

TÍTULO DEL PROYECTO:

Gobernanza desde la proximidad: “El día con el Delegado”



CANDIDATO: Antoni Herráez Pizarro 
Delegado de Protección de Datos (CDPD)

ENTIDAD: Ayuntamiento de Santa Coloma de Gramenet (Barcelona)

Diciembre de 2025

ÍNDICE DE CONTENIDOS

| | Página |
|---|--------|
| 1. RESUMEN DEL PROYECTO | 3 |
| 2. INTRODUCCIÓN Y JUSTIFICACIÓN: EL DPD EN ENTORNOS DE ALTA COMPLEJIDAD SOCIAL | 4 |
| 2.1. El contexto de Santa Coloma de Gramenet | |
| 2.2. Realidad Presupuestaria: El dato como activo financiero | |
| 2.3 La Singularidad Municipal: El Responsable de Tratamiento "Total" | |
| 2.4 La problemática concreta a gestionar: El DPD como figura distante | |
| 3. OBJETIVOS DEL PROYECTO | 6 |
| 3.1. Objetivo Cultural: Humanizar el cumplimiento. | |
| 3.2. Objetivo Operativo: La transición al modelo "Posibilista". | |
| 3.3. Objetivo Estratégico: Integración orgánica | |
| 4. METODOLOGÍA DE INTERVENCIÓN: «EL DÍA CON EL DELEGADO» | 7 |
| 4.1. Concepto: Invertir la carga del desplazamiento. | |
| 4.2. Dinámica de las sesiones: "Fuego Real" y con ausencia de guion. | |
| 4.3. El paradigma del DPD "Posibilista": Vehicular la necesidad de gestión. | |
| 4.4. Hibridación de perfiles: Privacidad (RGPD) + Ciberseguridad (ENS). | |
| 5. IMPACTO SECTORIAL (RESULTADOS TÁCTICOS) | 10 |
| 5.1. Servicios Sociales: Seguridad jurídica en la urgencia. | |
| 5.2. Seguridad Ciudadana: Tecnología policial, videovigilancia y cooperación judicial | |
| 5.3. Atención a la Ciudadanía: La primera línea | |
| 5.4 Padrón Municipal de Habitantes: La llave de los servicios públicos | |
| 5.5 Recursos y Prestaciones: Dignidad y datos | |
| 5.6 Deportes: La energía que mueve datos | |
| 5.7 Transparencia y Buen Gobierno | |
| 6. IMPACTO ORGANIZATIVO (RESULTADOS ESTRATÉGICOS) | 15 |
| 6.1. La conquista de la confianza de la Dirección de Tecnología. | |
| 6.2. La alianza preventiva con la Comunicación Institucional. | |
| 6.3. <i>Privacy by Design</i> como estándar de calidad. | |
| 7. INDICADORES Y MÉTRICAS DE ÉXITO | 16 |
| 7.1 Métricas de Alcance y Capilaridad | |
| 7.2 Análisis de la Evolución y Tipología de Consultas (2020-2025) | |
| 7.3 Indicadores Cualitativos: La percepción del cambio cultural. | |
| 7.4 Conclusión de los indicadores | |
| 8. INNOVACIÓN Y TRANSFERIBILIDAD DEL MODELO | 20 |
| 9. CONCLUSIONES | 20 |

1. RESUMEN DEL PROYECTO

El presente proyecto detalla la estrategia desplegada por el Delegado de Protección de Datos del Ayuntamiento de Santa Coloma de Gramenet para transformar la cultura de cumplimiento de una organización de gran tamaño sometida a una fuerte presión asistencial.

Bajo el título «**El día con el Delegado**», la iniciativa rompe con el modelo tradicional de supervisión burocrática para instaurar un modelo de **consultoría de proximidad radical**.

El DPD abandona los despachos centrales para desplazarse sistemáticamente a las unidades operativas (Policía, Servicios Sociales, Atención Ciudadana, Cultura, Deportes, etc.), resolviendo *in situ* y sin guion previo dudas sobre expedientes reales que le plantean los colectivos de trabajadores/as.

La clave del éxito del proyecto reside en el cambio de rol del DPD, que evoluciona de ser un tradicional «**Stopper**» (auditor de bloqueo) a un nuevo rol «**Posibilista**» (arquitecto de soluciones). Al entender **que los servicios tienen necesidades legítimas de tratamiento de datos para servir al ciudadano**, el DPD utiliza su doble perfil técnico-jurídico para diseñar los canales seguros que viabilicen dichas necesidades.

Como resultado directo de esta autoridad moral ganada "en la trinchera", se ha logrado que las Direcciones en general del Ayuntamiento, pero especialmente las de **Tecnologías de la información y la de Comunicación Corporativa** integren al DPD de manera proactiva en el diseño de nuevos proyectos, consolidando el principio de Privacidad desde el Diseño no por imposición, sino por la convicción de que será útil, no solo al principio del proyecto sino en el desarrollo y gestión del ciclo de vida total del mismo.

Es necesario subrayar una premisa fundamental: desde la óptica de la privacidad y la seguridad de la información, **un gran Ayuntamiento es posiblemente una de las empresas u organizaciones más complejas que existe**. A diferencia de la empresa privada, que se especializa en un sector, la administración local gestiona el ciclo de vida integral del ciudadano.

En Santa Coloma de Gramenet conviven **más de 100 Actividades de Tratamiento** distintas que abarcan la totalidad del espectro regulado: desde datos de infracciones penales y videovigilancia policial, hasta expedientes de protección a la infancia en riesgo, salud pública, tributos o movilidad. Se gestiona la información de colectivos extremadamente vulnerables (violencia de género, trabajadores, colectivos LGTBIQ+, ideología política, etc.) en un entorno social tensionado, lo que convierte el cumplimiento normativo no en un checklist, sino en una garantía de paz social."

