PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA PARA LA IMPLANTACIÓN DE UNA PLATAFORMA DE GESTIÓN Y PROTECCIÓN DEL DATO PARA LA AUTORIDAD PORTUARIA DE TARRAGONA

1. ANTECEDENTES

La Dirección de Sistemas de Información de la Autoridad Portuaria de Tarragona (en adelante APT) está siendo testigo de una profunda transformación en la forma en que se manejan y se utilizan los datos, siendo estos el núcleo de las operaciones y una de las fuentes más valiosas de ventaja competitiva. Sin embargo, a medida que el valor de los datos ha aumentado, también lo ha hecho su vulnerabilidad, planteando desafíos críticos para la seguridad y la gestión de la información.

La explosión de la información, la diversificación de plataformas y sistemas, y la colaboración en línea han dado como resultado una proliferación de datos dispersos en toda la red. Esto ha creado un escenario en el que es cada vez más difícil rastrear, administrar y proteger los datos de manera eficiente.

Para una administración pública, como la APT, la integridad y confidencialidad de la información no es solo una cuestión de eficiencia, sino también de confianza pública. Con la creciente sofisticación de las ciber amenazas, es vital contar con soluciones robustas que permitan salvaguardar estos datos y garantizar su disponibilidad.

La capacidad de comprender, categorizar y proteger la información se ha convertido en esencial para mantener la seguridad y la integridad de los datos en esta era digital. Las soluciones de gestión de datos se destacan al abordar estos desafíos mediante pilares esenciales que no solo garantizan la protección de la información, sino que también ofrecen la adaptabilidad necesaria en un paisaje tecnológico en constante cambio.

La alineación con estándares internacionales es crucial, y por lo tanto esta solución tiene un impacto profundo en varios controles de la norma ISO/IEC 27002:

- Clasificación y Control de la Información (D.8.2): Al clasificar y etiquetar, la información recibe la protección adecuada según su relevancia. La automatización de este proceso garantiza coherencia y eficiencia.
- Gestión de Derechos de Acceso de Usuario (D.9.2): Con una visión detallada del comportamiento de acceso, es posible ajustar y adaptar los derechos, garantizando que solo las personas adecuadas tengan acceso a la información.
- Control de Acceso a la Red (D.13.1): El comportamiento de acceso también influye en las políticas de red, determinando quién puede acceder y cómo, protegiendo la información incluso antes de que se solicite.
- Gestión de Incidentes de Seguridad de la Información (D.16.1): La visibilidad y alertas tempranas aseguran una respuesta rápida y efectiva, minimizando el daño y maximizando la recuperación.

Por otro lado, la normativa sobre protección de datos personales obliga a poner en marcha medidas técnicas y organizativas necesarias para garantizar la máxima seguridad de los datos. Las medidas adoptadas deben incluir mecanismos para evitar el tratamiento ilícito o no autorizado de información personal, y la protección frente a la pérdida o destrucción de datos.

Finalmente, el Esquema Nacional de Seguridad (ENS) impone la obligatoriedad de mantener un adecuado control de las autorizaciones y control de acceso a los sistemas, así como el registro de su actividad.

Así, en el artículo 17 del capítulo III (requisitos mínimos) del ENS sobre la autorización y control de los accesos, se establece:

"El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación de este real decreto deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas".

Igualmente, en el artículo 24 del mismo capítulo, sobre el Registro de actividad y detección de código dañino, se establece:

"Con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa".

Para cumplir con estas obligaciones normativas, la APT necesita contratar una plataforma que dé respuesta a todas estas necesidades.

2. OBJETO DEL PLIEGO

El objeto principal de la contratación es disponer de una plataforma para la gestión y seguridad del dato diseñada para ofrecer visibilidad, control y protección de extremo a extremo sobre los datos ayudando a mantener un equilibrio entre el acceso necesario y la seguridad de la información.

3. ALCANCE

El alcance de este proyecto englobará una solución que cubra las siguientes necesidades dentro del entorno de Microsoft Office 365:

1. **Descubrimiento del Dato:** Es esencial conocer dónde residen los datos en toda la organización. Una solución efectiva debe rastrear, descubrir y catalogar los datos, garantizando que no haya "puntos ciegos". Esto implica una exploración profunda de la infraestructura, desde servidores hasta endpoints, incluido la manipulación en los dispositives móviles dentro del entorno de Office 365, a través del identificador del usuario, obteniendo también la trazabilidad en este entorno.

2. **Clasificación de la Información:** Segmentar la información basada en su valor e importancia es vital. Las categorías deben ser claras y coherentes, permitiendo una rápida identificación de la criticidad de la información y las políticas de protección necesarias.

3. **Etiquetado:** Una vez que se ha realizado la clasificación, el etiquetado adecuado asegura su fácil identificación y manejo posterior. Esta etiqueta no solo facilita el acceso a los datos, sino que también sirve como filtro en reglas con el fin de automatizar políticas de protección basadas en la clasificación previamente definida.

