Pliego de Prescripciones Técnicas para la contratación de la prestación de Servicios de Ciberseguridad Gestionada.

Expediente CF050-21-039

ÍNDICE

1. INTRODUCCIÓN 4
2. ANTECEDENTES 4
3. ALCANCE 4
1. SERVICIOS INICIALES 5
1.1 Objetivos 5
1.2 Tareas 5
1.3 Resultados (Hitos y Entregables) 11
2 SERVICIOS CONTINUOS 12
2.1 Objetivos 12
2.2 Tareas 12
2.3 Resultados del paquete 2 (Hitos y Entregables) 16
3 SERVICIOS A DEMANDA 16
3.1 Objetivos 16
3.2 Tareas 17
3.3 Resultados del paquete 3 (Hitos y Entregables) 17
4. ORGANIZACIÓN DEL TRABAJO 17
a) No división por Lotes 18
b) Equipo de Proyecto 18
c) Metodologías 19
d) Conformidad con madeja 19
e) Marco de seguridad 20
f) Uso de Infraestructuras TIC y herramientas corporativas 20
g) Gestión del proyecto 20
h) Equipamiento necesario 23
4.1. Plazos 23
4.2. Sistemas de Gestión del servicio 24
5. NIVEL DE SERVICIO 25
i) Lugar de ejecución de los trabajos 25

j) Horario de atención 25
k) Acuerdos de Niveles de Servicio (SLA) 26
l) Criticidades 27
6. CONDICIONES GENERALES 28
m) Propiedad de los Trabajos 28
n) Transferencia tecnológica 28
o) Control de Calidad 28
p) Garantía 29
7. ANEXO I. SISTEMAS PREEXISTENTES, ARQUITECTURA Y NIVELES DE CRITICIDAD 31
8. ANEXO II- CLÁUSULA DE CONFIDENCIALIDAD 32

1. INTRODUCCIÓN

Verificaciones Industriales de Andalucía, S.A, en adelante VEIASA, es una empresa del Sector Público Andaluz, adscrita a la Consejería de Hacienda y Financiación Europea de la Junta de Andalucía, fundada en 1990 con el objetivo de realizar las actuaciones de inspección y control derivadas de la aplicación de las distintas reglamentaciones industriales y la prestación de todo tipo de servicios que contribuyan al desarrollo de la industria en la comunidad autónoma de Andalucía.

VEIASA cuenta con una serie de aplicaciones web, tanto de consumo interno como de servicio a la ciudadanía, que requieren de la implantación dentro del modelo organizativo de seguridad de la información de VEIASA, de servicios de seguridad gestionada que garantice un nivel de control razonable sobre los ciber-riesgos a los que se encuentra expuesta la organización, mediante la provisión integral de un conjunto de servicios en el ámbito de los servicios externos.

2. ANTECEDENTES

La publicación de aplicaciones web de VEIASA se explota actualmente a través de servicios externos de alojamiento, siendo necesario proteger los activos de información expuestos en cada caso.

Para dar cumplimiento al marco normativo y legal vigente actualmente (ENS, RGPD, Normativa Seguridad Junta de Andalucía) es necesario contar con mecanismos de vigilancia continuada a través de servicios de SOC, así como la posibilidad de realizar auditorías de seguridad a demanda, una vez evaluada la situación actual de exposición de estos activos de información.

3. ALCANCE

El objeto del presente documento es dotar a VEIASA de una solución técnica que asegure la correcta gestión de seguridad de los sistemas de información, entre otros:

- Servidores y aplicaciones CORE incluidos en el alcance del ENS
- Vigilancia Digital y Reputación Corporativa
- Webs Públicas y aplicaciones móviles

VEIASA proporcionará a los licitadores (Anexo I del PPT), un documento detallado con todos los sistemas preexistentes, su arquitectura y los niveles de criticidad a los efectos de su integración con la solución propuesta.

Este anexo es de carácter confidencial, por lo que será remitido al licitador previa solicitud al correo licitaciones@veiasa.es, debiendo aportar en dicha solicitud la Cláusula de Confidencialidad (Anexo II del PPT) debidamente cumplimentada, firmada y sellada por representante con poder suficiente (debiendo acreditarse igualmente el poder de representación).

1. SERVICIOS INICIALES

1.1 Objetivos

Los objetivos de este paquete son:

- Conocer la situación inicial a nivel tecnológico y de estado de ciberseguridad de los servicios, externos, como punto de partida para la realización del resto de las actuaciones.
- Implantar los servicios de protección necesarios para asegurar una correcta gestión de la seguridad y cumplimiento del ENS de los sistemas y aplicaciones de VEIASA

1.2 Tareas

1.2.1 Evaluación inicial de seguridad

Se propone realizar una auditoría técnica de seguridad con el fin de estudiar el estado general de las infraestructuras, sistemas y aplicaciones detectar las debilidades y proponer un plan de acción para corregirlas.

Para los análisis no se proporcionará información adicional ni se especificarán objetivos, ya que el objetivo de esta auditoría es detectar el máximo número de vulnerabilidades y analizar su posible explotación, adoptando el auditor el mismo papel que desempeñaría un eventual hacker para descubrir y explotar vulnerabilidades.

Se pretenden descubrir los siguientes tipos de vulnerabilidades:

- **Vulnerabilidades de los Sistemas Operativos y Aplicaciones Comerciales:** Se pretende encontrar aquellas vulnerabilidades que puedan existir en los sistemas operativos y en las aplicaciones comerciales de los servicios

auditados y que puedan ser explotadas para conseguir accesos no autorizados.

- **Vulnerabilidades en Aplicaciones Propietarias:** Se pretende verificar el nivel de seguridad que posee el desarrollo de los servicios web analizados, comprobando si existen deficiencias en la programación que pudieran ser aprovechadas por un atacante.

- **Vulnerabilidades en la Red Corporativa:** Se estudiarán las posibilidades de que un atacante se adentrase en la LAN de la arquitectura de red de VEIASA y la posibilidad de escalar privilegios.

Explotación de vulnerabilidades: Las vulnerabilidades detectadas se intentarán explotar, si es posible, demostrando los resultados obtenidos para justificar las consecuencias de un acceso no autorizado.

