TRACTAMENT I SELECCIÓ DE RESIDUS, S.A.

PLIEGO DE PRESCRIPCIONES TÉCNICAS

SERVICIO PARA LA CONTRATACIÓN DE UN RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN (CISO) Y OFICINA TÉCNICA DE SEGURIDAD PARA EL GRUPO TERSA.

NÚMERO DE EXPEDIENTE CTTE836

1. OBJETO.

El objeto del presente procedimiento es la contratación de la figura de un responsable de Seguridad de la Información (Chief Information Security Officer -CISO-) y de una Oficina Técnica de Seguridad para el grupo TERSA.

Dado que hoy en día los sistemas de información constituyen un pilar fundamental en los procesos de una organización y tras los recientes ataques cibernéticos perpetrados a empresas similares del sector público y privado, TERSA, plenamente consciente de la relevancia de la seguridad de la información para el correcto desarrollo de sus funciones, se ve en la necesidad de contratar este servicio con el objetivo de garantizar la protección de la información y la continuidad del negocio en un marco de mejora continua.

El objeto de esta contratación es la gestión de la seguridad en sistemas heterogéneos (servicios centralizados, comunicaciones, lugar de usuario final, aplicaciones...) mediante la contratación de un servicio que integre los diferentes elementos de seguridad e infraestructura para disponer de las mejores capacidades para resolver incidentes complejos donde la correlación, coordinación y gestión de las dependencias es un factor crítico que requiere de medios materiales y personales altamente cualificados con las últimas tecnologías de seguridad.

La finalidad del contrato es planificar, organizar y garantizar la seguridad de todos los activos de información de grupo TERSA y de los sistemas que los apoyan en relación con los niveles de seguridad derivados a partir de la categorización de seguridad de los sistemas de grupo TERSA y conforme a los acuerdos de nivel de servicio que se definan para cada caso y actores correspondientes.

A la vez, se prevé establecer un marco para la mejora continua de todos los procesos relacionados con la gestión de la seguridad de la información.

2. LUGAR DE EJECUCIÓN

Todos los servicios estarán vinculados de manera general a la totalidad del grupo TERSA, incluyendo todas las líneas de negocio del grupo. En la actualidad los centros del grupo son:

- Planta de Valorización Energética de Sant Adrià de Besòs (PVE).
- Plantas Fotovoltaicas (FV) gestionadas por TERSA.
- Selectives Metropolitanes, S.A. (SEMESA).
- Solucions Integrals per als Residus, S.A. (SIRESA), incluyendo deixalleries, puntos limpios de barrio y puntos limpios de zona.
- Planta de aprovechamiento energética de biogás de la Vall d'en Joan (BIOGAS).
- Barcelona Energia (BE).

Para ampliación de la información de las líneas de negocio del Grupo TERSA, consultar la web www.tersa.cat

3. DURACIÓN DEL CONTRATO.

Se prevé una duración de dos años a partir de la formalización del contrato, sin posibilidad de prórroga.

Una vez iniciado el contrato, se establecerán hitos intermedios en función de los objetivos establecidos por el adjudicatario en su oferta del sobre 2 y de conformidad con las consideraciones realizadas por TERSA.

4. DESCRIPCIÓN Y ALCANCE DEL SERVICIO.

4.1. Descripción del servicio.

TERSA inicia este proceso de licitación con el objetivo de obtener un apoyo experto para el departamento de informática con formato de Oficina Técnica de Seguridad + Responsable de seguridad (CISO As a Service) de manera externa, para acompañar en la gobernanza de la ciberseguridad del grupo de forma completa, con una visión estratégica 360°, orientado al objeto social del grupo TERSA.

Este servicio proporcionará apoyo a la formulación estratégica y al desarrollo de normativas y políticas proactivas de seguridad hasta la implementación de estas de una forma organizada, planificada, estructurada y orientada a la obtención de resultados a través de las mejores prácticas de gestión. Además, se precisa de una disponibilidad por parte de la empresa adjudicataria para atender cualquier incidente que pueda ocasionarse en materia de seguridad de la información durante la duración del contrato.

El servicio contemplará la asistencia para la recogida in situ de evidencias forenses relativas a incidentes de seguridad y su custodia y preservación a efectos legales y/o procesales.

En todo momento el contratista estará sujeto y ejercerá el servicio objeto de esta contratación teniendo en cuenta la perspectiva medioambiental, social, laboral y de innovación que se procedan en el marco de las funciones de este contrato.

