Puerto de Vigo
Autoridad Portuaria de Vigo

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SUMINISTRO, INSTALACIÓN Y SEGUIMIENTO OPERATIVO DE SISTEMAS DE CIBERSEGURIDAD PERIMETRAL PARA LA AUTORIDAD PORTUARIA DE VIGO

Septiembre 2022

Tabla de contenido

1 OBJETO

El objeto de la presente Especificación Técnica es la renovación y mejora de los sistemas de ciberseguridad perimetral de la Autoridad Portuaria de Vigo (en adelante APV).

Este contrato de servicios incluye la contratación del diseño del sistema propuesto, el suministro, instalación y puesta en marcha en condiciones plenamente operativas de los equipos ofertados, así como la prestación continua por un período de un (1) año de los servicios necesarios para llevar a cabo la adecuación de la infraestructura existente, el soporte, operación y mantenimiento de la totalidad del sistema, así como la asistencia técnica ante los posibles incidentes de ciberseguridad que puedan producirse durante el periodo contratado.

Será responsabilidad de cada uno de los licitadores definir el conjunto de su propuesta que, en todo caso, deberá responder a una tipología de infraestructuras multicapa, incluyendo el suministro de firewalls (sistemas dedicados) y sus correspondientes licencias, así como los servicios de valor añadido, orientados a la automatización y a una digitalización efectiva, que faciliten la integración, operación y evolución de la tecnología desplegada en el ecosistema de la APV.

2 ANTECEDENTES

La APV dispone en la actualidad de 2 Firewalls que protegen su infraestructura IT frente a cualquier intento de ataque desde el exterior.

En el contexto actual, las necesidades de protección frente a cualquier amenaza aumentan y es necesario proteger la infraestructura IT también a posibles intentos de ataques tanto desde la red interna como desde la externa. Por este motivo, y debido a la obsolescencia de la infraestructura actual de seguridad, es imprescindible renovar los firewalls actuales de la APV y dotar al conjunto de la red de una protección más robusta y acorde a las necesidades actuales. Por ende, este objetivo obliga al adjudicatario a reconfigurar y segmentar las comunicaciones IT para aplicar las buenas prácticas marcadas por el Centro Criptológico Nacional.

3 ALCANCE

El alcance de esta licitación, tal y como se ha dicho en el Capítulo 1 , incluye todos los trabajos y materiales necesarios para tener operativa una barrera de protección perimetral surgida como evolución de la infraestructura existente, así como la realización de servicios de explotación durante un año. Esto incluye al menos la adquisición, instalación, configuración inicial, monitorización, soporte y gestión de los nuevos sistemas.

De forma exhaustiva y no limitativa, las prestaciones que integran el objeto de la contratación son, al menos, las siguientes:

- Diseño de la solución que se pretende implementar, describiendo con detalle la arquitectura propuesta, la nueva solución debe contemplar la instalación de una doble barrera de seguridad.
- Suministro de la infraestructura de seguridad perimetral y sistema de gestión.
- Instalación física, configuración y puesta en funcionamiento de la infraestructura suministrada de forma coherente y óptima.
- Plena integración de todos los componentes entre sí y con la infraestructura existente actualmente en la sede de la APV.

- Migración de las reglas de seguridad y configuraciones de las redes VPN actuales a nuevo sistema objeto de contratación, aplicando las mejoras necesarias para el cumplimento de buenas prácticas en sistemas de ciberseguridad perimetral.

- Adecuación de las comunicaciones para obtener el mejor resultado posible en la doble protección perimetral y también en las comunicaciones de la infraestructura interna de la APV.

- Doce meses de Seguimiento Operativo (proactivo, preventivo y evolutivo), así como el Mantenimiento correctivo y soporte técnico de la infraestructura de seguridad perimetral objeto de contratación.

- Asistencia técnica ante posibles incidentes de ciberseguridad detectados durante la vigencia de contrato.

- Licencias y contratos de soporte con fabricante necesarias de los productos ofertados durante un periodo de tres años.

- Servicios de valor añadido a identificar por el licitador.

La APV exigirá la máxima disponibilidad de sus comunicaciones y para ello necesita la máxima calidad en los trabajos a realizar.

Los licitantes deberán de tener presente que es fundamental el seguimiento operativo y el mantenimiento del sistema, indispensable para la continuidad del negocio. Por todo ello se deberá de reducir en lo posible cortes de comunicaciones con el exterior, tanto durante la fase de implantación como durante la de soporte.

La APV necesita una proactividad por parte del proveedor proponiendo éste mejoras a nivel de arquitectura, dimensionamiento y optimización de recursos.

El soporte ante incidencias de todos los sistemas debe de ser proactivo y con un tiempo de detección y respuesta tal y como se detalla en el capítulo correspondiente.

Es muy importante la monitorización para detectar cualquier incidencia. Si hay una degradación o caída de servicio que no haya detectado el sistema de monitorización, sino que se haya reportado por el cliente, se considerará un incidente en el contrato y habrá que estudiarlo y tomar medidas para que no vuelva a suceder.

Según se indica en el punto **'**3.5 Horarios', además de los servicios de monitorización se debe de tener un sistema de atención 24x7 para atender las incidencias detectadas por los sistemas de monitorización desplegados por el adjudicatario o ante solicitudes urgentes de los Técnicos de la APV.

Todos los servicios inherentes a este contrato deberán realizarse desde España.

3.1 Solución Técnica

El Departamento de Tecnologías de la APV, teniendo en cuenta el contexto actual en materia de ciberseguridad, ha estimado la conveniencia de renovar y reforzar el nivel de seguridad perimetral de su entorno digital. Para ello, es necesario adecuar, definir, implantar y mantener los sistemas de ciberseguridad de las comunicaciones que se producen entre sus distintos escenarios operativos.

El personal propio de la APV asignado a las TIC dará el servicio de primer nivel, y por conocimiento, afinidad y facilidad de uso de nuestro propio departamento de TI, **se valorará el mayor grado de homogeneidad tecnológica adecuado a los fines a conseguir en la propuesta de cada licitador**, minimizando el número de tecnologías a gestionar y una excesiva necesidad de capacitación**. La APV marca también como imperativo que los equipos sean dedicados (appliance) y, por tanto, serán excluyentes aquellas propuestas del tipo virtual.**

La instalación in situ de los equipos será realizado por el propio suministrador, el cual debe tener **la experiencia y conocimiento demostrable en instalaciones del tipo CPD, en servicios de Ciberseguridad y en grandes infraestructuras. Por la criticidad de las tareas a desarrollar, la APV valorará que la cualificación del personal sea adecuada para la ejecución de dichas tareas en los CPDs objeto de la instalación de la solución.**

El adjudicatario suministrará los paneles, latiguillos y otro equipamiento menor necesario para la instalación de la solución en los racks ya existentes.

3.2 Servicios

A partir del diseño ofertado en la fase de licitación, el adjudicatario será el responsable de la instalación, configuración, puesta en marcha, seguimiento operativo y mantenimiento de la infraestructura ofertada.

La estructura de servicios propuesta tendrá que incluir la administración y operación de la solución durante los 12 meses siguientes a la entrada en producción de los sistemas, incluyendo al menos los siguientes apartados:

- Gestión de la infraestructura y su capacidad.
- Monitorización 24x7.
- Mantenimiento proactivo, preventivo, tunning.
- Mantenimiento correctivo, parcheo de vulnerabilidades.
- Gestión de backups.
- Upgrades técnicos, actualizaciones de versiones.
- Actualizaciones automáticas de firmas.
- Documentación de configuración, reglas…
- Adecuación de las comunicaciones y reglas entre las distintas subredes.
- Integración de la gestión de incidencias de manera automatizada e integrada dentro del ecosistema de la APV.
- Asistencia ante incidentes de Ciberseguridad.
- Actuaciones a petición del cliente.

3.3 Formación

Aunque la responsabilidad de este servicio es del adjudicatario incluyendo la administración de los equipos, el personal técnico de la APV realizará el servicio de primer nivel y para ello necesita actualizar o adquirir ciertos conocimientos sobre el funcionamiento de la tecnología propuesta, **valorándose por tanto la formación ofrecida incluida en la propuesta del licitador.**

También se deberá formar al personal técnico de la APV sobre la utilización de cualquier servicio planteado en este contrato.

3.4 Plan de implantación

Dado que estos elementos se insertarán en una infraestructura ya existente y que está prestando el servicio de conectividad con el exterior, es muy importante que los trabajos de instalación interfieran lo menos posible con la operativa diaria, por ello **se valorará un plan de implantación que los candidatos han de adjuntar en esta licitación, especificando tareas y cronograma, la metodología, plazos, gestión de riesgos y recursos implicados.**

Así mismo, destacamos la importancia de la coordinación del equipo del adjudicatario con los equipos ya existentes del Departamento IT de la APV.