Para descubrir los puntos débiles del sistema se realizarán tres tipos de ataques:

- **Pasivos:** recogiendo toda la información posible de los sistemas. Este tipo de ataque facilitará el tener un mejor conocimiento del objetivo para lanzar posteriormente ataques activos.
- **Activos:** aplicación de los conocimientos recogidos para intentar violar la seguridad existente.
- **Intrusivo:** si se ha logrado violar la seguridad existente, se intentará obtener un mayor nivel de acceso. En ningún caso se realizarán actividades potencialmente peligrosas para la integridad del sistema o servicio, este tipo de ataque será únicamente para recoger evidencias.

1.2.1.1 Actividades de la auditoría

Se llevarán a cabo una serie de pruebas a las aplicaciones simulando, en la medida de lo posible, un ataque real realizado por un usuario externo o interno dependiendo del servicio atacado. El objetivo de las pruebas es poder determinar qué vulnerabilidades tienen los servicios, cuáles se pueden explotar y qué nivel de acceso se puede conseguir una vez se vulnera la seguridad de un sistema.

El alcance de los trabajos para cada uno de los sistemas auditados Incluirá entre otros:

- Análisis de la Redes Públicas (Footprinting)
  - Análisis e identificación de Servicios
  - Seguridad en la red interna

i. Descubrimiento de dispositivos, redes, servicios y protocolos

ii. Descubrimiento de activos internos

iii. Análisis red Interna

- Seguridad en los accesos.
  - Análisis de los elementos de seguridad perimetral
  - Análisis de las aplicaciones

1.2.1.2 Resultados de la auditoría

Como resultado de la auditoría se emitirá un informe que contendrá los siguientes capítulos:

- Resumen ejecutivo, con una evaluación global del estado de seguridad de la aplicación y de las eventuales consecuencias que puede tener la no corrección de las vulnerabilidades detectadas, desde un punto de vista ejecutivo.
- Pruebas realizadas y resultado. Se detallarán los distintos aspectos probados y si se considera que la aplicación es segura o no para cada aspecto analizado.
- Vulnerabilidades detectadas. Se especificará cada vulnerabilidad detectada, los riesgos que conlleva y sugerencias para su resolución.
- Propuesta de plan de acción. Una lista de recomendaciones concretas que deberían llevarse a cabo para mejorar la seguridad de la aplicación.

1.2.2 Elaboración del Procedimiento de Respuesta ante Incidentes

Ante una incidencia de seguridad es preciso llevar a cabo una serie de actividades para dar respuesta al mismo, tanto de índole organizativo como técnico, que deben estar documentadas en un plan.

Estas tareas abarcarían desde el momento de detección de la incidencia hasta su recuperación y vuelta a la normalidad. Entre ellas, los aspectos de comunicaciones (tanto a nivel interno como externo) son un factor clave.

Así pues, dentro de esta actividad, el adjudicatario desarrollará un plan de respuesta a incidentes, con especial foco en el proceso de comunicación.

Este plan será realizado de forma que permita la estabilización, continuación, reanudación y recuperación de las actividades y sus recursos de apoyo a nivel de IT.

Este plan será de carácter organizativo, alineado con los requisitos regulatorios del ENS y la RGPD y contemplando la norma ISO 22301 de gestión de la continuidad. Asimismo, contemplará los diferentes planes que en materia de gestión de incidencias estén desarrollados o se estén desarrollando en la entidad.

El plan de respuesta a incidentes cubrirá los siguientes bloques temáticos:

- Documentación sobre los equipos de recuperación.
- Procedimientos de frenado de la emergencia.
- Procedimientos de notificación de la emergencia.
- Procedimiento de declaración de la emergencia
- Comunicación de la Emergencia, tanto a nivel interno como externo:
- Plan de movilización de recursos: Internos y externos.
- Plan de actuación para recuperación de los servicios.
- Monitorización continua de la situación y comunicación del estado.
  - Fin de la emergencia.

El plan contemplará las necesidades de coordinación con otras áreas en los aspectos en los que se requiera de su concurso.

El Plan recogerá los datos de contacto de los participantes en el mismo, tanto a nivel de empleados internos como de proveedores involucrados.

1.2.3 Servicios de protección avanzada

Se incluirán todos los sistemas de monitorización y protección necesarios para asegurar una correcta gestión de la seguridad, esto es:

- Sistema de protección de aplicaciones
- Sistema de monitorización y protección ante amenazas de eventos
- Sistema de guarda y custodia de eventos
- Sistema de monitorización y gestión de eventos

Toda la tecnología necesaria para la ejecución del proyecto, incluyendo hardware, software y suscripciones de cualquier tipo, será proporcionada por el licitante en modo servicio siendo obligatorio que disponga de mantenimiento y soporte en régimen 24x7 y actualizaciones durante toda la vigencia del contrato, comprometiéndose el adjudicatario a conservar todos

los elementos dentro de los parámetros necesarios para asegurar el soporte por parte de los respectivos fabricantes.

VEIASA pondrá a disposición del adjudicatario el espacio necesario dentro de bastidores de 19 pulgadas para los elementos que deban albergarse en sus instalaciones.

Se deberá incluir una descripción y un plan de implantación detallado de cada uno de los sistemas, justificando que se cumplen, al menos, los requisitos mínimos establecidos a continuación.

1.2.3.1 Sistema de Protección de Aplicaciones Web

Se incluirá la implantación de un servicio y de firewall de aplicaciones web (web application firewall).

