PLIEGO DE PRESCRIPCIONES TECNICAS

CONTRATACION DEL SERVICIO PARA LA ADECUACION AL ESQUEMA NACIONAL DE SEGURIDAD, REGLAMENTO GENERAL DE PROTECCION DE DATOS, LOPDGDD Y AUDITORIA DE SEGURIDAD INFORMATICA EN LA AUTORIDAD PORTUARIA DE VIGO

AUTORIDAD PORTUARIA DE VIGO

Enero 2019

1. INTRODUCCION.

El Esquema Nacional de Seguridad (ENS) tiene como objetivo establecer los requisitos mínimos de seguridad que deben adoptarse para la prestación de servicios de administración electrónica. Su alcance afecta a los sistemas de información, los datos, las comunicaciones y los servicios electrónicos de cualquier Administración Pública para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que se gestionen en el ejercicio de sus competencias.

Su creación se contempla en el artículo 42 de la LEY 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y se regula a través de Real Decreto del Gobierno de España 3/2010, de 8 de enero, modificado por el Real Decreto 951/2015, de 23 de octubre. Se desarrolla sobre las recomendaciones de la UE y los estándares internacionales en materia de Seguridad de la Información, especialmente la UNE/ISO 27001.

El Reglamento General de Protección de Datos Personales de la Unión Europea (RGPD) UE 2016/679, fue publicado en mayo de 2016 y entró en vigor en ese mismo mes, siendo de aplicación desde el 5 de mayo de 2018. La APV debe realizar las adaptaciones necesarias para alinear su actividad ajustándola a la nueva normativa. **La Ley Organica de Protección de Datos Personales y Garantía de los Derechos Digitales (LO 3/2018 de 5 de Diciembre)**, entró en vigor el pasado 6 de diciembre, teniendo como objeto adaptar el Reglamento Europeo de Protección de Datos Personales, así como completarlo.

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental, toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal.

El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas.

La seguridad de la información, seguridad informática o garantía de la información son utilizados con bastante frecuencia. El significado de dichas palabras es diferente, pero todos persiguen la misma finalidad que es proteger la confidencialidad, la integridad y la disponibilidad de la información sensible de la organización. La seguridad de la información es un concepto mucho más amplio que el de Seguridad Informática, ya que no solo está dirigida a los datos guardados en entornos tecnológicos, sino a todo tipo de dato critico que maneja una organización.

Una auditoría de seguridad informática es una evaluación de los sistemas informáticos cuyo fin es detectar errores y fallas en cuanto a la protección, accesibilidad y disponibilidad de los datos guardados en los mismos. Las auditorías de seguridad permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

24

2. OBJETO.

El objeto de este pliego es contratar los servicios de una empresa especializada para la realización de los siguientes trabajos:

- Adaptación de nuestros sistemas y procesos a lo requerido por el Esquema Nacional de Seguridad **(ENS)**. Elaboración del plan de adecuación e implantación de las medidas de seguridad definidas en el plan.
- Adaptación de nuestros sistemas y procesos a lo requerido en el Reglamento General de Protección de Datos (RGDP) **UE 2016/679** y Ley Organica de Protección de Datos Personales y Garantía de los Derechos Digitales **LO 3/2018 de 5 de Diciembre**.
- Realizar Auditorías de Seguridad de los sistemas de información y las comunicaciones para conocer el estado de la misma y obtener una relación de medidas a implantar para la mejora de esta.

3. ALCANCE.

Desglosaremos el alcance de este proyecto en los tres apartados objetos del mismo.

3.A. ESQUEMA NACIONAL DE SEGURIDAD (ENS).

3.A.1 REQUISITOS DEL SERVICIO.

3.A.1.1. PLAN DE ADECUACIÓN.