3.5 Horarios

A los efectos de la correcta planificación de los trabajos de implantación, hay que comentar que la jornada laboral ordinaria de la APV se realiza de Lunes a Viernes entre las 08:00 y las 15:00 horas.

El requisito fijado por la APV es disponer de las comunicaciones operativas los 7 días de la semana (24x7).

El servicio se prestará normalmente en modalidad 8x5 y desde las instalaciones del adjudicatario, no obstante, dada la naturaleza del mismo y su criticidad, tanto para garantizar el funcionamiento de las Comunicaciones como por los riesgos asociados a la Ciberseguridad, **será necesario disponer de un servicio 24x7 con capacidad técnica para dar respuesta a las alertas de la monitorización o requerimientos críticos del cliente. Se valorarán las opciones que ofrezcan los candidatos para resolver esta necesidad.**

4 INFORMACIÓN DEL ENTORNO Y REQUISITOS DE SUMINISTRO.

Detallaremos a continuación conocimiento de la arquitectura actual y cuáles son los requisitos necesarios para poder ofertar el equipamiento necesario para la solución.

4.1 Arquitectura actual

A continuación, se describen las características del equipamiento actual referido a infraestructura de seguridad perimetral, que será sustituido y formará parte del contrato de servicio propuesto:

- Dos firewall Fortigate 80D en HA.
    - 200 reglas de NAT (Network Access Table)
    - Lista de accesos (Access List)
    - Túneles VPN / IPSec: 7 túneles
    - Gestión de la red SSL VPN para usuarios
    - Rutas estáticas y policy routes, securización de VLANs, objetos (addreses, network y service), usuarios locales y ACL manager.
- Infraestructura de Servidores y Comunicaciones.
    - La APV dispone de un entorno virtualizado VmWare redundado entre dos CPDs, situados dentro del recinto portuario en ubicaciones alejadas entre sí y conectados mediante fibra óptica.
    - Las distintas dependencias dentro del recinto portuario están comunicadas mediante nodos de fibra óptica monomodo.
    - No existen sedes remotas.

4.2 Requisitos generales de la solución a ofertar

Será objeto de suministro una infraestructura de doble seguridad perimetral que permita renovar y mejorar la actual infraestructura descrita en el punto anterior 4.1. Asimismo, será objeto de contratación un sistema de gestión que permita la administración de dicha infraestructura, integrando gestión de logs y generación de informes.

La solución ofertada debe estar diseñenada con las redundancias necesarias para garantizar en la medida de lo posible la disponibilidad del sistema del 99,99% en los entornos productivos, sin puntos únicos de fallo.

Todo el equipamiento será nuevo y original del fabricante. **Los sistemas ofertados deberán tener plena vigencia de soporte de fabricante, no pudiendo estar prevista la finalización de esta en un periodo inferior a cinco (5) años** a contar desde la fecha de finalización de la presentación de las ofertas. Si durante la fase de adjudicación o instalación cambiase esa vigencia, los equipos ofertados deberán ser sustituidos, sin coste para la APV, por otros actualizados, del mismo fabricante y con las mismas o superiores características que los anteriores. Este cambio deberá ser aprobado por el responsable que la Autoridad Portuaria nombre para este contrato.

A continuación, se especifican las características de los distintos elementos a suministrar.

La renovación de la actual infraestructura de seguridad pretende solucionar la actual problemática derivada de las siguientes circunstancias:

- Equipamiento con capacidad de proceso insuficiente.
- Imposibilidad de actualizaciones a versiones actuales y seguras por parte del fabricante del equipamiento.
- Segmentación insuficiente de las redes internas.
- Securización de la actual segmentación basada en ACLs de la electrónica de red.
- Inexistencia de seguridad en el entorno OT.

La solución ofertada deberá estar basada en una arquitectura resiliente en todos los elementos que la conformen. Es decir, cada elemento deberá suministrarse con redundancia hardware para poder implementar sistemas en alta disponibilidad que proporcionen la tolerancia a fallos necesaria para garantizar la continuidad de los servicios.

4.3 Características hardware de la solución

Se suministrarán equipos firewall de última generación que, como mínimo, deben cumplir con las características técnicas relacionadas a continuación:

4.3.1 Características de rendimiento

Las características de rendimiento que cada equipo suministrado debe cumplir serán, al menos, las siguientes:

Bidirecional LAN-LAN

- 3 Gbps de throughput con las protecciones de “Threat Prevention” activas
- 4 Gbps de throughput con las Inspección SSL
- 13 Gbps de throughput con las protecciones de “IPS” activas

- 27 Gbps de throughput con las protecciones de “FW” activas en condiciones ideales
- 4 Gbps de throughput VPN en condiciones ideales
- 280.000 conexiones por segundo
- 3 millones de sesiones concurrentes (máxima memoria RAM)
- 16.000 para Clientes a túneles GW

Bidireccional LAN-WAN

- 1,5 Gbps de throughput con las protecciones de “Threat Prevention” activas
- 3 Gbps de throughput con las protecciones de “NGFW” activas
- 3,3 Gbps de throughput con las protecciones de “IPS” activas
- 3,6 Gbps de throughput con las protecciones de “FW” activas en condiciones no ideales.
- 4 Gbps de throughput con las protecciones de “FW” activas en condiciones ideales.
- 2,75 Gbps de throughput VPN en condiciones ideales
- 60.000 conexiones por segundo
- 4 millones de sesiones concurrentes (máxima memoria RAM)

4.4 Características funcionales

El sistema de seguridad perimetral debe contemplar, al menos, las siguientes características funcionales:

Generales para todo tipo de comunicaciones:

- Deberá reunir los requisitos y características previstos en los puntos 4.2 y 4.3 del presente Pliego y que resultan precisos para sustituir y mejorar el equipamiento de acceso, configuración y gestión de redes VPN actualmente activas en la APV en términos de compatibilidad.
- Módulo IPS que proteja la red frente ataques y amenazas.
- Control de aplicaciones que proporcione capacidades de identificación y control, así como aplicación de políticas granulares por usuario o grupo.
- Prevención de amenazas mediante “sandboxing”.

Según el tipo de comunicaciones, el equipamiento deberá cumplir las siguientes características:

Comunicaciones LAN to WAN

- La gestión se debe realizar desde un servidor independiente de los equipos que componen la infraestructura de seguridad perimetral.
- Los sistemas propuestos deben ser reconocidos como líder en el último Cuadrante Mágico de Gartner para Network Firewall (Leaders).
- Capacidad de visualización de los logs específicos de una regla en la misma vista en la que se visualizan las políticas.

- Habilitación para limitar el ancho de banda (tanto de subida como de bajada) en la misma base de reglas de firewall de aplicaciones. Esto es, para una determinada aplicación, se podrá limitar el ancho de banda, de subida o bajada. Es imprescindible que esto se pueda definir como acción por regla en la propia base de reglas.

- El panel de configuración de la base de reglas debe proporcionar un contador de cuántas veces hizo "match" cada regla (hit count), aunque la propia regla no registre el log.

- Correlación de logs y eventos, unificando los logs de los clústeres centrales y los distribuidos.

- Gestión de cumplimiento normativo y buenas prácticas. Posibilidad de generar informes de cumplimiento de acuerdo con las normativas de seguridad de referencia.

- Capacidad de definir una política de control de acceso a través de reglas anidadas.

- Separación de la gestión de reglas referidas a control de acceso y reglas referidas a prevención de amenazas.

- La gestión se debe realizar en 2 modalidades:
    - Servidor de gestión (físico o virtual). Este servidor debe ofrecer la posibilidad de gestión vía cliente pesado y vía interfaz web.

    - Servicio de gestión cloud.
- Plataforma de “Zero-Touch”. Esta plataforma permitirá que el equipo, en el arranque de la plataforma y de forma automática, conecte y descargue la configuración, quedando totalmente sincronizado con la consola de gestión sin necesidad de ninguna configuración adicional por parte de los administradores.

- El sistema de gestión contará con una plataforma de log y reporting integrados.

- La plataforma de log y reporting debe de tener la capacidad de mostrar tanto la información de control de acceso como de seguridad en una sola vista y poder hacer búsquedas texto libre, así como mostrar los resultados de forma inmediata y de forma gráfica.

- Presentación de vistas e informes filtrando por grupos de DA.

- Con capacidad de extraer y eliminar el malware contenido en documentos descargados o enviados por correo electrónico y entregar estos documentos libres de malware. (al menos de los documentos que son tipo del PDF y de Microsoft Office)

Comunicaciones LAN-LAN

- Deberá tener Doble factor de autentificación (2FA) nativos propios.
- Este doble factor deberá poderse desplegar en SSLVPN, VPN IPSec, Autenticación de servidor de seguridad o por Autentificación del administrador.