Los requisitos mínimos del sistema ofertado serán los siguientes:

- Protección de las aplicaciones y servicios web ante ataques a nivel de aplicación y ataques de denegación de servicio de nivel 7 de manera proactiva
- Soporte para múltiples servicios, hasta 5 FQDN
- Ancho de banda 25 Mbps, con capacidad de atender picos puntales de hasta 200 Mbps
- AntiScrapping 25 Mbps, con capacidad de atender picos puntales de hasta 200 Mbps
- Capacidad para repartir la carga de proceso de aplicaciones entre distintos servidores backend, incluyendo mecanismos de distribución con múltiples criterios.
- Mecanismos de protección básicos, Panel de control de cumplimiento del Top 10 OWASP
- Mecanismos de identificación y protección avanzados:
    - Generación de firmas dinámicas de capa 7 en tiempo real para la mitigación de ataques de DDoS incluyendo detección dinámica de latencias del servidor
    - Soporte de análisis de comportamiento para la mitigación de DDoS de nivel 7 en un número ilimitado de servicios
    - Protección frente ataques de DDoS en la negociación de TLS mediante fingerprinting del stack TLS presentado por el cliente
    - Protección mediante cifrado de los campos sensibles de las aplicaciones web en el navegador cliente

- Garantía de integridad de datos, detectando al menos la manipulación de parámetros en URLs y peticiones AJAX
- Protección anti-bot con mecanismos de captcha y challenge de javascript para detección e identificación de navegadores y comportamiento de usuario
- Identificación de URLs con gran consumo en los servidores como vector de ataque de DDoS
- Verificación de las firmas de ataque en las respuestas del servidor al usuario
- Enmascaramiento de información sensible enviada por el servidor
- Bloqueo basado en la ubicación geográfica (base de datos de geolocalización incluida)
- Descarte de paquetes de una IP sospechosa una vez detectado un ataque
- Verificaciones de seguridad y validación en protocolos FTP y SMTP

- Protección a Web Services XML y restricción al acceso mediante métodos definidos vía Web Services Description Language (WSDL)
- Opción de alimentarse de una base de datos reputación de IPs que permita bloquear tráfico desde y hacia direcciones IP en categorías como: scanners, Windows exploits, denial of services, proxies de phishing, botnets, proxies anónimos
- Capacidad de integración con firewalls de bases de dato, al menos, Oracle Database Firewall

1.2.3.2 Sistema de guarda y custodia de eventos.

Se incluirá una solución de Syslog interna, alojada en las instalaciones de VEIASA, que cumpla, al menos, con la siguientes condiciones:

- Capacidad de administrar y retener los mensajes de Syslog, capturas SNMP y registros de eventos de Windows.
- Capacidad de generar políticas de retención personalizadas que permitan retener los eventos al menos tres años.
- La solución debe contar con un almacenamiento de al menos 25 TB

- Se debe proporcionar un plan de backup que permita generar copias, semanales, mensuales y anuales de los eventos.

1.2.3.3 Sistema de monitorización y gestión de eventos

Se incluirá un sistema de gestión de eventos de información de seguridad (Security Information and Event Management), en adelante SIEM, que permita la monitorización y la correlación de eventos de seguridad, integrando las fuentes de datos dentro del alcance, con el objetivo de detectar anomalías de seguridad y generar alertas que permitan la adecuada clasificación del nivel de amenaza de cualquiera de los incidentes de seguridad detectados.

El licitador detallará la arquitectura de componentes del sistema SIEM propuesto, incluyendo todos los elementos de recolección, agregación y procesamiento de eventos, así como la ubicación de los mismos.

Se cumplirán, al menos , los siguientes requisitos:

- Licenciamiento para el uso de , al menos, 2500 EPS
- Posibilidad de acceso a la consola de administración a los perfiles que VEIASA.
- Posibilidad de ofuscar campos o parte del log para evitar que los analistas vean ciertos datos en claro.
- Incorporación de algoritmos de Machine Learning para modelar el comportamiento habitual de usuarios y detectar desviaciones
- Capacidad de detectar el uso de un nuevo nombre de usuario o de una nueva IP en el entorno
- Capacidad de análisis de comportamiento de usuarios estableciendo patrones de comportamiento habitual y alertando ante desviaciones de las mismas
- Capacidad de integración en aplicaciones cloud.
- Soporte para automatizaciones basadas en aprendizaje (machine learning).
- Soporte para automatizaciones basadas en análisis de comportamiento de entidades y usuarios (user and entity behavior analytics).
- Casos de uso propuestos para la correlación de eventos mantenido por un equipo de expertos.
- Integración con todos los elementos de la infraestructura de VEIASA y con el resto de las herramientas propuestas.

1.3 Resultados (Hitos y Entregables)

1.3.1 HITOS

- Auditoria inicial de seguridad

- Sistema de monitorización y protección implementados y funcionando correctamente

1.3.2 PRODUCTOS ENTREGABLES

- Informe de auditoría externa
- Informe de auditoría Interna
- Procedimiento de Respuesta ante Incidentes
- Documentación de instalación y configuración completa de los diferentes sistemas de protección

2 SERVICIOS CONTINUOS

2.1 Objetivos

El objetivo de este paquete de servicios es:

- Disponer de servicios de control de la ciberseguridad que permitan una monitorización y control de la seguridad permanentes (24x7x365).
- Gestionar los incidentes de seguridad cubriendo todo el ciclo de la gestión de incidentes.
- Disponer de un servicio de operación y mantenimiento de los sistemas de protección que aseguren su correcta evolución.
- Contar con un asesoramiento permanente tanto reactivo (consultas) como proactivo (información sobre novedades y alertas).

2.2 Tareas

Para abordar los objetivos del paquete se llevarán a cabo las siguientes tareas, dentro del plazo de duración del contrato, previsto para XXX meses:

- Monitorización y control 24x7x365 Asesoramiento permanente.

2.2.1 Monitorización 24x7 de seguridad e identificación de amenazas

Orientado principalmente a la detección continúa de vulnerabilidades, anomalías e incidentes de seguridad.

Las funciones contempladas en este servicio son:

- Escaneos de vulnerabilidades continuos de elementos de seguridad perimetral, redes y servidores, permitiendo conocer los puntos débiles de los sistemas de manera permanente y enviar avisos ante las debilidades encontradas.
- Análisis de los eventos reportados por las distintas fuentes de datos.
- Gestión de casos de uso de las diferentes herramientas.
- Seguimiento 24x7 de las alertas generadas por las diferentes herramientas gestionando aquellas que supongan un posible incidente de seguridad.
- Monitorización permanente de parámetros de seguridad en tiempo real con objeto de detectar y reportar anomalías de la manera más inmediata posible.
- Establecimiento de filtros en la herramienta SIEM para optimizar la detección de actividades potencialmente peligrosas.

