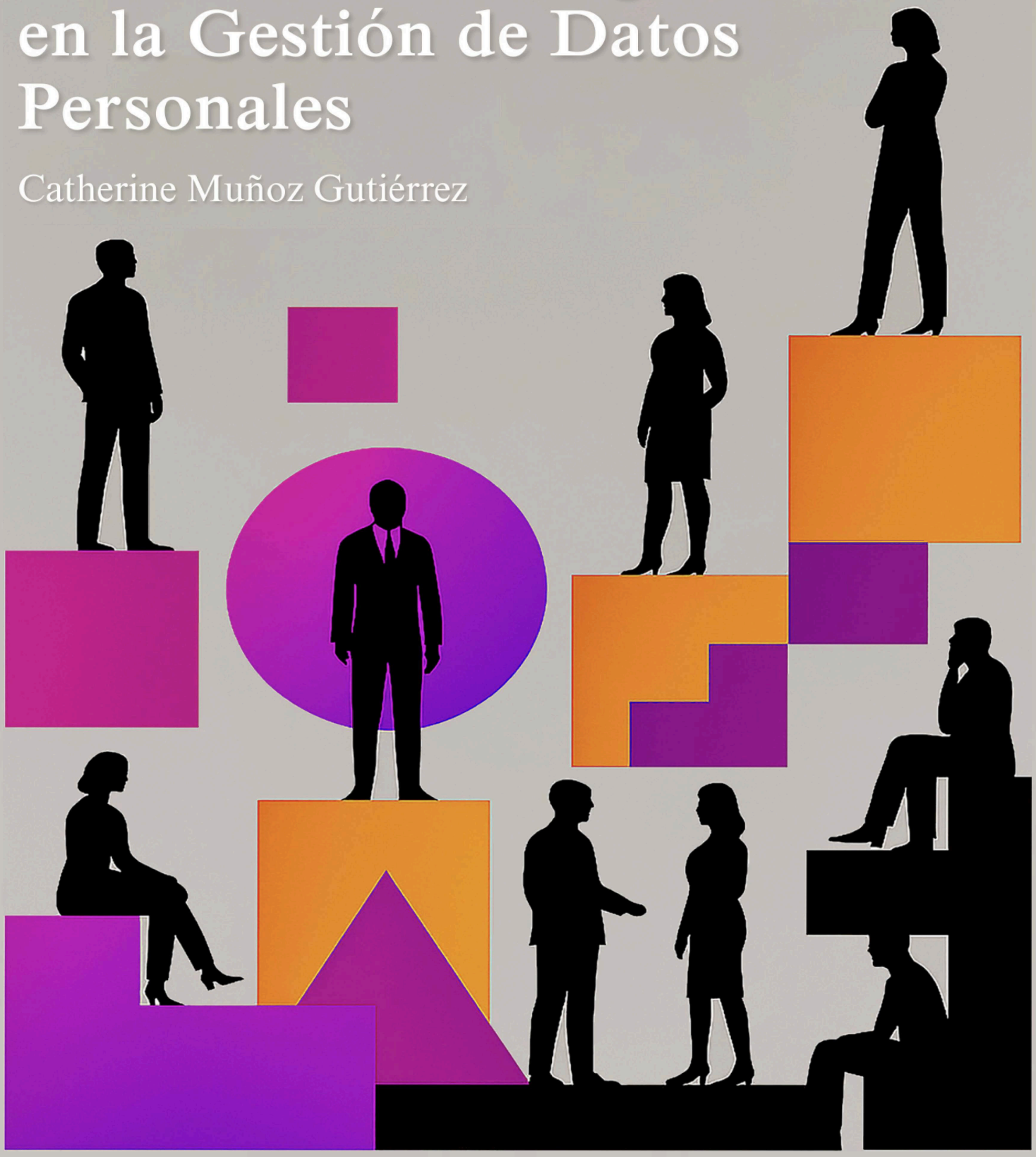
DPO: Pilar Estratégico en la Gestión de Datos Personales

Catherine Muñoz Gutiérrez



Whitepaper Serie
Idónea Consultores
Julio, 2025

idónea

Forma de Cita Sugerida

Muñoz Gutiérrez, C. (2025). DPO: Pilar estratégico en la gestión de datos personales. Whitepaper serie. Santiago, Chile: Idónea Consultores. Licencia CC BY-NC-ND 4.0.