- El doble factor debe soportar Token de hardware, Token software, Contraseña, además de certificado PKI, Código de acceso a través de SMS, Código de acceso por correo electrónico.

- Debe basarse en un dispositivo autónomo cuyo hardware esté basado en ASIC.

- El dispositivo debe formar parte de una familia de productos que disponga de certificaciones ICSA Labs para antivirus, cortafuegos corporativo, IPsec, NIPS y SSL-TLS.

- La solución propuesta debe ser capaz de actuar como controladora de la red WLAN/LAN para Switches y Puntos de Acceso del mismo fabricante ofreciendo una gestión unificada de Seguridad, SD-WAN, LAN y WLAN.

- La solución propuesta debe ser reconocida como líder en el último Cuadrante Mágico de Gartner para Network Firewall.

- La solución propuesta debe ser reconocida como líder en el último Cuadrante Mágico de Gartner para WAN Edge

- Ser propietario del sistema operativo para evitar heredar las vulnerabilidades del sistema operativo común.

- Residir en el disco flash para mejorar la fiabilidad frente a instalaciones sobre disco duro.

- Permitir el arranque dual

- Ser actualizable a través de interfaz de usuario web o TFTP.

- Las configuraciones en el dispositivo deberán:

    - Ser fácilmente guardadas o restauradas a través de GUI y CLI a / desde el PC local, la gestión centralizada o almacenamiento USB

    - Proporcionar archivos de configuración de comandos CLI legibles por el Bloc de notas de Windows

    - Posibilidad de exportar la configuración en formato YAML

    - Tener opción para el archivado cifrado de las copias de seguridad

    - Ofrecer las revisiones de configuración a través de la interfaz gráfica de usuario para facilitar su uso. La pantalla deberá permitir hacer un revert a la configuración seleccionada y hacer un diff entre 2 versiones. Los administradores deberán ser capaces de añadir comentarios para cada revisión.

5 SERVICIOS DE IMPLANTACIÓN

Se valorará la metodología que seguirá el adjudicatario para la prestación del servicio de implantación y las relaciones con el cliente, mejores prácticas, herramientas, recursos, etc.

El objeto del contrato comprende los servicios de instalación de los sistemas y configuración de la doble barrera de seguridad, así como la migración desde la infraestructura de seguridad perimetral y acceso VPN actual al nuevo sistema de seguridad perimetral y la adecuación o segmentación de la red actual para la aplicación de buenas prácticas de ciberseguridad.

La instalación, configuración y puesta en marcha de la nueva infraestructura de seguridad perimetral y del sistema de gestión se realizará con el mínimo impacto sobre la continuidad en la prestación de los servicios actuales, teniendo en cuenta que la atención de primer nivel será realizada por el personal de la APV (operativos 8x5), dentro del horario que el responsable del contrato de la APV determine a estos efectos y siguiendo los requisitos definidos en este pliego.

5.1 Análisis y diseño de la solución a implantar.

En una primera fase, se realizará una auditoría consistente en un análisis y toma de datos del entorno existente. A la vista de los datos obtenidos, se formulará una propuesta definitiva referida a la arquitectura y diseño de la solución que se propone implementar. A estos efectos, esta propuesta deberá incluir la configuración de la arquitectura del sistema de seguridad perimetral y la configuración de los puntos de conexión con la infraestructura de red existentes.

5.2 Instalación y configuración del suministro

El adjudicatario realizará la instalación física de los equipos, así como la instalación y configuración del sistema de gestión.

5.3 Migración de la infraestructura actual al nuevo sistema

Será objeto de contratación la migración desde la actual infraestructura seguridad perimetral hacia el nuevo sistema diseñado por el licitador. Para la realización de esta prestación, **el adjudicatario deberá presentar un Plan de migración, que incluya al máximo detalle el proceso de ejecución de la migración detallando todas y cada una de las fases de ejecución del plan, así como los hitos de dicho proceso migratorio.**

La ejecución de este proceso de migración se realizará de forma presencial en las instalaciones de la APV con carácter obligatorio y de acuerdo con las indicaciones del responsable del contrato que esta designe.

La migración será realizada garantizando, en todo momento, la continuidad en la prestación de servicios, de tal manera que se mantenga la disponibilidad de la información durante todo el proceso de migración. Si durante este proceso de migración se detectara la necesidad de realizar cualquier actividad de instalación o configuración de estos equipos que pudiera ser disruptiva para el servicio, el adjudicatario deberá comunicarlo, con carácter inmediato a la APV, indicando el tiempo estimado de afección a la continuidad del servicio. En este supuesto, la APV determinará el horario más adecuado para la ejecución de esta tarea, que incluye la posibilidad de ejecutar estos trabajos fuera del horario laboral.

El proceso migratorio y de implantación debe prever expresamente una fase correspondiente a un **Plan de pruebas de alta disponibilidad y de redundancia de todo el equipamiento**. Además, durante la fase de implantación de los servicios, el adjudicatario estará obligado a la elaboración y presentación de informes de progreso, como mínimo, quincenales.

5.4 Entrega de documentación técnica y formación

El adjudicatario deberá entregar a la APV, a la finalización de los trabajos de implantación y migración y con carácter previo al inicio de la formación prevista a continuación, toda la documentación relativa a la solución implantada.

La documentación deberá contener necesariamente:

- Documento definitivo de arquitectura y diseño técnico detallado de la solución de seguridad perimetral y sistema de gestión implantada.

- Documento descriptivo de las configuraciones de cada uno de los componentes referidos en el apartado 4 y de los servicios del apartado 5.

- Documento descriptivo de los procedimientos de operación.

- Acreditación de disponer de las licencias exigidas.

Asimismo, será objeto de contratación la formación para, al menos, dos personas pertenecientes al personal técnico de la APV en la solución implantada, certificada por la marca de los componentes propuestos e impartida de forma presencial en las instalaciones de la APV. La duración será de al menos diez horas repartidas en un mínimo de cuatro jornadas.

Una vez finalizada la formación o, en todo caso, fijadas las fechas para su impartición, se procederá a la firma del Acta de recepción del suministro y servicios de implantación, es en este momento cuando comenzará la vigencia del periodo de 12 meses destinado a la fase de seguimiento operativo (preventivo, proactivo y evolutivo) y mantenimiento correctivo de la solución implantada.

Será obligatoria la realización de una auditoria y, en su caso, revisión relativas al estado de operatividad, arquitectura y diseño de toda la solución propuesta, cuya fecha será determinada por el responsable del contrato por parte de la APV dentro del plazo de un año a contar desde la firma del Acta de recepción del suministro y de servicios de implantación. Una vez concluida la referida auditoría se entregará, en formato digital, un informe con el detalle de la situación, así como de aquellas actuaciones susceptibles de mejoras.

En la oferta técnica debe incluirse una descripción a alto nivel de los trabajos de auditoria a realizar ajustados a los sistemas y propuesta ofertada.

6 SEGUIMIENTO OPERATIVO (PROACTIVO, PREVENTIVO Y EVOLUTIVO).

La fase de seguimiento operativo comenzará a partir de la aceptación del Acta de Recepción de la implantación de los sistemas. Esta fase esta destinada a realizar sobre la solución instalada cualquier acción u operativa que optimice, mejore o actualice cualquier parte del sistema en el que, a través de la monitorización, tunnig del mismo o por parte del personal propio de la APV, se hayan detectado puntos de mejora, el fin de la misma no es la corrección de incidencias, si no la mejora y optimización del sistema implantado, así mismo, en esta fase estarán incluidas todas las actualizaciones de software o firmware necesarias para que los sistemas se encuentren siempre a la última versión estable de los mismos.

Las operativas realizadas dentro de este marco deberán quedar registradas en la herramienta informatica de Gestión del Servicio.

En la oferta técnica debe incluirse un plan de seguimiento operativo acorde a los sistemas y funcionalidades ofertadas.

Como mínimo se deberá cubrir:

- Gestión de la infraestructura y su capacidad.
- Monitorización 24x7.
- Mantenimiento preventivo, tunning.
- Gestión de backups.
- Upgrades técnicos, actualizaciones de versiones.
- Actualizaciones automáticas de firmas.
- Documentación de configuración, reglas…

- Adecuación de las comunicaciones y reglas entre las distintas subredes.
- Actuaciones a petición del cliente.

