PLIEGO DE PRESCRIPCIONES TÉCNICAS

PARA LA CONTRATACIÓN DE

“Servicio de CDN con control de ataques distribuidos y filtro de seguridad para las webs corporativas de la Autoridad Portuaria de Baleares”

Expediente INV25-0114

Índice

1 Antecedentes y justificación 3
2 Objeto del contrato 3
3 Legislación y normas que regirán los trabajos a realizar 3
4 Descripción de las tareas objeto del contrato 5
4.1 Gestión del proyecto 5
5 Requisitos técnicos 5
5.1 Infraestructura 6
5.2 Seguridad web (WAF) 6
5.3 Gestión de certificados 7
5.4 Visibilidad y control 8
5.5 Mitigación DDoS 8
5.6 Características avanzadas 8
6 Presupuesto máximo licitación 9
7 Requisitos mínimos empresa 10
8 Seguridad de la Información 10
8.1 Acceso a los sistemas de la APB 10
8.2 Cambios de la empresa 11
8.3 Incidentes de seguridad de la información 11
8.4 Confidencialidad de la información 12
8.5 Derecho de auditoría 12
8.6 Requisitos de seguridad en caso de subcontratación 12
8.7 Servicios críticos en disponibilidad o que afecten a servicios críticos en disponibilidad de la APB 13
8.8 Conformidad de sistemas, productos y equipos 13
9 Informes sobre el desarrollo de los trabajos 13
10 Defectos o deficiencias de los trabajos 13
11 Contradicciones y omisiones del presente documento 14
12 Consideración final 14

1 Antecedentes y justificación

Este proyecto surge de la necesidad de fortalecer la postura de seguridad de la organización en su infraestructura web ante un panorama de amenazas digitales en constante evolución, en el que recientes ataques a autoridades portuarias por parte de actores malintencionados evidencian el creciente riesgo al que se enfrentan estos entornos. Como parte de su compromiso con la ciberseguridad, la Autoridad Portuaria de Baleares, en adelante la APB, reconoce la importancia de dotarse de soluciones avanzadas que permitan proteger sus servicios esenciales, y en especial, sus portales web, así como garantizar la disponibilidad de sus plataformas y preservar la confidencialidad, trazabilidad, autenticidad e integridad de la información que gestiona.

2 Objeto del contrato

El objetivo de este pliego es establecer los requisitos técnicos necesarios para seleccionar una solución CDN (*Content Delivery Network*, Red de distribución de contenido) que proteja las aplicaciones web de la APB contra ataques externos -incluidos DDoS, intentos de intrusión, explotación de vulnerabilidades y filtrado mediante WAF- a la vez que permita una gestión centralizada y escalable de la seguridad en el perímetro de exposición.

Esta iniciativa se enmarca en la estrategia de transformación digital y resiliencia operativa de la APB, y tiene por objetivo garantizar que su infraestructura tecnológica esté preparada para afrontar los desafíos presentes y futuros en el entorno digital.

3 Legislación y normas que regirán los trabajos a realizar

El desarrollo de los trabajos solicitados en el presente expediente se realizará al amparo de la siguiente normativa, que se entiende de obligado cumplimiento:

- **Interoperabilidad**
  - Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica.
  - Normas Técnicas de Interoperabilidad derivadas del Esquema Nacional de Interoperabilidad.
- **Identificación y firma electrónica**
  - Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
  - Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- **Seguridad y protección de datos**
  - Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de

ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS2).

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.
- Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013 (Reglamento sobre la Ciberseguridad).
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección 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 (Reglamento general de protección de datos).
- Instrucciones Técnicas de Seguridad y las Guías de Seguridad derivadas del Esquema Nacional de Seguridad.
- Directiva NIS2 (Network and Information Security).

- **Accesibilidad**

  - Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público.
  - Directiva (UE) 2016/2102, de 26 de octubre de 2016, sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público
  - Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.

- Cualquier otra normativa, que se publique o desarrolle durante la duración del contrato, y sea de obligado cumplimiento a las Administraciones Públicas, y en particular, a la APB.

Asimismo, quedará incluida en el ámbito del proyecto cualquier adaptación -sea desarrollo o cualquier otro tipo de trabajo- a la legislación que pudiera surgir durante el desarrollo del proyecto y el posterior periodo de garantía.

