



PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR LA LICITACIÓN DEL CONTRATO DE ASISTENCIA TÉCNICA PARA LA ADAPTACIÓN DE AUXILIAR DE SERVICIOS DE PINTO AL REGLAMENTO 2016/679/UE 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 LOS DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS DE APLICACIÓN DESDE EL 25 DE MAYO DE 2018 Y AL ESQUEMA NACIONAL DE SEGURIDAD

1. ALCANCE DEL SERVICIO

Es objeto del presente documento fijar las condiciones técnicas que deben regir la contratación por parte de la Empresa Municipal de servicios de Pinto ASERPINTO, de los servicios necesarios para la adecuación a las siguientes normativas:

- ▣ **Reglamento General de Protección de Datos (RGPD)**
- ▣ **Esquema Nacional de Seguridad (ENS)**

La prestación de servicios, con carácter general, se realizará en las instalaciones de la empresa adjudicataria.

La duración del contrato es de 2 años, con posibilidad de prorrogar por tres años más mediante prórrogas anuales.

2. Servicios RGPD

2.1 Registro de actividades de tratamiento

Conforme se establece en el artículo 30 del RGPD, se confeccionará el registro de actividades de tratamiento. Se deberá de realizar un análisis previo al objeto de identificar la titularidad de los mismos.

2.2 Regular los canales de entrada de información

Se deberán adaptar los diferentes canales de entrada de información garantizando el derecho de información conforme a los requisitos del RGPD. En particular se deberán de analizar las bases jurídicas de los tratamientos identificados al objeto de adaptar los formularios, utilizado los modelos basados en capas.

2.3 Delegado de Protección de Datos

La empresa adjudicataria deberá proporcionar un servicio para prestar la figura del DPD durante toda la prestación del servicio.

2.4 Análisis de riesgos y evaluaciones de impacto

Se deberá realizar el análisis de riesgos al objeto de identificar las medidas de seguridad necesarias. Su desarrollo se realizará en base a la metodología MAGERIT y con la herramienta PILAR. Se realizará una integración del análisis con el realizado para el cumplimiento del ENS. Se deberá identificar los tratamientos de alto riesgo / necesidad de realizar posibles evaluaciones de impacto.

2.5 Atención de derechos de la ciudadanía

Se deberá elaborar/adaptar los protocolos que permitan garantizar el ejercicio de los derechos de la ciudadanía, incluyendo procedimientos y modelos.

2.6 Clausulado legal

Se deberán revisar, actualizar y, en su caso elaborar:

- o Las cláusulas de recogida de información
- o Las cláusulas de confidencialidad y seguridad
- o Aviso Legal y Política de Protección de Datos de la página web.
- o Los contratos de encargados del tratamiento.
- o Etc.

2.7 Gestión de brechas de seguridad

La empresa adjudicataria deberá elaborar los procedimientos necesarios para la gestión de brechas de seguridad.

2.8 Medidas de seguridad

La empresa adjudicataria deberá de comprobar la correcta aplicación de las medidas de seguridad derivadas del análisis de riesgos. Las medidas se implantarán de forma alineada con el ENS.

2.9 Canal de asistencia jurídica

La empresa adjudicataria proporcionará un canal de asistencia a la resolución de cuestiones jurídicas durante la prestación del servicio.

2.10 Plan de formación y concienciación



La empresa adjudicataria definirá y desarrollará un plan formativo para garantizar el cumplimiento de la normativa. En la presentación de la oferta se deberá detallar cada uno de los cursos programados.

3. Servicios ENS

La empresa adjudicataria deberá elaborar y mantener actualizada durante todo el ciclo de vida del contrato toda la documentación vinculada a la fase de implantación del sistema de gestión de seguridad de la información, así como el desarrollo de instrumentos, controles y auditorías que garanticen su cumplimiento conforme al oportuno plan de adecuación. Para ello definirá un plan de implantación y certificación progresivo, que permita la correcta adecuación y conformidad de la entidad al Esquema Nacional de Seguridad

3.1 Definición y puesta en marcha de medidas que cubran el marco organizativo

- Desarrollo y revisión de la política de seguridad
- Elaboración de la normativa de seguridad
- Desarrollo de los procedimientos de seguridad
- Definición del proceso de autorización

3.2 Definición y puesta en marcha de las medidas operacionales.

- Servicios de planificación
- Control de acceso
- Explotación
- Regulación de los servicios externos, y en particular, la regulación en la contratación con operadores del sector privado en cumplimiento de la Instrucción Técnica de Seguridad (ITS) de conformidad con el Esquema Nacional de Seguridad.
- Continuidad del servicio
- Monitorización de los sistemas.

3.3 Definición y puesta en marcha de las medidas de protección.

- Desarrollo y ejecución de un plan de formación
- Desarrollo y ejecución de un plan de concienciación
- Control de aplicaciones informáticas.

3.4 Servicios de seguridad particulares



Durante la prestación del servicio se pondrá en marcha un sistema que permita la correlación de eventos y alerta temprana en caso de incidentes de Firewalls. Se deberá detallar la solución tecnológica planteada.

Por otro lado, se realizarán pruebas de seguridad análisis de vulnerabilidades y pruebas de penetración sobre la página web <http://www.aserpinto.es/>