7 GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD.

A partir de la firma del contrato, la empresa adjudicataria queda obligada a prestarle a la APV, la asistencia necesaria para resolver cualquier incidente de seguridad informatica
que pueda surgir, esta asistencia se realizará siempre en coordinación con el personal técnico propio y la disponibilidad para prestar este servicio será absoluta, en cualquier día y horario. El periodo de duración finalizará cuando el incidente sea erradicado y se hayan finalizado todas las labores administrativas que el mismo haya generado en cumplimiento del Esquema Nacional de Seguridad, la empresa adjudicataria realizará tanto labores técnicas como la redacción de los informes pertinentes que será necesario elevar a los Organismos que corresponda.

Para la prestación de este servicio, en el equipo de trabajo debe figurar personal con la suficiente cualificación, en la relación de personal asignado al equipo de trabajo debe figurar la experiencia y certificaciones o cualificaciones a este respecto.

En la oferta técnica debe incluirse un plan de gestión ante incidentes de ciberseguridad adaptado al entorno particularizado a implantar.

8 GESTIÓN DE INCIDENCIAS TÉCNICAS. (mantenimiento correctivo).

Se valorará la metodología que seguirá el adjudicatario para la prestación de los servicios y las relaciones con el cliente, mejores prácticas, herramientas, recursos, etc.
La gestión de incidencias o solicitudes de cambios se realizará utilizando la herramienta de ticketing para tal efecto, con dicha herramienta se comprobará el complimiento de los Acuerdos de Nivel de Servicio

8.1 Acuerdo de Nivel de Servicio.

Para definir el acuerdo de nivel de servicio (ANS) requerido se establecen los siguientes indicadores de cumplimiento:

- Tiempo de respuesta: Tiempo transcurrido entre la detección y/o declaración de una incidencia por los canales establecidos hasta el tiempo de intervención de un operador técnico (no cuenta un e-mail de respuesta automática ni una locución telefónica)

- Tiempo de resolución: Tiempo transcurrido entre la detección y/o declaración de una incidencia por los canales establecidos hasta el momento en que el impacto desaparece o se ve reducido a un nivel aceptable por la APV.

- Tiempo de intervención presencial: En incidencias Criticas o Altas que no puedan ser resueltas mediante conexión remota, el que transcurre entre la detección y/o declaración de una incidencia por los canales establecidos hasta el comienzo de la intervención presencial en las instalaciones de la APV.

Las prioridades para las incidencias seguirán la siguiente clasificación

- Critica: Sistema parado, indisponible, gravemente inestable o corrupto ya sea en su totalidad o en más de un 50%.

- Alta: Sistema dañado o con impacto directo en parte del negocio en ese momento, o bien en todo el negocio de forma inminente, o un problema general de rendimiento.
- Media: Sistema dañado o con un impacto en negocio muy localizado.
- Baja: Otras incidencias.

La clasificación de las solicitudes de cambio será en función de la urgencia de las mismas, por ejemplo, la implementación de una nueva regla que impida el éxito de un ciberataque que esté en curso ha de ser Crítica, mientras que otra regla que permita determinada navegación de un nuevo servicio que se esté desplegando podría ser Media o incluso Baja.

Los Acuerdos de Nivel de Servicio mínimos exigidos por La APV ante cualquier solicitud o incidencia son los que a continuación se detallan.

Las penalizaciones se calcularían tomando como base el coste mensual del servicio.

I

I

I

I

SLAs en el Tiempo de respuesta

Prioridad	SLA de Respuesta	Explicación	Penalización
Crítica	< 15 minutos	En todas las incidencias Críticas el tiempo de respuesta debe de ser menor de 15 min.	1,50%
Alta	< 2 horas	Al menos en el 90% de las incidencias Altas el tiempo de respuesta debe de ser menor de 2 horas	1 %
Media	< 6 horas	Al menos en el 90% de las incidencias con criticidad Media el tiempo de respuesta debe de ser menor de 6 horas	0,5 %
Baja	< 24 horas	Al menos en el 90% de las incidencias con criticidad Baja el tiempo de respuesta debe de ser menor de 24 horas	0,25 %

SLAs en el tiempo de resolución

Prioridad	SLA de Resolución	Explicación	Penalización
Crítica	< 30 minutos	El 100% de las peticiones con	2%

		criticidad Crítica el tiempo de resolución debe de ser menor de 30 minutos.	
Alta	< 4 horas	Al menos en el 90% de las peticiones con criticidad Alta el tiempo de resolución debe de ser menor de 4 horas.	1,25%
Media	< 32 horas	Al menos en el 90% de las peticiones con criticidad Media el tiempo de resolución debe de ser menor de 32 horas.	0,5%
Baja	< 60 horas	Al menos en el 90% de las peticiones con criticidad Baja el tiempo de resolución debe de ser menor de 60 horas.	0,25%

SLAs en el tiempo de intervención presencial

Prioridad	SLA de Intevención presencial	Explicación	Penalización
Crítica y Alta	El ofertado por el adjudicatario.	El 100% de las peticiones con criticidad Crítica y Alta el tiempo de intervención presencial será el ofertado por el adjuciatario, máximo 4 horas.	2%

Para todos los ANS se tendrá en cuenta:

- Se realizarán los cálculos por mes natural.
- El importe de las penalizaciones no podrá superar el 10% del coste mensual del servicio.
- Sólo se considerarán los incumplimientos imputables al adjudicatario. No serán computables para el cálculo de las penalizaciones los incumplimientos de los ANS cuando éstos sean responsabilidad del personal de la APV o de terceros que impidan el correcto cumplimiento de los ANS.
- Para números bajos de incidencias en los que la ratio de fallo con el nivel de servicio definido para cada incidencia/solicitud sea menor que la unidad se permitirá tener al menos un fallo sin penalización. Ejemplo: si hay 9 incidencias de severidad media permitir al menos un fallo sin penalizar (9*0.10=0.9 permitir 1 fallo). Quedan excluidas las incidencias Críticas y Altas.
- Para las incidencias Bajas o Medias el cálculo de los valores de ANS no se contabilizarán los tiempos correspondientes a los siguientes periodos:

- Tiempo fuera de la jornada de soporte contratada, que será de lunes a viernes de 7:00 a 18:00 horas
- sábados, domingos y fiestas de ámbito nacional.
- Tiempo en que el ticket permanece en alguno de los siguientes estados: Espera o Resuelta, y cuando esta espera sea debida a solicitud de información o acciones por parte del Personal de la APV o de terceros.

- Los sistemas de Comunicaciones deben de estar operativos 24x7 por los que no hay exclusión de periodos a la hora del cálculo de penalizaciones para incidencias Altas o Críticas.

- Quedan también excluidas las solicitudes hechas por la APV que no puedan efectuarse en horario laboral y tengan que realizarse en una ventana de actuación en concreto, incluso en festivos o fines de semana.

8.2 Asistencia in situ.

Para aquellas incidencias de tipo Critica o Alta cuya recuperación de los servicios no puedan realizarse de manera remota, se debe contemplar la posibilidad de realizar asistencia presencial en las instalaciones de la APV, para ello, en la oferta debe especificarse el tiempo de intervención presencial para estos casos, estimándose la posibilidad de dos asistencias durante el periodo de vigencia de la prestación (12 meses). El ofertante deberá aportar la documentación que justifique los tiempos ofertados. Se valorarán dichos tiempos por ser estos sistemas críticos para la APV.

8.3 Herramientas y operativa general

En la oferta técnica debe de figurar, de forma detallada, la **descripción de la plataforma informática (a partir de ahora ServiceDesk) que servirá para el seguimiento de las labores de los distintos tipos seguimiento y mantenimiento, así como de las incidencias surgidas durante el contrato**. Se valorará que la gestión, tanto de los planes de mantenimiento como de las incidencias, sea centralizada en una única herramienta y, será necesario aportar en la oferta, demo o acceso remoto a ésta para su correcta valoración; el personal responsable que la APV designe, tendrá acceso a la apertura y seguimiento de las incidencias, así como a la consulta de la gestión de los planes de mantenimiento acordados.

Se valorará que el software ofertado permita generar informes y estadísticas de la información registrada, detallada y agrupada, así como su exportación a otros formatos, como mínimo a la herramienta ofimática Microsoft Excel.

Como ya hemos indicado, al fin de poder prestar este servicio con el mayor nivel de eficiencia, calidad y control posible, todas las incidencias se registrarán y comunicarán a través del ServiceDesk. El registro lo podrán hacer cualquiera de los actores que forman parte del servicio. Las incidencias se registrarán con el mayor detalle posible, adjuntando toda la información disponible.

En todo caso es obligación del proveedor mantener actualizado el ServiceDesk, que se usará posteriormente como herramienta de control y seguimiento del contrato.