2.2.2 Administración y gestión de los sistemas de protección avanzada

Se deberá incluir un servicio de operación, gestión y mantenimiento para todos los sistemas de protección ofertados, con un horario de atención 24x7 y realizando, entre otros, la siguientes actividades:

- Alta, bajas y modificaciones de reglas de acceso.
- Control, planificación y coordinación de actuaciones programadas (Cambios de configuración, actualizaciones, etc.).
- Mantenimiento preventivo y monitorización permanente.
- Resolución de incidencias.
- Mantenimiento correctivo y resolución de problemas.
- Definición de nuevos casos de uso según las necesidades detectadas durante la ejecución del proyecto.
- Consultoría para viabilidad de nuevas configuraciones a implementar.

2.2.3 Monitorización permanente de disponibilidad

Los servicios de monitorización de disponibilidad permitirán conocer la indisponibilidad de un servicio en el mismo momento que se produce con el objetivo de valorar si la indisponibilidad viene derivada de un problema de seguridad o por cualquier otro tipo de problema técnico.

El adjudicatario incluiría la monitorización de los servicios dentro del alcance de la propuesta a través de una herramienta que permita mantener una

monitorización de los sistemas 24x7 y evaluar la disponibilidad de manera externa, incluyendo la disponibilidad de las comunicaciones.

2.2.4 Gestión de incidentes de seguridad

El adjudicatario se compromete a apoyar con las acciones reactivas necesarias para dar respuesta a los ataques y/o incidentes de seguridad que pudiera requerir VEIASA, estas acciones se realizarán siempre de acuerdo con la Política de Seguridad de VEIASA ante los eventos contemplados en ella. Se desatacan en estas acciones:

- Identificación de sistemas y servicios afectados.
- Identificación del origen: acceso no autorizado, vulnerabilidad explotada, malware, etc.
- Revisión de los registros de los elementos de seguridad perimetral: IDS, proxy, firewall, etc.
- Revisión y análisis de trazas de los sistemas afectados.
- Determinación del alcance del incidente.
- Determinación de medidas correctivas..

2.2.4.1 Análisis Forense

Al término de la revisión de todos los datos adquiridos en fase de gestión del incidente de seguridad, se emitirá un informe técnico que lo describa detalladamente. El informe constará de los siguientes puntos.

- Objeto del informe, donde se describe el objeto principal del informe y se detallan todos los puntos tratados.
- Descripción, donde se describe de manera clara el incidente analizado y sus consecuencias.
- Evidencias, donde se describe y muestran de forma detallada los datos y evidencias obtenidas del estudio de los diferentes sistemas.
- Conclusiones y recomendaciones, donde se describen de manera detallada las conclusiones del estudio y se proponen las medidas necesarias para evitar que el incidente se repita.

2.2.5 Vigilancia digital y alerta temprana

Servicio 24x7 de monitorización y análisis de fuentes abiertas y ocultas en las que se halle información que pueda afectar a los activos digitales de VEIASA, detectando los siguientes riesgos:

- **Reputación y marca**
  - **Suplantación de identidad corporativa,** detección de cualquier actividad que suplanten la marca de VEIASA y/o haga uso indebido de logos y la imagen corporativa.
  - **Publicación de contenidos ofensivos,** Identificación de comentarios y contenidos fraudulentos y/o ofensivos, que puedan dañar la imagen o la reputación de VEIASA
  - **Counterfeit,** Identificación de sitios web o perfiles de redes sociales que se hagan pasar por canales oficiales de VEIASA.
- **Amenazas y fraude on-line**
  - **Hactivismo y Activismo,** búsqueda de los diferentes grupos activos de información relevante de posibles ataques a VEIASA, tanto contra los activos de la red como contra la seguridad física y de las personas pertenecientes a la organización. Búsqueda de publicaciones referentes a debilidades y como explotarlas.
  - **APTs contra el sector,** recopilación de información sobre ataques dirigidos o actividad maliciosa creciente en otros organismos del sector**.**
  - **Robo de credenciales corporativas,** credenciales y email corporativos con contraseña asociada expuestos públicamente o la Dark web.
  - **Phishing,** detección de campañas de correo enviadas con nombre VEIASA a otros usuarios de la red y de campañas que tengan como objetivo los usuarios de VEIASA.
- **Canal Móvil:** Detección y retirada de apps sospechosas de markets oficiales y/o alternativos,

2.2.6 Asesoramiento permanente

Bajo esta actividad se prestará un servicio de asesoramiento permanente que cubrirá los siguientes aspectos:

- Actualización sobre novedades y alertas de seguridad ("boletín de seguridad"). Se emitirá un boletín con carácter trimestral en el que aparecerán las principales novedades en materia de seguridad técnica y legal.
- Propuesta de medidas preventivas adicionales.
- Propuesta de iniciativas de formación.

2.3 Resultados del paquete 2 (Hitos y Entregables)

2.3.1 HITOS

Hitos de avance en la ejecución de los servicios.

2.3.2 PRODUCTOS ENTREGABLES

- Informes mensuales: Se realizará un informe mensual con el resumen de actividades del periodo, elaborado por la jefatura de proyecto, que recogerá todas y cada una de las actuaciones realizadas durante el periodo y el estado de las tareas pendientes. Se incluirá, además, un apartado resumen de los incidentes de seguridad detectados durante el periodo y apartado exclusivo de vulnerabilidades, con el contenido detallado de las vulnerabilidades encontradas y las soluciones propuestas para eliminar dichas vulnerabilidades. Este informe contendrá un apartado de cumplimiento de SLA y KPI.

- Informe específico de vulnerabilidades significativas: En el caso de la aparición de una vulnerabilidad significativa, bien por su gravedad o por el impacto que pueda tener en la infraestructura de VEIASA, el adjudicatario avisaría inmediatamente a VEIASA, por los cauces establecidos y elaboraría un informe específico con todos los datos necesarios para la identificación y corrección de la vulnerabilidad.
- Respuestas a las consultas realizadas a través del servicio de asesoramiento

3 SERVICIOS A DEMANDA

3.1 Objetivos

Los objetivos de este paquete son:

Disponer de un servicio bajo demanda para ejecutar pruebas de seguridad, formaciones y pruebas en herramientas adicionales a las contempladas en el resto de servicios.