El contratista proveerá los servicios de consultoría necesarios para la implantación de lo requerido en el presente pliego teniendo en cuenta todos los activos de información y actividades existentes en el grupo TERSA y del análisis de riesgos de los mismos, de manera mensual hasta un máximo de 2 años. En relación con el objeto contractual y tras el estudio de lo englobado por grupo TERSA, se estima a modo de previsión para los licitadores una dedicación estimada de 600 horas anuales para la figura del CISO y del equipo técnico de la OTS.

En el caso que de los trabajos realizados de análisis por parte del licitador, se determine la necesidad de tramitar procedimientos de licitación para obtener los objetivos determinados en el estudio y análisis, el licitador deberá dar soporte a TERSA en la redacción de los pliegos técnicos pertinentes, así como en la realización de los informes técnicos determinados de la tramitación del procedimiento.

4.1.1. ***Responsable de Seguridad (CISO Extern AAS)***

Actuará como coordinador del servicio y como soporte directo al departamento de informática de grupo TERSA.

Será el responsable de proteger la información ante posibles ciberataques y fugas de datos. De esta manera, se garantiza la seguridad dentro de las posibilidades tanto humanas, técnicas como económicas de grupo TERSA.

Su actividad se basará los siguientes pilares de actuación:

- Alinear la estrategia de ciberseguridad con los objetivos de grupo TERSA.
- Coordinar los proyectos y actividad de la OTS (Oficina Técnica de Seguridad).
- Definir el plan director de Ciberseguridad de TERSA y realizar el seguimiento específico de su cumplimiento.
- Identificar posibles necesidades en ciberseguridad y definir estrategias para resolverlas/mitigarlas.
- Soporte experto en ciberseguridad para el área IT de TERSA dependiendo de la Dirección de desarrollo corporativo y sostenibilidad del grupo y para el comité de seguridad, el cual se prevé crear próximamente. Informar y reportar a la dirección cualquier cuestión relacionada con la ciberseguridad.
- Reuniones periódicas de seguimiento semanales de manera presencial.

A continuación, se relacionan de manera no exhaustiva algunas de las responsabilidades asociadas a la figura del CISO Externo:

- Generar y supervisar la implantación de políticas de Seguridad de la Información a fin de garantizar la seguridad y privacidad de los datos.
- Dirigir y supervisar el cumplimiento normativo vigente aplicable de la Seguridad de la información y proponer las medidas para adecuarse a nuevos marcos normativos que puedan surgir.
- Participación activa en coordinación de acciones en caso de incidencias de ciberseguridad.
- Dar respuesta rápida ante cualquier incidente de ciberseguridad.
- Llevar a cabo el descubrimiento electrónico y las investigaciones forenses digitales.
- Establecer los planes de continuidad de negocio y recuperación de desastres en el ámbito de las TIC.
- Supervisar la administración del control de acceso a la información.
- Supervisar la arquitectura de seguridad de la información de Grupo TERSA.
- Dar soporte/asesoramiento a TERSA en caso de situaciones excepcionales para llevar a cabo actuaciones específicas.
- Coordinarse con el Delegado de Protección de datos de la entidad cuando se regule aspectos o se actúe ante incidentes donde hayan podido verse afectados datos personales.
- Otras circunstancias que puedan surgir durante la ejecución del contrato relacionadas con el objeto contractual.

4.1.2. ***Oficina Técnica de Seguridad de la información.***

La Oficina Técnica de Seguridad de la Información (OTSI) proporciona el servicio de soporte técnico adecuado en el ámbito de la ciberseguridad, abarcando desde la definición de la estrategia hasta la implantación de las políticas, procesos y procedimientos que permitan conseguir los niveles adecuados de integridad, confidencialidad y disponibilidad que aseguren su continuidad operacional y de servicios.

Les funciones serán:

- Definir el plan director de seguridad de la información.
- Ayudar a definir la estrategia de ciberseguridad de TERSA y dar soporte a las TIC.
- Analizar, actualizar y mejorar las políticas/procedimientos de seguridad.
- Proponer mejoras para las medidas de seguridad existentes
- Monitorizar el estado de la seguridad TIC, con auditorías y revisiones periódicas de aplicaciones.
- Ayudar en la detección y gestión de incidentes de seguridad.
- Seguir las acciones para solucionar las debilidades detectadas.