El proyecto que se inició como piloto hace años, ha consolidado su metodología y alcanzado su fase de madurez y tecnificación durante el periodo 2024-2025, objeto de esta convocatoria

2. INTRODUCCIÓN Y JUSTIFICACIÓN: EL DPD EN ENTORNOS DE ALTA COMPLEJIDAD SOCIAL, ECONÓMICA Y OPERATIVA.

2.1. El contexto de Santa Coloma de Gramenet

Para comprender la magnitud del reto de cumplimiento en este Ayuntamiento, es imprescindible analizar el "ecosistema de riesgo" único en el que opera. Santa Coloma de Gramenet, situada en el corazón del área metropolitana de Barcelona, **presenta una de las densidades de población más altas de Europa y una renta per cápita situada en la franja baja de la media estatal.**

Sin embargo, el factor diferencial más crítico desde la óptica del tratamiento de datos es su extraordinaria **diversidad demográfica**. El municipio se configura como un crisol multicultural donde conviven más de un centenar de nacionalidades distintas. Esta realidad implica que la gestión del dato personal no es solo un trámite administrativo, sino un desafío de gestión de la diversidad que impacta directamente en el cumplimiento del RGPD:

- Barreras en el Deber de Información (Art. 13 RGPD): La multiplicidad de idiomas obliga a los servicios de atención (OIAC, Servicios Sociales, Policía Local, etc.) a enfrentar situaciones donde garantizar que la ciudadanía comprende qué se va a hacer con sus datos requiere ir mucho más allá de la entrega de un formulario estándar en castellano o catalán.
- Complejidad en la Identificación Administrativa: La gestión de expedientes de la ciudadanía con casuísticas documentales heterogéneas (pasaportes extracomunitarios, NIEs provisionales, situaciones de irregularidad administrativa o solicitantes de asilo) genera una presión constante sobre los sistemas de información municipales (Padrón de Habitantes, OIAC, etc.) y requiere un criterio jurídico flexible pero riguroso por parte del DPD para evitar la exclusión administrativa sin vulnerar la seguridad jurídica.
- Sensibilidad Cultural de la Privacidad: Existen concepciones dispares sobre la intimidad familiar y el intercambio de información comunitaria según el origen cultural, lo que genera fricciones operativas que, a veces, el DPD debe mediar in situ.

En consecuencia, **el Ayuntamiento no trata meros datos burocráticos; gestiona la integración, la supervivencia y la convivencia de un tejido social heterogéneo y vulnerable.**

Esto convierte al DPD en una figura esencial para garantizar que el derecho fundamental a la protección de datos se aplique de manera universal y efectiva, independientemente del origen o la situación administrativa de la persona interesada.

2.2 Realidad Presupuestaria: El dato como activo financiero.

El análisis del presupuesto municipal para el ejercicio 2025 revela una arquitectura financiera que eleva la seguridad de la información a un **nivel estratégico crítico**.

Con un presupuesto total de ingresos de 153 M€, destaca un dato revelador:

- *Las Transferencias Corrientes (Capítulo IV) ascienden aproximadamente el 57% del total de ingresos.*
- *Si sumamos las Transferencias de Capital (Capítulo VII), la dependencia de la financiación externa (Estado, Generalitat, AMB, Fondos Europeos) es mayoritaria frente a los ingresos tributarios directos (aprox. 38,5 M€).*

Esta estructura de ingresos significa que **la viabilidad del municipio depende de la confianza y la interoperabilidad con otras administraciones públicas**. La recepción de estas transferencias está condicionada al cumplimiento estricto de obligaciones legales y técnicas. El Ayuntamiento debe garantizar la disponibilidad, integridad y trazabilidad de los datos que intercambia con los organismos financiadores.

Se debe destacar que, en el actual panorama de ciberamenazas (ransomware, exfiltración de datos), un incidente de seguridad no es solo un problema técnico. Un fallo en la seguridad de la información o una sanción por incumplimiento del RGPD o del ENS no solo supone un riesgo reputacional, sino un riesgo financiero directo que podría comprometer la llegada de fondos esenciales para los servicios públicos. Por tanto, **el cumplimiento normativo (Compliance) y la adecuación al Esquema Nacional de Seguridad (RD 311/2022) no son opciones burocráticas, sino garantías de sostenibilidad económica para la ciudad.**

2.3. La Singularidad Municipal: El Responsable de Tratamiento "Total"

A menudo se compara la gestión de datos pública con la privada, pero la realidad de un Ayuntamiento como el de Santa Coloma de Gramenet desborda cualquier equivalencia corporativa.

Jurídicamente, **un Ayuntamiento seguramente es la entidad de mayor complejidad en protección de datos que existe**. El motivo radica en sus competencias (Ley de Bases de Régimen Local): la entidad está obligada a tratar datos de todas las tipologías posibles para prestar los servicios públicos esenciales.

Mientras una multinacional puede tratar datos de clientes, proveedores y empleados, este Ayuntamiento gestiona un Registro de Actividades de Tratamiento (RAT) con más de 100 finalidades distintas, donde convergen simultáneamente:

- Datos de Categorías Especiales (Art. 9 RGPD): Salud (en deportes y salubridad), ideología y afiliación (en recursos humanos o subvenciones a entidades), origen racial o étnico (en servicios sociales), etc.
- Datos Policiales y Sancionadores: Tratamientos sujetos a la Directiva 2016/680 y LO 7/2021, con videovigilancia, bodycams y gestión de delitos, etc.
- Datos de Colectivos Vulnerables: Gestionamos la información crítica de menores de edad, mujeres víctimas de violencia de género, personas en riesgo de exclusión social y personas mayores dependientes, etc.

- Datos Económicos y Patrimoniales: Gestión tributaria y recaudatoria con el mismo nivel de detalle que una entidad financiera, etc.
- Datos sobre trabajadores/as: Selección de personal, Nóminas, Prevención de riesgos laborales, formación, etc.

Por tanto, estamos hablando de un entorno de alta tensión operativa, ya que esta amalgama de datos no se gestiona en un laboratorio estanco, sino en un entorno de alta tensión social. Santa Coloma es una ciudad viva y exigente, donde la ciudadanía reclama sus derechos con inmediatez. Esto obliga al DPD a operar en un **escenario de riesgo constante**, donde el equilibrio entre la obligación de atender (competencia municipal) y la obligación de proteger (RGPD/ENS) es un desafío diario que no admite soluciones teóricas, sino prácticas y seguras.