3.2 Tareas

Para prestar este servicio se propondrá una bolsa de horas , con un alcance mínimo de 200 horas, que podrán consumirse a demanda dependiendo del tipo de trabajo requerido, entre otros:

- Auditorías de seguridad adicionales para aplicaciones externa y/o internas
- Informes técnicos a demanda sobre herramientas de seguridad: DLP, MDM CASB ..etc
- Formación técnica especializada en Ciberseguridad:
    - Ejercicios de phishing
    - Formación de ciberseguridad para Administradores de sistemas
    - Formación de ciberseguridad para Administradores de redes
    - Formación de Desarrollo seguro

3.3 Resultados del paquete 3 (Hitos y Entregables)

3.3.1 HITOS

Consumo de la bolsa de auditorías

3.3.2 PRODUCTOS ENTREGABLES

- Resultados de las tareas solicitadas bajo demanda

4. ORGANIZACIÓN DEL TRABAJO

Todos los trabajos para realizar dentro del alcance de este proyecto se realizarán bajo la dirección técnica del responsable del proyecto por parte de VEIASA y dentro del marco general del proyecto.

Todas las actividades y entregables tienen que ser supervisados y acordados por el responsable del Proyecto por parte de VEIASA.

En virtud de lo dispuesto en el artículo 62 LCSP, se designa como responsable del contrato a la Jefatura de la Unidad de Mantenimiento de Sistemas de Información de VEIASA, a quien corresponderá supervisar su ejecución y adoptar las decisiones y dictar las instrucciones necesarias, con el fin de asegurar la correcta realización de todos los trabajos pactados, dentro del ámbito de facultades que el órgano de contratación le atribuya.

a) No división por 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.

b) Equipo de Proyecto

Para la realización de los trabajos descritos en el apartado anterior, el adjudicatario deberá contar con una serie de perfiles expertos en seguridad técnica y legal, en disposición de las certificaciones más relevantes en materia de seguridad.

De conformidad con lo dispuesto en el apartado 6 del Cuadro Resumen, en la siguiente tabla se recogen los perfiles propuestos:

Perfiles	Función en el servicio
1 Jefe de Proyecto	Ver funciones del jefe de Proyecto en el apartado 4.g) donde se detallan las funciones Responsable de la Empresa Adjudicataria/Jefe de Proyecto
2 Consultor en seguridad legal y estratégica	Tareas de seguridad legal y organizativa: auditorías de seguridad y procedimiento de gestión de incidentes

Perfiles	Función en el servicio
4 Consultores en seguridad técnica	Tareas de seguridad técnica: auditorías de vulnerabilidades, monitorización, análisis técnicos, tareas de seguridad bajo demanda (técnicas)
10 técnicos de seguridad técnica	Soporte a la realización de las tareas de seguridad en horario 24x7

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 a la mayor brevedad, sin que esto afecte ni a la planificación de trabajos prevista ni a la estimación de costes del proyecto.

c) Metodologías

El adjudicatario deberá entregar toda aquella documentación técnica y de gestión del proyecto, así como cualquier documentación adicional que, a juicio de VEIASA, sea necesaria para alcanzar los objetivos del producto en cada momento.

Tanto para la organización del trabajo como para las fases de desarrollo y los productos a obtener se tendrá como referencia la metodología para la planificación y el desarrollo de sistemas de información METRICA v3 publicada por el Ministerio de Política Territorial y Administración Pública. Dadas las especiales características de este trabajo, los procesos y las actividades que indica la metodología se adaptarán al mismo con el objeto de conseguir la mayor eficacia en su desarrollo.

La Dirección del Proyecto aprobará al comienzo del mismo las directrices metodológicas e interpretará de igual modo las posibles dudas que sobre su aplicación puedan surgir a lo largo de la ejecución del proyecto.

Todos los productos obtenidos en el marco de este proyecto se adaptarán a los estándares de todo tipo (codificación, identidad corporativa, nomenclatura, etc.) definidos por VEIASA.

d) Conformidad con madeja

Durante la realización de los trabajos se tendrán en cuenta los recursos proporcionados por madeja (marco de desarrollo de la Junta de Andalucía), así como las pautas y

procedimientos definidos en este. Como norma general, se aplicarán aquellas pautas y procedimientos de carácter obligatorio. Para el resto, el grado de aplicación será establecido por la dirección de proyecto.

La versión actual de madeja estará disponible en la dirección http://www.juntadeandalucia.es/servicios/madeja/ donde también podrá consultarse el histórico de versiones.

e) Marco de seguridad

Las proposiciones deberán garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información que constituye el Esquema Nacional de Seguridad, regulado por el Real Decreto 3/2010, de 8 de enero. En concreto, se deberá asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que son objeto de la presente contratación.

Para lograr esto, se aplicarán las medidas de seguridad indicadas en el anexo II del ENS, en función de los tipos de activos presentes en el sistema de información y las dimensiones de información relevantes, considerando que el sistema de información recae en la categoría de seguridad <<<BÁSICA | MEDIA | ALTA >> conforme a los criterios establecidos en el anexo I del ENS.

Además, se deberá atender a las mejores prácticas sobre seguridad recogidas en las series de documentos CCN-STIC (Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones), disponibles en la web del CERT del Centro Criptológico Nacional (http://www.ccncert.cni.es/), así como a las recomendaciones de Andalucía-CERT, como centro especializado en la materia en el ámbito andaluz.

f) Uso de Infraestructuras TIC y herramientas corporativas

Se tendrán en cuenta todas las infraestructuras TIC (sistemas de información, tecnologías, frameworks, librerías software, etc.) que en la junta de Andalucía tenga la consideración de corporativas u horizontales y sean susceptibles de su utilización.

g) Gestión del proyecto

Los objetivos en la gestión del proyecto son los siguientes:

- Garantizar que el proyecto es realizado en tiempo y forma, con los recursos previstos y cumpliendo con los compromisos de entrega y calidad, objetivos y planificación de los trabajos.
- Proveer las garantías de que el cliente dispondrá de los mecanismos para continuar con el proceso de mantenimiento de la seguridad una vez finalizado el proyecto.

