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

Expediente CF050-18-065

ÍNDICE

1. INTRODUCCIÓN 3
2. ANTECEDENTES 3
3. ALCANCE 3
a) Servicios Iniciales 4
b) Servicios Continuos 9
c) Servicios a Demanda 12
4. ORGANIZACIÓN DEL TRABAJO 14
4.1. No división por Lotes 14
4.2. Equipo de Proyecto 14
4.3. Metodologías 15
4.4. Conformidad con madeja 15
4.5. Marco de seguridad 16
4.6. Uso de Infraestructuras TIC y herramientas corporativas 16
4.7. Gestión del proyecto 16
4.8. Equipamiento necesario 18
4.9. Plazos 18
5. NIVEL DE SERVICIO 19
5.1. Lugar de ejecución de los trabajos 19
5.2. Horario de atención 19
5.3. Acuerdos de Niveles de Servicio (SLA) 20
5.4. Criticidades 21
6. CONDICIONES GENERALES 22
6.1. Propiedad de los Trabajos 22
6.2. Transferencia tecnológica 22
6.3. Control de Calidad 22
6.4. Garantía 23

1. INTRODUCCIÓN

Verificaciones Industriales de Andalucía, S.A, en adelante VEIASA, es una empresa del Sector Público Andaluz, adscrita a la Consejería de Empleo, Empresa y Comercio 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 servicios de Internet, entre otros:

- Intranet corporativa
- Portal corporativo
- Web de citas
- Servicios complementarios a los diferentes portales públicos (portales auxiliares, portales de estadística .. etc)

Para conseguir este objetivo se han dispuesto los siguientes requisitos:

a) Servicios Iniciales

3.1 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.

3.2 Tareas

3.2.1 Evaluación inicial de seguridad

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

Para los análisis de las aplicaciones no se proporcionará código fuente ni se especificarán objetivos, ya que el objetivo de esta auditoría externa 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.

- Riesgo en el acceso a 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:

i. 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.
ii. Activos: aplicación de los conocimientos recogidos para intentar violar la seguridad existente.
iii. 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.

3.2.2 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 incluye, entre otros, las siguientes actividades:

3.2.2.1 Análisis de la Redes Públicas (Footprinting)

El objetivo es encontrar la máxima información en internet sobre la infraestructura y máquinas implicadas en el sistema de información que puedan convertirse en objetivos, siempre sin exceder los límites legales.

Resultados esperados:

- Rango de redes y subredes Públicas
- Puertos abiertos y aplicaciones ejecutadas.
- Nombres de Dominios
- Nombres de Servidores
- Direcciones IP
- Versiones de sistemas operativos y software base
- Información del ISP
- Dueños de Sistemas y Servicios

3.2.2.2 Búsqueda de vulnerabilidades

En esta actividad se buscará la existencia de vulnerabilidades en todos los sistemas informáticos implicados en las aplicaciones (servidores, software base, código fuente, firewalls, routers, etc.). Se realizarán test automáticos y manuales con las últimas versiones de software de detección de vulnerabilidades.

Resultados esperados:

- Tipo de aplicación o servicio por vulnerabilidad.
- Nivel de actualización de sistemas y aplicaciones.
- Vulnerabilidades por denegación de servicio.
- Áreas securizadas por ocultación o visibles.
- Vulnerabilidades reales (sin contar las falsas alarmas).
- Topología de red.

3.2.2.3 Análisis de las aplicaciones

Recopilación de Información utilizando, motores de búsqueda, peticiones http, firma digital, análisis sobre códigos de error, nombres del dominio, nombre de servidores, etc.