2.4. La problemática concreta a gestionar: El DPD como figura distante.

En este contexto de urgencia, las personas que trabajan en el ayuntamiento operan bajo mucha presión. Antes de la implantación de este proyecto, existían debilidades a la operativa general que había que atender.

- El **Personal Operativo** (trabajadores/as sociales, agentes) percibían la normativa sobre protección de datos y de seguridad de la información como obstáculos burocráticos que ralentizaban la ayuda a la ciudadanía.
- Existía el riesgo de «**Shadow IT**» (Informática en la sombra): el personal público buscaba soluciones por su cuenta (ej.: uso de Apps de mensajería no corporativas) para agilizar gestiones, evitando consultar al DPD por miedo a recibir un "No" rotundo y tardío.
- El **DPD** corría el riesgo de convertirse en un validador documental, con un cumplimiento normativo perfecto sobre el papel, pero desconectado de la realidad del tratamiento de datos en la calle.

3. OBJETIVOS DEL PROYECTO

El proyecto «**El día con el Delegado**» nace con una ambición de reformar integralmente el modelo de gobernanza del dato, estableciendo tres niveles de objetivos:

3.1. Objetivo Cultural: Humanizar el cumplimiento

Transformar la percepción del DPD. Pasar de "la autoridad que fiscaliza" a "el compañero experto que soluciona". El objetivo era generar **seguridad psicológica**: que el personal público, que presta sus servicios en el ayuntamiento, prefiera preguntar una duda básica antes que cometer un error grave, eliminando el miedo a la reprobación o, peor todavía, a la sanción interna.

3.2. Objetivo Operativo: La transición al modelo "Posibilista"

Erradicar la cultura del "NO por defecto". El objetivo era implantar una metodología de trabajo donde el DPD asume la responsabilidad de buscar el camino legal y a veces técnico (ENS) para que los servicios puedan ejecutar sus políticas públicas. **Si un servicio necesita compartir un dato, el DPD no debe bloquearlo, debe blindarlo.**

3.3. Objetivo Estratégico: Integración Orgánica

Lograr que algunos de los ámbitos más expuestos a riesgos en el tratamiento de datos del Ayuntamiento — Tecnologías de la información y Comunicación— dejaran de ver al DPD como un trámite final para convertirlo en un socio de la fase de diseño, garantizando así la **Privacidad desde el Diseño y por Defecto (art. 25 RGPD)** de manera espontánea y como garantía de eliminación de futuros problemas, con los cuales se encontraban en fases avanzadas de los proyectos, y en aquel punto eran irresolubles.

4. METODOLOGÍA DE INTERVENCIÓN: «El día con el Delegado»

La herramienta táctica para lograr estos objetivos es la actividad «**El día con el Delegado**». No se trata de un curso de formación reglado, formación que por otra parte ya se ofrece a toda la plantilla del ayuntamiento a través del servicio de formación del mismo ayuntamiento, sino de una intervención de consultoría grupal itinerante.

4.1. Concepto: Invertir la carga del desplazamiento

En la administración clásica, la ciudadanía va a la ventanilla y el personal de los servicios del ayuntamiento van al despacho del Delegado de Protección de Datos. En este modelo, es el DPD quien se desplaza a las dependencias descentralizadas de los servicios (Comisarías, Centros Cívicos, Oficinas de Padrón, Áreas básicas de Servicios Sociales, etc.), para tratar temáticas comunes a todo un conjunto de personal adscrito a un servicio o a un determinado ámbito.

Este simple acto físico envía un mensaje poderoso: ***"Estoy aquí a vuestro servicio, para entender vuestro contexto y vuestras limitaciones operativas y tecnológicas y para ofrecer soluciones a las mismas"***.

4.2. Dinámica de las Sesiones: "En Fuego Real y con ausencia de guion"

Las sesiones, con una vocación de duración mínima de 2 horas, la cual nunca se ha cumplido porque lo habitual ha sido entre 3 l 4 horas por la demanda del personal, carecen de PowerPoint o temario cerrado.

Se basan en el Método Socrático Inverso, por tanto, las sesiones se diseñan como un **ejercicio de consultoría de campo sin red de seguridad**. El DPD se expone ante grupos multidisciplinares que plantean dudas operativas urgentes. Esta exposición de vulnerabilidad por parte del experto (al no llevar las respuestas preparadas) **genera**

una empatía inmediata y rompe la barrera jerárquica, fomentando un clima de confianza donde afloran los problemas reales (Shadow IT) que nunca se confesarían en una auditoría formal.

A título ilustrativo, la variedad de consultas inmediatas que el DPD debe gestionar en estas sesiones abarca tanto el espectro jurídico (RGPD) como el tecnológico (ENS), demostrando la necesidad de un perfil polivalente permanentemente actualizado.

- *"Tengo un menor en riesgo de exclusión que se ha mudado de municipio hoy mismo. ¿Puedo enviar su expediente médico por WhatsApp a la trabajadora social del otro Ayuntamiento para que no pierda la medicación, o necesito consentimiento?"*
- *"He recibido un correo urgente que parece del Ministerio de Justicia pidiendo que descargue una notificación. El remitente es extraño, pero tengo miedo de que se pase el plazo. ¿Hago clic o es una estafa?"*
- *"Ha venido un ciudadano exigiendo el certificado de empadronamiento de su expareja para un trámite de divorcio. Dice que tiene derecho legítimo. ¿Se lo doy o estoy vulnerando la protección de datos?"*
- *"¿Por qué Sistemas me obliga ahora a cambiar la contraseña tan habitualmente? Es muy molesto y me retrasa el trabajo. ¿No podemos quitarlo?"*
- *"En una actuación tensa en la vía pública de la policía, ¿puedo activar la cámara unipersonal (bodycam) si entramos en un domicilio privado persiguiendo un delito flagrante?"*
- *"Como el servidor corporativo va lento, hemos creado una carpeta en Google Drive personal para compartir los expedientes de las becas comedor con las direcciones de los colegios. ¿Eso está bien?"*
- *"Vamos a publicar en Instagram las fotos de la carrera popular. Se ven caras de niños entre el público. ¿Necesitamos la firma de todos los padres o es un evento público?"*
- *"Acabo de enviar un correo masivo a 500 ciudadanos convocándolos a una reunión y me he olvidado de ponerlos en CCO (Copia Oculta). Todo el mundo ve los correos de todos. ¿Qué hago? ¿Puede tener repercusiones para mí?"*
- *"Tengo muchas claves y se me olvidan. ¿Es seguro si las guardo en un Excel con contraseña en mi escritorio, o debo usar un gestor de contraseñas?"*
- *"Una persona que ha sido detenida varias veces pide ejercer su 'Derecho de Supresión' (Olvido) para que borremos todo su historial policial y de multas. ¿Estamos obligados a borrarlo?"*

