



Anexo II.- 1. Modelo de declaración responsable del cumplimiento de las condiciones exigidas para contratar con el Ayuntamiento de Pamplona.

D/D^a, con domicilio a efectos de notificaciones en y D.N.I. nºteléfono faxe-mail por sí o en representación de (según proceda) con domicilio enN.I.F. teléfonofax y enterado del Pliego Regulador, de las Condiciones Particulares del Contrato y Prescripciones Técnicas que han de regir en la "CONTRATACIÓN DE

DECLARA:

- Que reúne/que la entidad por mi representada reúne (indíquese según proceda si la declaración se hace en nombre propio o en representación de otra persona) las condiciones para contratar y que en caso de resultar licitadora a cuyo favor recaiga la propuesta de adjudicación.
- Que su finalidad o actividad tiene relación directa con el objeto del contrato y que dispone de una organización con elementos personales y materiales suficientes para la debida ejecución del contrato.
- Que se halla al corriente del cumplimiento de las obligaciones tributarias, de Seguridad Social y de seguridad, salud en el trabajo y prevención de riesgos laborales, impuestas por las disposiciones legales vigentes.
- Que conociendo los pliegos que rigen la presente contratación, se compromete a su realización con sujeción estricta a éstos, a su propuesta técnica en la prestación del servicio y a la oferta económica que se presentan.
- Que, de conformidad con el apartado 8 del art. 55 de la Ley Foral 2/2018, de 13 abril, de Contratos Públicos de Navarra, se compromete a acreditar la posesión y validez de los documentos exigidos en el apartado 5 de la cláusula 12 del pliego en el plazo máximo de siete días desde que reciba la notificación de la Mesa de Contratación del correspondiente requerimiento.
- Que identifica como dirección electrónica para la realización de notificaciones a través de medios telemáticos, en el caso de reclamaciones en materia de contratación pública la siguiente:
- La licitadora acepta voluntariamente dar transparencia institucional a todos los datos derivados de los procesos de licitación, adjudicación y ejecución hasta su finalización, con exclusión de aquellos que resulten confidenciales.
- Que la licitadora SI/NO (táchese lo que proceda) es una PYME.

Y para que así conste y surta los efectos oportunos, expido y firmo la presente.

En Pamplona, a de de 2026
(firma electrónica)



ANEXO IV.- OFERTA CUANTIFICABLE MEDIANTE FÓRMULAS.

D/D^a, con domicilio a efectos de notificaciones en y D.N.I. nº teléfono fax e-mail por sí o en representación de (según proceda) con domicilio en N.I.F. teléfono fax y enterado del Pliego Regulador de las Condiciones Particulares del Contrato y Prescripciones Técnicas que han de regir en el la Contratación de **SERVICIOS DE ANÁLISIS, DESCRIPCIÓN Y VALORACIÓN DE PUESTOS DE TRABAJO DEL AYUNTAMIENTO DE PAMPLONA** acepta el contenido íntegro de los mismos y se compromete/que la entidad por mi representada se compromete (según proceda) a la ejecución de dichos servicios, de acuerdo con las ofertas que se hacen a continuación:

OFERTA ECONÓMICA:

Sin IVA: (en número y letra)

Tipo de IVA: ... (en número y letra)

Con IVA (número y letra)

REDUCCIÓN DE PLAZO:

.....semanas.

CRITERIOS SOCIALES:

.....personas contratadas con carácter indefinido adscritas a ejecución de contrato

En Pamplona, a de de 2026.

(firma)

OTRAS NOTAS:

- 1.- No se admitirá ninguna oferta económica que supere el presupuesto de licitación.
- 2.- Respecto de las cantidades económicas recogidas en esta proposición prevalecerán las cantidades expresadas en letra respecto de las expresadas en cifras.
- 3.- Si la licitadora está exenta de IVA deberá hacerlo constar así en su oferta y acreditarlo.

PROTECCIÓN DE DATOS: El Ayuntamiento de Pamplona es el responsable de los datos de carácter personal que van a ser utilizados para la gestión del pliego y posterior contratación en caso de ser la adjudicataria en el ejercicio de los deberes públicos. Los datos se comunicarán en cumplimiento de la legislación vigente. Tiene derecho a acceder a



Ayuntamiento de
Pamplona | **Iruñeko**
Udala

T. 948 420 100 / 010
www.pamplona.es

los datos, rectificarlos en el caso de que no sean correctos y suprimirlos dirigiéndose al Registro General (C/Mayor 2, 31001 de Pamplona) o a la sede electrónica. Puede consultar el listado de tratamientos y la información adicional en www.pamplona.es

ANEXO V: MEDIDAS DE PROTECCIÓN EN EL TRATAMIENTO DE DATOS PERSONALES

COLECTIVOS Y DATOS TRATADOS

Las categorías de personas interesadas cuyos datos serán tratados por la organización ENCARGADA DE TRATAMIENTO son las siguientes:

- Personas empleadas.

