ANÁLISIS DE RIESGOS

1. Identificación de la organización Responsable del tratamiento

De conformidad con lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril de 2016, la organización Responsable del tratamiento es quien determina los fines y los medios del tratamiento de datos personales (Ficheros).

Nombre fiscal	Ayuntamiento de Quatretondeta
Marca comercial	Ayuntamiento de Quatretondeta
Actividad	Administración local
Dirección	Plaça Constitució, 8 - 03811 Alicante (Alacant)
Teléfono	965511094
E-mail	quatretondeta@quatretondeta.es
DPO	Oficina Provincial de Protección de Datos oficinapd@diputacionalicante.es

2. Identificación de los tratamientos de datos personales

Un fichero es un conjunto estructurado de datos personales accesibles con arreglo a criterios determinados y susceptibles de tratamiento para un fin específico.

Tratamiento	Descripción	Tipo	Sistema	Categoría
ÓRGANOS DE GOBIERNO Y CONCEJALES	Datos de los órganos de gobierno y concejales del Ayuntamiento	Responsable	Mixto	BÁSICO
HACIENDA PÚBLICA	Datos para la gestión contable del Ayuntamiento y los Organismos autónomos que dependen del mismo	Responsable	Mixto	BÁSICO
TRIBUTOS	Datos fiscales de ciudadanos para las remesas de impuestos y sus respectivos cobros IAE (Impuesto de Actividades), IBI (Impuesto Bienrs Inmuebles), IIVT (Impuesto Incremento Valor Terreno) y otras Tasas municipales	Responsable	Mixto	BÁSICO
FISCAL Y CONTABLE	Registro de las obligaciones fiscales y contables sujetos a la actividtat económica (trabajadores, proveedores y contratistas)	Responsable	Mixto	BÁSICO
CIUDADANOS	Datos de ciudadanos y residentes en sus relaciones con el Ayuntamiento y los organismos autónomos que dependen de este	Responsable	Mixto	BÁSICO
PADRÓN MUNICIPAL	Gestión de los datos relativos a los habitantes del municipio para las finalidades propias de la Ley que regula el Padrón Municipal (Ley de Bases del Régimen Local)	Responsable	Mixto	BÁSICO
SANCIONES ADMINISTRATIVAS	Datos para la gestión contable de sanciones recibidas o emitidas por incumplimientos administrativos	Responsable	Mixto	BÁSICO

PERSONAL: NÓMINAS Y RR HH	Datos para la confección y gestión de las nóminas de los funcionarios y personal laboral del Ayuntamiento y los Organismos Autónomos dependientes del mismo (Normativa de Función Pública Aplicable)	Responsable	Mixto	BÁSICO
PERSONAL: PRL Y PROTECCIÓN DE DATOS	Gestión de la prevención de riesgos laborales y protección de datos personales de los empleados	Responsable	Mixto	BÁSICO
PERSONAL: FORMACIÓN Y BECAS	Gestión de becas y cursos formativos y del personal inscrito a los mismos para mejorar la actividad, el perfil o la inserción laboral	Responsable	Mixto	BÁSICO
PERSONAL: BOLSA DE TRABAJO, CV Y PRÁCTICAS	Gestión de candidatos para la cobertura de puestos de trabajo mediante la incorporación a los procesos de selección de personal y ocupación de puestos vacantes y sus prácticas	Responsable	Mixto	BÁSICO
PERSONAL: EXPEDIENTES DISCIPLINARIOS	Sistema de información para poner en conocimiento la comisión de actos o conductas que pudieran resultar contrarios a la normativa general que fuera aplicable a la organización en tema laboral	Responsable	Digital	BÁSICO
REGISTRO CIVIL Y PAREJAS DE HECHO	Registro de datos de ciudadanos referentes a matrimonios	Responsable	Mixto	BÁSICO
REGISTRO DE ENTIDADES Y EMPRESAS	Registro de entitades y empresas que se dan de alta en el municipio	Responsable	Mixto	BÁSICO
REGISTRO DE DOCUMENTOS	Registro de entradas y salidas de los documentos presentados en el Ayuntamiento	Responsable	Mixto	BÁSICO
REGISTRO DEL CENSO DE ANIMALES	Registro y control de animales peligrosos y domésticos residentes al municipio	Responsable	Mixto	BÁSICO
REGISTRO DE VIVIENDAS TURÍSTICAS	Registro de casas rurales o pisos dedicados al turismo	Responsable	Mixto	BÁSICO
DERECHOS DEL INTERESADO	Atender las solicitudes de los ciudadanos en el ejercicio de los derechos que establece el GDPR	Responsable	Mixto	BÁSICO
VIOLACIONES DE LA SEGURIDAD	Registro, gestión y resolución de las brechas de seguridad en protección de datos.	Responsable	Digital	BÁSICO
ATENCIÓN CIUDADANA, QUEJAS Y SUGERENCIAS	Datos de ciudadanos y residentes en sus relaciones con el Ayuntamiento y los organismos autónomos que dependen de este y atención a quejas y sugerencias	Responsable	Mixto	BÁSICO
CULTURA, TURISMO Y FIESTAS	Gestión de servicios personales efectuados por diversos departamentos de cultura, turismo y promoción ciudadana (biblioteca, auditorio...)	Responsable	Mixto	BÁSICO
DEPORTES, PISCINA Y PABELLÓN DEPORTIVO, MERCADO MUNICIPAL	Gestión de las actividades que organiza el Ayuntamiento en espacios públicos y clubs deportivos	Responsable	Mixto	BÁSICO
CEMENTERIO	Gestión de datos relativos a los habitantes para la gestión del cementerio y derechos funerarios	Responsable	Mixto	BÁSICO
AYUDAS Y SUBVENCIONES	Gestión de tramitaciones para servicios de personas, asociaciones, comercios ...	Responsable	Mixto	BÁSICO
SERVICIOS SOCIALES BÁSICOS	Gestión de los datos obtenidos para la gestión de los servicios sociales del municipio	Responsable	Mixto	ESPECIAL

SERVICIOS SOCIALES A LA INFANCIA, ADOLESCENCIA Y JUVENTUD	Gestión de servicios sociales personales efectuados por varios departamentos de infancia y juventud	Responsable	Mixto	BÁSICO
SERVICIOS SOCIALES A MAYORES Y DEPENDENCIA	Gestión de los datos obtenidos para el desarrollo de servicios y actividades sociales a personas mayores y personas con discapacidad	Responsable	Mixto	BÁSICO
SERVICIOS SOCIALES A LA INMIGRACIÓN	Gestión de los datos obtenidos para el desarrollo de servicios y actividades sociales a personas inmigrantes	Responsable	Mixto	ESPECIAL
SERVICIOS SOCIALES DE ATENCIÓN A LA MUJER	Gestión de los datos obtenidos para el desarrollo de servicios y seguridad a la mujer	Responsable	Mixto	ESPECIAL
SERVICIOS SOCIALES AL COLECTIVO LGTBIQ+	Gestión de los datos obtenidos para el desarrollo de servicios y actividades sociales a lesbianas, transexuales, gays, bisexuales, intersexuales, queer y cualquier otro tipo de orientación sexual o identidad de género	Responsable	Mixto	ESPECIAL
SERVICIOS SOCIALES DE ATENCIÓN A PERSONAS CON ADICCIONES	Gestión de los datos obtenidos para el desarrollo de servicios, actividades sociales y seguimientos de procesos de desintoxicación	Responsable	Mixto	ESPECIAL
VOLUNTARIOS	Organización de actividades sociales. Personas, socias o no, que colaboran en la organización de las actividades de la asociación o públicas del Ayuntamiento	Responsable	Mixto	BÁSICO
AUDIOVISUALES	Gestión publicitaria audiovisual. Incluye imágenes (foto/vídeo) y sonido (voz) de personas	Responsable	Mixto	BÁSICO
AUDIOVISUALES DE ACTIVIDADES PÚBLICAS	Gestión publicitaria audiovisual. Incluye imágenes (foto/vídeo) y sonido (voz) de personas obtenidas en lugares de acceso público	Responsable	Mixto	BÁSICO
CONTACTOS, COMUNICACIÓN Y PRENSA	Comunicación, información y gestión sobre servicios, actividades, noticias. etc. Incluye contactos web y redes sociales	Responsable	Mixto	BÁSICO
CATASTRO	Información alfanumérica y cartográfica cadastral correspondiente a los bienes inmuebles de competencia de la Dirección General del Catastro	Responsable	Mixto	BÁSICO
PÁRKINGS E INMUEBLES	Información alfanumérica y cartografía catastral correspondiente a los bienes inmuebles y párkings privados competencia de la Dirección General del Catastro	Responsable	Mixto	BÁSICO
OBRAS PÚBLICAS Y LICENCIAS DE OBRA	Datos de licitaciones y obras adquiridas por el Ayuntamiento y organismas autónomos para la mejora de la ciudad	Responsable	Mixto	BÁSICO
CONCESIÓN DE SERVICIOS Y CONCURSOS PÚBLICOS	Contractación de empresas para la gestión de concursos de servicios públicos	Responsable	Mixto	BÁSICO
ESCUELA DE ADULTOS Y DE MÚSICA	Gestión de formación para las titulaciones de graduados, postgraduados, másteres, etc. suscritos a la enseñanza pública y formación musical	Responsable	Mixto	BÁSICO
GESTIÓN ESCOLAR	Gestión de los alumnos y profesorado del centro escolar	Responsable	Mixto	BÁSICO
ACTIVIDADES EXTRAESCOLARES	Gestión de datos de los participantes en actividades extraescolares	Responsable	Mixto	BÁSICO

Ayuntamiento de Quatretondeta
Plaça Constitució, 8 - 03811 Alicante (Alacant)

VIDEOVIGILANCIA	Grabación visual de personas por motivos de seguridad	Responsable	Digital	BÁSICO
REGISTRO JORNADA LABORAL	Registro horario de la jornada laboral para dar cumplimiento al RDL 8/2019, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo	Responsable	Mixto	BÁSICO
DENUNCIAS INTERNAS	Sistema de información para poner en conocimiento la comisión de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que fuera aplicable a la organización.	Responsable	Digital	BÁSICO
MUSEOS	Gestión de la información relativa a los usuarios de las museos	Responsable	Mixto	BÁSICO
ACCESO A REDES WIFI	Gestión técnica y administrativa de los usuarios de las Redes WiFi de la Diputación	Responsable	Digital	BÁSICO

3. Protección de datos desde el diseño y por defecto

De conformidad con el artículo 25 del Reglamento (UE) 2016/679, de 27 de abril de 2016 (GDPR), la protección de datos desde el diseño y por defecto se basa en la implementación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que entrañe el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, alcance, contexto y fines del tratamiento.

El Responsable del tratamiento ha analizado el cumplimiento de las siguientes medidas de seguridad, desde el diseño y por defecto, en todas las fases del tratamiento:

- **Finalidad del tratamiento:**
  - Tratamiento de los datos para fines determinados, explícitos y legítimos.
  - No realización de tratamientos posteriores de manera incompatible con dichos fines.
- **Minimización de datos:**
  - Obtención de datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- **Exactitud de datos**
  - Existencia de mecanismos adecuados para actualizar los datos.
- **Confidencialidad del tratamiento:**
  - Existencia de acuerdos de confidencialidad con el personal autorizado.
  - Existencia de contratos de protección de datos con los intervinientes en el tratamiento (encargados del tratamiento, corresponsables del tratamiento y destinatarios de datos).
  - Existencia de transmisiones de datos a países fuera de la UE.
- **Integridad y seguridad de los datos:**
  - Existencia de medidas de seguridad en los equipos y soportes informáticos, mobiliario y departamentos que contienen datos personales para restringir el acceso a personas no autorizadas y evitar que los datos sean accesibles a un número indeterminado de personas sin la intervención humana.
  - Existencia de medidas adecuadas para garantizar permanentemente la integridad y seguridad física de los datos, la disponibilidad y resiliencia de los sistemas de tratamiento, la restauración de datos mediante copias de respaldo y la supresión efectiva de los datos o la seudonimización

de los mismos.
    - Existencia de un protocolo para actuar ante las brechas de seguridad detectadas y, en el caso de producirse una violación de datos, proceder a activar los mecanismos necesarios para mitigar los riesgos que afecten a los derechos y libertades de los interesados, así como los procedimientos para la notificación de la misma a la autoridad de control y la comunicación a los interesados si fuese necesario.
- **Derechos del interesado:**
    - Existencia de un protocolo para posibilitar el ejercicio de los derechos del interesado y resolver sin dilación las solicitudes recibidas.

4. Análisis de los riesgos del tratamiento

De conformidad con el artículo 32 del Reglamento (UE) 2016/679, de 27 de abril de 2016 (GDPR), se ha analizado el nivel de seguridad a implantar en la Organización para garantizar la protección de datos, teniendo en cuenta los altos riesgos que pueda tener el tratamiento para los derechos y libertades de los interesados, a consecuencia de:

- La destrucción accidental o ilícita de datos.
- La pérdida, alteración o comunicación no autorizada.
- El acceso a los datos cuando sean transmitidos, conservados u objeto de algún otro tipo de tratamiento.

Para ello, se ha analizado la probabilidad/gravedad de riesgos que conlleva el tratamiento en seis apartados:

1. **Estructura de datos.**
2. **Cumplimiento normativo.**
3. **Organización.**
4. **Recursos.**
5. **Seguridad desde el diseño y por defecto.**
6. **Amenazas.**

La probabilidad/gravedad de riesgos se ha clasificado de la siguiente forma:

1. **Muy bajo** (tratamiento sin riesgos)
2. **Bajo** (tratamiento con pocos riesgos y asumible si se cumple la normativa de protección de datos)
3. **Medio** (tratamiento susceptible de algún riesgo, que precisa de procesos de verificación de las medidas adoptadas)
4. **Alto** (tratamiento susceptible de un alto riesgo, que precisa aplicar medidas adecuadas de seguridad y valorar la necesidad de realizar una evaluación de impacto)
5. **Muy Alto** (tratamiento con un alto riesgo, que precisa realizar una evaluación de impacto)

En las tablas siguientes se detallan todas las actividades de tratamiento de manera que se identifican los riesgos iniciales (en el momento del análisis), las medidas de seguridad adoptadas y los riesgos finales (una vez aplicadas dichas medidas). En el apartado 6 se detallan las amenazas identificadas en los apartados anteriores cuando el riesgo inicial es medio, alto o muy alto.