El modelo general de funcionamiento es el siguiente:

- Las incidencias y solicitudes son registradas por los diferentes actores del servicio en el ServicesDesk. Si es una Incidencia deberá de ser registrada por los técnicos del adjudicatario en cuanto sea detectada por su sistema de monitorización. Si es una solicitud será registrada por los Técnicos de la APV. Tanto las incidencias como las solicitudes se categorizarán en función de su criticidad.

- El equipo de trabajo del adjudicatario identificará la naturaleza de la incidencia o solicitud y asignará los recursos necesarios para la resolución y el cumplimiento de los ANS.

- Todas las actuaciones y comunicaciones se verán obligatoriamente reflejadas por todos los técnicos que intervengan en los trabajos hasta la resolución de la incidencia o solicitud. Para ello se utilizará la opción de "Seguimiento" en cada ticket.

- Una vez finalizados los trabajos de una solicitud o incidencia serán los técnicos de la APV quienes aprueben dichos trabajos pudiendo, en cualquier caso, rechazar la solución con su argumentación en el propio ServiceDesk.

En aquellas situaciones que por su urgencia u otro motivo la comunicación inicial no se efectúe mediante ServiceDesk sino, por ejemplo, con una llamada telefónica, el caso se registrará en el ServiceDesk en cuanto sea posible.

8.4 Equipo de trabajo

El equipo humano que se incorporará tras la formalización del contrato para la ejecución de los trabajos deberá estar constituido íntegramente por personal de plantilla de la empresa adjudicataria en la fecha de la contratación y, salvo causas de fuerza mayor, las personas asignadas deberán ser las que presten el servicio ofertado durante toda la vigencia del contrato.

Como recursos mínimos, el equipo de trabajo deberá estar formado por:

- Perfil 1.- Un jefe de Proyecto con las funciones de consultor encargado del análisis de necesidades iniciales y seguimiento del servicio, así como ser el responsable de la coordinación entre el equipo de trabajo y el personal técnico propio que la APV asigne al proyecto.

- Perfil 2.- Dos Técnicos de sistemas con la cualificación suficiente para la implantación de la solución ofertada.

- Perfil 3.- Dos Técnicos de sistemas con la suficiente cualificación para la gestión del seguimiento operativo y mantenimiento correctivo, estas funciones pueden ser desarrolladas por los técnicos de implantación siempre y cuando su cualificación sea suficiente para este cometido.

- Perfil 4.- Dos técnicos de Sistemas con la suficiente cualificación para la gestión de incidentes de ciberseguridad, al igual que en el punto anterior estas funciones pueden ser desarrolladas por los técnicos de implantación o seguimiento operativo, siempre y cuando su cualificación sea suficiente para este cometido.

Todos los licitadores deberán de indicar por cada persona:

- Perfil asignado a la ejecución del contrato

- Estimación de su dedicación.
- Calificación profesional
- Experiencia y Certificaciones aplicables a los trabajos a realizar.

Así mismo la APV podrá solicitar su CV ciego y TC2 sin nombre si lo considera conveniente.

Es exigible a todo adjudicatario un adecuado nivel de conocimiento técnico y diligencia en la ejecución de los trabajos contratados, de modo que se asegure un adecuado grado de calidad en los productos resultantes. Durante la ejecución del contrato, la APV podrá verificar que los conocimientos y experiencia profesional del equipo de trabajo corresponden con los datos presentado en la licitación.

No obstante, la falsedad en el nivel de conocimientos técnicos del personal ofertado, así como la sustitución de alguno de los componentes del equipo adscrito a la ejecución de los trabajos sin observar el procedimiento y requisitos exigidos en los párrafos siguientes, facultará a la APV para instar la resolución del contrato.

La valoración final de la calidad de los trabajos desarrollados corresponde al responsable del proyecto designado por la APV, siendo potestad suya adoptar las medidas necesarias para mantener la calidad exigida de los trabajos, pudiendo solicitar el reemplazo de alguno de los recursos humanos asignados si existen razones justificadas que lo aconsejen, con un preaviso de quince días, por otro de igual categoría. Asimismo, la APV podrá exigir la incorporación de más miembros al equipo de trabajo o refuerzos cuando sean necesarios para garantizar el cumplimiento de cada uno de los ANS comprometidos por el adjudicatario en su propuesta. Si la firma adjudicataria propone el cambio de una de las personas del equipo de trabajo, deberá solicitar por escrito con quince días de antelación, exponiendo las razones que obligan a la propuesta. En su caso, el cambio deberá ser aprobado por el responsable del proyecto designado por la APV.

La autorización de cambios puntuales en la composición del mismo requerirá de las siguientes condiciones:

- Justificación escrita, detallada y suficiente, explicando el motivo que origina el cambio.

- Presentación de posibles candidatos con un perfil de cualificación técnica igual o superior al de la persona que se pretende sustituir.

- Aceptación por el responsable del proyecto designado por la APV de alguno de los candidatos propuestos.

8.5 Incompatibilidades

El adjudicatario no podrá subcontratar la instalación, ni ninguno de los de servicios que se hayan propuesto para acometer este contrato, salvo en el caso de la formación sobre el equipamiento que puede ser subcontratado al fabricante.

Cada propuesta será evaluada teniendo en cuenta las guías de buenas prácticas del Centro Criptológico Nacional.

9 SOLVENCIA TÉCNICA Y PROFESIONAL.

Para garantizar la correcta implantación de los sistemas ofertados es necesario que **los licitadores cumplan de manera obligatoria** con los siguientes

requisitos de solvencia técnica y profesional, **la presentación de la documentación correspondiente será condición indispensable para la aceptación de las ofertas**, tal como se indica en el Pliego Administrativo esta documentación **deberá incluirse en el sobre A** de la oferta:

9.1 Requisitos de Solvencia Técnica.

- Que el licitador disponga de las siguientes **certificaciones vigentes** en las siguientes áreas de actividad relacionadas con la prestación del servicio:
    - ISO 20000-1: certificado de calidad de los servicios TI.
    - ISO 27001: certificado de los Sistemas de Gestión de la Seguridad..
    - ISO 9001: certificado de gestión de calidad.
    - Esquema Nacional de Seguridad (ENS), mínimo nivel medio.
- **El equipamiento ofertado** deberá tener una **certificación ALTA en el ENS**, y ser marcas de reconocido prestigio internacional. Este requisito puede ser documentado mediante declaración responsable del ofertante, solicitandose en el periodo de adjudicación las certificaciones correspondientes.
- **Mínimo de tres Certificaciones de buena ejecución por parte de cliente,** donde se haga referencia a la realización de trabajos y servicios prestados similares a los exigidos en este pliego en los dos (2) últimos años, por un valor mínimo de cien mil euros (100.000) cada uno.

9.2 Requisitos de Solvencia Profesional del Equipo de Trabajo.

Es condición indispensable para la aceptación de las ofertas que **el personal integrante del equipo de trabajo propuesto pertenezca a la plantilla laboral de la empresa licitadora en el momento de la presentación de la oferta**, dicha evidencia se realizará mediante declaración jurada relacionando nombre del trabajador, perfil profesional y antigüedad, la documentación acreditativa de esta situación será requerida en la fase de adjudicación.

Dentro del equipo de trabajo destinado a la instalación y prestación del servicio según los requisitos relacionados en este pliego, deberá haber, como mínimo, dos (2) técnicos con conocimientos y experiencia suficiente, para lo cual se debe acompañar, como mínimo:

- Certificado de fabricante de los sistemas a implantar de tener la formación suficiente para la instalación y configuración de la solución propuesta.

10 SEGURIDAD y CIBERSEGURIDAD.

La red desde la que la empresa adjudicataria preste el servicio motivo de esta licitación tendrá que ser una red aislada (VLAN) del resto de su red empresarial. La conexión será mediante una VPN siguiendo las instrucciones y procedimientos establecidos por la APV. Esta red podrá ser auditada para comprobar su seguridad siguiendo los criterios de la APV.

En el caso de Incidente de Ciberseguridad el equipo de trabajo de la empresa adjudicataria estará a plena disposición de la APV, según se especifica en el capítulo 7 de este pliego.

11 CONTROL, GESTIÓN Y SEGUIMIENTO DEL SERVICIO

Mensualmente el adjudicatario informará en reuniones programadas del estado del servicio de los últimos 30 días. Previamente habrá generado informes donde se detallará cualquier incidencia, estado de los sistemas, consumo, dimensionamiento y cualquier otra información que la APV solicite. El proveedor también incluirá información que considere relevante para el correcto funcionamiento de los sistemas de la APV. El objetivo de estas reuniones es hacer un seguimiento del estado de la infraestructura y el servicio y tomar acciones en base a la información disponible.