Para abordar los objetivos, en primer lugar, se establecerán los órganos de gestión del proyecto que, sin perjuicio de que sean modificados al arranque del proyecto, son los que a continuación se proponen, y que están alineados con el PPT:

Órgano de gestión	Funciones
Director de Proyecto de VEIASA (responsable del contrato)	* Dirigir, supervisar y coordinar la realización y desarrollo de los trabajos. * Asegurar el seguimiento de la planificación y programa de los trabajos. Hacer cumplir las normas de funcionamiento y las condiciones estipuladas en el RFP. * Aprobar y comunicar al Jefe de Proyecto los contenidos de los trabajos para su realización. * Velar por el nivel de calidad de los trabajos. * Coordinar las entrevistas entre usuarios y técnicos involucrados en el Proyecto. * Aprobar los resultados y certificaciones parciales o totales de la realización de los proyectos.
Responsable de la Empresa Adjudicataria/Jefe de Proyecto	* Interlocución con el Cliente. * Dirección, seguimiento y control del proyecto. * Generación de documentación de control del proyecto. * Revisión de los trabajos y la documentación realizada por el equipo de trabajo. * Garantizar la calidad de los productos finales. * Colaborar directamente en la dirección de los trabajos en estrecha relación con el responsable de los mismos.

	Estructurar el funcionamiento y las tareas del equipo de trabajo. * Organizar las relaciones del equipo de trabajo con el responsable de los trabajos. * Coordinación y asistencia a la dirección en las reuniones de seguimiento general de los trabajos.
Comité de Dirección del Proyecto (Jefe de Proyecto y Responsable del Contrato)	* Concreción de detalle de los plazos de ejecución del Proyecto. * Control de las desviaciones producidas frente a la planificación del Proyecto. * Seguimiento de acuerdos y métodos de trabajo. * Determinar la puesta en marcha de las distintas fases del proyecto. Posibles adaptaciones del Plan de Ejecución del Proyecto para un mejor cumplimiento de los objetivos finales perseguidos.
Comité Técnico del Proyecto (personal técnico del servicio de informática de VEIASA y consultores de la Empresa Adjudicataria)	* Proporcionarán información al Jefe de Proyecto sobre el avance de los trabajos. Participará en las reuniones de seguimiento de carácter técnico/jurídico, tomando decisiones de carácter técnico/jurídico relacionadas básicamente con el contenido de los entregables, en particular con la aprobación de las versiones finales.

La gestión se llevará a cabo a través de una serie de tareas que se dividirán en tres fases:

- Actividades de la Fase de gestión inicial.
- Actividades de la Fase de gestión de ejecución.
- Actividades de los Procesos de gestión de finalización.

h) Equipamiento necesario

El personal de la empresa adjudicataria prestará los servicios con sus propios equipos de trabajo (vehículos, ordenadores portátiles, etc.).

Según lo dispuesto en el apartado 6 del Cuadro Resumen, el equipamiento informático para el puesto de trabajo que debe utilizar el personal de la empresa adjudicataria consistirá en un ordenador fijo o portátil con los siguientes requerimientos:

- Sistema operativo Windows 10Profesional con las últimas actualizaciones del fabricante.
- Ofimática con Microsoft Office.
- Microsoft Project (como mínimo para los perfiles de Jefe de Proyecto). Cliente de Correo electrónico.

Estos requerimientos pueden ser gestionados con la Unidad de Mantenimiento de Sistemas de Información para su correcta integración con los sistemas de VEIASA.

4.1. Plazos

El contrato tendrá una duración máxima de 12 meses, con una carga de trabajo estimada de 3.620 horas. El contrato podrá ser prorrogado por otro periodo de 12 meses y una carga de trabajo estimada de otras 3.620 horas.

Así pues, el contrato podrá alcanzar una duración máxima total de 24 meses, con una carga de trabajo estimada de 7.240 horas.

En el caso de que se consuma el presupuesto máximo establecido (importe de licitación) antes del transcurso de los 12 MESES de vigencia inicial del contrato, las partes podrán acordar la entrada en vigor de la prórroga prevista en dicho momento, comenzando su vigencia, por tanto, a partir del instante en que se consuma dicho presupuesto máximo.

Por el contrario, si a la finalización de la vigencia inicial del contrato (12 meses) no se hubiese consumido la totalidad del presupuesto máximo establecido (importe de licitación), el importe restante no consumido podrá acumularse al presupuesto máximo establecido para la prórroga, en caso de que se haga efectiva.

En consecuencia, el importe total a abonar a la empresa adjudicataria, en ningún caso, podrá superar el valor estimado total indicado en el apartado 2.2 del Cuadro Resumen del PCAP.

El inicio de los trabajos deberá realizarse dentro de los 35 días laborables siguientes a la notificación del pedido a la empresa adjudicataria.

4.2. Sistemas de Gestión del servicio

Las empresas licitadoras deberán acreditar que disponen de:

- Un sistema de gestión del servicio TI tal como viene detallado en la norma ISO 20000. Las empresas licitadoras podrán acreditar el sistema de gestión requerido mediante la aportación de la certificación ISO 20000, certificación equivalente o cualquier sistema propio del licitador donde se acredite dicha gestión de servicio.

  La norma ISO 20000 sirve como control exhaustivo de la gestión de los servicios de gestión y soporte TI para operar bajo unos procesos que sirvan para conseguir un servicio efectivo. En la norma se especifican procesos relacionados con la configuración de los sistemas, así como la gestión y solución de problemas en la TI, de manera que se garantice la eficacia y disponibilidad del servicio. Además, y como una de las características más importantes, la norma se alinea con otras normas que son aplicables al servicio licitado como la 27001 y el ENS.