1. ESTRUCTURA DEL TRATAMIENTO

TRATAMIENTO 1: ÓRGANOS DE GOBIERNO Y CONCEJALES

Aplicación
Finalidades
Recursos humanos
Gestión de nóminas
Fines de interés público basados en la legislación vigente
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Cargos públicos
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Núm. de SS o mutualidad
Datos especialmente protegidos
Ideología
Otros datos tipificados
Características personales
Circunstancias sociales
Académicos y profesionales
Económicos, financieros y de seguro
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Registros públicos
Administración tributaria
Organismos de la Seguridad Social
Otros órganos de la administración pública

TRATAMIENTO 2: HACIENDA PÚBLICA

Aplicación
Finalidades

Gestión contable, fiscal y administrativa
Fines de interés público basados en la legislación vigente
Gestión tributaria, inspección y recaudación.
Gestión económico-financiera pública
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Proveedores
Ciudadanos y residentes
Contribuyentes y sujetos obligados
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Bancos, cajas de ahorro y cajas rurales
Administración tributaria
Otros órganos de la administración pública
Tribunal de Cuentas o equivalente autonómico

TRATAMIENTO 3: TRIBUTOS

Aplicación
Finalidades
Gestión contable, fiscal y administrativa
Fines de interés público basados en la legislación vigente
Gestión tributaria, inspección y recaudación.
Gestión económico-financiera pública
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Ciudadanos y residentes
Contribuyentes y sujetos obligados
Datos de carácter identificativo

DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Comptes bancaris
Otros datos tipificados
Económicos, financieros y de seguro
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable
Bancos, cajas de ahorro y cajas rurales
Administración tributaria
BASE

TRATAMIENTO 4: FISCAL Y CONTABLE

Aplicación
Finalidades
Gestión contable, fiscal y administrativa
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Proveedores
Clientes y usuarios
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Bancos, cajas de ahorro y cajas rurales
Administración tributaria

TRATAMIENTO 5: CIUDADANOS

Aplicación
Finalidades
Gestión contable, fiscal y administrativa
Procedimiento administrativo
Publicaciones
Fines de interés público basados en la legislación vigente
Gestión tributaria, inspección y recaudación.
Gestión económico-financiera pública
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Ciudadanos y residentes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Otros datos tipificados
Características personales
Circunstancias sociales
Académicos y profesionales
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Interesados legítimos
Fuerzas y cuerpos de seguridad
Instituto Nacional de Estadística

TRATAMIENTO 6: PADRÓN MUNICIPAL

Aplicación
Finalidades
Fines estadísticos, históricos o científicos
Fines de interés público basados en la legislación vigente
Padrón de habitantes

Gestión del padrón según la Ley de Bases de Régimen Local y demás normativa aplicable
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Ciudadanos y residentes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Otros datos tipificados
Características personales
Académicos y profesionales
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Interesados legítimos
Órganos judiciales
Fuerzas y cuerpos de seguridad
Otros órganos de la administración pública
Instituto Nacional de Estadística

TRATAMIENTO 7: SANCIONES ADMINISTRATIVAS

Aplicación
Finalidades
Gestión contable, fiscal y administrativa
Procedimiento administrativo
Gestión tributaria, inspección y recaudación.
Gestión económico-financiera pública
Gestión sancionadora pública
Origen y procedencia de los datos
El mismo interesado o su representante legal
Entidad privada
Colectivos o categorías de interesados
Proveedores
Ciudadanos y residentes

Ayuntamiento de Quatretondeta
Plaça Constitució, 8 - 03811 Alicante (Alacant)

Contribuyentes y sujetos obligados
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Otros datos tipificados
Infracciones administrativas
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable
Órganos judiciales
Bancos, cajas de ahorro y cajas rurales
Administración pública con competencia en la materia

TRATAMIENTO 8: PERSONAL: NÓMINAS Y RR HH

Aplicación
Finalidades
Gestión de nóminas
Fines de interés público basados en la legislación vigente
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Empleados
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Firma manual
Núm. de SS o mutualidad
COMPTES BANCARIS
Otros datos tipificados
Características personales
Académicos y profesionales

Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Bancos, cajas de ahorro y cajas rurales
Sindicatos y juntas de personal
Administración tributaria
Organismos de la Seguridad Social
Otros órganos de la administración pública

TRATAMIENTO 9: PERSONAL: PRL Y PROTECCIÓN DE DATOS

Aplicación
Finalidades
Prevención de riesgos laborales servicio externo
PROTECCIÓN DE DATOS
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Empleados
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Firma manual
Núm. de SS o mutualidad
Otros datos tipificados
Características personales
Sistema de tratamiento
Mixto

TRATAMIENTO 10: PERSONAL: FORMACIÓN Y BECAS

Aplicación
Finalidades
Educación enseñanzas obligatorias (primaria y secundaria)
Fines de interés público basados en la legislación vigente

Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Empleados
Estudiantes
Solicitantes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Otros datos tipificados
Características personales
Académicos y profesionales
Detalles de empleo
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Registros públicos
Otros órganos de la administración pública

TRATAMIENTO 11: PERSONAL: BOLSA DE TRABAJO, CV Y PRÁCTICAS

Aplicación
Finalidades
Recursos humanos
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Empleados
Demandantes de empleo
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Imagen

Firma manual
GUSTOS, ACTIVIDADES
Otros datos tipificados
Características personales
Circunstancias sociales
Académicos y profesionales
Detalles de empleo
Información comercial
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable

TRATAMIENTO 12: PERSONAL: EXPEDIENTES DISCIPLINARIOS

Aplicación
Finalidades
Recursos humanos
Denuncias internas
Origen y procedencia de los datos
El mismo interesado o su representante legal
Anónimo
Colectivos o categorías de interesados
Empleados
Clientes y usuarios
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Otros datos tipificados
Características personales (personalidad o comportamiento)
Actos o conductas contrarios a la normativa
Sistema de tratamiento
Automatizado
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable

Órganos judiciales
Notarios, abogados y procuradores
Administración pública con competencia en la materia

TRATAMIENTO 13: REGISTRO CIVIL Y PAREJAS DE HECHO

Aplicación
Finalidades
Procedimiento administrativo
Publicaciones
Fines de interés público basados en la legislación vigente
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Ciudadanos y residentes
DEFUNCIONS
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Firma manual
Otros datos tipificados
Características personales
Circunstancias sociales
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable
Administración pública con competencia en la materia

TRATAMIENTO 14: REGISTRO DE ENTIDADES Y EMPRESAS

Aplicación
Finalidades
Gestión de actividades asociativas, culturales, recreativas, deportivas y sociales
Procedimiento administrativo
Fines de interés público basados en la legislación vigente

Origen y procedencia de los datos
Entidad privada
Colectivos o categorías de interesados
Asociados y miembros
Representante legal
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Firma manual
DATOS DE LA ENTIDAD O EMPRESA
Otros datos tipificados
Características personales
Circunstancias sociales
Detalles de empleo
Información comercial
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Registros públicos

TRATAMIENTO 15: REGISTRO DE DOCUMENTOS

Aplicación
Finalidades
Procedimiento administrativo
Fines de interés público basados en la legislación vigente
Origen y procedencia de los datos
El mismo interesado o su representante legal
Entidad privada
Colectivos o categorías de interesados
Propietarios o arrendatarios
Solicitantes
Ciudadanos y residentes
Contribuyentes y sujetos obligados
Datos de carácter identificativo

DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Otros datos tipificados
Características personales
Circunstancias sociales
Académicos y profesionales
Detalles de empleo
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Registros públicos

TRATAMIENTO 16: REGISTRO DEL CENSO DE ANIMALES

Aplicación
Finalidades
Fines estadísticos, históricos o científicos
Fines de interés público basados en la legislación vigente
Padrón de habitantes
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Propietarios o arrendatarios
Ciudadanos y residentes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
CHIP IDENTIFICADOR ANIMAL
Otros datos tipificados
Características personales
Circunstancias sociales
Sistema de tratamiento
Mixto

Categorías de destinatarios de cesiones
Otros órganos de la administración pública

TRATAMIENTO 17: REGISTRO DE VIVIENDAS TURÍSTICAS

Aplicación
Finalidades
Procedimiento administrativo
Fines de interés público basados en la legislación vigente
Origen y procedencia de los datos
El mismo interesado o su representante legal
Entidad privada
Colectivos o categorías de interesados
Propietarios o arrendatarios
Solicitantes
Ciudadanos y residentes
Contribuyentes y sujetos obligados
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Otros datos tipificados
Características personales
Circunstancias sociales
Académicos y profesionales
Detalles de empleo
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Registros públicos

TRATAMIENTO 18: DERECHOS DEL INTERESADO

Aplicación
Finalidades
Gestión contable, fiscal y administrativa

Procedimiento administrativo
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Solicitantes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Firma manual
Sistema de tratamiento
Mixto

TRATAMIENTO 19: VIOLACIONES DE LA SEGURIDAD

Aplicación
Finalidades
Procedimiento administrativo
Gestión y resolución de las brechas de seguridad en protección de datos
Origen y procedencia de los datos
El mismo interesado o su representante legal
Entidad privada
Colectivos o categorías de interesados
Empleados
Personas de contacto
Proveedores
Clientes y usuarios
Representante legal
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Imagen
Firma manual
Otros datos tipificados

Características personales
Circunstancias sociales
Académicos y profesionales
Información comercial
Económicos, financieros y de seguro
Sistema de tratamiento
Automatizado
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable
Interesados legítimos
Entidades aseguradoras
Fuerzas y cuerpos de seguridad
Administración pública con competencia en la materia

TRATAMIENTO 20: ATENCIÓN CIUDADANA, QUEJAS Y SUGERENCIAS

Aplicación
Finalidades
Procedimiento administrativo
Publicaciones
Fines de interés público basados en la legislación vigente
Gestión económico-financiera pública
Gestión sancionadora pública
ATENCIÓN CIUDADANA, QUEJAS Y SUGERENCIAS
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Ciudadanos y residentes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Firma manual
Otros datos tipificados
Características personales
Circunstancias sociales

Sistema de tratamiento
Mixto

TRATAMIENTO 21: CULTURA, TURISMO Y FIESTAS

Aplicación
Finalidades
Educación enseñanzas obligatorias (primaria y secundaria)
Fines de interés público basados en la legislación vigente
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Solicitantes
Beneficiarios
Ciudadanos y residentes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
CARNETS DE BIBLIOTECA O AUDITORIO
Otros datos tipificados
Características personales
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Clubs deportivos y federaciones
Otros órganos de la administración pública

TRATAMIENTO 22: DEPORTES, PISCINA Y PABELLÓN DEPORTIVO, MERCADO MUNICIPAL

Aplicación
Finalidades
Gestión de actividades asociativas, culturales, recreativas, deportivas y sociales
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados

Asociados y miembros
Solicitantes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Imagen
Firma manual
Tarjeta sanitaria
CARNET DE SOCIO
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable
Clubs deportivos y federaciones

TRATAMIENTO 23: CEMENTERIO

Aplicación
Finalidades
Padrón de habitantes
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Ciudadanos y residentes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Otros datos tipificados
Circunstancias sociales
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Interesados legítimos

Administración tributaria

TRATAMIENTO 24: AYUDAS Y SUBVENCIONES

Aplicación
Finalidades
Gestión contable, fiscal y administrativa
Prestación de servicios de solvencia patrimonial y crédito
Cumplimiento/incumplimiento de obligaciones dinerarias
Gestión de asistencia social
Fines de interés público basados en la legislación vigente
Gestión económico-financiera pública
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Clientes y usuarios
Asociados y miembros
Propietarios o arrendatarios
Solicitantes
Beneficiarios
Ciudadanos y residentes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Firma manual
Firma electrónica
Núm. de SS o mutualidad
Otros datos tipificados
Características personales
Circunstancias sociales
Detalles de empleo
Económicos, financieros y de seguro
Transacciones de bienes y servicios
Sistema de tratamiento
Mixto

Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable
Bancos, cajas de ahorro y cajas rurales
Otras entidades financieras
Entidades dedicadas al cumplimiento o incumplimiento de obligaciones dinerarias
Otros órganos de la administración pública

TRATAMIENTO 25: SERVICIOS SOCIALES BÁSICOS

Aplicación
Finalidades
Gestión de bolsas de trabajo o gestión de procesos de selección (currículum)
Gestión de asociados o miembros de entidades sin ánimo de lucro, cuya finalidad sea política, religiosa o sindical
Gestión de asistencia social (con historial clínico)
Fines de interés público basados en la legislación vigente
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Personas de contacto
Solicitantes
Ciudadanos y residentes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Otros datos tipificados
Características personales
Académicos y profesionales
Económicos, financieros y de seguro
Sistema de tratamiento
Mixto

TRATAMIENTO 26: SERVICIOS SOCIALES A LA INFANCIA, ADOLESCENCIA Y JUVENTUD

Aplicación
Finalidades

Gestión de bolsas de trabajo o gestión de procesos de selección (currículum)
Gestión de actividades asociativas, culturales, recreativas, deportivas y sociales
Gestión de asistencia social
Fines de interés público basados en la legislación vigente
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Padres o tutores
Representante legal
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Imagen
Núm. de SS o mutualidad
Otros datos tipificados
Características personales
Circunstancias sociales
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable
Otros órganos de la administración pública

TRATAMIENTO 27: SERVICIOS SOCIALES A MAYORES Y DEPENDENCIA

Aplicación
Finalidades
Gestión de bolsas de trabajo o gestión de procesos de selección (currículum)
Gestión de asistencia social
Educación enseñanzas obligatorias (primaria y secundaria)
Fines de interés público basados en la legislación vigente
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Ciudadanos y residentes

Ayuntamiento de Quatretondeta
Plaça Constitució, 8 - 03811 Alicante (Alacant)

Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Imagen
Firma manual
Núm. de SS o mutualidad
DATOS DE DEPENDENCIA
Categorías especiales de datos
Salud, solo a efectos de bajas, grado de discapacidad o pago de servicios sanitarios
Otros datos tipificados
Características personales
Académicos y profesionales
Económicos, financieros y de seguro
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Asociaciones y organizaciones sin ánimo de lucro
Entidades sanitarias
Organismos de la Seguridad Social
Otros órganos de la administración pública

TRATAMIENTO 28: SERVICIOS SOCIALES A LA INMIGRACIÓN

Aplicación
Finalidades
Gestión de bolsas de trabajo o gestión de procesos de selección (currículum)
Gestión de asistencia social
Fines de interés público basados en la legislación vigente
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Personas de contacto
Migrantes
EMIGRANTES DE OTROS PAÍSES
Datos de carácter identificativo

DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Imagen
Firma manual
Núm. de SS o mutualidad
Categorías especiales de datos
Origen étnico o racial
Religión
Otros datos tipificados
Características personales
Académicos y profesionales
Económicos, financieros y de seguro
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable
Asociaciones y organizaciones sin ánimo de lucro
Órganos judiciales
Entidades sanitarias
Organismos de la Seguridad Social
Otros órganos de la administración pública

