



AYUNTAMIENTO DE GUARDAMAR DEL SEGURA

Información común a todos los tratamientos

| INFORMACIÓN | DESCRIPCIÓN GENERAL | | |
|---|--|---|--|
| Responsable de los tratamientos | Ayuntamiento de Guardamar del Segura Plaza de la Constitución, n.º 5 03140 Guardamar del Segura, Alicante Tel.: +34 965 72 90 14 | | |
| Delegado de Protección de Datos) | Miguel Angel Díaz Pintado Plaza de la Constitución, n.º 5 03140 Guardamar del Segura, Alicante Tel.: +34 965 72 90 14 email: protecciondatos@guardamardelsegura.es | | |
| Establecimiento Principal | Según el <i>Artículo 4, Definiciones</i> del Reglamento General de Protección de Datos, RGPD: <i>16) «establecimiento principal»:</i> <i>a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;</i> Siendo el Ayuntamiento de Guardamar del Segura una entidad pública de la administración local, no tiene establecimientos en otros países fuera de España y, por lo tanto, no existe el concepto de Establecimiento Principal | | |
| Transferencias a países terceros | No se realizan transferencias de datos a países terceros en ninguno de los tratamientos del Responsable | | |
| Autoridad de Control | Agencia Española de Protección de Datos www.aepd.es | | |
| ANÁLISIS DE RIESGOS | | | |
| Información común a todos los tratamientos | | | |
| Metodología 1 | MAGERIT, Método de Análisis y Gestión de Riesgos de las Tecnologías de la Información | | |
| Metodología 2 | Agencia Española de Protección de Datos, AEPD Guía Práctica de Análisis de Riesgos en los tratamientos de datos personales sujetos al RGPD | | |
| Metodología 3 | Esquema Nacional de Seguridad, ENS Centro Criptológico Nacional, CCN Guía de Seguridad CCN-STIC-803, Valoración de los Sistemas | | |
| Escala de Valoración Magerit Impacto y Probabilidad | Impacto | Valor | Probabilidad |
| | Muy Alto Alto Medio Bajo Muy Bajo | MA A MM B MB | Segura Probable Posible Poco Probable Muy rara |



| Escala de Valoración Magerit Riesgos (EVM) | probabilidad | | | | | |
|--|---|-----------|----------|----------|----------|-----------|
| | | MB | B | M | A | MA |
| Impacto | MA | A | MA | MA | MA | MA |
| | A | M | A | A | MA | MA |
| | M | B | M | M | A | A |
| | B | MB | B | B | M | M |
| | MB | MB | MB | MB | B | B |
| Escala de Valoración Esquema Nacional de Seguridad (ENS) (EV-ENS) | <p>Nivel ALTO:</p> <ul style="list-style-type: none"> Sólo debe tratarla un número muy reducido de personas Por disposición legal o administrativa Su revelación, alteración, falsedad, incapacidad para conocer los accesos, o no disponibilidad causaría daños de difícil reparación, o el incumplimiento grave de una norma, o pérdidas económicas elevadas, o daño reputacional grave a las personas o a la corporación, o alteraciones del orden público <p>Nivel MEDIO:</p> <ul style="list-style-type: none"> Sólo debe tratarla quienes lo necesiten para su trabajo, con autorización Su revelación, alteración, falsedad, incapacidad para conocer los accesos, o no disponibilidad causaría daños importantes subsanables, o el incumplimiento formal de una norma, o pérdidas económicas importantes, o daño reputacional importante a las personas o a la corporación, o dar lugar a protestas públicas <p>Nivel BAJO:</p> <ul style="list-style-type: none"> No deben tratarla personas ajenas a la unidad Su revelación, alteración, falsedad, incapacidad para conocer los accesos, o no disponibilidad causaría daños o algún perjuicio, o el incumplimiento leve de una norma, o pérdidas económicas apreciables, o daño reputacional apreciable a las personas o a la corporación, o dar lugar a protestas individuales <p>SV (sin valor, en blanco)</p> <ul style="list-style-type: none"> Información de carácter accesible y tratable por cualquier persona | | | | | |
| Dimensiones de Seguridad que se evalúan | <p>D Disponibilidad I Integridad C Confidencialidad A Autenticidad T Trazabilidad</p> | | | | | |
| Clasificación de la información ISO 27001 (en negrita nivel asignado) | <ul style="list-style-type: none"> Secreta Reservada Confidencial Difusión Limitada Sin clasificar | | | | | |
| Medidas Técnicas y de Seguridad | | | | | | |
| Medidas Técnicas y de Seguridad generales | Las medidas generales se describen en la Declaración de Aplicabilidad , documento <i>D05DeclaracióndeAplicabilidad</i> | | | | | |
| Medidas Técnicas y de Seguridad específicas | Si en los tratamientos se aplicaran medidas técnicas y de seguridad específicas y exclusivas, se documentarán en su ficha de tratamiento correspondiente | | | | | |