12 ACUERDOS DE CONFIDENCIALIDAD

El adjudicatario deberá de cumplimentar y firmar los siguientes documentos según las condiciones de la APV:

- Acuerdo de Confidencialidad suscrito por la empresa adjudicataria.
- Declaración de responsabilidad individual firmada por cada una de las personas que participen en el proyecto.
-

13 FASE DE DEVOLUCIÓN

Los servicios a prestar durante esta fase estarán incluidos en esta licitación. El proveedor realizará una devolución del servicio asumiendo el esfuerzo que pueda representar esta actividad y considerando como objetivo básico de esta fase la Transición ordenada de los servicios y activos a la APV con el menor impacto posible en el usuario.

Deberá incluirse en la oferta técnica un Plan de Devolución del Servicio particularizado para la instalación ofertada. Una vez recibida la solicitud de devolución del servicio por parte de la APV, se revisará dicho plan para comprobar su vigencia y aplicación, en caso contrario, se revisará entre ambas partes para proceder a su modificación, validación y aplicación.

Dicho plan profundizara en aquellos detalles técnicos que dependen directamente de la arquitectura técnica y del grado de implantación y automatización de las soluciones y servicios objeto del servicio.

El plan de devolución detallado contendrá todos los datos y la documentación del servicio que permitan a la APV asumir o transferir los servicios a otro proveedor.

14 CONFIDENC., SEGURIDAD y PROT. DATOS (ENS y LOPDGDD)

El presente capitulo tiene por objeto establecer las obligaciones y responsabilidades de las partes intervinientes al respecto de los ficheros que contengan datos de carácter personal propiedad de la Autoridad Portuaria de Vigo a los cuales el adjudicatario tenga acceso exclusivamente para el cumplimiento de los servicios objeto del presente contrato, de conformidad con lo previsto en el Reglamento General de Protección de Datos (UE) 2016/679 Y la Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales (3/2018 de 5 de diciembre), así como la forma de proceder ante accesos a sistemas de la APV y posibles incidentes de seguridad referidos a los sistemas y la información tratada (ENS).

Con carácter general, la entidad adjudicataria del contrato se obliga al cumplimiento de lo que establece el Reglamento (UE) 2016/679, de 27 de abril, relativo a la protección de datos personales de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en lo sucesivo, RGPD) y la normativa de protección de datos aplicable, Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales (3/2018 de 5 de diciembre).

Los datos personales a los que accederá y tratará –o sean susceptibles de tratamiento- la entidad adjudicataria en el ejercicio de la prestación de los servicios profesionales derivados de la formalización del presente contrato, son responsabilidad de la Autoridad Portuaria de Vigo (en los sucesivo, la APV), el cual es responsable del tratamiento.

La entidad adjudicataria ostentará la posición de encargado del tratamiento en relación con estos datos, de conformidad con lo que dispone el artículo 28 del RGPD. A tal efecto, se compromete a utilizarlas única y exclusivamente con la finalidad de prestar los servicios profesionales por los cuales ha sido contratada, así como a cumplir con todas las obligaciones que exige la normativa vigente. La entidad adjudicataria tratará los datos de conformidad con las instrucciones de la APV y, en ningún caso, utilizará los datos con una finalidad diferente a la establecida en el presente contrato, ni los comunicará ni cederá, ni siquiera para su conservación, a cualquier tercero ajeno al contrato. En el caso de que no pueda cumplir tales instrucciones por la razón que fuera o entienda que una de estas instrucciones infringe el RGPD, informará de ello, sin demora, a la APV.

Atendiendo al contenido del artículo 28.10 del RGPD, en caso de que la entidad adjudicataria, como encargado del tratamiento, destine los datos a una otra finalidad, los comunique o los utilice incumpliendo las estipulaciones indicadas, será considerada responsable del tratamiento y deberá responder de las infracciones en las cuales haya incurrido.

La entidad adjudicataria del contrato y la totalidad de sus trabajadores se obligan a mantener estricto deber de secreto y confidencialidad en relación con la información a la cual tenga acceso. Asimismo, las obligaciones de confidencialidad y deber de secreto por parte de la entidad adjudicataria subsistirán, también, con posterioridad a la extinción del presente contrato.

El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado la APV, excepto en los casos en que este último lo autorice de forma expresa. En estos casos, la contratación se efectuará en nombre y por cuenta de la APV. En caso de incumplimiento por parte del subencargado del tratamiento, el encargado del tratamiento seguirá siendo plenamente responsable ante la APV en lo referente al cumplimiento de las obligaciones.

Durante la vigencia del contrato formalizado entre las partes, y de acuerdo con lo que establece el artículo 32 del RGPD, la entidad adjudicataria del contrato se compromete a aplicar, tanto en el momento de determinar los medios de tratamiento como en el momento mismo del tratamiento de los datos personales responsabilidad de la APV y con el fin de evitar su alteración, pérdida, tratamiento o acceso no autorizado, medidas técnicas y organizativas apropiadas y acordes a los principios de protección de datos e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del RGPD y proteger los derechos de los interesados. Para ello, se tendrá en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas. La entidad adjudicataria deberá acreditar el cumplimiento de las medidas de seguridad descritas en el Esquema Nacional de Seguridad (ENS) cuando el contrato afecte a sistemas de información y/o a servicios prestados a través medios electrónicos.

La entidad adjudicataria deberá llevar, de acuerdo con el artículo 30 del RGPD, un registro de actividades de tratamiento efectuadas por cuenta del responsable del tratamiento, que contenga:

a) El nombre y los datos de contacto del encargado del tratamiento; de cada responsable del tratamiento por cuenta del cual actúe el encargado del tratamiento; en su caso, del representante del responsable del tratamiento o del encargado del tratamiento, y del delegado de protección de datos.

b) Las categorías de tratamientos efectuados por cuenta del responsable del tratamiento.

c) En su caso, las transferencias de datos personales que, a su vez, tengan lugar a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49.1. 2º RGPD, la documentación de garantías adecuadas.

d) Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

- La seudonimización y el cifrado de datos personales.
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
- El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento

En el caso de que se produjese cualquier reclamación derivada, directa o indirectamente, del uso indebido o ilegítimo de los datos personales por parte de la entidad adjudicataria o del personal a su servicio, la APV quedará exento de toda responsabilidad y al margen de cualquier reclamación que pudiera plantearse al respecto.

La entidad adjudicataria deberá asistir a la APV en la respuesta al ejercicio de los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición y a no ser objeto de decisiones individualizadas automatizadas, incluida la elaboración de perfiles.

En el supuesto de que el interesado solicite el ejercicio de derechos frente a la APV, este podrá encomendar a la entidad adjudicataria dicho ejercicio, que deberá llevarse a cabo en el plazo máximo de 10 días laborables. Cuando la persona afectada solicite el ejercicio de derechos frente a la entidad adjudicataria, esta deberá comunicar dicha solicitud a la APV en el plazo máximo de 5 días laborables.

La empresa adjudicataria estará obligada a facilitar, en caso de que se le encargue la recogida de los datos personales, la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe consensuar con la Organización antes del inicio de la recogida de los datos.

En caso de que se produzcan violaciones de seguridad, la entidad adjudicataria deberá notificarlas a la APV, sin dilaciones indebidas y, en cualquier caso, antes del plazo máximo de 24 horas, junto con toda la información relevante para la documentación y la comunicación de la incidencia.

La entidad adjudicataria deberá ayudar a la APV a garantizar el cumplimiento de las obligaciones concernientes a la seguridad de los datos personales y la realización de las evaluaciones de impacto relativas a la protección de datos personales y consulta previa, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado del tratamiento, además de poner a disposición de la APV sus instalaciones y toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones a realizar por la APV u otro auditor autorizado por este.

La entidad adjudicataria cumplirá con la obligación, en caso de ser aplicable, de designar un Delegado de Protección de Datos y comunicará su identidad y los datos de contacto a la APV.
Una vez finalizada la vigencia del contrato formalizado entre las partes, la entidad adjudicataria dará cumplimiento a lo que dispone el artículo 28.3.g) del RGPD. A tal efecto, la entidad procederá de forma inmediata a destruir o devolver, según lo pactado con la APV, los soportes en los cuales consten los datos personales obtenidos como consecuencia de la prestación del servicio, sin conservarse ninguna copia. Este extremo no será de aplicación únicamente en caso de que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados Miembros.

14.1 Acceso a los sistemas de la Autoridad Portuaria de Vigo.

En caso de que el personal del adjudicatario necesite conectarse a los sistemas de información de la APV, ya sea local o remotamente, el adjudicatario deberá identificar a todos y cada uno de sus empleados que vayan a realizar el mencionado tipo de actividades, con el fin de asignarles a cada uno de ellos credenciales de acceso personalizadas.