4. **Comportamiento de Acceso de Usuarios al Dato:** Una supervisión constante del comportamiento de los usuarios al acceder a los datos es crucial. Esto permite detectar comportamientos anómalos, potencialmente dañinos, y minimizar el riesgo de brechas o pérdidas de datos.

5. **Alerta de Actividad Sospechosa y Violación de las Políticas:** No basta con monitorizar; es esencial que la solución ofrezca capacidades avanzadas de alerta. Cuando se detecta actividad inusual o se violan políticas preestablecidas, es imperativo que los responsables de seguridad sean notificados de inmediato para actuar en consecuencia.

4. REQUERIMIENTOS Y ESPECIFICACIONES

4.1. Necesidades detectadas

La APT tiene la necesidad de adquirir una plataforma que permita un adecuado control de acceso, la clasificación de la información, el registro de actividad y capacidades de generación de alertas e informes sobre el Directorio Activo y los servidores de ficheros de la APT.

Para ello se solicita el suministro de la solución de software AREXDATA Data Security Platform la cual permitirá complementar las actuales capacidades, añadiendo sobre las actuales prestaciones nuevas funcionalidades que darán mayor robustez a los sistemas de IT y OT y extender las actuales estrategias de seguridad.

4.2. Requerimientos técnicos

La solución propuesta, se debe centrar principalmente en la protección de datos empresariales, incluyendo archivos y correos electrónicos sensibles, datos de clientes y empleados, registros financieros, planes estratégicos y otros activos intangibles. Dicha solución, debe cubrir áreas como protección de datos, gobierno del dato, confianza cero, cumplimiento normativo y detección y respuesta a amenazas.

La tecnología debe ser capaz de extraer información vital de los datos empresariales y utilizar esta información contextual, denominada metadatos, para mapear los datos y sistemas de archivos corporativos. La estructura de metadatos debe estar diseñada para manejar grandes cantidades de datos y metadatos asociados, con un impacto mínimo en la infraestructura TI existente.

Deberá cubrir las siguientes especificaciones técnicas:

- **Descubrimiento y clasificación de Datos:**

  - Descubrimiento continuo de datos en la nube y on-premise.
  - Clasificación precisa con biblioteca extensa de políticas como PCI, PII, GDPR y CCPPA entre otros.
  - Criterios de clasificación avanzados customizable.
  - Reglas personalizables.
  - Escaneo OCR en documentos e imágenes.
  - Escaneo incremental continuo para rápida clasificación.
  - Escaneo del cuerpo del correo y adjuntos en Exchange Online y buzones compartidos.
  - Etiquetado de datos automático.
  - Análisis de archivos ad-hoc en tiempo real.

- **Acceso a Datos con el mínimo privilegio:**

    - Análisis profundo de permisos.
    - Control sobre la modificación de los permisos de acceso a los datos sensibles desde plataforma SaaS.
    - Políticas de remediación personalizables.
    - Control de la exposición de links compartidos y de colaboración como OneDrive, Sharepoint entre otros.

- **Monitorización de actividad de datos y detección de amenazas:**

    - Alertas UEBA.
    - Alertas de acceso a datos obsoletos.
    - Alertas de acceso a datos sensibles.
    - Alertas de actividad anormal M365.
    - Alertas de actividad anormal en Exchange online.
    - Alertas de comportamiento anormal de usuarios Admin.
    - Alertas de comportamiento anormal de usuarios de servicio.
    - Alertas de comportamiento anormal de usuarios ejecutivos.
    - Respuesta automatizada.
    - Registro de auditoría.
    - Respuesta proactiva a incidentes.
    - Actualización continua de Modelos de amenaza.
    - Equipo especializado en búsqueda de vulnerabilidades.
    - Visión bidireccional de los accesos tanto desde el usuario como desde el dato.
    - Análisis de la superficie de ataque de Active Directory y Azure AD.
    - Correlación de identidades para la identificación de permisos y actividades en datos sensibles.

- **Postura de seguridad:**

    - Evaluación de riesgos continua.
    - Auditoría de seguimiento y registro del ciclo de vida del dato.
    - Gestión de errores de configuración.
    - Gestión de riesgos de terceros.
    - Paneles de control en una única plataforma SaaS.
    - La plataforma debe de cumplir con al menos los siguientes marcos normativos de seguridad:
    - ISO/IEC 27017:2015
    - ISO/IEC 27001:2013
    - ISO/IEC 27018:2019
    - ISO/IEC 27701:2019
    - SOC 2 Type 2
    - SOC 3
    - NIAP Common Criteria Certification

- **Identidad:**

    - Descubrimiento de Shadow Identities.
    - Monitorización de cuentas privilegiadas.
    - Eliminación segura de identidades obsoletas.
    - Seguimiento de usuarios no gestionados y sin SSO.

- **Gestión del cumplimiento:**

    - Paneles e informes de cumplimiento.
    - Paneles de riesgos en tiempo real sobre exposición, uso, propiedad y caducidad.
    - Actualizaciones automáticas de políticas sin necesidad de descargas de paquetes o parches.

4.3. Especificaciones de la plataforma

La plataforma deberá incluir:

- **Instalación, integración y configuración inicial:** La solución debe ser instalada y configurada según los casos de uso específicos de la APT mencionados en el punto anterior para el entorno Microsoft Office 365.