TRATAMIENTO 29: SERVICIOS SOCIALES DE ATENCIÓN A LA MUJER

Aplicación
Finalidades
Gestión de bolsas de trabajo o gestión de procesos de selección (currículum)
Gestión de asociados o miembros de entidades sin ánimo de lucro, cuya finalidad sea política, religiosa o sindical
Gestión de asistencia social (con historial clínico)
Fines de interés público basados en la legislación vigente
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Solicitantes
Ciudadanos y residentes

Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Imagen
Firma manual
Núm. de SS o mutualidad
Tarjeta sanitaria
Categorías especiales de datos
Salud
Violencia de género
Otros datos tipificados
Características personales
Circunstancias sociales
Académicos y profesionales
Económicos, financieros y de seguro
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable
Asociaciones y organizaciones sin ánimo de lucro
Entidades sanitarias
Fuerzas y cuerpos de seguridad
Organismos de la Seguridad Social
Otros órganos de la administración pública

TRATAMIENTO 30: SERVICIOS SOCIALES AL COLECTIVO LGTBIQ+

Aplicación
Finalidades
Gestión de bolsas de trabajo o gestión de procesos de selección (currículum)
Gestión de asociados o miembros de entidades sin ánimo de lucro, cuya finalidad sea política, religiosa o sindical
Gestión de asistencia social (con historial clínico)
Fines de interés público basados en la legislación vigente
Origen y procedencia de los datos
El mismo interesado o su representante legal

Colectivos o categorías de interesados
Asociados y miembros
Solicitantes
Ciudadanos y residentes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Imagen
Firma manual
Núm. de SS o mutualidad
Tarjeta sanitaria
Marcas físicas
Categorías especiales de datos
Datos genéticos
Salud
Vida u orientación sexual
Otros datos tipificados
Características personales (personalidad o comportamiento)
Características personales
Circunstancias sociales
Académicos y profesionales
Detalles de empleo
Económicos, financieros y de seguro
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable
Asociaciones y organizaciones sin ánimo de lucro
Entidades sanitarias
Organismos de la Seguridad Social
Otros órganos de la administración pública

TRATAMIENTO 31: SERVICIOS SOCIALES DE ATENCIÓN A PERSONAS CON ADICCIONES

Aplicación

Finalidades
Gestión de bolsas de trabajo o gestión de procesos de selección (currículum)
Gestión de asistencia social
Gestión de asistencia social (con historial clínico)
Fines de interés público basados en la legislación vigente
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Ciudadanos y residentes
PERSONAS CON ADICCIONES
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Firma manual
Núm. de SS o mutualidad
Categorías especiales de datos
Salud
Otros datos tipificados
Características personales
Circunstancias sociales
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable
Entidades sanitarias
Organismos de la Seguridad Social
Otros órganos de la administración pública

TRATAMIENTO 32: VOLUNTARIOS

Aplicación
Finalidades
Recursos humanos
Origen y procedencia de los datos
El mismo interesado o su representante legal

Ayuntamiento de Quatretondeta
Plaça Constitució, 8 - 03811 Alicante (Alacant)

Colectivos o categorías de interesados
Asociados y miembros
Solicitantes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Imagen
Firma manual
Núm. de SS o mutualidad
Otros datos tipificados
Características personales
Circunstancias sociales
Académicos y profesionales
Detalles de empleo
Sistema de tratamiento
Mixto

TRATAMIENTO 33: AUDIOVISUALES

Aplicación
Finalidades
Publicidad y prospección comercial
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Empleados
Proveedores
Clientes y usuarios
Representante legal
Datos de carácter identificativo
Imagen
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable

TRATAMIENTO 34: AUDIOVISUALES DE ACTIVIDADES PÚBLICAS

Aplicación
Finalidades
Publicidad y prospección comercial
Fines de interés público basados en la legislación vigente
Origen y procedencia de los datos
El mismo interesado o su representante legal
Fuentes accesibles al público
Colectivos o categorías de interesados
Beneficiarios
Datos de carácter identificativo
Imagen
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable

TRATAMIENTO 35: CONTACTOS, COMUNICACIÓN Y PRENSA

Aplicación
Finalidades
Publicidad y prospección comercial
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Personas de contacto
Clientes y usuarios
Solicitantes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Otros datos tipificados
Información comercial
Sistema de tratamiento

Mixto

TRATAMIENTO 36: CATASTRO

Aplicación
Finalidades
Procedimiento administrativo
Fines de interés público basados en la legislación vigente
Gestión tributaria, inspección y recaudación.
Origen y procedencia de los datos
El mismo interesado o su representante legal
Registros públicos
Colectivos o categorías de interesados
Propietarios o arrendatarios
Contribuyentes y sujetos obligados
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Otros datos tipificados
Transacciones de bienes y servicios
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Interesados legítimos
Registros públicos
Administración tributaria
Instituto Nacional de Estadística

TRATAMIENTO 37: PÁRKINGS E INMUEBLES

Aplicación
Finalidades
Gestión contable, fiscal y administrativa
Procedimiento administrativo
Fines de interés público basados en la legislación vigente

Gestión tributaria, inspección y recaudación.
Origen y procedencia de los datos
El mismo interesado o su representante legal
Registros públicos
Colectivos o categorías de interesados
Propietarios o arrendatarios
Contribuyentes y sujetos obligados
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Firma manual
Otros datos tipificados
Transacciones de bienes y servicios
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable
Interesados legítimos
Registros públicos
Administración tributaria
Instituto Nacional de Estadística

TRATAMIENTO 38: OBRAS PÚBLICAS Y LICENCIAS DE OBRA

Aplicación
Finalidades
Gestión contable, fiscal y administrativa
Procedimiento administrativo
Publicaciones
Fines de interés público basados en la legislación vigente
Origen y procedencia de los datos
Entidad privada
Administraciones públicas
Colectivos o categorías de interesados
Proveedores

Clientes y usuarios
Contribuyentes y sujetos obligados
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Firma manual
Otros datos tipificados
Económicos, financieros y de seguro
Transacciones de bienes y servicios
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable
Interesados legítimos
Bancos, cajas de ahorro y cajas rurales
Otras entidades financieras
Administración pública con competencia en la materia

TRATAMIENTO 39: CONCESIÓN DE SERVICIOS Y CONCURSOS PÚBLICOS

Aplicación
Finalidades
Fines de interés público basados en la legislación vigente
Contratación de servicios públicos
Origen y procedencia de los datos
Entidad privada
Colectivos o categorías de interesados
Representante legal
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Firma manual
Núm. de SS o mutualidad

Otros datos tipificados
Características personales
Circunstancias sociales
Detalles de empleo
Información comercial
Económicos, financieros y de seguro
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable
Registros públicos
Administración tributaria
Administración pública con competencia en la materia

TRATAMIENTO 40: ESCUELA DE ADULTOS Y DE MÚSICA

Aplicación
Finalidades
Educación enseñanzas obligatorias (primaria y secundaria)
Fines de interés público basados en la legislación vigente
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Estudiantes
Solicitantes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Imagen
Firma manual
Núm. de SS o mutualidad
Otros datos tipificados
Académicos y profesionales
Sistema de tratamiento
Mixto

Categorías de destinatarios de cesiones
Otros órganos de la administración pública
CENTROS DE EDUCACIÓN PÚBLICA Y PRIVADA

TRATAMIENTO 41: GESTIÓN ESCOLAR

Aplicación
Finalidades
Educación enseñanzas obligatorias (primaria y secundaria)
Fines de interés público basados en la legislación vigente
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Estudiantes
Representante legal
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Otros datos tipificados
Características personales (personalidad o comportamiento)
Características personales
Circunstancias sociales
Académicos y profesionales
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Otros órganos de la administración pública

TRATAMIENTO 42: ACTIVIDADES EXTRAESCOLARES

Aplicación
Finalidades
Educación enseñanzas obligatorias (primaria y secundaria)
Origen y procedencia de los datos
El mismo interesado o su representante legal

Colectivos o categorías de interesados
Estudiantes
Solicitantes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Imagen
Tarjeta sanitaria
Sistema de tratamiento
Mixto

TRATAMIENTO 43: VIDEOVIGILANCIA

Aplicación
Finalidades
Videovigilancia
Garantitzar la seguretat de les persones i instal·lacions
Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Ciudadanos y residentes
Datos de carácter identificativo
Imagen
Sistema de tratamiento
Automatizado
Categorías de destinatarios de cesiones
Fuerzas y cuerpos de seguridad

TRATAMIENTO 44: REGISTRO JORNADA LABORAL

Aplicación
Finalidades
Recursos humanos
Gestión de nóminas
Origen y procedencia de los datos

El mismo interesado o su representante legal
Colectivos o categorías de interesados
Empleados
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Identificador de usuario
Sistema de tratamiento
Mixto
Categorías de destinatarios de cesiones
Interesados legítimos
Organismos de la Seguridad Social

TRATAMIENTO 45: DENUNCIAS INTERNAS

Aplicación
Gestión de las denuncias para decidir iniciar una investigación, detectar posibles delitos, prevenir la imposición de responsabilidad y evitar cualquier tipo de conducta contraria a la normativa interna y externa de la entidad.
Origen y procedencia de los datos
El mismo interesado o su representante legal
Entidad privada
Anónimo
Colectivos o categorías de interesados
Empleados
Proveedores
Clientes y usuarios
Asociados y miembros
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Otros datos tipificados
Características personales (personalidad o comportamiento)
Actos o conductas contrarios a la normativa

Sistema de tratamiento
Automatizado
Categorías de destinatarios de cesiones
Organizaciones o personas directamente relacionadas con el responsable
Órganos judiciales
Notarios, abogados y procuradores
Administración pública con competencia en la materia

TRATAMIENTO 46: MUSEOS

Aplicación
Gestión de los usuarios de las bibliotecas
Gestión de los usuarios de museos
Origen y procedencia de los datos
El mismo interesado o su representante legal
Administraciones públicas
Colectivos o categorías de interesados
Estudiantes
Solicitantes
Ciudadanos y residentes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Imagen
Firma manual
Firma electrónica
Otros datos tipificados
Características personales
Sistema de tratamiento
Mixto

TRATAMIENTO 47: ACCESO A REDES WIFI

Aplicación
Identificación de los usuarios conectados a las Redes WiFi de la Diputación y gestión técnica y administrativa de los mismos.

Origen y procedencia de los datos
El mismo interesado o su representante legal
Colectivos o categorías de interesados
Empleado público
Empleados
Usuarios
Ciudadanos y residentes
Datos de carácter identificativo
DNI/NIF/NIE/Pasaporte
Nombre y apellidos
Dirección postal o electrónica
Teléfono
Dirección IP, dirección MAC de dispositivo
Sistema de tratamiento
Automatizado

2. CUMPLIMIENTO NORMATIVO

1. ÓRGANOS DE GOBIERNO Y CONCEJALES

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR) *RGPD 679/2016 y L.O. 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos legales.*	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
	-Acuerdos y actas del pleno de la Junta de Gobierno, Actas de las Comisiones de Plenos. - Decretos y Resoluciones de los órganos del ayuntamiento. -Actos administrativos que serán objeto de publicación cuando así lo establezcan las normas reguladoras de cada procedimiento o cuando lo aconsejen razones de interés público apreciadas por el órgano competente. -Secretaria. Gestión de los órganos colegiados del ayuntamiento. Transparencia, publicidad activa, acceso a información pública. Gestión archivística y administrativa de documentos electrónicos. Gestión de transferencias desde unidades administrativas municipales. Registro de los cargos públicos del ayuntamiento. Gestión archivística y administrativa de documentos en papel y en soportes audiovisuales. gestión de expurgos. Registro presencial de entrada. Ventanilla única. Registro físico de salida. declaración de Bienes y Derechos patrimoniales, así como la declaración de actividad y causas de posible incompatibilidad del cargo púb		Sí

Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados mientras existan prescripciones legales que dictaminen la custodia	Asegurarse de que exista una obligación que esté fundamentada en la legislación vigente.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			

Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

2. HACIENDA PÚBLICA

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			

Legitimación del tratamiento (licitud)	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
	-Depósito y gestión de los avales presentados ante el Ayuntamiento. -Gestión de los ingresos y pagos. -Gestión y recaudación de los impuestos no encomendados a entidades recaudatorias externas. -Relaciones con entidades recaudatorias externas. -Autoliquidaciones. -Tasas y precios públicos. -Cobro de sanciones . Inspección tributaria.		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados mientras existan prescripciones legales que dictaminen la custodia	Asegurarse de que exista una obligación que esté fundamentada en la legislación vigente.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			

Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si

Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

3. TRIBUTOS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados mientras existan prescripciones legales que dictaminen la custodia	Asegurarse de que exista una obligación que esté fundamentada en la legislación vigente.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si

Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si

Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

4. FISCAL Y CONTABLE

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
	-Gestión contable y financiera del Ayuntamiento. -Fiscalización de todos los actos del Ayuntamiento que den lugar al reconocimiento y liquidación de derechos y obligaciones o gastos de contenido económico, los ingresos y pagos que de aquéllos se deriven, y la recaudación, inversión y aplicación, en general, de los caudales públicos.		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados mientras existan prescripciones legales que dictaminen la custodia	Asegurarse de que exista una obligación que esté fundamentada en la legislación vigente.	Si

Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	**Los datos SON TRATADOS por Encargados del tratamiento** y EXISTEN CONTRATOS que garanticen medidas de seguridad adecuadas para la protección de datos y los derechos de los interesados	Asegurarse de que los Encargados del tratamiento hayan firmado los contratos de protección de datos y de que se guarden en un lugar seguro.	Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si

Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

5. CIUDADANOS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si

Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
	-Gestión de contenidos de la Sede Electrónica. -Gestión de notificaciones electrónicas. -Gestión de carpeta ciudadana. -Registro electrónica de entrada y registro electrónico de salida.		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de archivo en INTERÉS PÚBLICO	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si

Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

6. PADRÓN MUNICIPAL

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
	-Gestión integral del padrón municipal de habitantes del municipio, incluida la acreditación de residencia y domicilio habitual.		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados mientras existan prescripciones legales que dictaminen la custodia	Asegurarse de que exista una obligación que esté fundamentada en la legislación vigente.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos SON COMUNICADOS a Destinatarios y EXISTEN CONTRATOS de cesión de datos	Asegurarse de que se haya suscrito un contrato con el destinatario de datos y de que se disponga de procedimientos para comunicarle el derecho de rectificación, supresión o limitación cuando lo solicite el interesado.	Si
Política de información			

Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de los Destinatarios o categorías de Destinatarios a los que SE COMUNICAN los datos		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si

Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

7. SANCIONES ADMINISTRATIVAS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
	-Sanción que se produce cuando una persona no cumple lo establecido en el conjunto de normas que integran el derecho administrativo.		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de archivo en INTERÉS PÚBLICO	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si

Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si

Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

8. PERSONAL: NÓMINAS Y RR HH

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Para la ejecución de un CONTRATO o precontrato con el interesado (artículo 6.1.b GDPR)	Comprobar que se informe debidamente del tratamiento en el mismo contrato.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión LABORAL		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados mientras existan prescripciones legales que dictaminen la custodia	Asegurarse de que exista una obligación que esté fundamentada en la legislación vigente.	Si

Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si

Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

9. PERSONAL: PRL Y PROTECCIÓN DE DATOS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión LABORAL		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si

Conservación de datos (limitación del plazo de conservación)	Conservados mientras existan prescripciones legales que dictaminen la custodia	Asegurarse de que exista una obligación que esté fundamentada en la legislación vigente.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	**Los datos SON TRATADOS por Encargados del tratamiento** y EXISTEN CONTRATOS que garanticen medidas de seguridad adecuadas para la protección de datos y los derechos de los interesados	Asegurarse de que los Encargados del tratamiento hayan firmado los contratos de protección de datos y de que se guarden en un lugar seguro.	Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si

Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

10. PERSONAL: FORMACIÓN Y BECAS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Para la ejecución de un CONTRATO o precontrato con el interesado (artículo 6.1.b GDPR)	Comprobar que se informe debidamente del tratamiento en el mismo contrato.	Si
Finalidad del tratamiento (limitación de los fines)	Formación y becas		Sí

Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de INVESTIGACIÓN histórica, estadística o científica	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			

Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

11. PERSONAL: BOLSA DE TRABAJO, CV Y PRÁCTICAS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			

Legitimación del tratamiento (licitud)	Consentimiento INEQUÍVOCO mediante una clara acción del interesado (artículo 6.1.a GDPR)	Guardar registros probatorios del consentimiento	Si
Finalidad del tratamiento (limitación de los fines)	Gestión de CURRÍCULUMS		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines	Asegurarse de que no se conserven los datos durante más tiempo del necesario para alcanzar los fines por los que se tratan.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos SON COMUNICADOS a Destinatarios y EXISTEN CONTRATOS de cesión de datos	Asegurarse de que se haya suscrito un contrato con el destinatario de datos y de que se disponga de procedimientos para comunicarle el derecho de rectificación, supresión o limitación cuando lo solicite el interesado.	Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si

Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de los Destinatarios o categorías de Destinatarios a los que SE COMUNICAN los datos		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

12. PERSONAL: EXPEDIENTES DISCIPLINARIOS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión JURÍDICA		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines	Asegurarse de que no se conserven los datos durante más tiempo del necesario para alcanzar los fines por los que se tratan.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si

Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

13. REGISTRO CIVIL Y PAREJAS DE HECHO

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			

Legitimación del tratamiento (licitud)	Consentimiento EXPLÍCITO para fines determinados (artículo 6.1.a GDPR)	Guardar documentos probatorios del consentimiento.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
	-Gestión celebración matrimonios civiles.		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines	Asegurarse de que no se conserven los datos durante más tiempo del necesario para alcanzar los fines por los que se tratan.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si

Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

14. REGISTRO DE ENTIDADES Y EMPRESAS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	NO SE PUEDEN ACTUALIZAR los datos porque el fichero no admite manipulación	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para no manipular los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de archivo en INTERÉS PÚBLICO	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si

Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si

Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

15. REGISTRO DE DOCUMENTOS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
	-Gestión de contenidos y notificaciones de la Sede Electrónica. -Gestión de la carpeta ciudadana. -Registro electrónico de entrada y salida. -Gestión archivística histórica y administrativa de documentos en papel, soportes audiovisuales y gestión expurgos. -Registro de convenios con entidades y organismos. -		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	NO SE PUEDEN ACTUALIZAR los datos porque el fichero no admite manipulación	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para no manipular los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de archivo en INTERÉS PÚBLICO	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si

Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si

Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

16. REGISTRO DEL CENSO DE ANIMALES

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
	-Registro de animales de compañía. -Registro de animales potencialmente peligrosos.		Sí

Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de archivo en INTERÉS PÚBLICO	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			

Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

17. REGISTRO DE VIVIENDAS TURÍSTICAS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			

Legitimación del tratamiento (licitud)	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	NO SE PUEDEN ACTUALIZAR los datos porque el fichero no admite manipulación	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para no manipular los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de archivo en INTERÉS PÚBLICO	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si

Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si

Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

18. DERECHOS DEL INTERESADO

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Se conservarán durante el tiempo necesario para resolver las reclamaciones. Será de aplicación lo dispuesto en la normativa de archivos y documentación		Sí
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			

Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si

Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

19. VIOLACIONES DE LA SEGURIDAD

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	NO SE PUEDEN ACTUALIZAR los datos porque el fichero no admite manipulación	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para no manipular los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos		Sí
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			

Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si

Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

20. ATENCIÓN CIUDADANA, QUEJAS Y SUGERENCIAS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
	-Gestión de contenidos y notificaciones de la Sede Electrónica. -Gestión carpeta ciudadana. -Registro electrónica y documental de entrada y salida.		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de archivo en INTERÉS PÚBLICO	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si

Ayuntamiento de Quatretondeta
Plaça Constitució, 8 - 03811 Alicante (Alacant)

Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si

Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

21. CULTURA, TURISMO Y FIESTAS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
	-Gestión de bibliotecas y mediatecas municipales y personas usuarias de las mismas, así cómo de las aulas informáticas instaladas en las mismas. -Gestión de las personas usuarias del punto de acceso WIFI. -Gestión de eventos culturales y cursos. -Gestión de los museos municipales. -Gestión de las instalaciones y personas usuarias de las mismas. -Gestión de fiestas y eventos. Autorizaciones , controles. -Oficina de Turismo. Promoción turística. Concursos y actividades organizadas.		Sí

Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de archivo en INTERÉS PÚBLICO	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			

Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

22. DEPORTES, PISCINA Y PABELLÓN DEPORTIVO, MERCADO MUNICIPAL

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			

Legitimación del tratamiento (licitud)	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
	-Tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (art. 6.1 e del RGPD).		Sí
Finalidad del tratamiento (limitación de los fines)	Gestión de actividades ASOCIATIVAS		Si
	-Gestión de los cursos y actividades deportivas. -Gestión de las instalaciones y personas usuarias de las mismas. -Gestión de convenios con entidades externas y subvención a deportistas. -Gestión de las actividades de venta no sedentaria. -Gestión de los mercados municipales.		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines	Asegurarse de que no se conserven los datos durante más tiempo del necesario para alcanzar los fines por los que se tratan.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			

Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si

Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

23. CEMENTERIO

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Para la ejecución de un CONTRATO o precontrato con el interesado (artículo 6.1.b GDPR)	Comprobar que se informe debidamente del tratamiento en el mismo contrato.	Si
	-Tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (art. 6.1e del RGPD).		Sí
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
	-Gestión del cementerio municipal.		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de archivo en INTERÉS PÚBLICO	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si

Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si

Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

24. AYUDAS Y SUBVENCIONES

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión de intervención SOCIAL		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si

Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de archivo en INTERÉS PÚBLICO	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si

Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

25. SERVICIOS SOCIALES BÁSICOS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si

Excepción para categorías especiales de datos	Por interés público esencial derivado de una Ley (artículo 9.2.g GDPR)	Comprobar que derive de una ley, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión de intervención SOCIAL		Si
	-Equipo Específico de Intervención con Infancia y Adolescencia (EEIIA). -Coordinación con Policía Local-Absentismo. -Intervención familiar. Cursos padres/madres/tutores-as. -Gestión de las prestaciones a la Tercera Edad. Gestión de los Centros de Mayores, tanto centro de día como residenciales. -Gestión de planes de igualdad. Actividades de promoción de la mujer.		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de archivo en INTERÉS PÚBLICO	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			

Ayuntamiento de Quatretondeta
Plaça Constitució, 8 - 03811 Alicante (Alacant)

Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Acceso a categorías especiales de datos	EXISTEN MEDIDAS adicionales de seguridad (llaves, restricción de acceso, seudonimización, cifrado, etc.)	Se deberá llevar un control actualizado del personal con acceso a las categorías especiales de datos.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si

Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Conservación de categorías especiales de datos	Se guardan en mobiliario o departamentos CON MEDIDAS DE SEGURIDAD (llave, acceso restringido, etc.)	Se deberá llevar un control actualizado del personal con acceso al mobiliario o departamentos que contengan categorías especiales de datos.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

26. SERVICIOS SOCIALES A LA INFANCIA, ADOLESCENCIA Y JUVENTUD

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión de intervención SOCIAL		Si
	-Equipo Específico de Intervención con Infancia y Adolescencia (EEIIA). -Coordinación con Policía Local-Absentismo. -Intervención familiar. Cursos padres/madres/tutores-as. -Gestión de planes de igualdad. Actividades de promoción de la mujer.		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si

Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines	Asegurarse de que no se conserven los datos durante más tiempo del necesario para alcanzar los fines por los que se tratan.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si

Ayuntamiento de Quatretondeta
Plaça Constitució, 8 - 03811 Alicante (Alacant)

Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

27. SERVICIOS SOCIALES A MAYORES Y DEPENDENCIA

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			

Legitimación del tratamiento (licitud)	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión de intervención SOCIAL		Si
	-Gestión de las prestaciones a la Tercera Edad. Gestión de los Centros de Mayores, tanto centro de día como residenciales.		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de archivo en INTERÉS PÚBLICO	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			

Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si

Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

28. SERVICIOS SOCIALES A LA INMIGRACIÓN

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión de intervención SOCIAL		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de archivo en INTERÉS PÚBLICO	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			

Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si

Acceso a categorías especiales de datos	EXISTEN MEDIDAS adicionales de seguridad (llaves, restricción de acceso, seudonimización, cifrado, etc.)	Se deberá llevar un control actualizado del personal con acceso a las categorías especiales de datos.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de categorías especiales de datos	Se guardan en mobiliario o departamentos CON MEDIDAS DE SEGURIDAD (llave, acceso restringido, etc.)	Se deberá llevar un control actualizado del personal con acceso al mobiliario o departamentos que contengan categorías especiales de datos.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

29. SERVICIOS SOCIALES DE ATENCIÓN A LA MUJER

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión de intervención SOCIAL		Si
	-Gestión de planes de igualdad. Actividades de promoción de la mujer.		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si

Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de archivo en INTERÉS PÚBLICO	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si

Ayuntamiento de Quatretondeta
Plaça Constitució, 8 - 03811 Alicante (Alacant)

Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Acceso a categorías especiales de datos	EXISTEN MEDIDAS adicionales de seguridad (llaves, restricción de acceso, seudonimización, cifrado, etc.)	Se deberá llevar un control actualizado del personal con acceso a las categorías especiales de datos.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de categorías especiales de datos	Se guardan en mobiliario o departamentos CON MEDIDAS DE SEGURIDAD (llave, acceso restringido, etc.)	Se deberá llevar un control actualizado del personal con acceso al mobiliario o departamentos que contengan categorías especiales de datos.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

30. SERVICIOS SOCIALES AL COLECTIVO LGTBIQ+

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			

Legitimación del tratamiento (licitud)	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión de intervención SOCIAL		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de archivo en INTERÉS PÚBLICO	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si

Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Acceso a categorías especiales de datos	EXISTEN MEDIDAS adicionales de seguridad (llaves, restricción de acceso, seudonimización, cifrado, etc.)	Se deberá llevar un control actualizado del personal con acceso a las categorías especiales de datos.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si

Ayuntamiento de Quatretondeta
Plaça Constitució, 8 - 03811 Alicante (Alacant)

Conservación de categorías especiales de datos	Se guardan en mobiliario o departamentos CON MEDIDAS DE SEGURIDAD (llave, acceso restringido, etc.)	Se deberá llevar un control actualizado del personal con acceso al mobiliario o departamentos que contengan categorías especiales de datos.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

31. SERVICIOS SOCIALES DE ATENCIÓN A PERSONAS CON ADICCIONES

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión de intervención SOCIAL		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de archivo en INTERÉS PÚBLICO	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si

Ayuntamiento de Quatretondeta
Plaça Constitució, 8 - 03811 Alicante (Alacant)

Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Acceso a categorías especiales de datos	EXISTEN MEDIDAS adicionales de seguridad (llaves, restricción de acceso, seudonimización, cifrado, etc.)	Se deberá llevar un control actualizado del personal con acceso a las categorías especiales de datos.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si

Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de categorías especiales de datos	Se guardan en mobiliario o departamentos CON MEDIDAS DE SEGURIDAD (llave, acceso restringido, etc.)	Se deberá llevar un control actualizado del personal con acceso al mobiliario o departamentos que contengan categorías especiales de datos.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

32. VOLUNTARIOS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Consentimiento EXPLÍCITO para fines determinados (artículo 6.1.a GDPR)	Guardar documentos probatorios del consentimiento.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión de actividades ASOCIATIVAS		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines	Asegurarse de que no se conserven los datos durante más tiempo del necesario para alcanzar los fines por los que se tratan.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			

Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si

Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

33. AUDIOVISUALES

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Consentimiento EXPLÍCITO para fines determinados (artículo 6.1.a GDPR)	Guardar documentos probatorios del consentimiento.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Exposición y publicación de IMÁGENES		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si

Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia	Revisar periódicamente que siga existiendo una relación indefinida entre RT e Interesado para mantener el fin del tratamiento.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos se publican en los medios de comunicación propios de Responsable		Sí
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa que se podrán publicar los audiovisuales en los medios de comunicación propios de Responsable		Sí
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si

Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

34. AUDIOVISUALES DE ACTIVIDADES PÚBLICAS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
	-Gestión de la página web del ayuntamiento, publicación de contenidos y gestión de los perfiles en redes sociales del ayuntamiento.		Sí

Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines	Asegurarse de que no se conserven los datos durante más tiempo del necesario para alcanzar los fines por los que se tratan.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los audiovisiales pueden ser comunicados a los medios de comunicación para su publicación		Sí
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos NO SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos, derechos del interesado, categorías de datos y fuente de procedencia	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa que se podrán publicar los audiovisuales en los medios de comunicación		Sí
Política de seguridad			

Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

35. CONTACTOS, COMUNICACIÓN Y PRENSA

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			

Legitimación del tratamiento (licitud)	Consentimiento EXPLÍCITO para fines determinados (artículo 6.1.a GDPR)	Guardar documentos probatorios del consentimiento.	Si
Finalidad del tratamiento (limitación de los fines)	Exposición y publicación de IMÁGENES		Si
	Gestión de CONCURSOS O SORTEOS	Que los datos no se traten para otros fines	Si
	Gestión de actividades ASOCIATIVAS		Si
	-Gestión de la página web del ayuntamiento, publicación de contenidos y gestión de perfiles en redes sociales del ayuntamiento.		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia	Revisar periódicamente que siga existiendo una relación indefinida entre RT e Interesado para mantener el fin del tratamiento.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si

Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si

Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

36. CATASTRO

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines	Asegurarse de que no se conserven los datos durante más tiempo del necesario para alcanzar los fines por los que se tratan.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			

Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si

Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

37. PÁRKINGS E INMUEBLES

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines	Asegurarse de que no se conserven los datos durante más tiempo del necesario para alcanzar los fines por los que se tratan.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si

Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si

Ayuntamiento de Quatretondeta
Plaça Constitució, 8 - 03811 Alicante (Alacant)

Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

38. OBRAS PÚBLICAS Y LICENCIAS DE OBRA

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
	-Gestión de licencias de actividades. -Planificación Urbanística. -Gestión catastral, en caso de estar conveniada con la Dirección General del Catastro. -Certificaciones. -Inspecciones y sanciones en materias urbanística, así como la gestión de las diversas modalidades de licencias urbanísticas.		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines	Asegurarse de que no se conserven los datos durante más tiempo del necesario para alcanzar los fines por los que se tratan.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si

Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si

Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

39. CONCESIÓN DE SERVICIOS Y CONCURSOS PÚBLICOS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Consentimiento EXPLÍCITO para fines determinados (artículo 6.1.a GDPR)	Guardar documentos probatorios del consentimiento.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si
	-Gestión de limpieza viaria. -Gestión de recogida y tratamiento de basuras. -Gestión del servicio de agua. -Gestión del mantenimiento de activos. -Gestión de las brigadas de obras. -Gestión del alumbrado público. -Gestión de parques y jardines. -Gestión de limpieza de edificios.		Sí

Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines	Asegurarse de que no se conserven los datos durante más tiempo del necesario para alcanzar los fines por los que se tratan.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si

Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

40. ESCUELA DE ADULTOS Y DE MÚSICA

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si

Finalidad del tratamiento (limitación de los fines)	FORMACIÓN		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de INVESTIGACIÓN histórica, estadística o científica	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			

Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

41. GESTIÓN ESCOLAR

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			

Legitimación del tratamiento (licitud)	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
	Por interés legítimo de ORGANISMOS PÚBLICOS en el ejercicio de sus funciones (artículo 6.1.f GDPR)	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente por un interés legítimo de las Autoridades u Organismos públicos en el ejercicio de sus funciones.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	FORMACIÓN		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de INVESTIGACIÓN histórica, estadística o científica	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si

Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si

Ayuntamiento de Quatretondeta
Plaça Constitució, 8 - 03811 Alicante (Alacant)

Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

42. ACTIVIDADES EXTRAESCOLARES

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Para la ejecución de un CONTRATO o precontrato con el interesado (artículo 6.1.b GDPR)	Comprobar que se informe debidamente del tratamiento en el mismo contrato.	Si
Finalidad del tratamiento (limitación de los fines)	FORMACIÓN		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines	Asegurarse de que no se conserven los datos durante más tiempo del necesario para alcanzar los fines por los que se tratan.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			

Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si

Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

43. VIDEOVIGILANCIA

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
	Article 6.1 e) del GDPR: Compliment d'una misió d'interès públic		Sí
Finalidad del tratamiento (limitación de los fines)	Seguridad y VIGILANCIA		Si
	-Gestión de cámaras y grabaciones cuya competencia no corresponde a Cuerpos y fuerzas de Seguridad del Estado. -Controles de acceso y seguridad de las infraestructuras del Ayuntamiento.		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	NO SE PUEDEN ACTUALIZAR los datos porque el fichero no admite manipulación	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para no manipular los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Transcorregut un mes sinó s'han comunicat a les Forces i Cosos de Seguretat i/o Jutjats i Tribunals		Sí
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si

Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara mediante ICONOS FORMALIZADOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si

Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

44. REGISTRO JORNADA LABORAL

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión LABORAL		Si
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	NO SE PUEDEN ACTUALIZAR los datos porque el fichero no admite manipulación	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para no manipular los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante 4 años para el registro horario de jornada laboral	Comprobar que se hayan tomado medidas para conservar los registros de jornada durante cuatro años y que permanezcan a disposición de los trabajadores, de sus representantes legales y de la Inspección de Trabajo y Seguridad Social	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			

Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	**Los datos SON TRATADOS por Encargados del tratamiento** y EXISTEN CONTRATOS que garanticen medidas de seguridad adecuadas para la protección de datos y los derechos de los interesados	Asegurarse de que los Encargados del tratamiento hayan firmado los contratos de protección de datos y de que se guarden en un lugar seguro.	Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			

Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

45. DENUNCIAS INTERNAS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR) *Artículos 10 y 13 de la Ley 2/2023 reguladora de la protección de las personas que informen sobre infracciones*	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
Finalidad del tratamiento (limitación de los fines)	Poner en conocimiento la comisión de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si

Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante NO MÁS TIEMPO DEL NECESARIO para alcanzar los fines	Asegurarse de que no se conserven los datos durante más tiempo del necesario para alcanzar los fines por los que se tratan.	Si
	Conservados durante un máximo de 3 meses desde la introducción de los datos		Sí
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si

Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

46. MUSEOS

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			
Legitimación del tratamiento (licitud)	Por una OBLIGACIÓN LEGAL del Responsable del tratamiento (artículo 6.1.c GDPR)	Asegurarse de que la obligación esté fundamentada en la legislación vigente y de que las cesiones también.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
Finalidad del tratamiento (limitación de los fines)	Gestión DOCUMENTAL		Si

Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	NO SE PUEDEN ACTUALIZAR los datos porque el fichero no admite manipulación	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para no manipular los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante no más tiempo del necesario para mantener los fines de archivo en INTERÉS PÚBLICO	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si
Protección de datos (integridad y confidencialidad)	EXISTEN MEDIDAS adecuadas para proteger los datos contra tratamientos no autorizados y pérdidas o destrucción	Asegurarse de que se hayan implementado medidas técnicas y organizativas adecuadas para proteger los datos.	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si
Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos NO SE OBTIENEN DEL INTERESADO** y no se comunica la información porque el tratamiento está FUNDAMENTADO EN LA LEGISLACIÓN VIGENTE	Asegurarse de que el tratamiento esté fundamentado en la legislación vigente.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			

Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas	Asegurarse de que las medidas aplicadas impidan el acceso a personas no autorizadas.	Si
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos	Asegurarse de que no se pueda acceder directamente a los datos evitando dejar información al alcance de personas no autorizadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

47. ACCESO A REDES WIFI

Concepto	Aplicación	Medidas	Cumplimiento
Principios del tratamiento			

Legitimación del tratamiento (licitud)	Consentimiento EXPLÍCITO para fines determinados (artículo 6.1.a GDPR)	Guardar documentos probatorios del consentimiento.	Si
	Para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1.e GDPR)	Se deben tomar medidas para que el tratamiento se realice por un interés público basado en la legislación vigente y no se usen para otra finalidad no autorizada.	Si
	Normativa aplicable:		Sí
Finalidad del tratamiento (limitación de los fines)	Gestión técnica y administrativa de los usuarios de las Redes Wifi		Sí
Limitación del tratamiento (minimización de los datos)	Obtención de datos ADECUADOS, PERTINENTES Y LIMITADOS como mínimo para alcanzar los fines	Asegurarse de que los datos obtenidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. No se tratarán datos innecesarios para alcanzar los fines, por lo que se deberá eliminar la información que no se precise.	Si
Actualización de datos (exactitud)	EXISTEN PROCEDIMIENTOS para la actualización de datos	Asegurarse de que se hayan implementado procedimientos técnicos u organizativos para actualizar los datos.	Si
Conservación de datos (limitación del plazo de conservación)	Conservados durante el periodo establecido por el tratamiento, la legislación aplicable y los requerimientos aplicables a la conservación de información por parte de la ADMINISTRACIÓN PÚBLICA	Asegurarse de que se realicen revisiones para evaluar la necesidad de conservación y se adopten medidas para limitar el acceso sólo para los fines previstos.	Si
Protección de datos (integridad y confidencialidad)	Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica	Comprobar que se han adoptado las medidas de seguridad establecidas en el Anexo II del Real Decreto 311/2022	Si
Responsabilidad del tratamiento			
Personal autorizado	Los datos son tratados por el PERSONAL de la organización y EXISTEN ACUERDOS DE CONFIDENCIALIDAD con instrucciones del tratamiento	Asegurarse de que el personal autorizado para tratar datos haya firmado los acuerdos de confidencialidad y de que se guarden en un lugar seguro.	Si
Encargados del tratamiento (ET)	Los datos NO SON TRATADOS por Encargados del tratamiento		Si
Corresponsables del tratamiento (CoRT)	Los datos NO SON TRATADOS por Corresponsables del tratamiento		Si
Destinatarios de datos	Los datos NO SON COMUNICADOS a terceros, salvo obligación legal		Si
Política de información			
Transparencia de la información	Se facilita la información de forma clara por ESCRITO o por MEDIOS ELECTRÓNICOS	Asegurarse de que se facilite la información del tratamiento de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.	Si

Ayuntamiento de Quatretondeta
Plaça Constitució, 8 - 03811 Alicante (Alacant)

Información básica del tratamiento	**Los datos SE OBTIENEN DEL INTERESADO** y SE INFORMA del Responsable, finalidad, base jurídica, criterios de conservación, comunicación de datos y derechos del interesado	Asegurarse de que se facilite la información del tratamiento al interesado.	Si
Comunicación de la información al interesado	**Los datos SE OBTIENEN DEL INTERESADO** y SE COMUNICA la información previamente a la obtención de los datos	Asegurarse de que se comunique la información del tratamiento previamente a la obtención de datos.	Si
Comunicación de datos a terceros	Se informa de que NO SE COMUNICAN los datos a terceros, salvo por obligación legal		Si
Política de seguridad			
Derechos de los interesados	Los datos están organizados de manera que ES POSIBLE dar respuesta al ejercicio de los derechos del interesado.	Asegurarse de que los datos estén estructurados de manera efectiva para el ejercicio de los derechos de los interesados.	Si
Desde el diseño y por defecto	SE HAN IMPLEMENTADO medidas adecuadas para la protección de datos desde el diseño y por defecto	Asegurarse de que las medidas implementadas sean las adecuadas.	Si
Riesgos del tratamiento	SE HA ANALIZADO el tratamiento y NO EXISTE la probabilidad de un ALTO RIESGO para los derechos y libertades de los interesados	Se ha comprobado que el análisis de riesgos efectuado no determine la existencia de amenazas con la probabilidad de un alto riesgo para los derechos y libertades de los interesados.	Si
Violaciones de la seguridad	EXISTE un protocolo de actuación en caso de producirse una violación de la seguridad	Asegurarse de que exista un protocolo de actuación para el caso que se produzca una violación de seguridad y de que se haya puesto en conocimiento del personal de la organización.	Si
Medidas de protección de datos			
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados	Se deberá llevar un control actualizado del personal con acceso a los equipos y redes informáticas.	Si
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)	Comprobar que las medidas aplicadas son adecuadas.	Si
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados	Comprobar que los dispositivos y/o aplicaciones que protegen los equipos informáticos se mantienen actualizados (antivirus, *antispam*, *firewall*, etc.)	Si
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad	Comprobar que se realicen copias de seguridad regularmente y que se guarden con medidas de seguridad.	Si
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad	Asegurarse de que el transporte o transmisión de datos lo realice personal autorizado y de que las medidas de seguridad adoptadas sean adecuadas.	Si
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)	Asegurarse de que se destruyan o supriman con medidas de seguridad adecuadas.	Si

3. ORGANIZACIÓN

Locales o delegaciones

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
SEDE PRINCIPAL				
Tipo de acceso al local	Entrada libre con control de acceso (personal de recepción, vigilantes, etc.).	Bajo	Se deberán tomar medidas para que el control de acceso sea efectivo.	Muy bajo
Sistema general de control de llaves	Las llaves se guardan en un lugar seguro y con acceso autorizado a las mismas	Bajo	Se deberá llevar un control actualizado del personal con acceso a las llaves.	Muy bajo
Otras medidas de seguridad	Videovigilancia con grabación.	Muy bajo		Muy bajo

Departamentos

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
ADMINISTRACIÓN. ÁREA DE SERVICIOS MUNICIPALES				
Permiso:	Limitado a personal autorizado en los puestos de trabajo y archivos documentales.	Bajo	Se deberá llevar un control actualizado del personal con acceso a los puestos de trabajo y archivos documentales.	Muy bajo
Acceso:	Acceso al Departamento regido por las medidas de seguridad del Local.	Bajo	Se deberá evaluar si las medidas de seguridad del Local son suficientes para proteger los datos.	Muy bajo
Control de llaves:	Las llaves se guardan en un lugar seguro y con acceso autorizado a las mismas.	Bajo	Se deberá llevar un control actualizado del personal con acceso a las llaves.	Muy bajo
Otras medidas de seguridad:	NO EXISTEN otras medidas de seguridad.	Bajo	Se deberá evaluar la necesidad de implementar alguna medida de seguridad en el acceso a los locales.	Muy bajo
REGISTRO. SECRETARÍA-INTERVENCIÓN				
Permiso:	Limitado a personal autorizado en los puestos de trabajo y archivos documentales.	Bajo	Se deberá llevar un control actualizado del personal con acceso a los puestos de trabajo y archivos documentales.	Muy bajo
Acceso:	Acceso al Departamento regido por las medidas de seguridad del Local.	Bajo	Se deberá evaluar si las medidas de seguridad del Local son suficientes para proteger los datos.	Muy bajo
Control de llaves:	Las llaves se guardan en un lugar seguro y con acceso autorizado a las mismas.	Bajo	Se deberá llevar un control actualizado del personal con acceso a las llaves.	Muy bajo
Otras medidas de seguridad:	NO EXISTEN otras medidas de seguridad.	Bajo	Se deberá evaluar la necesidad de implementar alguna medida de seguridad en el acceso a los locales.	Muy bajo
ALCALDÍA				
Permiso:	Limitado a personal autorizado en todo el Departamento.	Bajo	Se deberá llevar un control actualizado del personal con acceso al Departamento.	Muy bajo