También se tendrá en cuenta para realizar los trabajos la adecuación a las certificaciones del Esquema Nacional de Seguridad, ISO-9001, ISO-14001 e ISO-33000 que posee la APB.

4 Descripción de las tareas objeto del contrato

Con carácter enunciativo y no exhaustivo, se relacionan las tareas que comprende el objeto del contrato.

4.1 Gestión del proyecto

El presente proyecto tiene como objetivo la **implementación de una solución de seguridad basada en la nube** para proteger las infraestructuras web de la APB frente al creciente volumen y sofisticación de las amenazas digitales.

La solución deberá cumplir los siguientes requisitos fundamentales:

- **Arquitectura distribuida globalmente**: La plataforma deberá estar desplegada sobre una red perimetral con presencia global, que permita mitigar ataques lo más cerca posible de su origen, reduciendo la latencia y mejorando la resiliencia del servicio.

- **Escalabilidad automática y sin intervención manual**: La solución debe ser capaz de absorber picos de tráfico o ataques volumétricos sin necesidad de dimensionamiento previo ni configuraciones específicas por parte del equipo técnico de la APB.

- **Despliegue sin interrupciones**: Se requiere una integración transparente con la infraestructura existente (dominios web, servidores de aplicaciones, DNS, etc.), sin necesidad de cambios disruptivos en la arquitectura o afectaciones al servicio.

- **Políticas de seguridad personalizables y centralizadas**: La plataforma deberá permitir la gestión granular de reglas de seguridad, adaptadas a los activos tecnológicos expuestos de la APB, todo ello desde una consola unificada.

- **Protección integral en capa 3 a capa 7**: Se valorará especialmente que la solución incluya funcionalidades de mitigación DDoS, firewall de aplicaciones web (WAF), control de bots, aislamiento de navegador, gestión de identidades y acceso seguro para usuarios y dispositivos.

Debe ser una solución comprobada y desplegada en entornos críticos del sector público, que acredite **alta disponibilidad**, soporte 24/7 y capacidades avanzadas de **monitorización y trazabilidad de los eventos de seguridad**.

5 Requisitos técnicos

Con objeto de dotar a la APB de una protección eficaz y escalable en su infraestructura tecnológica, se establecen a continuación las **características técnicas mínimas** que deberá cumplir la solución. Estas especificaciones constituyen el umbral básico de cumplimiento y servirán como referencia para la evaluación de las propuestas.

A modo de referencia, los servicios mínimos a cubrir incluyen: un volumen de **transferencia CDN** de 6 TB al mes, la gestión de **50 millones de peticiones mensuales en CDN**, **protección avanzada contra DDoS** sin límite de tráfico, la aplicación de **reglas de limitación de peticiones (Rate Limiting)** para hasta 10 millones de solicitudes mensuales, funcionalidades de **firewall de aplicaciones web (WAF)** sin límite de tráfico y la inclusión de un servicio estándar de soporte. Todo ello dando cobertura hasta **cuatro dominios principales de la APB.**

A continuación, se desglosan los distintos ámbitos sobre los que deberá aplicarse la solución propuesta, abarcando la infraestructura, la seguridad web, la gestión de certificados, la visibilidad y el control, la mitigación de ataques DDoS y las funcionalidades avanzadas.

5.1 Infraestructura

Con el fin de garantizar un servicio robusto y adaptado a las necesidades operativas de la APB, se establecen a continuación los requisitos técnicos mínimos que deberá cumplir la solución presentada en cuanto a su infraestructura. Estos requisitos constituyen el umbral básico exigible para asegurar la disponibilidad y el rendimiento de las aplicaciones web de la APB:

- El proveedor debe contar con presencia operativa de red en más de dos ciudades dentro del Estado español, así como disponer de infraestructura en Europa. Asimismo, debe garantizar baja latencia y la alineación con los marcos y certificaciones exigibles.

- La solución debe incluir, de forma nativa y en una única plataforma, los siguientes servicios: DNS, CDN, WAF, mitigación DDoS y Rate limiting, con el objetivo de centralizar la gestión, reducir la complejidad operativa y optimizar el rendimiento.

- La solución debe poder desplegar cualquier cambio de configuración en un tiempo inferior a 5 segundos.

- La solución no debe imponer limitaciones en cuanto a volumen de tráfico procesado, ya sea en número de peticiones por segundo o ancho de banda (Mbps).

- La plataforma debe ofrecer autenticación multifactor (MFA) para el acceso administrativo y gestión de la solución.