Los servicios a realizar para la elaboración del Plan de Adecuación son:

- Análisis previo y redacción de un documento de recomendaciones que permita establecer las responsabilidades asociadas al ENS y designar a los responsables de seguridad y los miembros del comité o comités de seguridad, así como establecer un calendario con los hitos del proyecto.
- Realización de un informe de situación actual para determinar la infraestructura tecnológica existente, la relación de activos y las normativas y procedimientos de seguridad actuales.
- Elaboración de la política de seguridad y redacción de los documentos que la integran.
- Catalogación de la información incorporando:
- Sistemas de información.
- Dimensiones de la seguridad afectadas.
- Niveles de seguridad.
- Relación entre tipos de información y dimensiones de la seguridad.
- Categorización de los sistemas.
- Elaboración del Inventario de Activos incorporando los sistemas de información, mecanismos de actualización periódica, sistematización y demás características exigidas por el ENS y el resto de normativa asociada.
- Realización del correspondiente análisis de riesgos mediante metodología Magerit y la herramienta EAR/PILAR (Procedimiento Informático Lógico para el Análisis de Riesgos), disponible de forma gratuita para las administraciones públicas. De este análisis se obtendrá:
- Informe de amenazas, vulnerabilidades e impactos
- Informe de recomendaciones para la gestión del riesgo
- Exportación de datos para su incorporación a la herramienta INES (Informe Nacional del Estado de Seguridad)
- Redacción de la declaración de aplicabilidad o documento de selección de controles. Incluirá los controles ya implantados y aquellos que se hayan seleccionado para minimizar el riesgo de los activos cruciales para cumplir con el nivel de seguridad deseado.
- Redacción del plan o planes de adecuación.

3.A.1.2. IMPLANTACIÓN DE LAS MEDIDAS DE SEGURIDAD DEFINIDAS EN EL PLAN

Los servicios a realizar para implantación de las medidas de seguridad definidas en el plan son:

- Elaboración, revisión, publicación y difusión entre los usuarios de la Política de seguridad.
- Desarrollo y redacción de las normativas de seguridad que establecerán:
- Instrucciones de uso de los recursos TIC
- Definir quién debe realizar las distintas tareas asociadas a la seguridad y sus responsabilidades
- Mecanismos que se establecerán para la identificación de las anomalías
- Sistemas de resolución de las anomalías detectadas
- Definir y describir los procesos de autorización
- Redacción documentos tipo para el registro y control de las incidencias de seguridad y los procedimientos asociados.
- Definición de las orientaciones preventivas y medidas de recuperación de los sistemas para la restauración de la información y los servicios evitando amenazas y discontinuidades.
- Redacción del plan de pruebas y monitorización de los sistemas.
- Redacción del plan de auditorías bienales como proceso de mejora continua. Deberá contemplar la revisión de la política de seguridad y su cumplimiento, los riesgos, normativas, procedimientos y controles establecidos.
- Elaboración y ejecución de un plan de formación y sensibilización para el personal de los organismos implicado en los procedimientos afectados por el ENS.
- Formación en la herramienta de Gestión aportada para el seguimiento de la implantación y cumplimiento, destinada a los responsables de mantener el análisis de riesgos.
- Soporte al personal de las distintas unidades orgánicas para la aplicación de los procedimientos establecidos.
- Evaluación de resultados que se someterá a los responsables y al Comité o Comités de Seguridad.
- Carga y puesta a disposición de herramienta informática de gestión.

3.A.1.3. ENTREGA DE DOCUMENTACIÓN

Para dar por concluida la realización total de los trabajos deberán entregarse en soporte digital todas las actas de reuniones y entrevistas realizadas y para cada fase desarrollada:

FASE I:

- Análisis previo y recomendaciones para la designación de responsabilidades.
- Informe de situación actual.
- Documentos integrantes de la política de seguridad.
- Inventario de activos.
- Informes definitivos asociados al análisis de riesgo.
- Declaración de aplicabilidad.
- Plan o planes de adecuación.

FASE II:

- Política de seguridad revisada.
- Instrucciones específicas para los usuarios y responsables de los sistemas.
- Documentos tipo.
- Recopilación de orientaciones preventivas y medidas de recuperación.
- Plan de pruebas y monitorización de los sistemas.
- Plan de auditorías bienales.
- Plan de formación al personal implicado.
- Informe de evaluación de resultados.

Asimismo, el adjudicatario facilitará, toda aquella información que, aunque no esté detallada en la relación anterior, sea necesaria para la correcta documentación de la ejecución del contrato.

3.B. REGLAMENTO GENERAL DE PROTECCION DE DATOS (RGPD) y LOPDGDD.
3.B.1 REQUISITOS DEL SERVICIO.
3.B.1.1. PLAN DE ADECUACIÓN.