El adjudicatario se obliga a transmitir al personal mencionado anteriormente la necesidad de custodiar diligentemente sus credenciales, evitando compartirlas o revelarlas. En caso de que las credenciales sean reveladas, el adjudicatario deberá comunicar tal circunstancia de forma inmediata a la APV para que sean revocadas.

En caso de que algún empleado con acceso a los sistemas de la Autoridad Portuaria de Vigo causara baja, el adjudicatario deberá poner en conocimiento de la APV tal circunstancia de forma inmediata.

Cualquier cambio que el adjudicatario vaya a realizar en sus procesos, sus infraestructuras y, en general, en su entorno, y que pudiera afectar directa o indirectamente a la APV o al objeto del contrato, debe ser previamente comunicado y consensuado con los responsables de esta.

14.2 Incidentes de seguridad de la información.

El adjudicatario deberá comunicar de inmediato a la APV cualquier incidente de seguridad de la información que hubiera afectado al entorno de los sistemas que gestione (malware, fugas de información, etc.) que pudiera afectar, a su vez, a la APV, ya sea a través de los propios equipos, de correos electrónicos, pendrives, equipos portátiles, el propio personal o por cualquier otro medio.

14.3 Derecho de auditoría.

El adjudicatario deberá admitir, y facilitará a la APV, la realización de auditorías que permitan comprobar que este cumple con los requisitos de seguridad establecidos en el marco del contrato.

14.4 Clausula adicional para caso de subcontratación.

En caso de que se subcontrate alguno de los servicios incluidos en el presente proyecto, el adjudicatario deberá transmitir a los posibles subcontratistas todos los requisitos establecidos en los pliegos de condiciones administrativas y técnicas, y muy especialmente, aquellos requisitos relacionados con la disponibilidad, integridad y confidencialidad de la información y de los servicios de la APV.

14.5 Contratos de servicios críticos en disponibilidad o que afecten a servicios críticos en disponibilidad de la Autoridad Portuaria de Vigo. Cláusula adicional de disponibilidad.

El adjudicatario deberá disponer de la suficiente redundancia en sus infraestructuras como para ofrecer un servicio con garantías de disponibilidad a la APV.

El adjudicatario deberá disponer de un plan de continuidad de su negocio o un plan de recuperación de desastres que afecten a sus infraestructuras relacionadas con el objeto del contrato. Estos planes estarán a disposición de la APV para ser revisados en caso de que se estimara oportuno por su parte.

14.6 Control del Software de Producción.

Asegurar la seguridad del software, una vez que ha sido puesto en producción en la Autoridad Portuaria de Vigo (APV), en el marco del Esquema Nacional de Seguridad (ENS).

La actualización de software (aplicaciones, parches, librería, etc.) en los sistemas en Producción debe ser realizada por administradores experimentados y mediante el *Procedimiento de Gestión de Cambios y Versiones.*

En el entorno de Producción solo se permitirá código ejecutable aprobado por el Responsable del Sistema o Responsable de la Aplicación. No estará permitida la instalación de herramientas de desarrollo o código fuente en dicho entorno.

El código fuente debe haber sido probado previamente en un entorno diferente al de Producción.

Después de realizar cambios y actualizaciones en el sistema, incluidos los de Sistema Operativo, se probarán todas las aplicaciones críticas de éste para comprobar que dichos cambios no afectan a su correcto funcionamiento. Se actualizarán, además, los planes de continuidad que se vean afectados por dichos cambios.

Se llevará un control de las configuraciones y documentación del sistema.

Se tendrá un registro de todas las actualizaciones cambios y pasos a producción realizados en los sistemas. Estos se realizarán teniendo preparado previamente un procedimiento de *marcha atrás*. Las versiones antiguas de software se almacenarán para poder ser utilizadas en caso de fallos en las nuevas.

Los parches de seguridad se aplicarán cuando se reduzca o elimine una vulnerabilidad de la versión de software existente. En sistemas críticos no se llevarán a cabo actualizaciones automáticas de parches.
El acceso a los servidores en Producción por parte de los proveedores o fabricantes estará solo permitido cuando sea estrictamente necesario para su administración o mantenimiento. Este hecho deberá ser aprobado por el Responsable del Sistema, y monitorizado.

14.7 Datos de Prueba y código fuente.

Se establecerán las medidas necesarias para proteger el acceso y controlar los datos usados para las pruebas del sistema/aplicaciones, así como el código fuente de los programas desarrollados.
La copia de los datos para hacer pruebas debe ser autorizada por el responsable de la Información. Cuando se trate de información *CONFIDENCIAL* se deberán haber implantado las mismas medidas de seguridad existentes en producción. Estos datos deben ser borrados inmediatamente después de terminar las pruebas.
Se recomienda el uso de un repositorio central o herramientas destinadas a esta tarea, para almacenar, actualizar y controlar las distintas versiones de código fuente. Este debe ser protegido contra accesos no autorizados. Este repositorio NO deberá estar en servidores de Producción. El acceso y actualización de las versiones de código fuente deberá quedar registrado.

14.8 Metodología del desarrollo software.

En este apartado deberá cumplirse con toda la normativa recogida en el ENS, para garantizar la fiabilidad y seguridad de las aplicaciones y sistemas sobre los que se realizan los desarrollos, las pruebas y la puesta en producción de estos, garantizándose la metodología que impida la construcción de herramientas informáticas que posibiliten la vulneración de las aplicaciones y sistemas a través de código mal construido.

15 DOCUMENTACIÓN A PRESENTAR.

En la oferta técnica debe presentarse toda la documentación solicitada en este pliego ajustándose a los requisitos y formatos establecidos, a excepción de la solicitada en el capítulo 9 **“Solvencia técnica y Profesional” que deberá incluirse en el sobre A de las ofertas.**

- Punto 19.1 apartado 19.1.1 “Memoria Técnica”: donde deberá aportarse la documentación necesaria para una correcta comprensión y valoración de los servicios ofertados, según se especifica en cada apartado de ese punto.

- Punto 19.1 apartado 19.1.2 “Otros criterios evaluables mediante fórmula”: donde se deben aportar evidencias de cumplir los requisitos solicitados para la obtención de la puntuación de este apartado.

16 DURACIÓN DEL CONTRATO.

El periodo de prestación del servicio se desglosará de la siguiente manera:

- Cuatro meses (4) para el suministro, instalación, configuración y puesta en marcha a pleno rendimiento de los sistemas y trabajos ofertados para su consecución.

- Doce meses (12), a contar desde el momento de entrada en producción (Acta de recepción) una vez completada la fase anterior, para la prestación del servicio de seguimiento operativo de los sistemas implantados según la oferta presentada.

17 PRESUPUESTO DE LICITACIÓN.

17.1 Presupuesto Base.

El presupuesto para la realización de los servicios correspondientes a la "CONTRATACIÓN SUMINISTRO, INSTALACIÓN Y SEGUIMIENTO OPERATIVO DE SISTEMAS DE CIBERSEGURIDAD PERIMETRAL PARA LA AUTORIDAD PORTUARIA DE VIGO", según se puede apreciar en el siguiente cuadro, se ha calculado **para un periodo de dieciséis (16) meses, según desglose expresado anteriormente**, a partir de la fecha de la firma, resultando un importe estimado de DOSCIENTOS CINCUENTA MIL EUROS(**250.000,00** Eur.), iva no incluido.
En la siguiente tabla figura un resumén orientativo de presupuesto por partidas.
I
I
I
I
I

Resumen presupuesto base por servicios (Exp. 3156/2022)	
Descripción	**IMPORTE**
Servicios de Implantación	165,000.00
Servicios de Seguimiento Operativo	45,000.00
Servicios de Incidencias Ciberseguridad y Técnicas.	40,000.00
TOTAL	**250,000.00**

En el sobre de la oferta económica deberá reflejarse **el importe total por la prestación completa de los suministros y servicios a prestar sin incluir el IVA**, este importe será el que se utilizará para el cálculo de la puntuación económica. Importe máximo 250.000 Euros.

17.2 Valor Total Estimado del Contrato.

El valor total estimado del contrato se calcula teniendo en cuenta las posibles prorrogas y un adicional del 20% anual en la partida del segundo concepto, para cubrir las posibles nuevas necesidades o modificaciones previstas, según se recoge en el artículo 204 de la Ley 9/2017

Las posibles modificaciones se enmarcan en las siguientes circunstancias:

- Posibles desviaciones surgidas en el coste de los sistemas a suministrar debido a la volatilidad del mercado producida por la falta de componentes y la situación bélica en Ucrania.

- Posibles desviaciones por aumento de incidentes de ciberseguridad sobre los estipulados como posibles en este pliego (2).