Exención de Responsabilidad

La información contenida en este White Paper se proporciona con fines informativos y de orientación general. No constituye asesoramiento legal, técnico ni profesional. Los lectores no deben actuar únicamente sobre la base de la información aquí contenida sin buscar asesoramiento específico de un profesional calificado. Ni la autora ni Idónea Consultores asumen responsabilidad alguna por las decisiones tomadas o no tomadas con base en el contenido de esta publicación.

Tabla de contenido

INTRODUCCIÓN

La protección de datos personales no es una disciplina nueva; es la manifestación moderna de un derecho fundamental, consagrado en declaraciones universales desde hace más de medio siglo.[1] Sin embargo, fue la irrupción de la informática lo que transformó este derecho en un desafío regulatorio, dando origen a las primeras leyes de protección de datos y a los principios que hasta hoy nos rigen. La historia de esta regulación va de la mano de una adaptación continua a la par de los desarrollos tecnológicos de los últimos años.

Aunque la idea de una persona encargada de la protección de datos ya se había desarrollado en varios Estados miembros, cuyo origen específico se encuentra en Alemania[2], el concepto y la función del Delegado de Protección de Datos (DPO), tal como se conoce hoy, con su carácter obligatorio y estandarizado, fue establecido indiscutiblemente por el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. El GDPR, vigente en la UE desde el 25 de mayo de 2018, introdujo esta función de una manera nunca antes vista en esta forma, armonizando en todo el bloque comunitario.[3]El rol y la función correcta del DPO hasta el día de hoy, es considerado uno de los mayores desafíos aun presentes después de 7 años de aplicación de este reglamento.[4]

Para entender el rol del DPO, es necesario conocer el espíritu del reglamento europeo. El objetivo principal del GDPR es establecer un nivel uniforme y adecuado de protección sobre potenciales afectación de derechos fundamentales a propósito de un tratamiento de datos personales, reconociendo en primer lugar, la existencia de un desequilibrio de poder e información entre los ciudadanos (titulares de los datos) y las organizaciones que procesan sus datos.[5] Ante la asimetría de poder que suele existir entre los ciudadanos (titulares de los datos) y las organizaciones que los procesan, el GDPR y la normativa inspirada en él buscan reequilibrar la balanza. Para ello, concretan las expectativas y derechos de los interesados y prohíben la explotación indebida.

Es precisamente para abordar este desafío de reequilibrio donde la figura del Delegado de Protección de Datos (DPO) adquiere su máxima relevancia. Se constituye como una piedra angular de la rendición de cuentas y un poderoso instrumento de autocontrol dentro de las organizaciones. El DPO es, en esencia, el eje central de la nueva gobernanza de datos, actuando como el "director de orquesta"[6] que asegura que todas las áreas de la organización actúen en armonía con los principios de privacidad.

La reforma a la Ley N° 19.628 en Chile, al igual que nuevas regulaciones en otras partes del mundo, se inscribe directamente en esta tradición global. Es el paso decisivo del país para

[1] Declaración Universal de Derechos Humanos, Artículo 12.
[2] La figura del DPO tiene su antecedente directo en el Betriebsbeauftragter für den Datenschutz (Encargado de protección de datos de la empresa), establecido por primera vez en la ley federal alemana de protección de datos (Bundesdatenschutzgesetz - BDSG) de 1977. Esto subraya la larga tradición alemana en la materia, que influyó significativamente en el diseño del GDPR.
[3] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
[4] fit4privacy - GDPR, Privacy, AI, «Look Back & Forward at 7 Years of EU GDPR», Vídeo, YouTube, junio de 2025, https://www.youtube.com/watch?v=-zIea6a49zc.
[5] Article 29 Data Protection Working Party (2017). Guidelines on Data Protection Officers (‘DPOs’) (WP 243 rev.01).
[6] Commission Nationale de l'Informatique et des Libertés [CNIL] (2021). *Practical guide GDPR: Data protection officers*.

alinearse con los más altos estándares internacionales, reconociendo que la confianza digital es el activo más valioso en la economía del siglo XXI. Para cualquier empresa que opere en este contexto, la implementación del rol de DPO trasciende el mero cumplimiento normativo; se trata de una redefinición estratégica de cómo se gestiona la información, se mitigan los riesgos y se construye una relación de confianza duradera con clientes, empleados y la sociedad en su conjunto.