Los servicios a realizar para la elaboración del Plan de Adecuación son:

- Análisis previo del tratamiento de datos de carácter personal dentro del organismo y redacción de un documento denominado "plan de adecuación al RGPD Y LOPDGDD en la APV" que sirva de guía personalizada a través de todo el proceso.
- Análisis del tratamiento que permita establecer las responsabilidades asociadas al RGPD Y LOPDGDD, y si procede, designar al responsable de protección de datos (delegado de protección de datos DPO).
- Elaborar el Registro de Actividades del Tratamiento, prestando atención especial a los tratamientos que incluyan categorías especiales de datos o datos de menores.
- Analizar las bases jurídicas de los tratamientos.
- Efectuar un análisis de riesgos en el tratamiento de los datos de carácter personal.
- Identificar las medidas técnicas y organizativas necesarias para hacer frente a los riesgos detectados en el análisis de riesgos.
- Verificar las medidas de seguridad a implantar, así como establecer protocolos para gestionar y, en su caso, notificar las quiebras de seguridad a la unidad de control.
- Confeccionar políticas de protección de datos a implantar. En tratamientos de alto riesgo, detallar e implantar un procedimiento para realizar una evaluación de impacto de la privacidad.
- Revisión de acuerdos con los encargados de tratamiento para valorar sus garantías y adaptar estas al RGPD.

3.B.1.2. IMPLANTACIÓN DE LAS MEDIDAS DE SEGURIDAD DEFINIDAS EN EL PLAN

Los servicios a realizar para implantación de las medidas de seguridad definidas en el plan son:

- Desarrollo y redacción de las normativas adaptadas al funcionamiento administrativo y tecnológico de la APV en materia de tratamientos de datos personales:
- Instrucciones de uso de los recursos TIC y operativas manuales relacionadas.
- Definir quién debe realizar las distintas tareas asociadas a la seguridad y sus responsabilidades.
- Mecanismos que se establecerán para la identificación de las quiebras de seguridad.
- Sistemas de resolución y notificación de las quiebras.
- Elaboración, revisión, publicación y difusión entre los usuarios de las políticas a implantar encaminadas a la protección de datos.
- Redacción documentos tipo para el registro y control de las quiebras de seguridad y los procedimientos asociados.
- Redacción del plan de auditorías como proceso de mejora continua. Deberá contemplar la revisión de la política de seguridad y su cumplimiento, los riesgos, normativas, procedimientos y controles establecidos.
- Elaboración y ejecución de un plan de formación y sensibilización para el personal del organismo implicado en los procedimientos afectados por el RGPD y LOPDGDD.
- Soporte al personal de las distintas unidades orgánicas para la aplicación de los procedimientos a implantar.
- Formación en la herramienta de Gestión aportada para el seguimiento de la implantación y cumplimiento, destinada a los responsables de mantener el cumplimiento del RGPD Y LOPDGDD.
- Evaluación de resultados que se someterá a los órganos de dirección de la APV.
- Carga y puesta a disposición de herramienta informática de gestión.

27

3.B.1.3. ENTREGA DE DOCUMENTACIÓN

Para dar por concluida la realización total de los trabajos deberán entregarse en soporte digital todas las actas de reuniones y entrevistas realizadas y para cada fase desarrollada, a lo largo del proyecto se deberán entregar los documentos generados en cada fase del mismo:

- Documento de normas adaptadas a la APV.
- Plan de adecuación al RGPD Y LOPDGDD en la APV.
- Registro de Actividades del Tratamiento.
- Documento de bases jurídicas.
- Análisis de riesgos.
- Protocolos ante quiebras de seguridad.
- Plan de formación y concienciación a usuarios adaptado al funcionamiento de la APV.

Así mismo, el adjudicatario facilitará, toda aquella información que, aunque no esté detallada en la relación anterior, sea necesaria para la correcta documentación de la ejecución del contrato.

3.C. AUDITORIA DE SEGURIDAD DE SISTEMAS.

3.C.1 REQUISITOS DEL SERVICIO.

3.C.1.1. PLAN DE ACTUACION.

Como complemento al proceso de adecuación al Esquema Nacional de Seguridad (ENS) y adecuación al RGDP y LOPDGDD, se hace necesario un servicio de auditoría de seguridad informática que permita testear la situación de los sistemas de información de la APV y poder recabar la información necesaria para implantar políticas que reduzcan y mitiguen los riesgos de ciberseguridad a los que están expuestos los activos y sus servicios web.

