- Atos IT Solutions and Services Iberia, S.L.

3. EMPRESAS QUE CUMPLEN TODOS LOS REQUISITOS TÉCNICOS EXIGIDOS EN EL PPT

Tras analizar la documentación técnica presentada por las licitadoras, relativa al cumplimiento del pliego de prescripciones técnicas (PPT), se constata, mediante informe emitido por la Unidad de Mantenimiento de Sistemas de Información de VEIASA, que todas ellas cumplen con los requisitos establecidos en el PPT.

4. CRITERIOS TÉCNICOS VALORADOS MEDIANTE JUICIOS DE VALOR

Los aspectos a valorar, de conformidad con el Anexo 8 del CR del PCAP son:

Los criterios de valoración y la puntuación que podrá alcanzar a cada uno de ellos son los siguientes:

1.- CRITERIOS TÉCNICOS VALORADOS MEDIANTE JUICIOS DE VALOR.....25 puntos

Los apartados a puntuar son los siguientes:

A. Calidad conceptual, funcional y técnica de la propuesta (de 0 a 5 puntos):

Se valorará que el nivel de detalle de la propuesta demuestre conocimiento necesario para la realización de todos los tipos de actividades a realizar, así como su nivel de adaptación a VEIASA. Para ello se analizarán, de forma separada, las siguientes áreas de actividad:

- Recopilación y organización de la documentación de seguridad
- Seguimiento del cumplimiento normativo

- Concienciación, formación y apoyo al resto de áreas

Para este criterio se otorgarán las siguientes puntuaciones:

* **5 puntos** si la calidad técnica es excelente y tiene un alto nivel de detalle y alineamiento con los requisitos.

* **2 puntos** si la calidad técnica es media, el detalle es suficiente pero mejorable, o tiene carencias menores en el nivel de detalle o alineamiento con los requisitos

* **0 puntos** si la calidad es baja, precisa de un mayor nivel de detalle, el alineamiento con los requisitos no es adecuado, o no se incluye el apartado o es muy deficiente.

B. Puesta en marcha de una Oficina de Seguridad (De 0 a 20 puntos)

Descripción de la prestación que exponga exhaustivamente el enfoque que el contratista propone seguir en el desarrollo de los trabajos para conseguir los objetivos, según lo establecido en el Pliego de Prescripciones Técnicas.

Método de valoración:

- Se describe y detalla insuficientemente: **0 puntos**

- Se describe y detalla de forma suficiente, pero superficial: **5 puntos**

- Se describe y detalla en profundidad y se particulariza de forma muy adecuada al proyecto, pero sin incluir aspectos novedosos significativos: **10 puntos**

- Se describe y detalla en profundidad y se particulariza de forma muy adecuada al proyecto, incluyendo aspectos novedosos significativos: **20 puntos.**

5	Calidad conceptual, funcional y técnica de la propuesta		Valoración	Puntos
	Telefonica	Descripción de los servicios: Correcta descripción de la solución propuesta para satisfacer la necesidad de cumplir con las 3 áreas de actividad descritas en el criterio de valoración: Recopilación y organización de la documentación de seguridad Seguimiento del cumplimiento normativo Concienciación, formación y apoyo al resto de tareas Metodología, equipo y seguimiento: Buena descripción del modelo PDCA y su relación con la adecuación al RGPD y ENS pero sin entrar en detalle sobre cómo se van a realizar los trabajos concretos descritos en la oferta La concurrencia de personal en cada uno de los perfiles permite soportar posibles bajas y/o picos de trabajo Servicios de valor añadido: Recursos para reforzar acciones de concienciación: Píldoras formativas de 15 minutos Ejercicios formativos en formato de juego Vídeos de 2 minutos Telefónica ha trabajado en múltiples guías del CCN Incluye un equipo consultivo de soporte Licencia de uso, durante el proyecto, de la herramienta SANDAS GRC como sistema de soporte a la adecuación normativa	5	**5**
	Atos	Descripción de los servicios: Excelente descripción de su metodología y modelo de trabajo propuesto pero parece ser demasiado genérica y válida para todo tipo de proyectos. En el apartado 4 no se encuentran factores orientados específicamente a proyectos de adecuación normativa, auditoría y/o formación y concienciación	5	**2**