Por su parte, el rol del DPO se fundamenta en una combinación de atributos clave. Debe poseer cualidades profesionales y, en particular, conocimientos expertos en leyes y prácticas de protección de datos,[7] así como la capacidad de cumplir con las tareas establecidas en la legislación correspondiente[8]. Aunque el GDPR no prescribe una única vía de formación, permite a las organizaciones adaptar la cualificación del DPO a la complejidad de su contexto. Al seleccionar un programa de capacitación, se deben considerar factores como la reputación del organismo acreditador y el reconocimiento internacional de la certificación, asegurando que el DPO adquiera y mantenga el nivel de pericia adecuado para su crítico rol.

Es importante destacar que el rol del DPO no puede ser reducido a un mero apéndice legal o a una función de cumplimiento normativo. El DPO es, en su esencia, el custodio de la confianza digital de una organización. Es el guardián que se sitúa en la frontera donde los intereses corporativos se encuentran con los derechos fundamentales. Su misión no es simplemente aplicar la ley, sino infundir en el ADN de la organización una cultura de respeto por la privacidad.

Ser un DPO requiere más que conocimiento. **Exige coraje:** el coraje para defender los principios éticos frente a las presiones comerciales, para cuestionar el *statu quo* y para ser la voz de los que no están en la sala de juntas. **Requiere diplomacia:** la habilidad de un constructor de puentes para conectar los mundos, a menudo dispares, de la tecnología, el derecho, el marketing y la alta dirección, traduciendo complejos requisitos legales en acciones prácticas y comprensibles para todos. Y, sobre todo, **requiere visión:** la capacidad de guiar a la organización no solo hacia el cumplimiento, sino hacia una innovación que sea, ante todo, humana y responsable.

El trabajo de cada DPO es una pieza fundamental en la construcción de un ecosistema digital más justo, transparente y respetuoso. Cada evaluación de impacto que supervisan, cada cláusula de contrato que revisan y cada programa de formación que imparten, fortalece el frágil tejido de la confianza entre las organizaciones y las personas a las que sirven.

Este texto, por lo tanto, trasciende el formato de un manual de funciones. Se erige como un informe estratégico para los arquitectos de la confianza digital, ofreciendo un recurso para empoderarse en su misión fundamental: asegurar que, en la incesante marcha del progreso, la dignidad y los derechos humanos no queden atrás.

---

[7] Ibid.
[8] Véanse Directrices del WP29 sobre los DPOs (WP 243 rev.01), que detallan las cualidades y conocimientos esperados.

1. El Rol Estratégico del Delegado de Protección de Datos (DPO)

1.1. El Delegado de Protección de Datos

El Delegado de Protección de Datos (DPO o Data Protection Officer) es un profesional especializado cuya función principal consiste en supervisar, de manera independiente, desde dentro de una organización, el cumplimiento de la normativa de protección de datos, actuando como un nexo crítico entre la alta dirección, los equipos operativos, los titulares de los datos y las autoridades de control.[9]

En esencia, el DPO actúa como un puente entre los diversos intereses involucrados en el tratamiento de datos personales, equilibrando las necesidades operativas de la organización con los derechos de los titulares y las exigencias regulatorias.[10]

Por lo tanto, no se trata simplemente de un asesor jurídico más, ni de un auditor convencional, ni de un oficial de seguridad de la información; es un rol específico con características distintivas que lo sitúan en una posición única dentro de la estructura organizacional y con un conjunto de responsabilidades claramente definidas que combinan elementos de supervisión, asesoramiento, formación e intermediación.