- Un sistema de seguridad de la Información tal como viene detallado en la norma ISO 27001. Las empresas licitadoras podrán acreditar el sistema de seguridad de la información requerido mediante la aportación de la certificación ISO 27001, certificación equivalente o cualquier sistema propio del licitador donde se acredite dicho sistema de seguridad de la información.

  Dado que el servicio licitado es el Alojamiento del Portal de Proveedores que está expuesta de manera pública en Internet, el objetivo de solicitar esta certificación es, por un lado, que el licitador tenga implantada en su organización la ciberseguridad para proteger los activos de información objeto del servicio, y por otro, disponer de los controles y procedimientos más eficaces y coherentes para proteger esos activos y minimizar los riesgos, de tal manera que se garantice:

  - La *confidencialidad* de la información, asegurando que sólo quienes estén autorizados puedan acceder a la información.
  - La *integridad*, asegurando que la información y sus métodos de proceso son exactos y completos.
  - La *disponibilidad*, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

- Un sistema de seguridad de la Información tal como viene detallado en el Esquema Nacional de Seguridad (ENS) de nivel medio. Las empresas licitadoras podrán acreditar el sistema de seguridad de la información requerido mediante la aportación de la certificación ENS nivel medio o superior, certificación equivalente o cualquier sistema propio del licitador donde se acredite dicho sistema de seguridad de la información.

El ámbito de aplicación del Esquema Nacional de Seguridad es el establecido en el artículo 2 de la Ley 11/2007, de manera que es de aplicación:

- A la Administración General del Estado, Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas.
- A los ciudadanos en sus relaciones con las Administraciones Públicas.
- A las relaciones entre las distintas Administraciones Públicas.

Los Sistemas de Información de VEIASA están catalogados como nivel medio en términos del ENS, y VEIASA como empresa pública que es, está obligada por ley a cumplir con los controles del ENS nivel medio, y por extensión, exigir ese cumplimiento a todos los proveedores que presten servicio que impliquen un tratamiento de datos.

5. NIVEL DE SERVICIO

En este apartado se describen una serie de consideraciones adicionales que VEIASA entiende como claves a la hora de establecer las condiciones del servicio ofertado.

i) Lugar de ejecución de los trabajos

El adjudicatario realizará las labores de soporte de los sistemas, con carácter general, desde sus propias instalaciones, pudiéndose contemplar desplazamientos para aquellas tareas que, por su naturaleza, solo puedan ser ejecutadas in-situ. En base a esto, se articularán dos tipologías de soporte:

- **Soporte remoto:** Se trata del mecanismo de soporte habitual, prestado desde el Centro de Servicio de la empresa adjudicataria por el equipo de proyecto asignado. Comprende la operativa rutinaria asociada al Servicio de Soporte.
- **Presencial in-situ**: Se contemplan desplazamientos de un técnico de la empresa adjudicataria a las instalaciones de Servicios Centrales de VEIASA para la resolución de aquellas incidencias de para aquellas tareas que, por su gravedad o naturaleza, deban ser ejecutadas in-situ.

j) Horario de atención

De forma general, se establecen los siguientes horarios para trabajar sobre el equipamiento objeto de esta oferta:

- **Horario habitual**: En la que se articularán las peticiones generales o incidencias con gravedad menor que no supongan impacto en el servicio.

Día (Excluyendo Festivos)	Horario
Lunes a Viernes	De 7:00 a 21:00
Sábados	De 8:00 a 13:00

Tabla 1. Horario habitual

- **Horario de soporte de incidencias**: En el que se podrá atender cualquier tipo de incidencia técnica que tenga un impacto en el servicio, ya sea corte total o degradación.

Día	Horario
Lunes a Domingo	24 horas

Tabla 2. Horario de soporte

k) Acuerdos de Niveles de Servicio (SLA)

VEIASA establece los siguientes tiempos de atención sujetos a SLA para el tratamiento de incidencias:

Ilustración 1. Diagrama de tiempos de incidencia

- **Tiempo de respuesta:** tiempo transcurrido desde el registro de la incidencia (T0), hasta el momento en que la misma es atendida por un técnico de soporte de la empresa adjudicataria (T1).

- **Tiempo de restauración:** tiempo transcurrido desde el registro de la incidencia (T0), hasta el momento en que se recupera el servicio (T2).

- **Tiempo de resolución:** tiempo transcurrido desde el registro de la incidencia (T0), hasta el momento en que la incidencia ha sido resuelta (T3).

De forma habitual, el tiempo de restauración y resolución serán el mismo (T2=T3), pero pueden darse ocasiones en las que, siendo posible la restauración del servicio, la resolución definitiva de la incidencia pueda requerir acciones adicionales.

VEIASA establece unos **tiempos máximos** para cada uno de los tiempos de atención definidos, constituyendo de esta forma el Acuerdo de Nivel de Servicio.

Los tiempos máximos se definen de acuerdo al **nivel de criticidad de la incidencia,** permitiendo establecer un mecanismo de priorización de las mismas. La empresa adjudicataria se compromete a establecer los siguientes tiempos de respuesta, contabilizados dentro del horario de atención definido en el apartado anterior:

Criticidad	Tiempo de respuesta	Tiempo de resolución	% de incidencias atendidas en tiempo trimestralmente
Critica	≤ 1h	≤ 4 h	95%
Media	≤ 2 h	≤ 8 h	95%
Baja	≤ 4 h	≤ 24	95%

Tabla 3. Condiciones de respuesta y resolución

I) Criticidades

Se definen los siguientes niveles de criticidad:

- **Incidencias Críticas**: Se considera incidencia crítica aquella incidencia de carácter general que supone una parada en el servicio.
- **Incidencias medias:** No cesan la actividad cotidiana de servicios pero interrumpen algunas actividades y necesitan atención para seguir operando con normalidad.

- **Incidencias leves**: No tienen impacto importante ni criticidad considerable.