5.2 Seguridad web (WAF)

A continuación, se establecen las características técnicas mínimas en materia de seguridad web (WAF), que deberán cumplir la solución para garantizar la protección integral de las aplicaciones y servicios esenciales de la APB.

- Visibilidad de seguridad completa

- Capas de protección contra ataques OWASP y exploits emergentes, así como disponibilidad de conjuntos adicionales de reglas de seguridad gestionadas.

- Evaluación en tiempo real del riesgo de los ataques para mitigar **amenazas desconocidas** (ataques 0day).

- Capacidad de **inspección de tráfico HTTPS cifrado**, sin comprometer la privacidad ni el rendimiento.

- Posibilidad de **definir y aplicar reglas personalizadas de seguridad** por aplicación, subdominio o servicio.

- La solución debe utilizar tecnologías de **machine learning e inteligencia artificial para clasificar las solicitudes HTTP en tiempo real** según su riesgo potencial.

- La plataforma debe incluir **protección nativa frente a tráfico automatizado y bots maliciosos**, con mecanismos de fácil despliegue y sin necesidad de agentes.

- La solución debe incluir un **Rate limiting para limitación de cantidad de peticiones** que puede hacer un usuario, sistema o IP en periodo determinado de tiempo.

- La solución debe contemplar una **edición o propagación de cambios de reglas WAF** en menos de 10 segundos.

- Funcionalidades específicas para **protección de APIs** con validación de esquemas, tokens y autenticación reforzada.

- Identificación de **credenciales comprometidas** de la APB para prevenir tomas de control de cuentas.

5.3 Gestión de certificados

En materia de gestión de certificados, se establecen los requisitos técnicos mínimos en gestión de certificados que deberán cumplir la solución, garantizando tanto la operatividad como la preparación frente a nuevos escenarios tecnológicos y de ciberseguridad.

- Posibilidad de **emitir y renovar manualmente al menos 200 certificados por dominio**, con hasta **50 SAN por certificado**.

- Capacidad de **emitir y renovar automáticamente certificados SSL/TLS** para todos los subdominios protegidos, sin limitación.

- Soporte para **algoritmos criptográficos resistentes a computación cuántica** (post-quantum encryption) en el intercambio de claves.

5.4 Visibilidad y control

En el ámbito de visibilidad y control, se establecen las **características técnicas mínimas** que deberán cumplir las soluciones ofertadas, con el objetivo de asegurar una supervisión continua, trazabilidad completa y capacidad de respuesta inmediata ante incidentes de seguridad o de rendimiento.

- Disponibilidad de un **panel de control en tiempo real**, con métricas claras sobre tráfico, ataques y rendimiento.
- Acceso a **paneles analíticos avanzados**, con filtros por hostname, dirección IP, código de estado, URL, etc., y con capacidad de análisis por rangos temporales específicos.
- Los paneles deben actualizarse en **tiempo real** sin necesidad de recarga manual.
- La plataforma debe ser integrable con **soluciones SIEM** ya en uso por la APB.
- Soporte para **alertas configurables** por correo electrónico o webhook ante eventos de seguridad o indisponibilidad del servicio.
- Exportación de logs en tiempo real mediante **Syslog, API o conectores SIEM**.
- Capacidad de generar y enviar **reportes automáticos periódicos** con métricas clave de seguridad y cumplimiento.

5.5 Mitigación DDoS

Se definen a continuación los **requisitos técnicos mínimos en materia de mitigación DDoS**, de obligado cumplimiento para las soluciones ofertadas, con el fin de asegurar la detección y neutralización automática de ataques, preservando la disponibilidad y resiliencia de las plataformas digitales de la APB.

- Protección a nivel de **red (capas L3 y L4)** contra ataques volumétricos y de protocolo.
- Protección a nivel de **aplicación (capa L7)** contra ataques dirigidos a vulnerabilidades web o recursos lógicos.
- Capacidad de **detección y mitigación automática** de ataques sin necesidad de intervención manual, con respuestas en segundos.

5.6 Características avanzadas

En lo relativo a funcionalidades avanzadas, se establecen las **características técnicas mínimas** que deberán cumplir la solución, con el fin de garantizar la incorporación de capacidades de

última generación en materia de rendimiento, automatización y protección frente a amenazas emergentes.

- Integración con redes de entrega de contenido (CDN) de gran capacidad con tecnología **Anycast**, presente a nivel global.
- Los puntos de presencia deben proporcionar todos los servicios ofrecidos.
- Uso de **reglas gestionadas actualizadas automáticamente** basadas en inteligencia global sobre amenazas.
- Soporte para ejecución de lógica personalizada mediante tecnologías **serverless**, como funciones para gestión de tráfico, control de bots o limitación de tasas (**rate limiting**).
- Soluciones avanzadas de control de bots con mecanismos de **detección, desafío y verificación sin fricción** para el usuario legítimo.

6 Presupuesto máximo licitación

El presupuesto de licitación se desglosa en el siguiente cuadro:

Presupuesto			
Partida	**Cantidad**	**Importe**	**Total**
1. Servicios profesionales de implantación (única)	1	4.700,00 €	4.700,00 €
2. Servicio de CDN, Incluye: WAF, Anti ddos, CDN, Rate limiting, logpush y soporte (1 año)	3	44.600,00 €	133.800,00 €

PRESUPUESTO BASE DE LICITACIÓN (IVA excluido) (3 AÑOS)	**138.500,00 €**
IVA (21%)	29.085,00 €
PRESUPUESTO BASE DE LICITACIÓN CON IVA (3 AÑOS)	**167.585,00 €**

El **Presupuesto Base de Licitación** excluido IVA es de CIENTO TREINTA Y OCHO MIL QUINIENTOS EUROS (138.500,00 €), resultando el IVA (21%) VEINTINUEVE MIL OCHENTA Y CINCO EUROS (29.085,00 €) y el **Presupuesto Base de Licitación con IVA incluido** asciende a CIENTO SESENTA Y SIETE MIL QUINIENTOS OCHENTA Y CINCO EUROS (167.585,00 €).

A efectos de justificación de precios, en el anexo correspondiente (*Anexo III. Justificación de precios*), se tiene en cuenta los artículos 100 y 102 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.

Están incluidos en los precios anteriores todos los costes derivados de la ejecución material de los servicios, los gastos generales de estructura y el beneficio industrial, además dichos precios incluyen todos los costes laborales, ajustándose al Convenio Colectivo vigente. También está incluido en el coste de cada servicio el coste de elaboración de los entregables correspondientes solicitados en esta licitación.

Los gastos de desplazamientos y dietas y otros costes complementarios por los distintos viajes y servicios que deberá realizar el personal de la empresa adjudicataria para la ejecución de los trabajos, así como cualquier otro gasto para el desarrollo de los mismos, están incluidos en los costes indicados de los servicios.

7 Requisitos mínimos empresa

La Empresa Licitadora deberá estar en condiciones de poder evidenciar la conformidad con el ENS (Esquema Nacional de Seguridad) de los sistemas de información en los que se sustenten los servicios de consultoría, instalación y soporte de software de ciberseguridad. Para ello, deberá presentar el Certificado de Conformidad con el **ENS en categoría (como mínimo) MEDIA.**

La empresa proveedora deberá mantener la conformidad vigente durante todo el ciclo de vida del contrato. Esta exigencia se extenderá también a la cadena de suministro de dichos contratistas (en especial, a los subcontratistas), en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos. La pérdida o retirada temporal de la conformidad debe ser comunicada de manera inmediata y sin dilación indebida a la entidad contratante, quien deberá considerar el impacto en contrato, de tal condición. La renovación de la conformidad durante la vigencia del contrato se notificará inmediatamente, incluyéndose el proceso de la adaptación del sistema de información al Real Decreto 311/2022

La empresa Licitadora deberá disponer de un Sistema de Gestión Ambiental basado en la norma **ISO 14001 o EMAS** o certificación/documento que avale que aplica criterios similares de gestión ambiental (medidas, métodos, controles, reglas, etc.).

8 Seguridad de la Información

8.1 Acceso a los sistemas de la APB

La APB pondrá a disposición del adjudicatario los medios necesarios para realizar la conexión de uno o varios equipos informáticos a su red, con el fin de cumplir con lo especificado en este pliego. Será a criterio de la APB, previa consulta con el adjudicatario, la definición última de las características y capacidad de la conexión, que podrá ser mediante acceso remoto seguro y/o poniendo a disposición en la sede del adjudicatario un punto de red para la interconexión. El adjudicatario podrá disponer, si así lo decide, de un cortafuegos en este punto, en cuyo caso será necesaria la adaptación y coordinación con la infraestructura y técnicos de la APB. En todo caso será necesario definir y restringir los accesos desde los dispositivos del adjudicatario a la red de la APB para su implementación en los cortafuegos corporativos.