Se requiere, por lo tanto, una auditoría técnica que permita conocer el estado actual de las vulnerabilidades de los sistemas de información y aplicaciones web publicadas, identificación de las medidas de prevención aplicadas en los activos de la APV, y un análisis GAP que identifique las necesidades para el cumplimiento de las medidas previstas por el ENS. En la auditoría se incluirá un muestreo de seguridad de las familias de activos conectados a la red LAN de la APV destinados a la vigilancia y sensorización de servicios para verificar su grado de vulnerabilidad y seguridad, (cctv, ccaa, ordenadores personales, suministro de agua....), aleatoriamente la autoridad portuaria seleccionará una muestra de estos dispositivos para ser auditados.

Como paso previo a la ejecución de la auditoría, la empresa adjudicataria deberá realizar un plan de actuación en el que se indique la planificación del mismo, detallando los procedimientos y actuaciones que se llevarán a cabo y sobre que universos.

Al ser una contratación integrada con la adaptación al ENS y al RGPD, las auditorias de seguridad debe ser un complemento a estas dos actuaciones, por lo tanto, deberán de realizarse **2 (dos)** auditorías a lo largo del proceso, con esto se pretende medir el grado de adecuación de los sistemas de la APV a las recomendaciones y políticas que se obtengan del análisis GAP inicial y los niveles de seguridad alcanzados.

3.C.1.2. EVALUACION DEL NIVEL DE SEGURIDAD ACTUAL.

La auditoría técnica de los sistemas es necesario para identificar los activos reales, sus vulnerabilidades y por lo tanto el nivel de riesgo asumido. A modo orientativo, debe cubrir los siguientes aspectos: identificar y categorizar los activos reales existentes en la red con los pertinentes escaneos o exploraciones automáticas, identificar las vulnerabilidades de seguridad que pudieran permitir el acceso no autorizado a un atacante o afectar a la disponibilidad de los servicios prestados, verificar el impacto real de las debilidades o escenarios, identificar el nivel de riesgo que supone la posibilidad de un fallo de seguridad y por último, definir unas pautas y medidas de mitigación para poder remediar las distintas debilidades y posibles peligros detectados.

A modo orientativo, el servicio de auditoría de los servicios web de la APV contará con pruebas Hackeo Ético de las aplicaciones web a nivel técnico y funcional, ejecutando un test de intrusión externo en modo Caja Negra (se realiza sin información adicional a la de un atacante externo) y un test de Caja Blanca (con las credenciales de un usuario legítimo del sistema con funcionalidad limitada). El objetivo de estas comprobaciones es el de identificar, analizar y explotar los puntos vulnerables de los activos y aplicación web indicados por la APV, que puedan ser explotados por atacantes maliciosos (internos o externos).

Las pruebas que tengan un impacto sobre la disponibilidad de servicios se realizarán exclusivamente en horario nocturno y en las ventanas de tiempo que se hayan acordado con los responsables de la APV.

Las tareas se realizarán desde una máquina remota, cuya dirección IP pública se pondrá en conocimiento de la Autoridad Portuaria de Vigo (APV) antes de iniciar la auditoria, o a través de una conexión VPN creada al efecto.

Dentro del objeto, alcance y presupuesto de este pliego, el adjudicatario podrá recomendar cualquier otro tipo de actuación destinado a mejorar los resultados de las auditorías a realizar.

3.C.1.3 METODOLOGIAS A UTILIZAR.

Este servicio se llevará a cabo en función de las distintas metodologías reconocidas de buenas prácticas del mercado, como son:

- **OSSTMM** (*Open Source Security Testing Methodology*), uno de los estándares profesionales más completos y comúnmente utilizados en Auditorías de Seguridad para revisar la Seguridad de los Sistemas desde Internet. Incluye un marco de trabajo que describe las fases a realizar durante la ejecución de la auditoría.
- **OWASP** (*Open Web Application Security Proyect*), metodología abierta para el análisis de la seguridad en aplicaciones web. El análisis se centrará especialmente en las vulnerabilidades descritas en el OWASP Top 10 (documento de alto nivel que se centra en las vulnerabilidades más críticas de las aplicaciones web) cuyos controles se actualizan constantemente.
  Deberán especificarse las metodologías a utilizar, el equipo de trabajo y certificaciones del personal que realice las actuaciones.