Identificación de los posibles puntos débiles desde el punto de vista de la seguridad:

- Pruebas de los mecanismos de autenticación.
- Pruebas de los mecanismos de sesión.
- Pruebas del sistema de permisos y autorización.
- Pruebas de la lógica de negocio.
- Pruebas de la validación de datos.
- Pruebas de denegación de servicio.
- Pruebas sobre los servicios web.
- Pruebas sobre AJAX.
- Explotación de fallos de programación (SQL injection, XSS, inyección de ficheros, escalado de privilegios, etc.).
- Vulnerabilidades en la autenticación:
- Enumeración de usuarios.
- Pruebas de diccionario sobre cuentas de usuario o cuentas predeterminadas.
- Pruebas de fuerza bruta.
- Pruebas para saltarse el sistema de autenticación.

- Pruebas de gestión del caché de navegación y de salida de sesión.
- Comprobar Sistemas de recordatorio/restauración de contraseñas vulnerables.
- Pruebas de CAPTCHA.

3.2.2.4 Realización de la auditoría

La auditoría constará de las siguientes fases:

- Inspección manual y recolección de información.
- Realización de tests con herramientas automáticas.
- Revisión de los resultados de las herramientas automáticas y comprobación manual de los resultados.
- Elaboración de informe, incluyendo una propuesta de plan de acción.

Durante la realización de la auditoría y, especialmente, durante la fase de realización de tests con herramientas automáticas, podría ocurrir que las pruebas afectaran a la disponibilidad de los servicios publicados. Por este motivo, VEIASA y el adjudicatario acordarán el horario y calendario en el que las pruebas están autorizadas. El adjudicatario se compromete a no realizar pruebas fuera del horario autorizado.

3.2.2.5 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.

3.2.3 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.

3.3 Resultados del paquete 1 (Hitos y Entregables)

HITOS

- Auditoria inicial de seguridad

PRODUCTOS ENTREGABLES

- Informe de auditoría
  Procedimiento de Respuesta ante Incidente

b) Servicios Continuos

4.1. Objetivos

Los objetivos de este paquete son:

- Disponer de una monitorización y control de la seguridad permanentes (24x7x365).
- Contar con un asesoramiento permanente tanto reactivo (consultas) como proactivo (información sobre novedades y alertas).

Para las aplicaciones actualmente publicadas y aquellas que se publiquen durante la vigencia del contrato.

4.2 Tareas

Para abordar los objetivos del paquete se llevarán a cabo las siguientes tareas, dentro del plazo de duración del contrato, previsto para 24 meses:

- Monitorización y control 24x7x365
- Asesoramiento permanente.

4.2.1 Monitorización y control 24x7x365

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
- 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.

- Seguimiento de actividades sospechosas. Ante la detección de una actividad de este tipo se cruzarán las informaciones obtenidas de las trazas de los distintos sistemas para determinar el alcance de la actividad de un usuario.

4.2.2 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.

4.2.3 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.
- Emisión de un análisis forense.

4.2.4 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.

4.2.4.1 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. A la vista del servicio de monitorización y de las nuevas alertas de seguridad se realizarán propuestas sobre posibles mecanismos preventivos que podrían ser de interés, justificando su conveniencia y beneficios esperados. Sin perjuicio del carácter continuo de este asesoramiento, al menos se realizará una recomendación con carácter trimestral.

Propuesta de iniciativas de formación. A la vista de las novedades en seguridad técnica y legal, se propondrán posibles acciones formativas en las materias que puedan ser de interés para el personal de VEIASA. Sin perjuicio del carácter continuo de este asesoramiento, al menos se realizará una recomendación con carácter semestral

4.3 Resultados del paquete 2 (Hitos y Entregables)

HITOS

Hitos de avance en la ejecución de los servicios.

PRODUCTOS ENTREGABLES

- Informes mensuales: Se realizará un informe mensual con el resumen de actividades del periodo, elaborado por la jefatura de proyecto de Ingenia, 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

c) Servicios a Demanda

5.1 Objetivos

Los objetivos de este paquete son:

Disponer de un servicio bajo demanda para ejecutar pruebas de seguridad a las nuevas aplicaciones antes de su puesta en producción y certificar que mantienen unos niveles de seguridad adecuados.