La empresa adjudicataria deberá identificar a todos y cada uno de sus empleados que necesite conectarse a los sistemas de información de la APB que vayan a realizar el mencionado tipo de actividades, con el fin de asignarle a cada uno de ellos credenciales de acceso personalizadas.

La empresa adjudicataria 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, la empresa adjudicataria deberá comunicar tal circunstancia de forma inmediata a la APB para que sean revocadas.

En caso de que algún empleado con acceso a los sistemas de la APB causara baja, la empresa adjudicataria deberá poner en conocimiento de la APB tal circunstancia de forma inmediata.

8.2 Cambios de la empresa

Cualquier cambio que la empresa adjudicataria vaya a realizar en sus procesos, sus infraestructuras y, en general, en su entorno, y que pudiera afectar directa o indirectamente a la APB o al objeto del contrato, debe ser previamente comunicado y consensuado con la misma.

8.3 Incidentes de seguridad de la información

La empresa adjudicataria, se compromete a implementar y mantener un sistema robusto y efectivo de gestión de incidentes de seguridad para los servicios proporcionados a la APB, de acuerdo con los principios y requisitos establecidos por el ENS.

- Notificación de incidentes: La empresa adjudicataria notificará a la APB de manera inmediata y sin demora injustificada después de haber tomado conocimiento de cualquier incidente de seguridad que pueda afectar a los servicios objeto de este contrato.
- Investigación y corrección: La empresa adjudicataria se compromete a investigar de manera inmediata todos los incidentes de seguridad, a tomar las medidas correctivas necesarias para resolver el incidente y a mitigar su impacto. Además, cooperará con la APB en todas las etapas de la investigación y corrección.
- Reportes de incidentes: La empresa adjudicataria proporcionará a la APB informes regulares sobre la naturaleza y el estado de cualquier incidente de seguridad, incluyendo los detalles de las medidas correctivas tomadas y las recomendaciones para evitar incidentes similares en el futuro.
- Cooperación con las autoridades: Si el incidente de seguridad implica una violación de la ley, la empresa adjudicataria cooperará con las autoridades competentes y asistirá a la APB en el cumplimiento de sus obligaciones legales relacionadas con el incidente de seguridad.
- Auditorías y pruebas: La empresa adjudicataria permitirá y colaborará con las auditorías de seguridad y las pruebas de penetración que la APB pueda realizar o encargar, con el fin de evaluar la efectividad de las medidas de seguridad del Proveedor y su cumplimiento con esta cláusula y con el ENS.

En definitiva, el objetivo asegurar que cualquier incidente de seguridad en los servicios proporcionados a la APB se gestione de una manera que minimice los daños, preserve la confidencialidad, la integridad y la disponibilidad de la información, y cumpla con las obligaciones legales y reglamentarias.

8.4 Confidencialidad de la información

La APB considera que toda la información y documentación manejada durante el proyecto, del tipo que sea (electrónica, escrita o impresa, visual, verbal…), es estrictamente confidencial, por lo que cualquier vulneración de este principio que se observe será objeto de sanción de acuerdo a los términos establecidos en el apartado correspondiente de este pliego, incluso llegando a ser causa de resolución inmediata del contrato si así se estimara, todo ello sin perjuicio de las responsabilidades penales o de otro tipo a que hubiera lugar.

Toda la información y documentación que se maneje en el ámbito del presente contrato es propiedad de la APB. El adjudicatario se compromete a no difundir ni divulgar esta información, ni hacer uso alguno de ella más allá de las actividades vinculadas al contrato y que hayan sido expresamente autorizadas por escrito por la APB, así como a devolver la documentación que obre en su poder a la finalización del mismo, incluso aquella almacenada en formato electrónico o por cualquier otro medio existente o futuro. Esta obligación ostentará el carácter de indefinida, desde el momento de la adjudicación de los trabajos.

El adjudicatario está obligado a comunicar a la APB la relación del personal de la organización implicado en el servicio, solicitando autorización previa para aquellos que deban hacer uso de esta información, así como informar de cualquier modificación en esta relación que pueda ocurrir durante el desarrollo del servicio.