3.C.1.4 ENTREGA DE DOCUMENTACION.

Durante las distintas fases de la realización del proyecto en cuanto a las auditorias de seguridad se refiere, la empresa adjudicataria deberá entregar la documentación que se relaciona:

- **Plan de auditoría:** definición de las comprobaciones a realizar en la auditoría y los recursos dedicados a la misma, la planificación del mismo, detallando los procedimientos y actuaciones que se llevarán a cabo.
- **Informe de nivel actual de seguridad:** resultado de las pruebas, las vulnerabilidades localizadas y el nivel de acceso alcanzado debido a ellas. Deberá especificarse la metodología utilizada y los resultados en base a dicha metodología. Para cada vulnerabilidad o mejora de seguridad se indicarán las recomendaciones y soluciones necesarias tratando en cada caso de ofrecer la solución más económica.
- **Evaluación, política y estrategia de seguridad:** análisis GAP respecto a los modelos de referencia reflejados en el ENS y las guías CNN (Centro Criptológico Nacional) para entornos web (CCN-STIC-812). Se centrará en analizar las medidas aplicadas, identificar deficiencias y sugerir medidas correctoras o complementarias que sean necesarias.

- **Seguimiento de auditorías:** Documento de trazabilidad de las 2 (dos) auditorías a realizar, pudiéndose comprobar la trazabilidad de las medidas correctoras aplicadas a cada una de ellas (si procede), y su grado de corrección o mitigación, con un resumen final de las actuaciones y situación a la finalización del proyecto.

4. SOTWARE DE GESTION.

Independientemente de la obligación de la utilización de herramientas informáticas de la AGE, la empresa adjudicataria podrá aportar un software, bien a instalar en los sistemas de la APV o en la nube, que le permita gestionar el seguimiento del plan de adecuación al ENS, RGPD y LOPDGDD de una manera clara y sencilla, permitiendo incorporar los cambios y actualizaciones que se vayan produciendo en el mismo. Se valorará la usabilidad de este, por lo tanto, deberá presentarse en la oferta técnica sus características técnicas, funcionales y una demo o presentación que permita tal evaluación, este software no deberá tener costes económicos añadidos al presupuesto del contrato, ni durante la prestación de este ni a posteriori.

5. SEGURIDAD Y PROTECCION DE DATOS.

El adjudicatario queda expresamente obligado a mantener absoluta **confidencialidad** y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato, especialmente los de carácter personal, que no podrá copiar o utilizar con fin distinto al que figura en este pliego, ni tampoco ceder a otros ni siquiera a efectos de conservación.

El adjudicatario y quienes intervengan en cualquier fase de la ejecución de este contrato guardarán secreto sobre los datos, las informaciones y asuntos a los que tengan acceso o conocimiento durante su vigencia, estando obligados a no hacer públicos, ceder, enajenar o permitir el acceso de terceros a cuantos datos o información conozcan o posean como consecuencia de la ejecución de este contrato, incluso después de finalizar el plazo contractual, so pena de incurrir en las responsabilidades legales que correspondan. Todos los datos manejados en ejecución de este contrato, el resultado de las tareas realizadas a su amparo y el soporte o soportes empleados para su ejecución serán propiedad de la APV, sin que pueda conservar una copia o utilizarlos para fines distintos de los que figuran en este contrato. El adjudicatario estará obligado a presentar la relación de empresas subcontratadas, si las hubiese, para la implantación o prestación del servicio contratado, en dicha relación deben figurar las competencias y certificaciones de las mismas para el desempeño de los trabajos.

La empresa adjudicataria no aplicará o utilizará los datos de los que tenga conocimiento en ejecución de este contrato, o los ficheros y bases de datos y su contenido que le sean entregados por la APV con fin/es distinto/s al que figure en el mismo, ni permitirá su conocimiento y acceso, ni los comunicará, siquiera para su conservación, a terceros distintos a la propia APV.

El adjudicatario quedará obligado al cumplimiento de la normativa en vigor referente a la protección de datos de carácter personal y especialmente en lo indicado en relación al acceso a datos por cuenta de terceros.