5.2 Tareas

Para abordar los objetivos del paquete se llevarán a cabo las siguientes tareas:

- Tareas bajo demanda bajo la modalidad de una bolsa de auditorías de seguridad, incluyendo cada auditoría:
- Análisis de seguridad (ver apartado 3.2.2)

5.2.1 Tareas bajo demanda bajo la modalidad de una bolsa de horas por perfiles

Para prestar el servicio bajo demanda se propone una bolsa de auditorías de seguridad, de forma que esta bolsa vaya siendo consumida en función de las necesidades demandadas por VEIASA.

Dependiendo del tipo de aplicación se consumirán un número de auditorías de la bolsa, conforme al cómputo que se indica en la siguiente tabla:

Perfil	Nº de auditorías de la bolsa
Aplicación TIPO 1: Portal informativo. Portales que publican información, sin partes privadas abiertas a usuarios	1
Aplicación TIPO 2: Aplicación corporativa Aplicación que necesita autorización pero abierta a un número seleccionado de usuarios, sin partes privadas abiertas al público en general	1,5
Aplicación TIPO 3: Aplicación pública Aplicación con partes autorizadas abierta al público en general	2

El alcance mínimo será una bolsa de 15 auditorías, que podrán consumirse a demanda dependiendo del tipo de aplicación, dentro del periodo de 24 meses de vigencia establecido para el contrato.

5.2.2 Resultados del paquete 3 (Hitos y Entregables)

HITOS

Consumo de la bolsa de auditorías

PRODUCTOS ENTREGABLES

- Resultados de las tareas solicitadas bajo demanda:
- Informes de auditorías incluyendo plan de acción.

4. ORGANIZACIÓN DEL TRABAJO

Todos los trabajos a 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.

4.1. 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.

4.2. 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 Anexo 4 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 2.g) donde se detallan las funciones Responsable de la Empresa Adjudicataria/Jefe de Proyecto
1 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
1 Consultor en seguridad técnica	Tareas de seguridad técnica: auditorías de vulnerabilidades, monitorización, análisis técnicos, tareas de seguridad bajo demanda (técnicas)
4 Técnicos de seguridad técnica	Soporte a la realización de las tareas de seguridad

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.

4.3. 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 Administraciones Públicas. 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.

4.4. 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.

4.5. 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.ccn-cert.cni.es/), así como a las recomendaciones de Andalucía-CERT, como centro especializado en la materia en el ámbito andaluz.

4.6. 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.

4.7. 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.

4.8. 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 Anexo 4 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 7 Profesional 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 Sistemas de Información para su correcta integración con los sistemas de VEIASA.

4.9. Plazos

El contrato tendrá una duración máxima de 24 meses, con una carga de trabajo máxima estimada de 2.100 horas. El contrato podrá ser prorrogado por otro periodo de 24 meses y una carga de trabajo máxima estimada de otras 2.100 horas.

Así pues, el contrato podrá alcanzar una duración máxima total de 48 meses, con una carga de trabajo máxima estimada de 4.200 horas.

El inicio de los trabajos deberá realizarse dentro de los 35 días laborables siguientes a la adjudicación del contrato.

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.

5.1. 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.

5.2. 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

5.3. 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

5.4. 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

6.1. 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.

6.2. 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.

6.3. 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. El responsable del contrato velará por la idónea gestión contractual de modo que en su ejecución no se den situaciones que puedan propiciar la existencia de una cesión ilegal de trabajadores o dar lugar a la declaración de relaciones de laboralidad entre VEIASA y el personal de la empresa adjudicataria.

En el supuesto que el profesional seleccionado no cumpla lo exigido por VEIASA, deberá ser sustituido a la mayor brevedad posible por otro profesional de igual o superior experiencia, siendo siempre requisito la validación por VEIASA para su incorporación al proyecto.

Durante la duración del contrato el profesional ofertado y admitido no será susceptible 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.

6.4. Garantía

El licitador 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 licitador.