Para la ejecución del contrato objeto de este pliego la adjudicataria pudiera ser que necesite acceder a los siguientes tipos de datos:

- Datos identificativos (nombre y apellidos).
- Datos de características personales (sexo).
- Datos académicos y profesionales (formación/titulaciones, experiencia profesional, pertenencia a colegios o asociaciones profesionales).
- Datos de detalles de empleo (profesión, puesto de trabajo).
- Datos económicos de nómina
- Datos de salud.

DERECHO DE INFORMACIÓN.

En el caso de que la organización encargada, recoja datos a través de cuestionarios, debe facilitar 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 el responsable antes del inicio de la recogida de los datos.

Corresponde al Ayuntamiento de Pamplona facilitar el derecho de información.

MEDIDAS DE SEGURIDAD

La entidad adjudicataria deberá ofrecer las garantías suficientes para aplicar las medidas técnicas y organizativas que aseguren que el tratamiento de los datos de carácter personal del que es responsable el Ayuntamiento de Pamplona es conforme a los requisitos de la normativa de protección de datos y garantiza la protección de los derechos de las personas interesadas para lo que deberá implementar al menos las siguientes medidas de seguridad:

Definir, y documentar, las funciones y obligaciones de las diferentes personas usuarias, o perfiles de usuarios, difundirlas entre el personal, así como las consecuencias de su incumplimiento.

Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

Disponer de un procedimiento de notificación, registro y gestión de incidencias y violaciones de seguridad, conforme a lo previsto en el RGPD que recoja: tipo de incidencia/violación, momento de su detección, persona que la notifica, efectos y medidas correctoras. Cualquier incidencia que afecte a la integridad, confidencialidad, autenticidad y disponibilidad del tratamiento de los datos de carácter personal llevada a cabo por la organización encargada de tratamiento será comunicada de inmediato al responsable del tratamiento.

Disponer de un procedimiento para la gestión de los derechos de acceso, rectificación, supresión, oposición y limitación del tratamiento como encargados de tratamiento.

Establecer métodos de cifrado y seudoanonimización en caso de que gestión de soportes fuera de los locales de la organización responsable o encargada de tratamiento.

Incluir sistemas de auditoría y registro (logs de acceso) en las aplicaciones que tratan datos de categorías especiales.

No debe utilizar herramientas que no ofrezcan garantías del cumplimiento de la normativa de protección de datos.

Todos los equipos que se conecten a sistemas o traten datos personales del Ayuntamiento deben disponer al menos de:

- antivirus activado y actualizado con periodicidad diaria
- Firewall.

Se debe establecer un control de acceso según las funciones asignadas a las personas trabajadoras, que eviten el acceso a datos o recursos distintos de los autorizados. Las mismas condiciones deberán existir para el personal ajeno con acceso datos personales.

Las credenciales de acceso identificarán a los usuarios de manera inequívoca y personalizada. En caso de usuarios externos, se permitirá el acceso a los datos personales a usuarios con los permisos adecuados mediante conexiones Red Privada Virtual (VPN) o similares que garanticen la confidencialidad de la información. Dichos permisos de acceso sólo podrán concederse por personal autorizado.

Cuando el acceso a los sistemas del responsable del tratamiento para la prestación de un servicio por parte de la organización encargada se realice en modo remoto, queda expresamente prohibido que la organización encargada del tratamiento incorpore datos en sus sistemas o en soportes distintos a los del responsable del tratamiento.

La organización encargada de tratamiento deberá disponer de un sistema de identificación y autenticación personalizada, los usuarios y contraseñas, deberán almacenarse de forma ininteligible y cambiarse periódicamente al menos de forma anual, disponiendo de un límite de intentos reiterados de acceso no autorizado.

Los dispositivos portátiles dispondrán de una contraseña a nivel de BIOS.

Se dispondrá de sistemas de control de acceso físico a la ubicación de los sistemas de información mediante llave, tarjeta magnética o similar, código de acceso, la documentación en papel con datos especialmente protegidos deberá estar custodiada en armarios, cajones etc. con llave ubicados en áreas con acceso protegido mediante puertas con llave.

La organización encargada de tratamiento de tratamiento dispondrá de procedimientos documentados de copias de respaldo y recuperación de los datos personales que trate por cuenta del Responsable. El acceso a los soportes de copia se encontrará restringido, evitando accesos no autorizados.

Semestralmente se verificará el proceso de copias de seguridad en el caso de que contengan información de la que sea responsable el Ayuntamiento de Pamplona.

Las copias de respaldo se conservarán en lugar diferente del que se encuentren los equipos sobre los que se hace la copia.

Los documentos en formato papel deben archivar en lugares que impidan el acceso a personas no autorizadas. Deberá estar custodiada en armarios, cajones etc. con mecanismos que impidan su apertura.

Igualmente, durante la tramitación o traslado de documentos, la persona a cargo de los mismos debe custodiarla para evitar accesos no autorizados. El traslado se realizará con mecanismos que impidan el acceso o manipulación u obstaculicen su apertura. Los soportes deberán estar etiquetados mediante sistemas únicamente comprensible a nivel interno de la organización.

Se dispondrá de sistemas de control de acceso físico a la ubicación de los sistemas de información.