En consecuencia, si en ejecución del contrato fuera necesario el acceso del adjudicatario a datos de carácter personal contenidos en ficheros titularidad de la APV, el adjudicatario únicamente podrá tratar tales datos conforme a las instrucciones de la APV, responsable del tratamiento, y no los aplicará o utilizará con fin distinto al aquí referenciado.

El adjudicatario mantendrá el secreto profesional respecto a la información relacionada con su relación profesional con la APV, con la información del negocio y de los clientes y proveedores de la APV, así como los datos particulares de la configuración de sus sistemas, red informática, y otros detalles particulares sobre las infraestructuras tecnológicas, siendo especialmente relevante los mecanismos de control de acceso, usuarios y contraseñas. Asimismo, el adjudicatario deberá considerar las siguientes precauciones cuando pueda darse la situación de que se requiera un acceso de forma remota a los sistemas de la APV:

- Utilizar una conexión cifrada o bien que disponga de algún otro mecanismo que evite que un tercero no autorizado pueda interceptar o alterar los datos intercambiados en la comunicación.
- Utilizar equipos que cuenten con medidas de seguridad pertinentes que eviten la propagación a los equipos y sistemas de la APV de virus u otro tipo de malware.

A la extinción de la relación contractual por cualquier causa, los datos a los que hubiera tenido acceso el adjudicatario deberán ser destruidos o devueltos a la APV, al igual que cualquier soporte o documento en el que conste algún dato de carácter personal objeto del tratamiento. A la finalización del periodo de garantía del contrato, el contratista entregará un certificado de destrucción de los datos gestionados.

El incumplimiento de estas obligaciones por parte del adjudicatario le hará responder personalmente de las infracciones que cometa como si ocupara la posición de responsable del tratamiento. La vulneración de las estipulaciones contenidas aquí será considerada como causa justificada de resolución del contrato, sin derecho a la percepción de indemnización alguna por parte del adjudicatario ni observancia de ningún plazo de preaviso por parte de la APV.

En el supuesto de incumplimiento de las obligaciones asumidas en virtud de esta cláusula, y con independencia de lo anteriormente expuesto, la APV se reserva en todo caso el derecho de reclamar el resarcimiento de los daños y perjuicios que se le pudieran causar como consecuencia de dicho incumplimiento.

Asimismo, el adjudicatario incluirá en su oferta la designación de la persona o personas que, sin perjuicio de la responsabilidad propia de la empresa, estarán autorizadas para las relaciones con el personal de la APV responsables del proyecto a efectos del uso correcto del material y de la información a manejar. Se adjuntará una descripción de su perfil profesional, y sólo podrán ser sustituidas con la conformidad de la APV.

El adjudicatario se asegurará de que los servicios prestados en virtud de este pliego, así como los sistemas de información que los sustentan, se prestan de conformidad a los requisitos de seguridad establecidos en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, así como las disposiciones legales o reglamentarias relacionadas con la misma, o cualquier actualización de esta normativa a lo largo de la vigencia del contrato.

6. MODELO DE RELACION.

La empresa adjudicataria nombrará un interlocutor único (Responsable de Servicio), que será el encargado de planificar las distintas fases del servicio, entre sus funciones estará:

- Planificar, coordinar y vigilar el cumplimiento de cada uno de los capítulos establecidos dentro del alcance de de este pliego.
- Remitir a la APV los canales de comunicación necesarios para la correcta prestación del servicio y las credenciales del personal que bajo su responsabilidad se encargarán de realizar las distintas fases del servicio, o de las modificaciones que en este apartado se produzcan.
- Será la persona encargada, junto con el responsable que la APV designe, de planificar, supervisar y validar todos los hitos que se definan dentro de la planificación del proyecto.
- Será el interlocutor directo ante cualquier situación inesperada, seguimiento de la prestación o cualquier incidencia que requiera de su conocimiento o intervención.

7. EQUIPO DE TRABAJO Y REQUISITOS PARA LA PRESTACIÓN DEL SERVICIO.

Al inicio del periodo del contrato, se incorporará al servicio el personal técnico necesario para la realización de los trabajos solicitados en este pliego, se especificarán en la oferta técnica las titulaciones y certificaciones de dicho personal y se detallará la distribución de los trabajos a realizar y la forma de ejecución de los mismos.