Además de las anteriores obligaciones, el personal del adjudicatario está obligado a:

- Adaptarse a, y cumplir estrictamente, las normas internas de las APB en cuanto a políticas de seguridad, así como cualquier otra que sea de aplicación durante este proyecto.
- Mantener la información confidencial en estricta reserva y debidamente protegida mientras obre en su poder.
- Divulgar la información confidencial únicamente a las personas autorizadas para su recepción dentro de la organización.
- Instruir al personal que estará encargado de recibir la información confidencial en el correcto uso de la misma y sus responsabilidades adquiridas.

8.5 Derecho de auditoría

La empresa adjudicataria deberá admitir, y facilitará a la APB, la realización de auditorías que permitan comprobar que la empresa adjudicataria cumple con los requisitos de seguridad establecidos en el marco del contrato.

8.6 Requisitos de seguridad en caso de subcontratación

En caso de que se subcontrate alguno de los servicios incluidos en el presente proyecto, la empresa adjudicataria 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 APB.

8.7 Servicios críticos en disponibilidad o que afecten a servicios críticos en disponibilidad de la APB

La empresa adjudicataria deberá disponer de la suficiente redundancia en sus infraestructuras como para ofrecer un servicio con garantías de disponibilidad a la APB.

La empresa adjudicataria 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 APB para ser revisados en caso de que se estimara oportuno por parte de la APB.

8.8 Conformidad de sistemas, productos y equipos

La empresa adjudicataria utilizará sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

9 Informes sobre el desarrollo de los trabajos

La empresa adjudicataria informará al Responsable del Contrato, con una periodicidad mínima mensual y en todo caso cada vez que le sea solicitado, y en la forma que el Responsable del Contrato considere oportuna en cada momento, sobre la marcha general de los trabajos encomendados.

El Responsable del Contrato podrá convocar periódicamente reuniones con la empresa adjudicataria para comprobar la calidad de los trabajos y el cumplimiento del Plan de Trabajos y del Pliego de Prescripciones Técnicas.

10 Defectos o deficiencias de los trabajos

Todos los trabajos desarrollados por el contratista deberán ser aceptados por la APB, antes de considerarse entregados a efectos de responsabilidad del contratista.

En el caso de que el Responsable del Contrato presentara reparos para la aceptación de los trabajos debidamente comunicados a la empresa adjudicataria, y éstos se derivaren de errores, incumplimientos de normas o reglamentos técnicos; o bien errores de cualquier aspecto de los trabajos cuya realización haya incumbido a la empresa adjudicataria, será obligación de ésta subsanar las deficiencias en los términos que se señalen por el Responsable del Contrato, y en los plazos que éste conceda, sin que por ello tenga derecho a compensación económica alguna.

La posibilidad de apreciación de defectos por la APB con responsabilidad del adjudicatario no expira hasta transcurrido el período de garantía del contrato.

11 Contradicciones y omisiones del presente documento

Las omisiones erróneas de los detalles que sean indispensables para llevar a cabo los trabajos descritos según el espíritu e intención expuestos en estas prescripciones técnicas, o que, por uso y costumbre deban ser realizados, no sólo no eximen a la empresa adjudicataria de la obligación de ejecutar estos detalles omitidos o erróneamente descritos, sino que, por el contrario, deberán ser ejecutados como si hubieran sido completos y correctamente especificados en este Documento.

12 Consideración final

Las condiciones del presente Documento prevalecen, en lo que pudiera ocurrir de oposición, sobre cualesquiera otros de carácter técnico o administrativo que pudiera tener establecidos la empresa adjudicataria para la prestación de servicios a personas físicas o jurídicas privadas, siendo en todo caso de aplicación al Contrato cuanto previene la normativa vigente.

El desconocimiento del Contrato o de cualquiera de sus términos, de los documentos anexos que forman parte del mismo, o de las instrucciones, pliegos o normas de toda índole aprobadas por la Administración que puedan ser de aplicación en la ejecución de los servicios objeto del Contrato, no eximirá a la empresa adjudicataria de la obligación de su cumplimiento.

Palma, a fecha de firma del documento

Autor del Documento	Revisado y Conforme
José Miguel Esteve Lledó Responsable de Sistemas	***Javier Segovia Mascaró*** Jefe Departamento Desarrollo Tecnológico e Innovación
Conforme	VºBº
Santiago Alejos Fernández Subdirector	***Antonio Ginard López*** Director