

ANEXO V “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 usuarias de la web

Para la ejecución del contrato objeto de este pliego el Ayuntamiento la adjudicataria puede acceder a los siguientes tipos de datos:

- Dirección IP

DERECHO DE INFORMACIÓN. La organización encargada, en el momento de la recogida de los datos, debe facilitar, a través de la plataforma web, la información relativa a los tratamientos de datos que se van a realizar, en cumplimiento del deber de información establecido por la normativa de protección de datos. La redacción y el formato en que se presentará dicha información deberán ser consensuados previamente con el responsable del tratamiento, antes de iniciar la recogida de los datos.

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 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 encargada de tratamiento.
- Garantizar:
 1. PROACTIVIDAD, adoptando medidas para evitar la pérdida, alteración o filtración de la información, todas las medidas aplicables se adaptarán al artículo 32 del Reglamento de Protección de datos (RGPD)
 2. RESILIENCIA, adoptando, entre otras, las medidas para:
 - a. Limitar el riesgo de daños por causas naturales u otras causas (agua, humedad, fuego, temperatura inadecuada)
 - b. Proteger la integridad y la disponibilidad de la información antes fallos del sistema, de suministro eléctrico, errores humanos o ataques intencionados.
 - c. Permitir la recuperación de la información de manera efectiva en el menor tiempo posible.
- No debe utilizar herramientas que no ofrezcan garantías del cumplimiento de la normativa de protección de datos.
- No realizar de transferencias internacionales de datos
- La entidad adjudicataria establecerá, entre otras, medidas que:
 - limiten el riesgo de daños por causas naturales, ambientales o industriales (agua, fuego, humedad, temperatura inadecuada, etc.),
 - protejan la integridad y disponibilidad de los datos ante fallos del suministro eléctrico,
 - permitan la recuperación de la información y de los sistemas de manera efectiva en el menor tiempo posible y sin pérdidas de datos.
- Todos los equipos que se conecten a sistemas o traten datos personales deben disponer al menos de:
 - Antivirus activado y actualizado con periodicidad diaria
 - Firewall.
 - Cifrado de contraseñas almacenadas.
 - Los dispositivos portátiles dispondrán de una contraseña a nivel de BIOS.
- CONTROL DE ACCESOS. Entre otras medidas:
 - 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.

- 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
- 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.
- COPIAS DE SEGURIDAD:
 - 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 objeto del contrato.
 - Las copias de respaldo se conservarán en lugar diferente del que se encuentren los equipos sobre los que se hace la copia.