- Proporcionar soporte experto en los proyectos de desarrollo, mantenimiento y evolución de los sistemas de información, o puesta en marcha de nuevos servicios e infraestructuras.
- Apoyo en la gestión de la continuidad del negocio.
- Dar soporte a posibles auditorías externas.
- Proponer acciones y simulacros para la formación y concienciación continua.
- Colaborar con la comunicación con terceros.
- Comunicar al Delegado cualquier incidente que afecte o pueda haberse implicados datos personales.
- Proporcionar soporte experto para la aplicación óptima de las diferentes normativas que sean de aplicación

En consecuencia, según lo establecido anteriormente en los puntos anteriores (CISO y OTS) y en base a las necesidades actuales del grupo TERSA, la planificación de acción inminente una vez adjudicado el contrato, de manera resumida, se establecería de la siguiente manera en base a los siguientes hitos:

1: Análisis de los requerimientos a cumplir por parte de TERSA.
2: Análisis de la situación actual del grupo.
3: Definición del plan director y los objetivos de seguridad y del plan de acción.
4: Seguimiento.

Una vez realizados los análisis, definidos los objetivos, el plan director y el plan de acción, y consensuado de forma explícita -documentalmente- con TERSA, se llevará a cabo la ejecución del mismo y se realizará un seguimiento para garantizar permanentemente la seguridad y la mejora continua dentro del marco de realización de la estrategia y el plan de objetivos de seguridad a corto, medio y largo plazo.

De manera puntual y externa a las reuniones periódicas, ante las dudas/consultas que puedan surgir por parte del interlocutor y responsable del contrato, el CISO y/o OTS deberán responder en un plazo máximo de 24 horas en días laborables.

4.2. Equipo de respuesta ante incidencias críticas de seguridad (disponibilidad).

El adjudicatario deberá de garantizar su disponibilidad y dar respuesta ante incidentes críticos de seguridad de la información del grupo.

En este sentido, se indican tres tipos de niveles de incidencia, sobre el cual el licitador deberá dar respuesta como máximo.

Incidencia	**Tiempo de Respuesta máximo**
Leve	72 horas
Moderada	24 horas
Grave	12 horas

Se define tiempo de respuesta como el tiempo desde la notificación de la incidencia por parte de TERSA hasta que el licitador contacta con él mismo, y inicia la resolución, ya sea de manera remota o presencial, en función de la incidencia.

Los tipos de incidencia se encuentra indicados en la siguiente tabla:

TIPOS DE INCIDENCIAS	
Incidencia	**Situación**
Leve	Incidencias de funcionamiento que no afectan al trabajo habitual y que pueden resolverse de forma planificada. Pueden ser consultas sobre relacionadas con el objeto del servicio.
Moderada	Repetición reiterativa o reincidente de determinadas incidencias leves o que se prevé un impacto inminente en algún servicio.
Grave	Denegación de servicio, parada de servicios, imposibilidad de acceso local o remoto, imposibilidad de realizar el trabajo habitual, cuando afecta a la capacidad de generar negocio en la empresa.

El presente servicio lo deberá realizar el licitador en horario laboral de lunes a viernes (de 9:00h hasta las 20:00h).

El licitador en su oferta, podrá mejorar la disponibilidad indicada en este apartado, incrementando el horario establecido como mínimo así como los días.

Con periodicidad mensual se elaborarán informes de los incidentes de seguridad, clasificados por tipologías y nivel de gravedad.

Además de con TERSA, en nombre de quien ejercerá su rol, el CISO se coordinará estrechamente con la Agencia Catalana de Ciberseguridad y con cualquier otro ente de orden superior a TERSA que en materia de Ciberseguridad sea preceptivo y/o necesario.

4.3. Intervención.

En caso de requerir intervención técnica por parte del contratista para solucionar una incidencia, la empresa adjudicataria ejecutará la misma en base a la partida alzada establecida en el procedimiento a tal fin, entre otros. Para ello, el licitador deberá ofertar un precio/hora en relación con el máximo establecido, según lo establecido en el Pliego de Cláusulas Administrativas Particulares.

La partida alzada establecida se haría efectiva en caso de incidente de ciberseguridad, donde por una cuestión de agilidad y siempre relacionado con el objeto contractual, el licitador pudiera hacer frente y dar respuesta a la incidencia detectada. TERSA se reserva el derecho de requerir a otros proveedores soluciones por otras vías, con el fin de solucionar cualquier problemática de seguridad con la mayor rapidez y diligencia posible.