4.3. Rapidez, Compromiso de Rigor y Respuesta Diferida:

El DPD responde y resuelve en tiempo real. Esto exige una alta solvencia técnica y jurídica, ya que no hay tiempo para "estudiarlo". Se da la solución operativa al momento, sobre todo en lo que son dudas comunes y por tanto repetitivas a lo largo de las diferentes sesiones.

A pesar de la agilidad que caracteriza al modelo, el DPD mantiene un **principio ético de prudencia**. El DPD resuelve en directo aquellas cuestiones donde la respuesta jurídica o técnica es inequívoca. Advirtiéndolo, a pesar de todo, que a veces los pequeños detalles de cada caso condicionan las respuestas en un sentido o en el contrario. Se pone de manifiesto que los detalles de cada caso concreto son muy importantes en protección de datos.

No obstante, la organización sabe que el DPD no posee todas las respuestas de forma instantánea. Si surge una consulta de alta complejidad jurídica o que requiere un análisis de riesgos profundo, **el DPD recoge la consulta y se compromete a estudiarla** con la jurisprudencia o normativa técnica en la mano, para retornar al grupo una respuesta posterior debidamente reflexionada y fundamentada, en un plazo razonable.

Este mecanismo refuerza la autoridad del DPD: los trabajadores perciben que no se está improvisando, sino que se ofrece una seguridad jurídica real, combinando la cercanía del trato presencial con el rigor del análisis de despacho.

Por tanto, los asistentes plantean dudas sobre **expedientes vivos y casos hipotéticos o incluso personales** con los que se encuentran a diario, a una persona (DPD) que al final les ofrece "**seguridad**" y/o criterios que les son de aplicación tanto en su vida profesional como en la personal.

4.4. El Paradigma del DPD «Posibilista»: Vehicular la necesidad de gestión

El gran factor diferencial de este proyecto es la adopción, por parte del DPD, de una postura «**Posibilista**» frente a la tradicional postura «**Stopper**».

Los servicios municipales tienen necesidades legítimas de tratamiento de datos para servir al ciudadano. Un/una Policía necesita identificar; un/una Técnico/a de Deportes necesita listas de salud para un campus deportivo; Servicios Sociales debe verificar situaciones de riesgo.

- El DPD Stopper: "No puedes hacerlo porque no tienes consentimiento o la herramienta no es corporativa". Resultado: Parálisis o Shadow IT.
- El DPD Posibilista: "Tu necesidad de compartir datos para proteger al menor es legítima. No uses WhatsApp (riesgo inaceptable según ENS). Habilitaremos un intercambio seguro a través de la carpeta interadministrativa cifrada. Jurídicamente, no necesitamos consentimiento, pues se puede amparar en el Cumplimiento de una Misión de Interés Público (Art. 6.1.e RGPD) o en la

Obligación Legal (Art. 6.1.c RGPD) derivada de la Ley de Servicios Sociales. "Hazlo de esta manera y te haré un informe que lo avale".

Esta labor convierte al DPD en el ingeniero que construye el "puente legal y seguro" (Medidas de seguridad adecuadas, Art. 32 RGPD) por donde transita la información necesaria.

4.5. Hibridación de Perfiles: Privacidad + Ciberseguridad

En el caso concreto del DPD del Ayuntamiento de Santa Coloma, se aprovecha el doble perfil del DPD actual (**DPD** certificado + **CISO**), las sesiones abordan de manera indisoluble el cumplimiento legal (RGPD) y la seguridad técnica (ENS). Al responder dudas técnicas (phishing, gestión de contraseñas, doble factor), el DPD gana legitimidad ante perfiles que habitualmente desconfían de perfiles más jurídicos, hablando su mismo idioma, adaptándose al nivel del público reunido.

5. IMPACTO SECTORIAL (RESULTADOS TÁCTICOS)

El éxito de la metodología "posibilista" se evidencia, sobre todo, en los departamentos de mayor complejidad operativa. A través de las sesiones presenciales ("El día con el Delegado"), **se consiguieron aflorar problemáticas latentes que generaban gran inseguridad jurídica a todo personal.** Lejos de la fiscalización, estas sesiones han fomentado un clima de colaboración real: **los servicios exponen sus inquietudes "de trinchera" y el DPD diseña las soluciones** para adecuarlas a la normativa de privacidad y seguridad de la información.

A continuación, se detallan algunos de los impactos concretos **más relevantes** por ámbitos, que se desarrollaron a partir de las reuniones establecidas a través de cada uno de los colectivos.

5.1. Servicios Sociales: Seguridad jurídica en la urgencia

La intervención en este departamento crítico ha supuesto un cambio de paradigma: se ha pasado de un cierto bloqueo por miedo al incumplimiento de la normativa de protección de datos, a una seguridad jurídica proactiva que facilita la intervención social.

a) Erradicación de la parálisis y canales seguros (ENS)

Se ha superado el temor a compartir datos críticos legítimamente solicitados. Gracias a los nuevos protocolos, los profesionales saben cómo enviar información sensible mediante canales cualificados y cifrados, desterrando definitivamente el uso del correo electrónico simple para datos de categoría especial (Art. 9 RGPD). Priorizamos la protección efectiva de la persona vulnerable amparándonos en la base jurídica correcta, eliminando el "miedo administrativo" y garantizando la trazabilidad de los accesos tal y como exige el Esquema Nacional de Seguridad (ENS).

b) Consultoría de Alto Nivel en Expedientes Complejos

El DPD ha asumido un rol de consultor experto en casos de alta sensibilidad (protección a la infancia, violencia de género o doméstica). El Delegado analiza, caso por caso, las dudas de los trabajadores sociales, aportando la confianza necesaria para discernir qué información exacta se debe facilitar a cada parte involucrada.

Este análisis es vital cuando tratamos información vertida en la intimidad de las entrevistas psicosociales. Se ha establecido criterios estrictos para "blindar" esta información cualitativa, evitando que datos facilitados en un entorno de confianza puedan ser instrumentalizados por una parte enfrentada (ej. un agresor o una expareja en litigio) bajo la excusa del derecho de acceso, protegiendo así la integridad del expediente y la seguridad de la víctima.

c) Gestión de la Rotación: Acompañamiento desde el "Minuto Cero"

Conscientes de la alta rotación de personal en Servicios Sociales, **el DPD ha sistematizado un protocolo de acogida**. No esperamos a que surja el error; realizamos reuniones de integración regulares con las nuevas incorporaciones. En estas sesiones de "puesta a punto", transmitimos los criterios específicos del Ayuntamiento desde el primer día. De este modo, detectamos carencias formativas y ofrecemos la mano del DPD como soporte inmediato, asegurando que el personal interino opere con las mismas garantías que el veterano y sepa, ante la duda, a quién acudir (el DPD).

5.2. Seguridad Ciudadana: Tecnología policial, videovigilancia y cooperación judicial

El cuerpo de la Policía Local afronta una doble presión: la demanda de seguridad física por parte de la ciudadanía y la exigencia de seguridad jurídica en el manejo de datos sensibles. En este contexto de intensa tecnificación (cámaras corporales, lectores de matrículas, drones), la intervención del DPD mediante sesiones presenciales ha sido determinante para **resolver las dudas operativas** de mandos, agentes y personal de gestión administrativa, legitimando la modernización tecnológica del servicio.

a) Videovigilancia y legitimidad de la prueba

Especialmente relevante ha sido el asesoramiento estratégico sobre la instalación y gestión de cámaras de videovigilancia en la vía pública. La intervención del DPD ha garantizado que el despliegue de estos dispositivos supere rigurosamente el test de proporcionalidad y obtenga la preceptiva autorización de la Comisión de Control de los Dispositivos de Videovigilancia de Cataluña.

Este rigor en el cumplimiento normativo no es un mero trámite, sino un activo operacional: ha legitimado el uso de las imágenes captadas, convirtiéndolas en herramientas eficaces tanto para la disuasión como para la investigación, y dotándolas de plena validez probatoria ante la autoridad judicial. De este modo, **la privacidad se**

convierte en un factor que contribuye de manera determinante a la mejora de los índices de seguridad en los ámbitos monitorizados.

b) Cooperación Judicial y Canales Seguros (ENS)

En paralelo, se ha redefinido el tratamiento de los expedientes requeridos por la Fiscalía y otros Cuerpos de Seguridad del Estado, **transformando un proceso manual en un procedimiento estandarizado y seguro.**

El DPD ha establecido protocolos estrictos para verificar la legitimación de cada petición (analizando la competencia y el marco de la Ley Orgánica 7/2021), asegurando que la información se comparte exclusivamente mediante canales seguros y trazables conforme al Esquema Nacional de Seguridad (ENS). Esta metodología protege al agente municipal ante posibles responsabilidades por revelación de secretos y garantiza una colaboración con la Justicia leal, ágil y escrupulosa con los derechos fundamentales.

El resultado global es una policía que utiliza la tecnología avanzada con plenas garantías procesales, donde la seguridad jurídica actúa como palanca de la eficacia operativa.

5.3. Atención a la Ciudadanía (OIAC): La primera línea

La Oficina de Información y Atención Ciudadana es el punto de mayor fricción entre la administración y el ciudadano. El proyecto ha intervenido en tres ejes para transformar esa tensión en seguridad jurídica:

a) A) El DPD como "Escudo Jurídico" ante la agresividad

El personal de ventanilla sufre a menudo la presión de ciudadanos que solicitan datos de terceros (exparejas, vecinos). En las sesiones, el DPD ha dado argumentos al personal para atender a la ciudadanía de manera asertiva: el trabajador no deniega el dato por capricho, sino por mandato legal.

Además, **se ha dotado a la OIAC de informes específicos** que el personal puede exhibir ante solicitudes improcedentes. Este respaldo documental reduce drásticamente la conflictividad y el estrés del empleado, quien se siente avalado por una autoridad de control interna.

b) Minimización Real: **El fin de la "Cultura de la fotocopia del DNI"**

Aplicando el Principio de Minimización (Art. 5.1.c RGPD), se ha eliminado la obligatoriedad sistemática de adjuntar la fotocopia íntegra del DNI en gran cantidad de procedimientos. Se ha impulsado el cambio hacia la "verificación" en lugar de la "retención": si el/la trabajador público/a verifica la identidad in situ o mediante plataformas de interoperabilidad, no es necesario custodiar una copia del documento.

Esto reduce el riesgo de seguridad (pérdida de papeles) y el volumen de destrucción documental.

c) Autodeterminación del Menor (Art. 7 LOPDGDD)

Se ha actualizado la relación con la juventud, desterrando el automatismo de exigir la mayoría de edad o el consentimiento paterno/materno para todo. Siguiendo la LOPDGDD, se ha instruido al personal para **reconocer la capacidad de obrar de los mayores de 14 años en materia de protección de datos**. Esto permite que los adolescentes realicen trámites propios (ej. derechos ARSOPL, inscripciones) sin tutela paterna/materna, salvo que una norma específica exija lo contrario, fomentando su autonomía digital.

5.4. Padrón Municipal de Habitantes: La llave de los servicios públicos

El Padrón es el activo de información más crítico. En un municipio con la rotación residencial de Santa Coloma, el DPD ha intervenido **para equilibrar el rigor del dato con la realidad social**.

a) Garantía de derechos y seguridad del personal público

Se han establecido criterios claros para trámites complejos, evitando que el rigor en el Principio de Exactitud se convierta en una barrera para acceder a servicios básicos (sanidad, escolarización). El DPD "blinda" la actuación del personal municipal mediante informes jurídicos que avalan empadronamientos en situaciones atípicas pero reales, evitando la exclusión administrativa sin que el/la trabajador/a incurra en responsabilidad.

b) Control de acceso y minimización

El acceso al Padrón por otros departamentos (Policía, Servicios Sociales) ha dejado de ser un "grifo abierto". Se analiza caso por caso la base de legitimación y se aplica la minimización: cada departamento ve solo la "parcela" de datos necesaria para su función, bloqueando la visualización de datos excesivos. Se informa a todo el personal que habitualmente se hacen auditorias de esos accesos que son reportadas al DPD para su estudio y donde el mismo podrá solicitar información sobre las condiciones que requirieron ese acceso concreto, las cuales deberán de ser documentalmente justificadas.

c) Ciclo de vida de los permisos (Cumplimiento ENS)

Desde la óptica de seguridad (ENS), Se ha implantado una política rigurosa de gestión de identidades. Existen canales automatizados con Recursos Humanos i Sistemas de información para que las altas, bajas y rotaciones se reflejen inmediatamente en los permisos de los aplicativos. Esto **evita la acumulación de privilegios obsoletos** y garantiza que los accesos se revisen y revoquen periódicamente bajo criterios de necesidad.

5.5. Recursos y Prestaciones: Dignidad y datos

En la gestión de ayudas, el riesgo no es solo la fuga de datos, sino la "revictimización". Se ha impulsado la **aplicación estricta de la minimización**:

recabar solo el dato financiero o social imprescindible. Asimismo, se trabaja la interoperabilidad segura con otras administraciones (AOC, AEAT, Seguridad Social) para hacer efectivo el derecho de la ciudadanía a no aportar documentos que ya tiene la administración reduciendo la burocracia sin sacrificar la seguridad de la información tributaria.

5.6. Deportes: La energía que mueve datos

El ámbito de Deportes maneja volúmenes masivos de datos con la complejidad añadida, a veces, de tratar categorías especiales (salud) y datos de menores en eventos públicos.

a) Gestión de imagen y resultados

Se ha clarificado la distinción entre la captación de imágenes generales (interés público o informativo) y los primeros planos, sobre todo de menores, donde se debe de exigir consentimiento explícito.

Además, en las competiciones deportivas, **se ha equilibrado la transparencia de las clasificaciones con la seguridad**: se informa de la publicación de resultados, pero ofreciendo mecanismos de seudonimización para participantes en riesgo (ej. víctimas de violencia) que necesitan ocultar su participación, o simplemente personas que no desean constar en las clasificaciones. Siempre que es posible solo se indica la clasificación indicando el número de dorsal, sin la identidad de la persona deportista, sobre todo en las competiciones no oficiales.

b) Salud: Ciclo de vida y destrucción

Se ha protocolizado la recogida de certificados médicos, y intolerancias alimenticias. Aplicando la limitación del plazo de conservación, sistematizando la destrucción segura de estos datos al finalizar el evento o temporada. Así evitan la acumulación de "datos tóxicos" en bases de datos olvidadas, mitigando el riesgo de brechas de seguridad.

c) Autonomía del menor deportista

Al igual que en la OIAC, se aplica el criterio de los 14 años para permitir que los jóvenes gestionen sus inscripciones de forma autónoma, agilizando la gestión administrativa de los servicios deportivos, velando al mismo tiempo, porque los menores de esa edad, tengan la autorización paterna/materna correspondiente.

5.7. Transparencia y Buen Gobierno

La tensión entre la publicidad activa (Leyes de Transparencia estatal y catalana) y la protección de datos es constante. El DPD ha intervenido estableciendo protocolos de anonimización previos a la publicación en el Portal de Transparencia.

El objetivo es evitar el "efecto mosaico": que el cruce de datos económicos públicos permita reidentificar a ciudadanos vulnerables (ej. perceptores de ayudas).

Garantizamos que el Ayuntamiento sea transparente en "qué gasta" sin desnudar la intimidad de "quién lo recibe".

Especialmente compleja es la ponderación necesaria para renovar anualmente el Sello INFOPARTICIPA de la UAB (Universidad Autónoma de Barcelona), sello que el ayuntamiento de Santa Coloma consigue mantener desde la primera edición en el año 2013, hasta la actualidad. El DPD trabaja estrechamente con Comunicación para asegurar que se publican todos los contenidos exigidos para la máxima puntuación, pero filtrando previamente cualquier dato personal excesivo. Este éxito demuestra que **la excelencia en transparencia es compatible con el respeto escrupuloso al RGPD.**

6. IMPACTO ORGANIZATIVO: EL "EFECTO CASCADA" EN LA ESTRATEGIA

Lo más destacable de este proyecto no son las sesiones en sí mismas, sino el cambio estructural que han provocado en las altas esferas técnicas y administrativas del Ayuntamiento.

6.1. La Conquista de la Confianza de la Dirección de Tecnología

Tradicionalmente, en muchas administraciones, TI y el DPD mantienen una relación de tensión (Innovación vs. Control). En el Ayuntamiento de Santa Coloma, esto ha cambiado radicalmente gracias a la demostración de competencia técnica del DPD en las sesiones de proximidad, las cuales en el caso de TI se realizan casi a diario.

El Cambio: Al comprobar que el DPD entiende los flujos de datos, las arquitecturas de servidores y las necesidades de interoperabilidad, y que aplica una visión **posibilista**, la Dirección de Sistemas de Información ha modificado espontáneamente sus procesos.

Situación Actual:

- **Tecnología exige la validación del DPD** en la fase 0 (toma de requerimientos) de cualquier nuevo software o nuevo circuito a implementar. Saben que la intervención del DPD no será para bloquear ("Stopper"), sino para definir los requisitos funcionales de seguridad y privacidad que harán viable el proyecto.
- El DPD se ha convertido en un "**consultor de calidad**" para TI.

6.2. La Alianza Preventiva con la Comunicación institucional

Del mismo modo, la Dirección de Comunicación, testigo de la eficacia del DPD resolviendo crisis en otros departamentos, ahora integra al DPD en la mesa de diseño de campañas. Se consulta proactivamente el uso de imágenes, el diseño de formularios de captación de datos en la web o la presencia en nuevas redes sociales.

La validación del DPD se busca como un sello de "Blindaje Reputacional" y garantía de cumplimiento.

6.3. Privacy by Design como estándar de calidad

Este es el gran triunfo estratégico. La participación del DPD ha dejado de ser un trámite para convertirse en un indicador de calidad. Tanto la Dirección como el conjunto de los trabajadores y trabajadoras, han interiorizado el principio de Privacidad desde el Diseño (Art. 25 RGPD) no solo por ética, sino por eficiencia: corregir un error de privacidad una vez el software está comprado o la campaña lanzada es infinitamente más costoso (económica y reputacionalmente) que prevenirlo en la fase de arquitectura. **El "visto bueno" inicial del DPD se percibe ahora como un seguro de vida para la viabilidad del proyecto.**

7. INDICADORES Y MÉTRICAS DE ÉXITO

La evaluación del impacto del proyecto «El día con el Delegado» no se limita a un recuento administrativo de reuniones, sino que se analiza a través de la evolución de la cultura de privacidad y seguridad en la organización. A continuación, se presentan los resultados desglosados en métricas de alcance y métricas de calidad.

7.1. Métricas de Alcance y Capilaridad (2021-2025)

La estrategia de proximidad ha permitido permear en la estructura municipal, superando la barrera de los servicios centrales para llegar a las unidades operativas.

Cobertura Estructural: Se han ejecutado sesiones presenciales de consultoría en una gran parte de los ámbitos municipales, priorizando aquellos con mayor riesgo en el tratamiento de datos. La intervención ha abarcado:

- **Áreas de Atención Directa y Colectivos Vulnerables:** Servicios Sociales (5 ediciones), Atención a la Infancia, Atención a las Mujeres y colectivos LGTBIQ+, Gente Mayor, Juventud, Educación, Deportes y Recursos y Prestaciones.
- **Seguridad y Espacio Público:** Policía Local (2 ediciones específicas con mandos intermedios), Mantenimiento de Vía Pública, Servicios Urbanos y Mantenimiento de Edificios.
- **Ciudadanía y Gestión:** Oficina de Información y Atención Ciudadana (OIAC), Participación Ciudadana, Transparencia y Buen Gobierno, Defensora de la Ciudadanía y Alcaldía.
- **Áreas de Soporte Interno:** Recursos Humanos, Prevención de Riesgos Laborales y Asuntos Generales.
- **Organismos y Empresas Municipales:** Empresa municipal de Guarderías Patronatos (Música).

Impacto en la Plantilla: Se estima que aproximadamente unas 450 personas han participado directamente en alguna de las sesiones presenciales. Esta cifra representa, aproximadamente, el 50% de la plantilla total del Ayuntamiento. Este dato confirma la creación de un "cortafuegos humano" extenso, donde la mitad de la organización ha recibido instrucción directa y efectiva sobre cómo gestionar la información de manera segura y legal.

7.2. Análisis de la Evolución y Tipología de Consultas (2020-2025)

El análisis detallado del registro de consultas al DPD permite extraer conclusiones claras sobre la madurez de la cultura de privacidad en la organización. Se observa una transición desde la "urgencia burocrática" hacia la "consultoría de alto nivel".

A) Análisis Cuantitativo: Del pico de gestión a la estabilidad

La fluctuación en el volumen de expedientes responde a ciclos lógicos de adaptación y madurez:

I. Fase de Emergencia y Regularización (2020-2021):

2020 (127 Expedientes): Año marcado por la COVID-19. Actividad reactiva centrada en teletrabajo y datos de salud.

2021 (171 Expedientes - Pico Máximo): Volumen máximo histórico debido a la regularización masiva de contratos de Encargado del Tratamiento y consolidación de procedimientos.

II. Fase de Madurez y Autonomía (2022-2023):

2022 (74 Expedientes) y 2023 (75 Expedientes): Se registra una caída drástica del volumen (>50%). Este descenso es un indicador de éxito: demuestra que los departamentos han interiorizado los procedimientos básicos y ya no requieren la intervención del DPD para trámites estándar. La organización ha alcanzado su "velocidad de crucero".

III. Fase de Tecnificación y Complejidad (2024-2025):

2024 (88 Expedientes) y Proyección 2025: Se inicia un repunte (~17%) y una tendencia al alza. Este aumento no responde a burocracia básica, sino a la introducción de tecnologías disruptivas (IA, videovigilancia avanzada) y retos de seguridad ciudadana.

B) Análisis Cualitativo: Evolución de las temáticas

La naturaleza de las consultas ha mutado, reflejando una **mayor sofisticación en los riesgos gestionados**:

- **Tecnologías de Control y Seguridad** (Tendencia: Fuerte Alza): Es la categoría de mayor crecimiento desde 2023, alineada con el Esquema Nacional de Seguridad (ENS). Incluye videovigilancia (ZBE, vía pública), uso de bodycams policiales, drones y ciberseguridad (gestión de contraseñas, validación de software SaaS).
- **Nuevos Retos Tecnológicos** (2024-2025): Emergencia de consultas sobre Inteligencia Artificial (ej. traductores neuronales en Servicios Sociales) y gestión compleja del Padrón de Habitantes.
- **Servicios Sociales** (Tendencia: Constante): Se mantiene el flujo de consultas sobre situaciones de riesgo (infancia, violencia), donde se busca el equilibrio entre asistencia urgente y confidencialidad.
- **Gestión Interna y RR.HH.** (Tendencia: A la baja): Las consultas sobre control horario o datos de salud laboral se han reducido significativamente, evidenciando que los departamentos de RR.HH. y PRL operan ya con autonomía y criterios consolidados.

7.3. Indicadores Cualitativos: La percepción del cambio cultural.

Más allá de las métricas cuantitativas, el verdadero indicador de éxito del proyecto es la percepción de utilidad por parte de quienes operan los servicios. La transición del DPD "fiscalizador" al DPD "de trinchera" ha generado una adhesión que se refleja en los testimonios de las jefaturas i técnicos/as de los servicios clave. Algunos ejemplos de esos testimonios se reflejan en las siguientes opiniones:

R.C.- Responsable del Servicio de Sistemas de Información:

“Desde el Servicio de Sistemas de Información del Ayuntamiento de Santa Coloma de Gramenet, se intentó gestionar la adecuación de las aplicaciones y conjuntos de datos a la primera ley de protección de datos. La organización, o mejor dicho, sus miembros, entendían que era un tema exclusivo de sistemas informáticos y no había conciencia de que el cumplimiento de las normativas en materia de protección de datos afecta a toda la organización.

La entrada en vigor del RGPD y de la LOPDGDD obligó a instaurar la figura del Delegado de Protección de Datos en las organizaciones. Esta figura, en nuestro Ayuntamiento, ha ayudado a poner orden en la organización respecto al tratamiento de los datos que esta realiza, así como a desbloquear cambios propuestos por Informática que encontraban mucha resistencia por parte de los Servicios gestores.

Es la primera vez que trabajamos con un perfil jurídico que entiende qué es una API, un log de trazabilidad o el cifrado de extremo a extremo. Antes, veíamos a la persona del ámbito jurídico encargada de temas de protección de datos como alguien para quien esta era una tarea más entre las muchas que tenía asignadas.

En las reuniones de la primera comisión de protección de datos, creada hacia el 2012, solo ponía obstáculos que impedían avanzar en el desarrollo de la normativa en el Ayuntamiento.

Con este modelo de proximidad, el DPD participa con nosotros en las diferentes fases de los proyectos. Hemos pasado de la fricción a la

colaboración: ahora nos ayuda a definir los requisitos de seguridad del ENS desde el inicio, ahorrándonos meses de correcciones posteriores.”

M.J.B Y S.P Responsables de Servicios Sociales:

“La figura del DPD es una figura clave dentro de nuestro servicio de atención a la infancia y las familias. Su marco teórico y jurídico ha delimitado nuestra actuación teniendo presente la protección de datos tanto de las personas y/o familias que atendemos como de nuestro propio ejercicio profesional. La posibilidad de consultar ante cualquier duda, siempre desde la proximidad y la accesibilidad, ha ayudado a que los profesionales realicen su praxis profesional con más seguridad y conocimiento del ámbito de la protección de datos.”

M.A.- Abogada de Servicios Sociales:

“En la mayoría de los casos, desde Servicios Sociales tenemos por obligación legal el deber de intercambiar datos personales de usuarios para cumplir con las funciones que tenemos encomendadas. Disponer de un DPD accesible nos da la tranquilidad de estar actuando con las debidas garantías de proporcionalidad y confidencialidad.”

R.A.- Reposable de Departamento Padrón Municipal de Habitantes:

“La gestión del Padrón de Habitantes soporta una doble presión: la urgencia social y la seguridad de los datos que se gestionan. En nuestro caso, la proximidad del DPD ha sido determinante en ambos frentes. Por un lado, su presencia 'in situ' nos da seguridad jurídica para resolver empadronamientos complejos sin miedo a cometer irregularidades, blindando nuestras decisiones con informes sólidos.

Pero también ha sido muy importante el orden que nos ha permitido poner en la 'trastienda': hemos trabajado juntos para vincular los permisos de acceso a la legitimidad de cada puesto de trabajo. Saber que ahora el sistema garantiza que nadie ve más de lo que su función justifica, y que a la vez tenemos respaldo legal para los casos difíciles, nos da mucha tranquilidad”

7.4. Conclusión de los Indicadores

Este proyecto **ha consolidado su metodología y alcanzado su fase de madurez y tecnificación durante el periodo 2024-2025, cuando los datos validan el cambio de modelo.** La reducción del volumen bruto de consultas (de 171 a unas 80 anuales) no refleja inactividad, sino eficiencia pedagógica: el equipo ha aprendido a resolver las cuestiones básicas y solo plantea aquellas que considera de alta complejidad, las cuales, a su vez, representan desafíos estimulantes para el DPD.

Esto ha permitido liberar recursos para que, en el periodo actual, el DPD se centre en consultas de alto valor añadido: la validación de tecnologías complejas y la resolución de casos sensibles, actuando no como un gestor administrativo, sino como un arquitecto de seguridad jurídica y técnica.

8. INNOVACIÓN Y TRANSFERIBILIDAD DEL MODELO

Este modelo innova porque invierte los recursos: en lugar de gastar presupuesto en licencias de software de Gobernanza, gestión de riesgos y cumplimiento normativo (GRC), invierte en **Capital Relacional** dentro del ayuntamiento.

- **Innovación:** Metodología "**Sin Red**". Aceptar el riesgo de no tener todas las respuestas preparadas genera una credibilidad inigualable.
- **Transferibilidad:** Este proyecto es replicable mañana mismo en cualquier administración pública española a coste cero. Solo requiere voluntad política y un perfil de DPD dispuesto a asumir el rol de **Facilitador de Negocio** en lugar de mero Auditor de Cumplimiento.

Una clave del éxito es el doble rol formativo en protección de datos y seguridad de la información del DPD actual, pero si éste DPD se ha aproximado formándose a la técnica jurídica, cualquier jurista también puede aproximarse a la técnica de sistemas de información y seguridad a través de una adecuada formación.

9. CONCLUSIONES

El Proyecto «**El día con delegado**» demuestra que, en la administración del siglo XXI, la autoridad no la otorga el BOE ni el nombramiento oficial, sino la utilidad percibida por las personas que forman parte de la organización.

Mediante una estrategia de proximidad a los servicios y un enfoque posibilista, el DPD del Ayuntamiento de Santa Coloma de Gramenet ha conseguido **incrementar el nivel de protección de los derechos de la ciudadanía mientras se agiliza la operativa de los servicios públicos manteniendo el control sobre la seguridad de los sistemas.**

Lo que empezó como unas charlas informales se ha convertido en la piedra angular de un sistema de gobernanza donde la Privacidad y la Seguridad son componentes indiscutibles de cualquier nuevo proyecto tecnológico o comunicativo, no por miedo a la sanción de las autoridades de control, sino por convicción de excelencia.

Santa Coloma de Gramenet, 12 de diciembre de 2025.

Antoni Herráez Pizarro 
Delegado de Protección de Datos