		No se indican como se analizará la necesidad de cumplir con las 3 áreas de actividad descritas en el criterio de valoración: Recopilación y organización de la documentación de seguridad Seguimiento del cumplimiento normativo Concienciación, formación y apoyo al resto de tareas <u>Metodología, equipo y seguimiento:</u> El equipo de trabajo parece adecuado y bien dimensionado aunque se detecta poca diferencia entre las tareas del experto en seguridad y el consultor en seguridad <u>Servicios de valor añadido:</u> Los servicios de valor añadido son muy generales y de poca aplicación en VEIASA		
	Ingenia	<u>Descripción de los servicios:</u> La planificación propuesta es correcta en general. Se replanificará la realización del informe INES asi como la programación de las acciones formativas online ofertadas. <u>Metodología, equipo y seguimiento:</u> Excelente descripción de las herramientas, fuentes de información y estándares existentes para la realización de las tareas La metodología incluye un análisis de las relaciones existentes entre los requisitos del ENS, el RGPD y la ISO 27.001 El equipo de trabajo propuesto es muy variado y completo lo que ayudaría a suplir bajas, vacaciones o picos de trabajo Descripción muy detallada de la metodología de trabajo propuesta y parece adecuada para la realidad del proyecto <u>Servicios de valor añadido:</u> Uso de un RedMine para la gestión del servicio de asesoramiento. Metodología centrada en la integración de varias normas. Realización de estudios de satisfacción	5	**5**

20	**Puesta en marcha de una oficina de seguridad**		**Valoración**	**Puntos**
	Telefonica		20	**10**
		<u>Servicios de la oficina técnica:</u> • Generación de normativa: Excelente listado de documentos a generar por parte de telefónica • Catálogo de indicadores: Buena descripción de varios indicadores de ejemplo derivados del ENS que se pueden crear indicando las características que deben incluir los indicadores a crear • Servicio de asesoramiento: Servicio de asesoramiento por correo electrónico y telefónico con un equipo de trabajo en dos niveles. No indica servicio presencial de asesoramiento Plazos de respuesta acorde a los solicitados en pliegos. Incluye el soporte al DPD con una buena descripción de las funciones de este. No se indica a que nivel se dará el soporte • Auditorías: Indican que la auditoría anual se usará para recabar la información del informe INES. Excelente descripción de la metodología de auditoría propuesta aunque un poco excesiva para el contexto de la oferta . • Otros servicios a demanda: Incluyen la misma información que aparece en el pliego <u>Soporte en seguridad de la información:</u> • Actividades de control, seguimiento y monitorización: Parece mezclar dos apartados en esta parte de la oferta ya que primero habla de las actividades de control y seguimiento del propio proyecto y luego habla de la supervisión del cumplimiento legal por parte de VEIASA.		

		• Soporte al comité de seguridad: Incluyen información del ENS sobre las funciones del comité de seguridad pero apenas detalla en qué consiste las labores de soporte • Otros servicios a demanda: Incluyen la misma información que aparece en el pliego <u>Formación y concienciación:</u> • Cursos online: Indican que los cursos están desarrollados en un gestor de contenidos propio pero que es compatible con SCORM 1.2 y 2004.Los cursos tienen una buena descripción de su contenido pero no incluyen ni la duración de los cursos ni los requisitos de conocimiento del público objetivo al que se dirige • Acciones presenciales: Buena descripción de los posibles contenidos propuestos pero no se indica la duración de cada curso ni los contenidos concretos de cada uno de ellos • Ingeniería social: Proponen 4 posibles tipos de spear-phising, con diferentes requisitos de dedicación y trabajo, para implementar en VEIASA con una jornada final de concienciación a los trabajadores de VEIASA • Acciones formativas técnicas: Incluyen la misma información que aparece en el pliego sin más detalle. Además incluyen formación sobre la herramienta Sandas GRC		
	Atos	<u>Servicios de la oficina técnica:</u> • Generación de normativa: No se describe la propuesta inicial de documentos a generar ni se indica un mínimo o máximo de documentos a generar. La metodología propuesta para crear cada documento parece correcta aunque no está muy detallada • Catálogo de indicadores: No se incluye una propuesta inicial de indicadores o un listado de indicadores entre los que se podría escoger. La descripción de la metodología para obtener este catálogo es demasiado escueta e imprecisa	20	**10**

		• Servicio de asesoramiento: Incluye el asesoramiento a los responsables TI, empleados y DPD de VEIASA. Las materias sobre las que ofrece asesoramiento y la metodología de trabajo es correcta y está suficientemente detallada. En la oferta no indican si podrán hacer o no asesoramiento presencial. La oferta no indica nada de crear un CAU. • Auditorías: Indican que la auditoría anual se usará para recabar la información del informe INES. Excelente descripción de la metodología de auditoría propuesta aunque un poco excesiva para el contexto de la oferta. • Otros servicios a demanda: Incluyen la misma información que aparece en el pliego <u>Soporte en seguridad de la información:</u> • Actividades de control, seguimiento y monitorización: Proponen un modelo de gestión de proyectos basado en PMI que puede ser correcta para grandes proyectos tecnológicos pero puede ser excesivo para un proyecto de este presupuesto y plazo de ejecución. En todo caso, las metodologías de gestión de la calidad y de riesgos del proyecto parecen adecuadas y realistas" • Soporte al comité de seguridad: Se centrarán en preparar la agenda de la reunión del comité, envío de las convocatorias y acta posterior • Otros servicios a demanda: No se indican aunque los servicios descritos en la página 46 podrían aplicar aquí <u>Formación y concienciación:</u> • Cursos online: Los cursos de ENS, RGPD y buenas prácticas se puede impartir en una sesión on-line de 30 minutos pero la formación de Análisis de riesgos requiere mucha más dedicación. • Acciones presenciales: La información nueva incluida en la oferta sobre este apartado es muy poca, casi nula. La mayoría de la información de la oferta es la incluida en el pliego		

		• Ingeniería social: Proponen 4 posibles tipos de spear-phising, con diferentes requisitos de dedicación y trabajo, para implementar en VEIASA con una jornada final de concienciación a los trabajadores de VEIASA • Acciones formativas técnicas: Incluyen la misma información que aparece en el pliego sin más detalle. Además incluyen formación sobre la herramienta Sandas GRC		
	Ingenia	<u>Servicios de la oficina técnica:</u> • Generación de normativa: Se incluye un listado inicial de los documentos a generar relacionándolo con las medidas concretas del ENS y con las guías y estándares a usar en cada documento. Incluye un índice inicial de alguno de los documentos a generar • Catálogo de indicadores: No se incluye un apartado concreto sobre los indicadores a generar pero se encuentra incluido en las tareas del apartado anterior (generación de documentación de seguridad) • Servicio de asesoramiento: Incluye la realización de asesoramiento tanto de forma presencial como remota telefónicamente. Proponen realizar la gestión de las consultas por medio de un RedMine. El asesoramiento se usará para resolver dudas sobre el plan de seguridad y soporte al DPD.Descripción breve pero adecuada de la metodología usada para este apartado" • Auditorías: Buena descripción de la auditoría ENS a realizar e incluyen, específicamente, el reporte para el informe INES • Otros servicios a demanda: Incluyen en este apartado la creación de un plan de formación/concienciación con un pequeño listado de cursos a realizar. Pero este proceso de creación está pobremente descrito <u>Soporte en seguridad de la información:</u>	20	**10**

		• Actividades de control, seguimiento y monitorización: Descripción adecuada de las actividades de control propuestas en la oferta, centrado en la recopilación de información, seguimiento de los indicadores y comunicación con el CISO y DPD • Soporte al comité de seguridad: No indican más información aparte de la incluida en el pliego • Otros servicios a demanda: No indican más información aparte de la incluida en el pliego <u>Formación y concienciación:</u> • Cursos online: Excelente descripción de los cursos online solicitados incluyendo los contenidos iniciales, público objetivo, requisitos de realización y duración. La duración de cada uno de los cursos es adecuado a su contenido y público objetivo. El curso sobre ENS incluye la realización de sesiones presenciales • Acciones presenciales: Se incluye un listado inicial del contenido de 2 de los posibles cursos a impartir aunque el contenido final de los cursos se decidirá durante la fase de creación del plan de formación del paquete 1 • Ingeniería social: Breve descripción de la acción propuesta y del informe de conclusiones final • Acciones formativas técnicas: Solo incluyen la información existente en el pliego sin más detalle aunque indican que durante el plan de formación se definirá este apartado		

5. CONCLUSIONES

De los resultados obtenidos, la valoración técnica de los criterios subjetivos para cada una de las empresas es, de mayor a menor puntuación, la siguiente:

Criterios de Valoración	Peso	Ingenia	Telefonica	Atos
		P.	P.	P.
Valoración Subjetiva	**25**			
Calidad conceptual, funcional y técnica de la propuesta	5	5	5	2
Puesta en marcha de una oficina de seguridad	20	10	10	10
Valoración Final:		**15**	**15**	**12**

Sevilla, a 14 de mayo de 2019

Fdo.: Rafael Rodriguez Morales
Jefe de Unidad de Mantenimiento de SSII