El valor total de la partida alzada establecida en el presupuesto no es vinculante, se determinará en función de las tareas finalmente realizadas y solo se facturará la cantidad efectivamente ejecutada, en base al precio unitario ofertado (precio unitario máximo establecido en 60,00.-€/hora, sobre el cual el licitador podrá realizar oferta según lo establecido en el Pliego de Cláusulas Administrativas Particulares).

4.4. Equipo de trabajo y organización.

El adjudicatario deberá de poner a disposición de TERSA durante el plazo de ejecución del contrato un equipo de trabajo suficiente, con los perfiles adecuados de personas suficientemente cualificadas, con la titulación correspondiente y formación y experiencia especializada en las materias que son objeto del contrato con los conocimientos necesarios para su correcto desarrollo, con los requisitos mínimos que se indican a continuación.

El equipo deberá de estar compuesto de como mínimo:

- Un consultor experto (director del proyecto), para la figura de CISO externo con un mínimo de 7 años de experiencia en servicios similares, en relación con la gestión de proyectos y consultorías de ciberseguridad. Deberá de disponer formación universitaria en el ámbito de la informática, telecomunicaciones o equivalentes.

  Se encargará de las funciones de planificación y seguimiento del proyecto, comunicación con el cliente, organización del equipo de trabajo, distribución de tareas, consultoría,… Liderará el equipo de trabajo y el proyecto en todas sus fases para dar cumplimiento a las obligaciones contractuales y a las prioridades y calendario establecido. En ningún caso la supervisión de este equipo de trabajo será realizada por personal de TERSA.

- Un equipo técnico debidamente dimensionado y capacitado en la Oficina Técnica de la Seguridad de la Información, con el fin de realizar el servicio con la máxima diligencia. Los miembros del equipo deberán de disponer de un mínimo de 5 años de experiencia cada uno en servicios similares. El equipo deberá de disponer formación universitaria en el ámbito de la informática, telecomunicaciones o equivalentes. Se encargará de dar soporte técnico específico al director del proyecto y de realizar las tareas concretas que le sean encargadas por el mismo.

- Servicio complementario según lo indicado en la cláusula 4 (disponibilidad e intervención).

El equipo propuesto en conjunto deberá de disponer de formación específica dentro del ámbito del objeto contractual con las siguientes certificaciones acreditativas: ITIL, CISA, LEAD AUDITOR ISO27001 o equivalentes.

La totalidad del personal propuesto (CISO y equipo técnico) no se podrá modificar en el transcurso de los trabajos sin la autorización previa de TERSA y deberá personarse en las oficinas de TERSA siempre que sea necesario.

En el supuesto de modificación de personal, el adjudicatario deberá de proponer personal con la formación y experiencia mínimas requeridas en la licitación y en su caso, teniendo en cuenta las características de las personas del equipo valorado en la licitación, de acuerdo a su oferta.

TERSA se reserva la facultad de requerir al adjudicatario la sustitución de cualquier de los miembros que componen el equipo para conseguir un cumplimiento óptimo del contrato. Los gastos que se deriven como consecuencia de cambios en el equipo de trabajo irán a cargo del adjudicatario.

Se deja constancia de que TERSA queda desvinculada, a todos los efectos, de cualquier relación laboral con el personal de la entidad adjudicataria, debido a que se trata de un contrato de soporte y asistencia que debe de ser considerado como tal en su conjunto.

Por parte de TERSA, se designará:

- Un responsable del contrato para la interlocución y seguimiento.
- Un interlocutor técnico único.

La interlocución pertinente entre el Adjudicatario y TERSA, durante la ejecución de los servicios, se realizará entre el responsable TIC del grupo TERSA, y el responsable del Servicio asignados por el Adjudicatario. El adjudicatario garantizará reuniones periódicas de seguimiento semanales presenciales durante la ejecución del servicio con la dirección de responsabilidad de desarrollo corporativo y sostenibilidad.

4.5. Responsabilidades del Adjudicatario.

El adjudicatario está obligado a cumplir con todos los requisitos que se describen en el presente pliego de prescripciones técnicas en las condiciones que se indican y será el responsable de todos los efectos.