Acceso:	Acceso al Departamento regido por las medidas de seguridad del Local.	Bajo	Se deberá evaluar si las medidas de seguridad del Local son suficientes para proteger los datos.	Muy bajo
Control de llaves:	Las llaves se guardan en un lugar seguro y con acceso autorizado a las mismas.	Bajo	Se deberá llevar un control actualizado del personal con acceso a las llaves.	Muy bajo
Otras medidas de seguridad:	NO EXISTEN otras medidas de seguridad.	Bajo	Se deberá evaluar la necesidad de implementar alguna medida de seguridad en el acceso a los locales.	Muy bajo
ÁREA DE HACIENDA Y PROMOCIÓN ECONÓMICA				
Permiso:	Limitado a personal autorizado en los puestos de trabajo y archivos documentales.	Bajo	Se deberá llevar un control actualizado del personal con acceso a los puestos de trabajo y archivos documentales.	Muy bajo
Acceso:	Acceso al Departamento regido por las medidas de seguridad del Local.	Bajo	Se deberá evaluar si las medidas de seguridad del Local son suficientes para proteger los datos.	Muy bajo
Control de llaves:	Las llaves se guardan en un lugar seguro y con acceso autorizado a las mismas.	Bajo	Se deberá llevar un control actualizado del personal con acceso a las llaves.	Muy bajo
Otras medidas de seguridad:	Videovigilancia con grabación y alarma.	Muy bajo		Muy bajo
URBANISMO				
Permiso:	Limitado a personal autorizado en los puestos de trabajo y archivos documentales.	Bajo	Se deberá llevar un control actualizado del personal con acceso a los puestos de trabajo y archivos documentales.	Muy bajo
Acceso:	Acceso al Departamento regido por las medidas de seguridad del Local.	Bajo	Se deberá evaluar si las medidas de seguridad del Local son suficientes para proteger los datos.	Muy bajo
Control de llaves:	Las llaves se guardan en un lugar seguro y con acceso autorizado a las mismas.	Bajo	Se deberá llevar un control actualizado del personal con acceso a las llaves.	Muy bajo
Otras medidas de seguridad:	NO EXISTEN otras medidas de seguridad.	Bajo	Se deberá evaluar la necesidad de implementar alguna medida de seguridad en el acceso a los locales.	Muy bajo
AREA DE PERSONAL				
Permiso:	Limitado a personal autorizado en los puestos de trabajo y archivos documentales.	Bajo	Se deberá llevar un control actualizado del personal con acceso a los puestos de trabajo y archivos documentales.	Muy bajo
Acceso:	Acceso al Departamento regido por las medidas de seguridad del Local.	Bajo	Se deberá evaluar si las medidas de seguridad del Local son suficientes para proteger los datos.	Muy bajo
Control de llaves:	Las llaves se guardan en un lugar seguro y con acceso autorizado a las mismas.	Bajo	Se deberá llevar un control actualizado del personal con acceso a las llaves.	Muy bajo
Otras medidas de seguridad:	NO EXISTEN otras medidas de seguridad.	Bajo	Se deberá evaluar la necesidad de implementar alguna medida de seguridad en el acceso a los locales.	Muy bajo
SERVICIOS SOCIALES				
Permiso:	Limitado a personal autorizado en los puestos de trabajo y archivos documentales.	Bajo	Se deberá llevar un control actualizado del personal con acceso a los puestos de trabajo y archivos documentales.	Muy bajo

Acceso:	Acceso al Departamento regido por las medidas de seguridad del Local.	Bajo	Se deberá evaluar si las medidas de seguridad del Local son suficientes para proteger los datos.	Muy bajo
Control de llaves:	Las llaves se guardan en un lugar seguro y con acceso autorizado a las mismas.	Bajo	Se deberá llevar un control actualizado del personal con acceso a las llaves.	Muy bajo
Otras medidas de seguridad:	NO EXISTEN otras medidas de seguridad.	Bajo	Se deberá evaluar la necesidad de implementar alguna medida de seguridad en el acceso a los locales.	Muy bajo
DEPORTES				
Permiso:	Limitado a personal autorizado en los puestos de trabajo y archivos documentales.	Bajo	Se deberá llevar un control actualizado del personal con acceso a los puestos de trabajo y archivos documentales.	Muy bajo
Acceso:	Acceso al Departamento regido por las medidas de seguridad del Local.	Bajo	Se deberá evaluar si las medidas de seguridad del Local son suficientes para proteger los datos.	Muy bajo
Control de llaves:	Las llaves se guardan en un lugar seguro y con acceso autorizado a las mismas.	Bajo	Se deberá llevar un control actualizado del personal con acceso a las llaves.	Muy bajo
Otras medidas de seguridad:	NO EXISTEN otras medidas de seguridad.	Bajo	Se deberá evaluar la necesidad de implementar alguna medida de seguridad en el acceso a los locales.	Muy bajo

4. RECURSOS

Software

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
APP MunicicipApp (ADMINISTRACIÓN. ÁREA DE SERVICIOS MUNICIPALES, ALCALDÍA, ÁREA DE HACIENDA Y PROMOCIÓN ECONÓMICA, REGISTRO. SECRETARÍA-INTERVENCIÓN, URBANISMO)				
Control de acceso	Acceso mediante usuario y contraseña.	Bajo	Comprobar que existen mecanismos para verificar que la contraseña es segura y que se cambia periódicamente.	Muy bajo
Accesos no autorizados	Se ha implementado un sistema que impide los intentos reiterados no autorizados	Bajo	Comprobar que el sistema avise al RT de los intentos no autorizados.	Muy bajo
Transmisión de datos	La aplicación permite transmitir los datos encriptados	Bajo	Asegurarse de que exista un protocolo para encriptar los datos en las transmisiones de información.	Muy bajo
Registro de accesos	Se registran los accesos mediante una aplicación informática	Muy bajo	Asegurarse de que exista un procedimiento para acceder a los registros en caso de incidencias.	Muy bajo
Ayuntamiento en la nube (ADMINISTRACIÓN. ÁREA DE SERVICIOS MUNICIPALES, ALCALDÍA, ÁREA DE HACIENDA Y PROMOCIÓN ECONÓMICA, REGISTRO. SECRETARÍA-INTERVENCIÓN, URBANISMO)				
Control de acceso	Acceso mediante usuario y contraseña.	Bajo	Comprobar que existen mecanismos para verificar que la contraseña es segura y que se cambia periódicamente.	Muy bajo
Accesos no autorizados	No existe un control de accesos no autorizados a la aplicación	Medio	Plantearse la necesidad de activar mecanismos que impidan los intentos reiterados no autorizados.	Bajo
Transmisión de datos	La aplicación permite transmitir los datos encriptados	Bajo	Asegurarse de que exista un protocolo para encriptar los datos en las transmisiones de información.	Muy bajo
Registro de accesos	No existe un registro de accesos a la aplicación y accede más de un usuario	Medio	Cuando se traten categorías de datos ESPECIALES o PENALES es recomendable registrar los accesos de los usuarios al programa.	Bajo
Padrón municipal de habitantes. (ADMINISTRACIÓN. ÁREA DE SERVICIOS MUNICIPALES, REGISTRO. SECRETARÍA-INTERVENCIÓN)				
Control de acceso	Acceso mediante usuario y contraseña.	Bajo	Comprobar que existen mecanismos para verificar que la contraseña es segura y que se cambia periódicamente.	Muy bajo
Accesos no autorizados	Se ha implementado un sistema que impide los intentos reiterados no autorizados	Bajo	Comprobar que el sistema avise al RT de los intentos no autorizados.	Muy bajo
Transmisión de datos	No se transmiten datos desde la aplicación	Muy bajo	Asegurarse que No se transmiten datos desde la aplicación.	Muy bajo
Registro de accesos	Se registran los accesos mediante una aplicación informática	Muy bajo	Asegurarse de que exista un procedimiento para acceder a los registros en caso de incidencias.	Muy bajo

Ayuntamiento de Quatretondeta
Plaça Constitució, 8 - 03811 Alicante (Alacant)

Portal web municipal (ADMINISTRACIÓN. ÁREA DE SERVICIOS MUNICIPALES, ALCALDÍA, ÁREA DE HACIENDA Y PROMOCIÓN ECONÓMICA, REGISTRO. SECRETARÍA-INTERVENCIÓN, URBANISMO)				
Control de acceso	Acceso mediante usuario y contraseña.	Bajo	Comprobar que existen mecanismos para verificar que la contraseña es segura y que se cambia periódicamente.	Muy bajo
Accesos no autorizados	No existe un control de accesos no autorizados a la aplicación	Bajo	Plantearse la necesidad de activar mecanismos que impidan los intentos reiterados no autorizados.	Muy bajo
Transmisión de datos	La aplicación permite transmitir los datos encriptados	Bajo	Asegurarse de que exista un protocolo para encriptar los datos en las transmisiones de información.	Muy bajo
Registro de accesos	No existe un registro de accesos a la aplicación y accede más de un usuario	Bajo	Cuando se traten categorías de datos ESPECIALES o PENALES es recomendable registrar los accesos de los usuarios al programa.	Muy bajo

ADOBE ACROBAT (ADMINISTRACIÓN. ÁREA DE SERVICIOS MUNICIPALES, ALCALDÍA, ÁREA DE HACIENDA Y PROMOCIÓN ECONÓMICA, REGISTRO. SECRETARÍA-INTERVENCIÓN, URBANISMO)				
Control de acceso	Acceso regido por el control de acceso a los equipos informáticos.	Bajo	Comprobar que existan métodos de identificación y autenticación para acceder a los equipos informáticos.	Muy bajo
Accesos no autorizados	Se ha implementado un sistema que impide los intentos reiterados no autorizados	Bajo	Comprobar que el sistema avise al RT de los intentos no autorizados.	Muy bajo
Transmisión de datos	No se transmiten datos desde la aplicación	Muy bajo	Asegurarse que No se transmiten datos desde la aplicación.	Muy bajo
Registro de accesos	Se registran los accesos mediante una aplicación informática	Bajo	Asegurarse de que exista un procedimiento para acceder a los registros en caso de incidencias.	Muy bajo

CORREO ELECTRÓNICO (ADMINISTRACIÓN. ÁREA DE SERVICIOS MUNICIPALES, ALCALDÍA, ÁREA DE HACIENDA Y PROMOCIÓN ECONÓMICA, REGISTRO. SECRETARÍA-INTERVENCIÓN, URBANISMO)				
Control de acceso	Acceso mediante usuario y contraseña.	Bajo	Comprobar que existen mecanismos para verificar que la contraseña es segura y que se cambia periódicamente.	Muy bajo
Accesos no autorizados	Se ha implementado un sistema que impide los intentos reiterados no autorizados	Bajo	Comprobar que el sistema avise al RT de los intentos no autorizados.	Muy bajo
Transmisión de datos	La aplicación permite transmitir los datos encriptados	Bajo	Asegurarse de que exista un protocolo para encriptar los datos en las transmisiones de información.	Muy bajo
Registro de accesos	Se registran los accesos mediante una aplicación informática	Muy bajo	Asegurarse de que exista un procedimiento para acceder a los registros en caso de incidencias.	Muy bajo

eNotum (AOC) (REGISTRO. SECRETARÍA-INTERVENCIÓN)				
Control de acceso	Acceso mediante usuario y contraseña.	Bajo	Comprobar que existen mecanismos para verificar que la contraseña es segura y que se cambia periódicamente.	Muy bajo
Accesos no autorizados	Se ha implementado un sistema que impide los intentos reiterados no autorizados	Bajo	Comprobar que el sistema avise al RT de los intentos no autorizados.	Muy bajo

Ayuntamiento de Quatretondeta
Plaça Constitució, 8 - 03811 Alicante (Alacant)

Transmisión de datos	La aplicación permite transmitir los datos encriptados	Bajo	Asegurarse de que exista un protocolo para encriptar los datos en las transmisiones de información.	Muy bajo
Registro de accesos	Se registran los accesos mediante una aplicación informática	Muy bajo	Asegurarse de que exista un procedimiento para acceder a los registros en caso de incidencias.	Muy bajo
esPUBLICO (URBANISMO)				
Control de acceso	Acceso mediante usuario y contraseña.	Bajo	Comprobar que existen mecanismos para verificar que la contraseña es segura y que se cambia periódicamente.	Muy bajo
Accesos no autorizados	Se ha implementado un sistema que impide los intentos reiterados no autorizados	Bajo	Comprobar que el sistema avise al RT de los intentos no autorizados.	Muy bajo
Transmisión de datos	La aplicación permite transmitir los datos encriptados	Bajo	Asegurarse de que exista un protocolo para encriptar los datos en las transmisiones de información.	Muy bajo
Registro de accesos	Se registran los accesos mediante una aplicación informática	Muy bajo	Asegurarse de que exista un procedimiento para acceder a los registros en caso de incidencias.	Muy bajo
GPA Gestión Patrimonial (ADMINISTRACIÓN. ÁREA DE SERVICIOS MUNICIPALES, ALCALDÍA, ÁREA DE HACIENDA Y PROMOCIÓN ECONÓMICA, REGISTRO. SECRETARÍA-INTERVENCIÓN, URBANISMO)				
Control de acceso	Acceso mediante usuario y contraseña.	Bajo	Comprobar que existen mecanismos para verificar que la contraseña es segura y que se cambia periódicamente.	Muy bajo
Accesos no autorizados	No existe un control de accesos no autorizados a la aplicación	Bajo	Plantearse la necesidad de activar mecanismos que impidan los intentos reiterados no autorizados.	Muy bajo
Transmisión de datos	La aplicación permite transmitir los datos encriptados	Bajo	Asegurarse de que exista un protocolo para encriptar los datos en las transmisiones de información.	Muy bajo
Registro de accesos	No existe un registro de accesos a la aplicación y accede más de un usuario	Bajo	Cuando se traten categorías de datos ESPECIALES o PENALES es recomendable registrar los accesos de los usuarios al programa.	Muy bajo
MICROSOFT OFFICE (ADMINISTRACIÓN. ÁREA DE SERVICIOS MUNICIPALES, ALCALDÍA, ÁREA DE HACIENDA Y PROMOCIÓN ECONÓMICA, REGISTRO. SECRETARÍA-INTERVENCIÓN, URBANISMO)				
Control de acceso	Acceso regido por el control de acceso a los equipos informáticos.	Bajo	Comprobar que existan métodos de identificación y autenticación para acceder a los equipos informáticos.	Muy bajo
Accesos no autorizados	Se ha implementado un sistema que impide los intentos reiterados no autorizados	Bajo	Comprobar que el sistema avise al RT de los intentos no autorizados.	Muy bajo
Transmisión de datos	La aplicación permite transmitir los datos encriptados	Bajo	Asegurarse de que exista un protocolo para encriptar los datos en las transmisiones de información.	Muy bajo
Registro de accesos	Se registran los accesos mediante una aplicación informática	Bajo	Asegurarse de que exista un procedimiento para acceder a los registros en caso de incidencias.	Muy bajo
PORTAL ADMINISTRACIÓN (ALCALDÍA, ÁREA DE HACIENDA Y PROMOCIÓN ECONÓMICA, REGISTRO. SECRETARÍA-INTERVENCIÓN, URBANISMO)				

Control de acceso	Acceso mediante usuario y contraseña.	Bajo	Comprobar que existen mecanismos para verificar que la contraseña es segura y que se cambia periódicamente.	Muy bajo
Accesos no autorizados	Existe un control de accesos, pero NO se impiden los intentos reiterados no autorizados	Bajo	Plantearse la necesidad de activar mecanismos que impidan los intentos reiterados no autorizados.	Muy bajo
Transmisión de datos	La aplicación permite transmitir los datos encriptados	Bajo	Asegurarse de que exista un protocolo para encriptar los datos en las transmisiones de información.	Muy bajo
Registro de accesos	Se registran los accesos mediante una aplicación informática	Muy bajo	Asegurarse de que exista un procedimiento para acceder a los registros en caso de incidencias.	Muy bajo
PORTAL CONTRATACIÓN (REGISTRO. SECRETARÍA-INTERVENCIÓN, URBANISMO)				
Control de acceso	Acceso mediante usuario y contraseña.	Bajo	Comprobar que existen mecanismos para verificar que la contraseña es segura y que se cambia periódicamente.	Muy bajo
Accesos no autorizados	Se ha implementado un sistema que impide los intentos reiterados no autorizados	Bajo	Comprobar que el sistema avise al RT de los intentos no autorizados.	Muy bajo
Transmisión de datos	La aplicación permite transmitir los datos encriptados	Bajo	Asegurarse de que exista un protocolo para encriptar los datos en las transmisiones de información.	Muy bajo
Registro de accesos	Se registran los accesos mediante una aplicación informática	Muy bajo	Asegurarse de que exista un procedimiento para acceder a los registros en caso de incidencias.	Muy bajo
PORTAL TRANSPARENCIA (REGISTRO. SECRETARÍA-INTERVENCIÓN, URBANISMO)				
Control de acceso	Acceso mediante usuario y contraseña.	Bajo	Comprobar que existen mecanismos para verificar que la contraseña es segura y que se cambia periódicamente.	Muy bajo
Accesos no autorizados	Se ha implementado un sistema que impide los intentos reiterados no autorizados	Bajo	Comprobar que el sistema avise al RT de los intentos no autorizados.	Muy bajo
Transmisión de datos	La aplicación permite transmitir los datos encriptados	Bajo	Asegurarse de que exista un protocolo para encriptar los datos en las transmisiones de información.	Muy bajo
Registro de accesos	Se registran los accesos mediante una aplicación informática	Bajo	Asegurarse de que exista un procedimiento para acceder a los registros en caso de incidencias.	Muy bajo
PRIVACY DRIVER (REGISTRO. SECRETARÍA-INTERVENCIÓN)				
Control de acceso	Acceso mediante usuario y contraseña.	Bajo	Comprobar que existen mecanismos para verificar que la contraseña es segura y que se cambia periódicamente.	Muy bajo
Accesos no autorizados	Se ha implementado un sistema que impide los intentos reiterados no autorizados	Bajo	Comprobar que el sistema avise al RT de los intentos no autorizados.	Muy bajo
Transmisión de datos	La aplicación permite transmitir los datos encriptados	Bajo	Asegurarse de que exista un protocolo para encriptar los datos en las transmisiones de información.	Muy bajo

Registro de accesos	Se registran los accesos mediante una aplicación informática	Muy bajo	Asegurarse de que exista un procedimiento para acceder a los registros en caso de incidencias.	Muy bajo
SICALWIN (ÁREA DE HACIENDA Y PROMOCIÓN ECONÓMICA, REGISTRO. SECRETARÍA-INTERVENCIÓN, URBANISMO)				
Control de acceso	Acceso mediante usuario y contraseña.	Bajo	Comprobar que existen mecanismos para verificar que la contraseña es segura y que se cambia periódicamente.	Muy bajo
Accesos no autorizados	Se ha implementado un sistema que impide los intentos reiterados no autorizados	Bajo	Comprobar que el sistema avise al RT de los intentos no autorizados.	Muy bajo
Transmisión de datos	La aplicación permite transmitir los datos encriptados	Bajo	Asegurarse de que exista un protocolo para encriptar los datos en las transmisiones de información.	Muy bajo
Registro de accesos	Se registran los accesos mediante una aplicación informática	Muy bajo	Asegurarse de que exista un procedimiento para acceder a los registros en caso de incidencias.	Muy bajo
VIDEOVIGILANCIA				
Control de acceso	Acceso mediante usuario y contraseña.	Bajo	Comprobar que existen mecanismos para verificar que la contraseña es segura y que se cambia periódicamente.	Muy bajo
Accesos no autorizados	Se ha implementado un sistema que impide los intentos reiterados no autorizados	Bajo	Comprobar que el sistema avise al RT de los intentos no autorizados.	Muy bajo
Transmisión de datos	No se transmiten datos desde la aplicación	Muy bajo	Asegurarse que No se transmiten datos desde la aplicación.	Muy bajo
Registro de accesos	Se registran los accesos mediante una aplicación informática	Muy bajo	Asegurarse de que exista un procedimiento para acceder a los registros en caso de incidencias.	Muy bajo

Hardware

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
PC ADMINISTRACIÓN (ADMINISTRACIÓN. ÁREA DE SERVICIOS MUNICIPALES)				
Control de acceso	Usuario y contraseña personalizados.	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos informáticos.	Muy bajo
Actualización de software	Se actualiza periódicamente a las últimas versiones disponibles.	Bajo	Comprobar que se actualicen periódicamente los sistemas operativos y las aplicaciones informáticas con las últimas versiones disponibles.	Muy bajo
Sistemas de protección	Se han instalado sistemas de protección (antivirus, antispam...).	Bajo	Comprobar que se hayan implementado sistemas adecuados de detección de intrusos y de prevención de fuga de información.	Muy bajo
PC ALCALDIA (ALCALDÍA)				
Control de acceso	Usuario y contraseña personalizados.	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos informáticos.	Muy bajo

Actualización de software	Se actualiza periódicamente a las últimas versiones disponibles.	Bajo	Comprobar que se actualicen periódicamente los sistemas operativos y las aplicaciones informáticas con las últimas versiones disponibles.	Muy bajo
Sistemas de protección	Se han instalado sistemas de protección (antivirus, antispam...).	Bajo	Comprobar que se hayan implementado sistemas adecuados de detección de intrusos y de prevención de fuga de información.	Muy bajo
PC SECRETARIA (REGISTRO. SECRETARÍA-INTERVENCIÓN)				
Control de acceso	Usuario y contraseña personalizados.	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos informáticos.	Muy bajo
Actualización de software	Se actualiza periódicamente a las últimas versiones disponibles.	Bajo	Comprobar que se actualicen periódicamente los sistemas operativos y las aplicaciones informáticas con las últimas versiones disponibles.	Muy bajo
Sistemas de protección	Se han instalado sistemas de protección (antivirus, antispam...).	Bajo	Comprobar que se hayan implementado sistemas adecuados de detección de intrusos y de prevención de fuga de información.	Muy bajo
Smartphone (ALCALDÍA)				
Control de acceso	Usuario y contraseña personalizados.	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos informáticos.	Muy bajo
Actualización de software	Se actualiza periódicamente a las últimas versiones disponibles.	Bajo	Comprobar que se actualicen periódicamente los sistemas operativos y las aplicaciones informáticas con las últimas versiones disponibles.	Muy bajo
Sistemas de protección	Se han instalado sistemas de protección (antivirus, antispam...).	Bajo	Comprobar que se hayan implementado sistemas adecuados de detección de intrusos y de prevención de fuga de información.	Muy bajo
Smartphone (ÁREA DE HACIENDA Y PROMOCIÓN ECONÓMICA)				
Control de acceso	Usuario y contraseña personalizados.	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos informáticos.	Muy bajo
Actualización de software	Se actualiza periódicamente a las últimas versiones disponibles.	Bajo	Comprobar que se actualicen periódicamente los sistemas operativos y las aplicaciones informáticas con las últimas versiones disponibles.	Muy bajo
Sistemas de protección	Se han instalado sistemas de protección (antivirus, antispam...).	Bajo	Comprobar que se hayan implementado sistemas adecuados de detección de intrusos y de prevención de fuga de información.	Muy bajo
Smartphone (ADMINISTRACIÓN. ÁREA DE SERVICIOS MUNICIPALES)				
Control de acceso	Usuario y contraseña personalizados.	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos informáticos.	Muy bajo
Actualización de software	Se actualiza periódicamente a las últimas versiones disponibles.	Bajo	Comprobar que se actualicen periódicamente los sistemas operativos y las aplicaciones informáticas con las últimas versiones disponibles.	Muy bajo

Ayuntamiento de Quatretondeta
Plaça Constitució, 8 - 03811 Alicante (Alacant)

Sistemas de protección	Se han instalado sistemas de protección (antivirus, antispam...).	Bajo	Comprobar que se hayan implementado sistemas adecuados de detección de intrusos y de prevención de fuga de información.	Muy bajo
Smartphone (REGISTRO. SECRETARÍA-INTERVENCIÓN)				
Control de acceso	Usuario y contraseña personalizados.	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos informáticos.	Muy bajo
Actualización de software	Se actualiza periódicamente a las últimas versiones disponibles.	Bajo	Comprobar que se actualicen periódicamente los sistemas operativos y las aplicaciones informáticas con las últimas versiones disponibles.	Muy bajo
Sistemas de protección	Se han instalado sistemas de protección (antivirus, antispam...).	Bajo	Comprobar que se hayan implementado sistemas adecuados de detección de intrusos y de prevención de fuga de información.	Muy bajo

Mobiliario

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
ARM SERVICIOS MUNICIPALES (ADMINISTRACIÓN. ÁREA DE SERVICIOS MUNICIPALES)				
Control de acceso	Cerrado sin mecanismo de seguridad.	Bajo	Se deberán emplear mecanismos que dificulten e impidan el acceso a personal no autorizado mediante llaves u otros dispositivos similares.	Muy bajo

SEGURIDAD DESDE EL DISEÑO Y POR DEFECTO

CONFIDENCIALIDAD DE LA INFORMACIÓN

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
Información del tratamiento al interesado				
¿Se informa al interesado de los detalles del tratamiento?	Sí, con cláusulas personalizadas de protección de datos.	Bajo	Asegurarse de que se facilite la información específica del tratamiento de forma clara y transparente.	Muy bajo
¿Se informa al interesado de los derechos que le asisten?	Sí, con cláusulas personalizadas de protección de datos.	Bajo	Asegurarse de que se facilite la información de todos los derechos que asisten al interesado.	Muy bajo
Contratos con los intervinientes en el tratamiento				
El personal autorizado para tratar datos, ¿se ha comprometido a respetar la confidencialidad de los mismos?	SÍ, EXISTE un procedimiento para que el personal firme el compromiso de confidencialidad.	Bajo	Comprobar que se hayan firmado todos los compromisos de confidencialidad con el personal autorizado.	Muy bajo
¿Se suscriben contratos con los encargados del tratamiento?	SÍ, EXISTE un procedimiento para que los encargados del tratamiento firmen contratos conforme el art. 28 GDPR.	Bajo	Comprobar que se hayan firmado todos los contratos con los encargados del tratamiento.	Muy bajo
¿Se suscriben contratos cuando nosotros actuamos como encargados del tratamiento?	SÍ, EXISTE un procedimiento para que los responsables del tratamiento firmen contratos conforme al art. 28 GDPR.	Bajo	Comprobar que se hayan firmado todos los contratos con los responsables del tratamiento.	Muy bajo
Transporte y transmisión de datos				
Transporte de los soportes dentro de la empresa	Por personal autorizado por el Responsable del tratamiento con medidas de seguridad.	Bajo	Se deberá llevar un control actualizado del personal autorizado y que garantice que las medidas de seguridad son adecuadas.	Muy bajo
Transporte de los soportes fuera de la empresa	Por personal autorizado por el Responsable del tratamiento con medidas de seguridad.	Bajo	Se deberá llevar un control actualizado del personal autorizado y que garantice que las medidas de seguridad son adecuadas.	Muy bajo
Procedimientos con datos automatizados (digital)				
Acceso durante el tratamiento digital (pantallas)	Se tratan impidiendo la visión de los datos a personas no autorizadas.	Bajo	Asegurarse de que se tomen medidas de seguridad que impidan la visión de la información a personas no autorizadas.	Muy bajo
Almacenamiento de los soportes digitales	Se guardan en un Mobiliario y/o Departamento con medidas de seguridad.	Bajo	Asegurarse de que las medidas de seguridad adoptadas sean adecuadas.	Muy bajo
Destrucción de soportes digitales	Destructora de soportes digitales.	Bajo	Asegurarse de que el personal use la destructora cuando se desea eliminar información.	Muy bajo
Procedimientos con datos no automatizados (documentos)				

Acceso durante el tratamiento manual (documentos)	Se tratan impidiendo el acceso a los datos a personas no autorizadas.	Bajo	Asegurarse de que se tomen medidas de seguridad que impidan la visión de la información a personas no autorizadas.	Muy bajo
Almacenamiento de documentos	Se guardan en un Mobiliario y/o Departamento con medidas de seguridad.	Bajo	Asegurarse de que las medidas de seguridad adoptadas sean adecuadas.	Muy bajo
Destrucción de documentos	Destructora de papel.	Bajo	Asegurarse de que el personal use la destructora cuando se desea eliminar información.	Muy bajo
Otras medidas de seguridad				
¿Se lleva un registro de accesos a categorías especiales de datos?	Sí, mediante una aplicación informática.	Bajo	Asegurarse de que exista un procedimiento para acceder a los registros en caso de incidencias.	Muy bajo
¿Se cifran los datos personales cuando salen de las instalaciones de la organización?	Nunca salen datos de las instalaciones de la organización.	Bajo	Asegurarse de que nunca salen datos personales de las instalaciones en dispositivos externos.	Muy bajo

SISTEMAS DE INFORMACIÓN

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
Acceso a equipos informáticos				
Control de acceso a equipos informáticos	Usuario y contraseña personalizados.	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos informáticos.	Muy bajo
Control de acceso a ficheros con datos personales	Acceso a los ficheros y/o programa mediante contraseña.	Bajo	Se deberá llevar un control actualizado del personal con acceso a las aplicaciones informáticas.	Muy bajo
Otros tipos de acceso a equipos informáticos	Ninguno	Muy bajo	Asegurarse que no existe ningún otro sistema de acceso.	Muy bajo
Medidas alternativas				
Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, las cuales se encuentran descritas en los documentos que conforman la política de protección de datos y seguridad de la información de nuestra entidad.				
Acceso a redes informáticas				
Acceso directo a los sistemas de información (conexión de red)	Usuario y contraseña personalizados.	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos informáticos.	Muy bajo
Acceso inalámbrico a los sistemas de información (Wifi, Bluetooth, etc.)	Acceso restringido por clave de seguridad.	Bajo	Cambiar la clave de seguridad ofrecida por el proveedor para evitar que sea usada por personas no autorizadas.	Muy bajo
Acceso remoto a los sistemas de información	Usuario y contraseña personalizados.	Bajo	Se deberá llevar un control actualizado del personal con acceso remoto a los sistemas.	Muy bajo
Cifrado de las conexiones remotas	Sí.	Bajo	Comprobar que la conexión remota esté cifrada punto a punto.	Muy bajo

Sistema de identificación y autenticación				
Sistema de identificación (USUARIO)	Palabra identificativa y personalizada para cada usuario.	Bajo	Se deberá llevar un control actualizado del personal con acceso a los equipos informáticos.	Muy bajo
Sistema de autenticación (CONTRASEÑA)	Contraseña personalizada para cada usuario.	Bajo	Comprobar que existen mecanismos para verificar que la contraseña es segura y que se cambia periódicamente.	Muy bajo
Cifrado de la contraseña	La contraseña está cifrada	Bajo	Comprobar que el cifrado de la contraseña no pueda descifrarse.	Muy bajo
Combinación de caracteres	La contraseña se compone al menos de 8 caracteres, con algún número, mayúscula, minúscula y símbolo o carácter especial	Bajo	Comprobar que el sistema no deje guardar una contraseña insegura.	Muy bajo
Intentos reiterados de acceso	Se ha implementado un sistema que impide los intentos reiterados no autorizados	Bajo	Comprobar que el sistema avise al RT de los intentos no autorizados.	Muy bajo
Caducidad de la contraseña	La contraseña se cambia al menos una vez al año	Bajo	Comprobar que el sistema obligue a cambiar la contraseña periódicamente.	Muy bajo
Almacenamiento de la contraseña	Se memorizan, sin guardarlas en ningún dispositivo, archivo o documento físico.	Bajo	Comprobar que no se almacenan ni en soporte papel ni digital.	Muy bajo
Recuperación de la contraseña	Envío automático de credenciales al correo electrónico/número de teléfono/SMS que identifica al usuario.	Bajo	Comprobar que se envía la nueva contraseña, cuando se solicita la recuperación de la misma.	Muy bajo

INTEGRIDAD DE LA INFORMACIÓN

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
Copias de respaldo				
Ubicación de las copias	Se guardan en un Hardware distinto del que las crea (copia de red).	Bajo	Se deberá llevar un control actualizado del personal con acceso a las copias de seguridad.	Muy bajo
Periodicidad de programación	Semanalmente, como mínimo.	Bajo	Comprobar que se realizan las copias, al menos semanalmente.	Muy bajo
Periodicidad de comprobación de datos	Como máximo, 6 meses desde la creación.	Bajo	Verificar que se realicen las comprobaciones, al menos semestralmente.	Muy bajo
Método de comprobación de datos	Aplicación informática de verificación de copias.	Bajo	Comprobar que la verificación de copias contenga los datos copiados.	Muy bajo
Copias de respaldo externas				
Ubicación de las copias externas	Servicios Backup de Internet.	Bajo	Asegurarse de que los servicios de internet tengan implementadas medidas adecuadas de protección de datos.	Muy bajo
Periodicidad de programación de las copias externas	Semanalmente, como mínimo.	Bajo	Comprobar que se realizan las copias, al menos semanalmente.	Muy bajo
Cifrado de los datos de las copias externas	Sí.	Bajo	Asegurarse de que exista un protocolo para encriptar los datos.	Muy bajo
Disponibilidad de los datos				

Actualización de *software*	SE ACTUALIZAN periódicamente los sistemas operativos y las aplicaciones informáticas con las últimas versiones disponibles	Bajo	Comprobar que se actualicen periódicamente los sistemas operativos y las aplicaciones informáticas con las últimas versiones disponibles.	Muy bajo
Sistemas de detección de intrusos y prevención de fuga de información	EXISTEN sistemas de protección tipo firewall, antivirus, antispam, antiphishing, antimalware, antiransomware, etc.	Bajo	Comprobar que se hayan implementado sistemas adecuados de detección de intrusos y de prevención de fuga de información.	Muy bajo
Disponibilidad de los servicios de información	EXISTEN medidas para garantizar la disponibilidad de los datos	Bajo	Comprobar que las medidas implementadas garanticen la disponibilidad de los datos (copias de respaldo, antivirus, SAI, etc.)	Muy bajo
Restauración de los servicios de información	EXISTEN medidas para restaurar rápidamente la disponibilidad y el acceso a los datos	Bajo	Comprobar que las medidas implementadas garanticen la restauración de la disponibilidad y el acceso a los datos.	Muy bajo
Resiliencia de los servicios de información	EXISTEN medidas para anticiparse y adaptarse a cambios imprevistos en los servicios de información	Bajo	Asegurarse de que exista un protocolo para anticiparse y adaptarse a cambios imprevistos en los servicios de información.	Muy bajo
Procesos de verificación, evaluación y valoración de las medidas de seguridad	SE HAN ESTABLECIDO procesos para verificar, evaluar y valorar la eficacia de las medidas de seguridad	Bajo	Asegurarse de que exista un protocolo para verificar, evaluar y valorar la eficacia de las medidas de seguridad.	Muy bajo

TRATAMIENTOS ESPECÍFICOS

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
Tratamientos específicos				
Tratamiento de datos de niños menores de 14 años	Se tratan datos OCASIONALMENTE de niños menores de 14 años	Bajo	Se deben analizar los riesgos del tratamiento para determinar si existe un alto riesgo para los derechos y libertades de los interesados.	Muy bajo
Tratamiento de datos de personas en situación de vulnerabilidad	Se tratan datos HABITUALMENTE de personas en situación de vulnerabilidad y NO EXISTE riesgo para sus derechos y libertades	Bajo	Se deben analizar los riesgos del tratamiento para determinar si existe un alto riesgo para los derechos y libertades de los interesados.	Muy bajo
Tratamiento de datos que puede invadir la intimidad de las personas	Se tratan datos OCASIONALMENTE que pueden invadir la intimidad de las personas	Bajo	Se deben analizar los riesgos del tratamiento para determinar si existe un alto riesgo para los derechos y libertades de los interesados.	Muy bajo
Vulneración de los derechos y libertades fundamentales	NO SE REALIZAN tratamientos que vulneren los derechos o libertades fundamentales	Muy bajo	Asegurarse que NO SE REALIZAN tratamientos que vulneren los derechos o libertades fundamentales.	Muy bajo
Medidas alternativas				

INTERNET

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
Comunicaciones electrónicas				
Correo electrónico	SE UTILIZA correo electrónico seguro mediante cifrado punto a punto.	Muy bajo	Comprobar que el servidor de correo utiliza un cifrado SSL/TLS para la transmisión de mensajes.	Muy bajo

Mensajería instantánea	NO SE ENVÍA mensajería instantánea para comunicarse con los interesados.	Muy bajo	Comprobar que no se utiliza ninguna mensajería instantánea para la comunicación con los interesados.	Muy bajo
Videoconferencia	SE UTILIZA un sistema de videoconferencia segura mediante cifrado punto a punto.	Muy bajo	Comprobar que el servicio de videoconferencia utiliza un cifrado SSL/TLS para comunicarse con los interesados.	Muy bajo
Software profesional (business)	SE UTILIZA software profesional para realizar comunicaciones electrónicas.	Muy bajo	Comprobar que el software utilizado para las comunicaciones electrónicas tiene una cuenta corporativa o profesional, o sea, que no se utilizan cuentas personales para comunicarse.	Muy bajo
Cláusula de protección de datos	SE HA PUBLICADO una cláusula de protección de datos con información adecuada del tratamiento.	Muy bajo	Comprobar que la cláusula de protección de datos contiene el nombre del responsable y DPO si existe, el fin y legitimación del tratamiento, los criterios de conservación de los datos, la comunicación a terceros, los derechos que asisten al usuario y los datos de contacto para ejercer los derechos.	Muy bajo
Cláusula de publicidad	NO SE ENVÍAN comunicados comerciales, por lo que no se requiere publicar ninguna cláusula de publicidad.	Muy bajo	Comprobar que no se envían comunicados comerciales que puedan considerarse publicitarios.	Muy bajo
Página web				
Certificado de seguridad web (https)	SE HA INSTALADO un certificado de seguridad (SSL/TLS).	Muy bajo	Comprobar que existe un candado a la izquierda de la dirección URL y que esta tiene el prefijo «https» en lugar de «http».	Muy bajo
Avisos legales	SE HA PUBLICADO un aviso legal con la información adecuada y accesible desde cualquier lugar del sitio web.	Muy bajo	Comprobar que el aviso legal contiene los datos identificativos del responsable de la web, los derechos de propiedad intelectual e industrial, la exención de responsabilidades por el uso de cookies, política de enlaces, direcciones IP y la ley aplicable y jurisdicción.	Muy bajo
Política de privacidad	SE HA PUBLICADO una Política de privacidad con la información adecuada y accesible desde cualquier lugar del sitio web.	Muy bajo	Comprobar que la política de privacidad contiene el nombre del responsable y DPO si existe, el fin y legitimación del tratamiento, los criterios de conservación de los datos, la comunicación a terceros, los derechos que asisten al usuario y los datos de contacto para ejercer los derechos, el carácter obligatorio o facultativo de la información facilitada por el usuario y las medidas de seguridad implementadas para la protección de datos.	Muy bajo
Formularios para la obtención de datos	SE INFORMA adecuadamente del tratamiento de datos personales previo al envío del formulario.	Muy bajo	Comprobar que se informa adecuadamente del tratamiento según lo dispuesto en los art. 13 y 14 GDPR previo al envío del formulario.	Muy bajo

Política de cookies	SE INFORMA adecuadamente del tratamiento de datos y de las cookies utilizadas.	Bajo	Comprobar que se ha publicado la información sobre las cookies, el tratamiento de datos, el listado de cookies utilizadas (nombre, tipo, propietario, finalidad y vencimiento), sobre cómo revocar el consentimiento y cómo eliminar las cookies del navegador.	Muy bajo
Banner para obtener el consentimiento de cookies	SE OBTIENE el consentimiento y SE INFORMA adecuadamente del tratamiento de datos personales previo a la instalación de cookies.	Muy bajo	Comprobar que se informa adecuadamente sobre las cookies prescindibles (analíticas, publicitarias, etc.) que se pretende instalar y que no se instalan antes de obtener el consentimiento.	Muy bajo
Otros servicios de Internet				
Comercio electrónico	NO SE REALIZAN transacciones comerciales mediante una pasarela de pago o TPV virtual.	Muy bajo	Asegurarse que no existe e-comerce.	Muy bajo
Redes sociales	NO EXISTE cuenta en ninguna red social.	Muy bajo	Asegurarse que no tiene cuentas abiertas en RRSS	Muy bajo
App	NO EXISTE ninguna app.	Muy bajo	Asegurarse que NO EXISTE ninguna app.	Muy bajo

ORGANIZACIÓN

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
Organización				
Política de información	EXISTE un protocolo documentado para informar y comunicar el tratamiento al interesado	Bajo	Comprobar periódicamente que haya un responsable de actualizar el protocolo y de hacer que se cumpla.	Muy bajo
Derechos del interesado	EXISTE un protocolo documentado para gestionar y registrar los derechos del interesado	Bajo	Comprobar periódicamente que haya un responsable de actualizar el protocolo y de hacer que se cumpla.	Muy bajo
Política de seguridad	EXISTE un protocolo documentado para garantizar la seguridad de los datos personales y su protección desde el DISEÑO Y POR DEFECTO	Bajo	Comprobar periódicamente que haya un responsable de actualizar el protocolo y de hacer que se cumpla.	Muy bajo
Formación en protección de datos	[Se facilita suficiente formación al personal autorizado para tratar datos] mediante la publicación de la política de seguridad	Bajo	Comprobar que se facilite suficiente formación al personal autorizado para tratar datos mediante la publicación de la política de seguridad.	Muy bajo
Violaciones de la seguridad	EXISTE un protocolo documentado para gestionar y registrar las violaciones de la seguridad	Bajo	Comprobar periódicamente que haya un responsable de actualizar el protocolo y de hacer que se cumpla.	Muy bajo
Evaluación de impacto (DPIA)	[No precisa realizar una DPIA porque] el tratamiento no comporta un alto riesgo para los derechos y libertades de las personas físicas.	Bajo	Asegurarse de que el tratamiento no comporte un alto riesgo para los derechos y libertades de las personas físicas.	Muy bajo
Delegado de protección de datos (DPO)	[Se ha designado un DPO] porque la empresa es una autoridad u organismo PÚBLICO	Bajo	Comprobar que se haya designado un DPO y que su contrato sea vigente.	Muy bajo

6 AMENAZAS

1. CUMPLIMIENTO NORMATIVO

No existen riesgos en los recursos utilizados

2. ORGANIZACIÓN

No existen riesgos en los recursos utilizados

3. RECURSOS

Software

Concepto	Aplicación	Riesgo inicial	Medidas	Riesgo final
Ayuntamiento en la nube (ADMINISTRACIÓN. ÁREA DE SERVICIOS MUNICIPALES, ALCALDÍA, ÁREA DE HACIENDA Y PROMOCIÓN ECONÓMICA, REGISTRO. SECRETARÍA-INTERVENCIÓN, URBANISMO)				
Accesos no autorizados	No existe un control de accesos no autorizados a la aplicación	Medio	Plantearse la necesidad de activar mecanismos que impidan los intentos reiterados no autorizados.	Bajo
Registro de accesos	No existe un registro de accesos a la aplicación y accede más de un usuario	Medio	Cuando se traten categorías de datos ESPECIALES o PENALES es recomendable registrar los accesos de los usuarios al programa.	Bajo

SEGURIDAD DESDE EL DISEÑO Y POR DEFECTO

No existen riesgos en los recursos utilizados

Oficina Provincial de Protección de Datos