El Órgano de Contratación resolverá el procedimiento de modificación de acuerdo con lo establecido en los artículos 191 y 203 de la LCSP.

En todo caso, las modificaciones se formalizarán conforme a lo dispuesto en el artículo 153 LCSP y se publicarán de conformidad con los artículos 63 y 207 de dicha Ley.

El valor total estimado del contrato teniendo en cuenta el posible 20% al aplicar (art. 204 ley 9/2017) asciende a TRESCIENTOS MIL EUROS (300.000,00) Euros.

En el siguiente cuadro se puede observar el desglose por conceptos de dicha estimación total:

Detalle Estimación Económica total licitación (20% art, 204 LCSP incluido) (Exp. 3156/2022)			
Descripción	**IMPORTE**	**20% Art. 204 Ley 9/2017**	**TOTAL**
Servicios de Implantación	165,000.00	33,000.00	198,000.00
Servicios de Seguimiento Operativo	45,000.00	0.00	45,000.00
Servicios de Incidencias Ciberseguridad y Técnicas.	40,000.00	8,000.00	48,000.00
TOTAL	**250,000.00**	**50,000.00**	**300,000.00**

El resumen económico total estimado de la licitación por todos los conceptos se refleja en el siguiente cuadro:
I
I
I

RESUMEN VALOR ESTIMADO TOTAL DEL CONTRATO (Exp. 3156/2022)	
CONCEPTO	**IMPORTE**
Presupuesto base de licitación (IVA excluido)	**250,000.00**
Importe de las modificaciones previstas 20% art. 204 lcsp(IVA excluido)	**50,000.00**
Importe de opciones eventuales (IVA excluido)	0.00
Importe de las primas pagaderas a los licitadores (IVA excluido)	0.00
Prorrogas (IVA excluido)	0.00
TOTAL	**300,000.00**

18 OMISIONES.

Las omisiones o errores de los detalles que sean indispensables para llevar a cabo el espíritu e intención expuestos en estas especificaciones, o que, por uso y costumbre deban ser realizados, no sólo no exime al contratista de la obligación de ejecutar estos detalles erróneamente omitidos o descritos, en su caso, sino que, por el contrario, deberán ser ejecutados como si hubieran sido completos y correctamente especificados en este documento.

19 CRITERIOS DE VALORACIÓN, OBTENCIÓN DE PUNTUACIONES.

De acuerdo con la Ley 9/2017 de 8 de noviembre de contratos del sector público, la valoración de las ofertas para determinar la oferta más ventajosa responderá a la utilización de una pluralidad de criterios en base a la mejor relación calidad-precio.

La modalidad de adjudicación que se propone para los trabajos a desarrollar es mediante “procedimiento abierto”.

Como se ha hecho constar en el capítulo 7 “Requisitos de Solvencia Técnica y Profesional”, para un correcto desempeño del objetivo de este concurso y garantizar el perfecto cumplimiento normativo y funcional de los servicios a prestar, **será obligatoria la presentación, en el sobre A de la oferta, de la documentación requerida en dicho capítulo, quedando descartadas todas las ofertas que no cumplan todas y cada uno de los requisitos solicitadas**. Las ofertas que resulten aceptadas técnicamente se valorarán según los criterios relacionados a continuación.

La puntuación global de las ofertas (PG) responderá a la siguiente fórmula:

$$PG = \left(\frac{X}{100}\right) \cdot PT + \left(\frac{Y}{100}\right) \cdot PF$$

Donde:

- X = Ponderación de criterios de carácter cualitativo (X=50)
- Y = Ponderación de criterios de carácter cuantitativo (Y=50)
- PT = Puntuación técnica (puntuación de los criterios cualitativos)
- PF =Puntuación total correspondientes a los criterios de carácter cuantitativo.

19.1 Criterios de Valoración de Carácter Cualitativo (PT)

Los criterios de adjudicación de carácter cualitativo que servirán para la valoración de la calidad técnica se puntuarán sobre un total de 100 puntos.

Las valoraciones se realizarán atendiendo a la claridad y ordenación expositiva, alcance de las propuestas, detalle de los trabajos técnicos y servicios a realizar y todo aquello que permita poder valorar de una manera clara y objetiva la idoneidad de la oferta presentada.

Dentro de los distintos planes de actuación aquí solicitados para la valoración de las ofertas, se valorarán positivamente aquellos que ofrezcan servicios de valor añadido que enriquezcan la solución ofertada más allá de los mínimos requeridos en este pliego, para su correcta estimación estos servicios deben de relacionarse en un apartado dentro de cada plan.

Las puntuaciones por valoración de carácter cualitativo se repartirán de la siguiente manera:

19.1.1 Memoria Técnica (A- Hasta 70 puntos).

a) Plan detallado de implantación de la solución, incluyendo sistemas ofertados, gráficos o esquemas de la infraestructura propuesta, plan de migración de configuraciones de la infraestructura actual, interacción y dependencias entre los sistemas propuestos y los sistemas y la infraestructura de red de la APV. **(Hasta 25 puntos).** Max. 15 Pag.

b) Plan detallado de contingencia ante incidentes de ciberseguridad, gestión de la incidencia, detalle de roles y funciones. **(Hasta 25 puntos),** Max. 10 pag.

c) Plan detallado de prestación del servicio de seguimiento operativo, acciones proactivas, preventivas y evolutivas, así como una descripción a alto nivel de la auditoria a realizar durante el periodo de doce meses. **(Hasta 10 puntos),** Max. 10 pag.

d) Plan detallado de Gestión de Incidencias Técnicas (mantenimiento correctivo) y Herramienta Informática para la gestión de los apartados b, c y d. **(Hasta 10 puntos).** Max. 10 Pag.

19.1.2 Otros Criterios Evaluables mediante formula, (B – Hasta 30 Puntos).

a) Otras Certificaciones.

- Miembro del FIRST organization: 10 Puntos.

b) Asistencia in situ.

- Mas de 3 horas: 0 Puntos.
- Entre 2,5 y 3 horas: 1 Puntos.
- Entre 2 y 2,5 horas: 4 puntos.
- Entre 0 y 2 horas: 8 Puntos.

c) Certificaciones dentro del equipo de trabajo (CISA, CISM, CISSP, GSEC o CEH):

- 1 punto por cada recurso asignado y certificación, hasta un máximo de 12 Puntos.

19.1.3 Obtención Puntuación Técnica total y ofertas no contemplables.

Una vez evaluados los criterios anteriores, cada licitante obtendrá su valoración técnica.

La puntuación técnica (Pt)= A+B

Se declararán ofertas no contemplables aquellas cuya puntuación técnica (Pt) no sea superior a 60 puntos. Estas ofertas quedarán excluidas de la fase de valoración.

19.1.4 Presentación de la Documentación.

La documentación incluida en la memoria técnica de las ofertas (19.1.1) evitará la transcripción literal del Pliego. No se tendrán en cuenta aquellas propuestas que en su exposición contengan, en un porcentaje elevado como parte de la oferta, transcripciones literales o muy aproximadas de textos que forman parte de prestaciones o requisitos solicitados en este pliego.

En el número de páginas máximo no se computarán portadas, subportadas, separadores ni páginas de índices, así como aquellos certificados, currículum vitae, etc que el ofertante crea pertinente aportar que se incorporarán como anejos. La inclusión de una oferta que supere el número máximo de páginas por epígrafe dará lugar a que sólo se evalúe lo desarrollado hasta el máximo permitido en cada epígrafe.

Los formatos en los que se presentará la documentación serán los siguientes (formato A4 orientación vertical).

FUENTE DE PÁRRAFOS: Arial tamaño 11.
FUENTE DE TÍTULOS**: Arial tamaño 12 negrita**.
MARGEN SUPERIOR/INFERIOR/IZQUIERDO/DERECHO: 3cm/3cm/2,5cm/2,5cm.
INTERLINEADO: sencillo, con separación posterior entre párrafos 12.

19.2 Criterios de Valoración de Carácter Cuantitativo (PF).

La puntuación total (PF) correspondiente a criterios evaluables mediante fórmulas (criterios de carácter cuantitativo) relativa a una oferta cualquiera se basará única y exclusivamente en el valor económico de esta.

PF = PE

Las fórmulas detalladas para el cálculo de la valoración de carácter cuantitativo, así como las indicadas para el cálculo de ofertas incursas en presunción de anormalidad por su bajo importe figuran en el pliego administrativo de esta licitación.

20. CONCLUSIONES.

Con todo lo expuesto anteriormente, se considera suficientemente justificado el presente Pliwego de Prescripciones Técnicas Particulares.

En Vigo, a 22 de Septiembre de 2022

Firmado Digitalmente:
El Jefe del Departamento de Tecnologías. David Silveira Vila.