6. CONDICIONES GENERALES

m) Propiedad de los Trabajos

Todos los trabajos realizados dentro del ámbito de este contrato serán propiedad exclusiva de la Junta de Andalucía, sin que el contratista pueda conservarlos, ni obtener copia de los mismos o facilitarlos a terceros sin la expresa autorización de la Junta de Andalucía.

n) Transferencia tecnológica

Durante la ejecución de los trabajos objeto del 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 técnico de los trabajos realizados así como de las circunstancias en que se desarrollan, de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

El proveedor asegurará que toda la documentación relativa al proyecto se encuentra actualizada a la finalización de los trabajos.

o) Control de Calidad

Los trabajos realizados deberán cumplir lo exigido y estándares de VEIASA, y atenderán a los principios de eficiencia y calidad de realización, requiriéndose la aceptación formal de VEIASA.

Le corresponden a VEIASA los poderes de verificación y control de la empresa adjudicataria establecido en la LCSP, absteniéndose para ello de ejercer función alguna de control, dirección u organización del personal de la empresa adjudicataria. Así, corresponde a VEIASA, a través de la persona designada como responsable del contrato, supervisar su ejecución y adoptar las decisiones y dictar las instrucciones necesarias con el fin de asegurar la correcta realización de la prestación pactada, así como reforzar el control del cumplimiento de éste y agilizar la solución de los diversos incidentes que puedan surgir durante su ejecución, sin que en ningún caso estas facultades puedan implicar el ejercicio de potestades directivas u organizativas sobre el personal de la empresa adjudicataria.

En el supuesto que los profesionales seleccionados, durante la ejecución del servicio, no cumplan con lo exigido por VEIASA, deberán ser sustituido a la mayor brevedad posible por otro profesional de igual o superior perfil, siendo siempre requisito la validación por VEIASA para su incorporación al proyecto.

Durante la duración del contrato los profesionales ofertados y admitidos no serán susceptibles de sustitución, salvo causa de fuerza mayor que justifique el cambio.

El incumplimiento repetido en la calidad, tiempos y eficiencias en los trabajos, será razón para la resolución del contrato con la empresa adjudicataria.

p) Garantía

El adjudicatario deberá garantizar los trabajos realizados al menos por un año, a contar desde la entrega y validación del correcto funcionamiento de los mismos.

Cualquier modificación o corrección que se requiera por defecto en la calidad de los productos entregados, correrá por cuenta del adjudicatario.

7. ANEXO I. SISTEMAS PREEXISTENTES, ARQUITECTURA Y NIVELES DE CRITICIDAD.

C

O

N

F

I

D

E

N

C

I

A

L

Este anexo será remitido a los licitadores, previa solicitud al correo licitaciones@veiasa.es, debiendo aportar en dicha solicitud la Cláusula de Confidencialidad (Anexo II del PPT), debidamente cumplimentada, firmada y sellada por representante con poder suficiente (debiendo acreditarse igualmente el poder de representación).

8. ANEXO II- CLÁUSULA DE CONFIDENCIALIDAD

Don _____, con D.N.I. nº._____, actuando en nombre y representación de _____ (en lo sucesivo, la EMPRESA), entidad con domicilio en _____ y C.I.F. _____, con motivo de la licitación con nº de Expediente CF050-21-039, PRESTACIÓN DE SERVICIOS DE CIBERSEGURIDAD GESTIONADA.

EXPONE Y ACEPTA QUE

1. Se compromete a guardar la máxima reserva y secreto sobre la información clasificada como confidencial. Se considerará Información Confidencial cualquier información de VERIFICACIONES INDUSTRIALES DE ANDALUCÍA, S.A. (en adelante, VEIASA) relacionada con la licitación del procedimiento de contratación de la PRESTACIÓN DE SERVICIOS DE CIBERSEGURIDAD GESTIONADA, Expediente: CF050-21-039, a la que EL LICITADOR accede en el marco de la referida licitación, y en particular la información contenida en el Pliego de Prescripciones Técnicas, Pliego de Condiciones Administrativas Particulares y Cuadro Resumen aplicables a la referida licitación que se entrega en este acto a EL LICITADOR.

2. EL LICITADOR únicamente podrá utilizar dicha Información Confidencial con las finalidades relacionadas directamente con la preparación de su oferta para participar en la licitación del procedimiento de contratación referido anteriormente, y se obliga a no utilizar dicha Información Confidencial para cualquier finalidad distinta de la anterior.

3. EL LICITADOR se compromete a no divulgar dicha Información Confidencial, así como a no publicarla ni de cualquier otro modo, bien directamente bien a través de terceras personas o empresas, ponerla a disposición de terceros sin el previo consentimiento por escrito de VEIASA.

4. De igual modo, EL LICITADOR se compromete, tras la finalización del procedimiento de licitación o, en su caso, la extinción de la relación contractual con VEIASA a no conservar copia alguna de la Información Confidencial, en cualquier tipo de soporte.

5. EL LICITADOR informará a su personal, colaboradores y subcontratistas, en su caso, de las obligaciones establecidas en el presente compromiso sobre confidencialidad. EL LICITADOR realizará cuantas advertencias y suscribirá cuantos documentos sean necesarios con su personal y colaboradores, con el fin de asegurar el cumplimiento de tales obligaciones.

6. Las obligaciones de confidencialidad establecidas en el presente compromiso tendrán una duración indefinida, manteniéndose en vigor con posterioridad a la finalización del procedimiento de licitación o, en su caso, de la extinción de la relación entre VEIASA y EL LICITADOR.

7. VEIASA podrá, por sí mismo o por medio de terceros, inspeccionar el cumplimiento por parte de EL LICITADOR de las estipulaciones reguladas en virtud del presente compromiso, incluso, en las propias instalaciones de EL LICITADOR.

8. El incumplimiento por parte de EL LICITADOR de cualquiera de las obligaciones establecidas en el presente compromiso, dará derecho a VEIASA a percibir una indemnización por los daños y perjuicios que le sean causados.

9. Asimismo, dicho incumplimiento generará, en su caso, el derecho de VEIASA a dar por resuelto el Contrato que pudiera serle adjudicado en el marco del referido procedimiento de licitación, sin corresponder indemnización alguna a favor de EL LICITADOR por tal concepto.

Y para que así conste, y en prueba de conformidad y aceptación al contenido del presente escrito, quien comparece lo firma, en ……, a……de ……de……..

(Sello de la empresa)

Fdo.: