CONCELLO DE AVIÓN, Pza. do Concello, 1, 32520, Avión, Ourense. Tlfn: 988 486 000
datos@concelloavion.org www.concelloavion.org

REGISTRO DE ACTIVIDAD DE TRATAMIENTO VIDEOVIGILANCIA DEL CONCELLO DE AVIÓN

<table>
<tr><td>RESPONSABLE Y DPD</td><td>Responsable: CONCELLO DE AVIÓN., con C.I.F.: P-3200500A
Dirección: Pza. do Concello, 1, 32520, Avión, Ourense
Teléfono: 988 486 000
Correo Electrónico: datos@concelloavion.org
Delegado en Protección de Datos: ARIAS AVOGADOS S.C.
N.I.F: J-42.739.680
Dirección: Rúa da Concordia nº1 Entlo A-B, 32003, Ourense
Teléfono: 988 609 224
Correo Electrónico: protecciondedatos@ariasavogados.com</td></tr>
<tr><td>BASE JURÍDICA</td><td>-RGPD: 6.1.c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.
-RGPD: art 6.1 d) El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física.</td></tr>
<tr><td>FINALIDAD TRATAMIENTO</td><td>EL CONCELLO DE AVIÓN llevará a cabo el tratamiento de datos con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones (Art. 22 LOPDGDD 3/2018)
-No existirán decisiones automatizadas ni se elaborarán perfiles a partir del tratamiento de sus datos.</td></tr>
<tr><td>COLECTIVO</td><td>Habitantes, trabajadores y demás personal del Concello de Avión</td></tr>
<tr><td>CATEGORÍA DE DATOS</td><td>Datos identificativos: imagen. Interés legítimo del responsable, Imagen, características personales e inequívocas que permiten identificar al colectivo.</td></tr>
<tr><td>DESTINATARIOS</td><td>No se cederán las imágenes captadas salvo por imperativo legal</td></tr>
<tr><td>TRANSFERENCIA INTERNACIONAL</td><td>-No están previstas transferencias internacionales de los datos</td></tr>
<tr><td>PLAZO DE CONSERVACIÓN</td><td>Las imágenes captadas por las cámaras de videovigilancia del CONCELLO DE AVIÓN, se conservarán durante un plazo máximo de 30 días, finalizado el mismo, se procederá a su destrucción.</td></tr>
<tr><td>MEDIDAS DE SEGURIDAD</td><td>
<table>
<tr><th colspan="2">PROTECCIÓN DE LA INFORMACIÓN</th></tr>
<tr><th colspan="2">DISPONIBILIDAD</th></tr>
<tr><td>Pérdida o borrado no intencionado de datos personales</td><td>Copias de Seguridad.
Almacenamiento en dos ubicaciones diferentes</td></tr>
<tr><th colspan="2">CONFIDENCIALIDAD</th></tr>
<tr><td>Acceso no autorizado a los datos personales</td><td>Mecanismo de control de acceso.
Segmentación de la red</td></tr>
<tr><td>Información al interesado del tratamiento</td><td>Si: Cláusulas informativas, consentimiento expreso, 1ª y 2ª capa (responsable, finalidad, destinatarios, procedencia y derechos).</td></tr>
<tr><td>Información al interesado de sus derechos</td><td>Si: Cláusulas informativas, consentimiento expreso, formulario de ejercicio derechos disponible dos vías.</td></tr>
<tr><td>Transporte de soportes con datos dentro de la empresa</td><td>Por personal autorizado por el Responsable, con medidas de seguridad.</td></tr>
<tr><td>Transporte de soporte con datos fuera de la empresa</td><td>Por personal autorizado por el Responsable, con medidas de seguridad.</td></tr>
<tr><td>Acceso durante el tratamiento digital</td><td>Se impide el acceso y visión de los datos a personas no autorizadas</td></tr>
<tr><td>Acceso durante el tratamiento manual de datos</td><td>Se tratan impidiendo el acceso a los datos por personas no autorizadas.</td></tr>
<tr><td>Almacenamiento de datos en soporte físico</td><td>En mobiliario y oficina mediante medidas de seguridad, llave, control presencial.</td></tr>
<tr><td>Destrucción de los datos en soporte manual</td><td>Una vez no se utilizan, bien finalización de la relación profesional o por baja comunicada, siempre que haya expirado la obligación legal de conservación. Destrucción del propio soporte físico (quema de papel) eliminado así los datos e impidiendo cualquier acceso ilegítimo.</td></tr>
<tr><td>Control de acceso a equipos informáticos</td><td>Usuario y contraseña personalizados, con registro de accesos.</td></tr>
<tr><td>Acceso directo a conexión red</td><td>Usuario y contraseña, cambio periódico.</td></tr>
<tr><td>Acceso inalámbrico a red (wi-</td><td>Usuario y contraseña, no se facilita a terceros.</td></tr>
</table>
</td></tr>
</table>

fi, bluetooth…)	
Acceso remoto	Nunca
Sistema de identificación	Usuario exclusivo y personal.
Sistema de identificación	Contraseña personalizada para cada usuario, personal, intransferible, cifrada y que contenga al menos 8 caracteres, con algún número, mayúscula y minúscula.
INTEGRIDAD DE LA INFORMACIÓN	
Copias de seguridad	Diaria
CUMPLIMIENTO NORMATIVO	
Ausencia de procedimientos de ejercicio de los derechos de los interesados	Procedimientos y canales para el ejercicio de derechos: formulario disponible al interesado en formato físico y por correo electrónico.
Ausencia de legitimidad para el tratamiento de los datos personales	Cláusulas informativas y base legitimadora para el tratamiento de datos: formulario de consentimiento expreso, físicamente y por correo electrónico. Prestación de servicios y ejecución de contrato.
Tratamiento ilícito de datos personales	Monitorización del uso de datos personales.