Los técnicos que formen parte del equipo que prestará el servicio deberá estar en posesión como mínimo de una de las siguientes certificaciones en el ámbito de la seguridad TIC:

- ISACA: cualquiera de las emitidas por este organismo que tengan relación con la seguridad de la información (CISM, CISA, etc.).
- ISC2: cualquiera de las emitidas por este organismo.
- EC-Council: cualquiera de las emitidas por este organismo.
- GIAC: cualquiera de las emitidas por este organismo.

La empresa adjudicataria debe estar certificada en las normas ISO 9000 sobre calidad y gestión de calidad de organizaciones orientadas a la producción de bienes o servicios, ISO 27000 de sistemas de gestión de seguridad de la información e ISO 20000 de provisión de servicios gestionados de TI.

8. REGISTRO, DOCUMENTACION Y ACCESO.

La APV dará acceso a la empresa adjudicataria, mediante las medidas de seguridad necesarias, a la plataforma propia de monitorización de sistemas "SmartViport" y a la plataforma de gestión de incidencias "OTRS", para tener un punto de acceso único de gestión de monitorización y seguimiento de incidencias e intervenciones sobre los sistemas objeto de este contrato.

El prestador del servicio documentará adecuadamente cada intervención realizada, a través de la mencionada plataforma OTRS. La empresa adjudicataria dispondrá de un usuario que le permita acceder, consultar los estados de monitorización, las alertas, y gestionar el registro y seguimiento de las incidencias que vayan surgiendo relacionadas con este contrato.

Se requerirá al prestador del servicio una adecuada gestión de la configuración de los sistemas y documentación asociada al proyecto (CMDB), para lo cual se pondrá a su disposición la plataforma web que la propia APV dispone para documentación relacionada con los sistemas informáticos (WIKIPEDIA INFORMATICA). Independientemente de la gestión de la documentación que se proponga en la oferta técnica, la APV podrá exigir que dicha gestión se también se realice sobre dicha plataforma.

9. CONTENIDO DE LAS OFERTAS.

9.1 CALIDAD TECNICA DE LA OFERTA.

En el sobre de la oferta técnica deberán especificarse:

- 9.1.1 Descripción Metodológica: protocolos, herramientas y procedimientos detallados, aplicados a cada uno de los tres trabajos a desarrollar.
- 9.1.2 Relación de personas asignadas: experiencia en trabajos similares y suficiencia técnica de las mismas para el desarrollo de los trabajos.
- 9.1.3 Relación de trabajos similares realizados en otros organismos públicos según magnitud.
- 9.1.4 Planificación temporal del desarrollo de cada uno de los trabajos a realizar y planificación de la interacción entre ellos.
- 9.1.5 Software de Gestión: Descripción y/o demo del software de gestión solicitado en el capítulo 4.

9.2 Precio del contrato, oferta económica.

En ningún caso se desglosarán importes por partidas o módulos.
En el sobre de la oferta económica deberá figurar el **precio final** por la prestación completa del servicio, sin incluir el IVA.

10. PENALIZACIONES.

El plazo de prestación del servicio según se estipula en el capítulo 13 es de obligado cumplimiento, ante cualquier retraso injustificado, se estipula una penalización del 0,5% del importe final contratado por cada semana que exceda de la fecha de finalización.

11. FORMAS Y CRITERIOS DE VALORACIÓN.

Se atenderá en este punto a lo dispuesto en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público. Los criterios para la adjudicación serán los recogidos en el Cuadro de Características del Pliego de Cláusulas Administrativas.

12. PRESUPUESTO DE LICITACION.

El presupuesto base de licitación será de 90.000 euros, IVA no incluido.

13. PLAZO DE PRESTACION DEL SERVICIO.

Para una correcta prestación del servicio se estima un periodo de ejecución máximo de **14 (Catorce) meses** a partir de la firma del contrato, no siendo admitida ninguna oferta que contemple un periodo superior.

Vigo, 30 de Enero de 2019

La Directora

Fdo.: Beatriz Colunga Fidalgo

El Jefe de la División de Sistemas De Información.

AUTORIDAD PORTUARIA DE VIGO

Fdo.: David Silveira Vila

32