4.6. Subcontratación.

El Adjudicatario no podrá en ningún caso ceder a terceros la subcontratación de ninguna parte del alcance establecido en los pliegos sin el previo consentimiento escrito de TERSA.

TERSA podrá pedir al Adjudicatario la documentación que sea necesaria para proceder a dar su consentimiento.

El Adjudicatario tendrá que aplicar un plan específico para las empresas subcontratadas por él para que las mismas cumplan con las disposiciones contenidas en la Ley de Prevención de Riesgos Laborales, además de cualquier normativa vigente de seguridad existente en relación a la naturaleza de la acción que se tenga que desarrollar en la empresa contratista, y será responsable que los servicios se ajusten al que se establece en este PPT.

4.7. Sujeción en el marco legal vigente.

El Adjudicatario deberá cumplir fielmente con lo dispuesto en la legislación y en la reglamentación dictada por los organismos competentes, tanto europeos, estatales, autonómicos, así como locales y vigentes en cada momento.

5. RETRIBUCIÓN DEL SERVICIO

El adeudo de los servicios se hará de manera mensual en función del precio total anual ofertado por el licitador.

En los casos que sea necesaria una intervención a causa de una incidencia, los trabajos se facturarán en base a las horas efectivamente realizadas al precio hora ofertado por el contratista.

Mensualmente, el Adjudicatario procederá a la realización de un Certificado de actuación donde consten:

- Nº de pedido.
- Report mensual: Informe con una relación de las diferentes actuaciones realizadas por cada servicio (CISO / OTS), la fecha de realización y el número de horas destinadas en cada actuación.
- Concepto, deberá indicar el nº de expediente.

La Certificación de realización de los servicios mensuales deberá ser revisada y aprobada por TERSA.

Una vez aprobada la certificación, el Adjudicatario emitirá una factura con los cargos o adeudos que procedan en concepto de trabajos realizados.

6. GARANTIA

Se establece una garantía contractual de 3 meses a contar desde la finalización del servicio.

7. CONDICIONES GENERALES DE EJECUCIÓN

7.1. CLÁUSULA DE PROPIEDAD INTELECTUAL

La propiedad de los documentos y herramientas resultantes de la prestación de los servicios corresponderá en exclusividad a TERSA.

7.2. CONFIDENCIALIDAD Y SEGURIDAD

El adjudicatario se compromete a no dar ninguna información ni datos proporcionados por TERSA, ni a hacer cualquier uso no previsto en el presente pliego; en particular no proporcionará, sin previa autorización expresa del organismo, copia de los documentos y/o datos a terceras personas.

El no cumplimiento de la confidencialidad y seguridad mencionados será causa de resolución de contractual y ejercicio por parte de TERSA de las reclamaciones legales que le correspondan.

8. RESOLUCIÓN DEL CONTRATO

Además de las penalizaciones descritas en el Pliego de Cláusulas Administrativas Particulares y las establecidas en la legislación vigente, y sin perjuicio de las causas de resolución legalmente establecidas, TERSA podrá resolver el contrato, por las siguientes causas:

a) Por incumplimiento de la legislación vigente.

b) Evidencia de perfiles no cualificados en los recursos humanos aportados por el Adjudicatario, que puedan llegar a ocasionar un retraso en las actividades o perjuicio en las instalaciones.

c) No aportación de los recursos humanos necesarios para satisfacer en tiempo y forma los trabajos contemplados.

d) La falta de documentación o documentación caducada de manera reiterada en la plataforma de gestión documental de seguridad y salud.

e) Por indisponibilidad prolongada de los equipos por causas achacables a los trabajos desarrollados por el Adjudicatario.

f) Por una infracción que puede suponer un riesgo grave e inminente para la seguridad y la salud de las personas o para el medio ambiente.

Cuando se evidencie cualquiera de las causas anteriores, el Adjudicatario dispondrá de un período de tiempo, que será acordado con TERSA y cuya extensión dependerá de la gravedad del defecto, para realizar las modificaciones que estime necesarias al objeto de subsanar los defectos y conseguir el cumplimiento de las garantías. Dichas modificaciones no deberán suponer coste alguno para TERSA, ni suponer alteración alguna de las condiciones contractuales.

En caso de que TERSA decrete la suspensión forzosa de las actividades en aplicación del presente procedimiento, el Adjudicatario no podrá reclamar pago alguno en concepto de indemnización o lucro cesante.