- **Integración con el SIEM:** Una integración fluida con el SIEM existente en la APT (Rapid7 Insight IDR) es esencial para garantizar una visión completa y coherente de la seguridad.

- Deberá cumplir con **los estándares auditables del Centro Criptológico Nacional (CCN)**, y estar en proceso de certificación en el catálogo CPSTIC.

4.4. Mantenimiento y soporte

El mantenimiento y soporte comprenderá los siguientes apartados:

- **Mantenimiento:** se engloban todas las acciones, recursos y servicios encaminados a reparar incidencias y/o errores presentados en todas sus formas y situaciones en el ámbito de los equipos, componentes, aplicaciones, servicios, integraciones, datos, etc. que son prestadas y gestionadas. En cualquier caso, siempre habrá que hacer la detección de problemas, la identificación de la gravedad y el apoyo total para solucionarlos y restablecer el sistema reparando todos los daños y teniendo en cuenta todas las implicaciones de la incidencia y/o error. Esto incluye tanto el material como la mano de obra en el caso de intervenciones in-situ con reposición de equipos, componentes y materiales necesarios.

  La solución objeto del presente pliego estará sujeta al mantenimiento del fabricante que incluye derechos a nuevas versiones de productos, planificación de implementación, aprendizaje técnico y de usuarios finales, soporte técnico y un conjunto único de tecnologías y servicios.

- **Soporte 24x7 en castellano:** Dadas las operaciones críticas y la naturaleza siempre activa de las amenazas, se requiere soporte constante para abordar las alertas y los problemas que puedan surgir.

- **Soporte telefónico** en horario laboral (de lunes a viernes de 09:00 a 14:00 y de 16:00 a 19:00h), resolución de problemas y servicios de consulta.

- **Sesiones de asistencia de personalización de la solución:** Durante estas sesiones, el equipo del adjudicatario ayudará a ajustar alertas, configurar políticas de clasificación y optimizar la plataforma para satisfacer las necesidades de cumplimiento y seguridad de datos.

- **Revisiones trimestrales:** Reuniones periódicas para revisar los objetivos, discutir la hoja de ruta, escuchar comentarios y ayudar a optimizar la tecnología para ofrecer el máximo valor.

4.5. Aceptación y pruebas

El adjudicatario deberá comunicar el momento de la puesta en marcha y disponibilidad de la plataforma contratada a la APT para que sus técnicos den aprobación, tras haber verificado la puesta en marcha de la misma.

El objetivo de las pruebas es la verificación de la disponibilidad de los softwares contratados y su calidad.

5. CRITERIOS DE ADJUDICACIÓN

5.1. Evaluable mediante fórmulas. Hasta 100 puntos

Criterio	Puntos
Precio	100

Los licitadores deberán presentar en el sobre 1, la descripción del suministro a entregar, que deberá cumplir con todos los requisitos técnicos establecidos en este PPT.

En el caso de no presentación de este documento, que no es valorable, así como, si el mismo, no cumple estrictamente con las especificaciones técnicas que se solicitan en el PPT, el licitador no será admitido para continuar en el procedimiento de adjudicación y, por tanto, no se abrirá su oferta económica.

6. PLAZO DE EJECUCIÓN

La nueva plataforma deberá estar disponible en el plazo máximo de 1 (un) mes desde la firma del contrato. El mantenimiento y soporte técnico de las presentes especificaciones deberá estar operativo durante 35 (treinta y cinco) meses a contar desde la puesta a disposición de las licencias tras la firma del contrato.

7. PRESUPUESTO MÁXIMO ESTIMADO

Consultados los precios del mercado para la contratación del suministro objeto del presente pliego, se ha calculado un coste aproximado a nivel global, según la siguiente distribución:

Detalle	Unidades	Precio Ud.	Precio
AREXDATA Data Security Platform	400	116,25€	46.500,00€
Servicio implantación, configuración y parametrización	1	--	36.000,00€
Importe total			**82.500,00€**

El valor estimado se cifra en **82.500,00€** (sin IVA), lo que supone un presupuesto máximo de contrata de **82.500,00€** (IVA incluido).

8. FORMA DE PAGO

El abono del servicio se realizará mediante factura única una vez se haya firmado el contrato y se verifique la puesta a disposición y configuración de la plataforma.

9. CÓDIGOS CPV

48000000-8 Paquetes de software y sistemas de información
48517000-5 Paquetes de software de TI
48781000-6 Paquetes de software de gestión de sistemas
48900000-7 Paquetes de software y sistemas informáticos diversos
72263000-6 Servicios de implementación de software
72268000-1 Servicios de suministro de software
72267100-0 Mantenimiento de software de tecnología de la información

DAVID GONZALEZ MAS - 39719489F

Firmado digitalmente por DAVID GONZALEZ MAS - 39719489F
Fecha: 2024.09.03 10:34:56 +02'00'

El presente documento ha sido firmado electrónicamente por David González Mas, en su condición de Jefe de departamento de Sistemas de Información en la fecha que consta en la validación del mismo.