Para entender su naturaleza, es crucial definirlo tanto por sus responsabilidades y obligaciones, como por las funciones que no le corresponden. Entre las centrales, encontramos:

- Es un Asesor y Supervisor: Su labor es informar, asesorar y supervisar. Actúa como el "director de orquesta" de la privacidad, [11] asegurando que todas las partes de la organización actúen de manera armónica, pero sin ser él quien ejecuta cada tarea.

- No es el Responsable del Cumplimiento: El DPO no es personalmente responsable en caso de una infracción. La responsabilidad legal recae siempre en la organización (el "responsable" o "encargado" del tratamiento). La función del DPO es facilitar el cumplimiento, no garantizarlo por sí mismo.[12]

- No puede ser "Juez y Parte": El DPO no puede ocupar un cargo que le lleve a determinar los fines y medios del tratamiento de datos (ej. Director de Marketing, RRHH o TI), ya que esto crearía un conflicto de interés insalvable con su función de supervisión.[13]

---

[9] Ciclosi, F., & Massacci, F. (2023). The Data Protection Officer: A Ubiquitous Role That No One Really Knows. *IEEE Security & Privacy, 21*(1), 60-69. https://doi.org/10.1109/MSEC.2022.3222115

[10] La autoridad francesa (CNIL) describe al DPO como el "director de orquesta" de la conformidad de los datos personales en una organización. Esta metáfora subraya su rol de coordinación y supervisión, en lugar de ejecución directa. Véase CNIL, "Le Délégué à la Protection des Données", 2021.

[11] Commission Nationale de l'Informatique et des Libertés. (2021). *Practical guide GDPR: Data protection officers*.

[12] Article 29 Data Protection Working Party. (2017). Guidelines on Data Protection Officers (‘DPOs’) (WP 243 rev.01). European Commission.»

[13] Ibid. Véase Sección 3.5 "Conflictos de interés". Esta sección es la base doctrinal para la prohibición de que el DPO ocupe cargos que determinen los fines y medios del tratamiento.

1.2. El origen histórico del Delegado de Protección de Datos

1.2.1. El Contexto Histórico: Alemania 1970 y las Cicatrices de la Memoria

Para comprender verdaderamente la figura del Delegado de Protección de Datos en su plenitud —su propósito fundamental, sus funciones esenciales y sus límites estructurales— resulta insuficiente analizarla únicamente como una creación del Reglamento General de Protección de Datos (RGPD) de 2016. El DPO no constituye un mero oficial de cumplimiento; representa la encarnación institucional de una filosofía jurídica y política que se gestó durante décadas como respuesta a las experiencias más traumáticas del siglo XX.

Viajemos a Alemania en 1970. La informática comenzaba a consolidarse con grandes ordenadores mainframe, bases de datos centralizadas y la promesa revolucionaria de gestionar millones de registros en segundos. Sin embargo, en Alemania esa promesa tecnológica portaba un lado profundamente oscuro: todavía permanecía extraordinariamente viva la memoria colectiva de los censos utilizados sistemáticamente por el régimen nazi para identificar y perseguir minorías, así como los exhaustivos archivos de la Stasi en la Alemania Oriental. Esa experiencia histórica había dejado una herida profunda e indeleble en la conciencia colectiva: el terror visceral a que los datos personales se transformaran nuevamente en armas contra los ciudadanos.

1.2.2. Spiros Simitis: El Arquitecto de un Nuevo Paradigma

En este contexto de memoria histórica y ansiedad tecnológica emerge la figura del Profesor Spiros Simitis (1934-2023), jurista greco-alemán reconocido unánimemente como el "padre de la protección de datos".[14] A finales de la década de 1960, el gobierno del estado federado alemán de Hesse enfrentaba un desafío aparentemente técnico: la modernización de los hospitales públicos mediante la utilización de la incipiente tecnología informática para centralizar y procesar masivamente los datos de los pacientes. Esta iniciativa generó una inquietud fundamental sobre el control y el potencial abuso de información tan extraordinariamente sensible.[15]

Fue precisamente en este momento histórico cuando el gobierno de Hesse recurrió a Simitis, entonces un joven y brillante profesor de la Universidad Goethe de Fráncfort. Sin embargo, Simitis trascendió completamente el encargo técnico inicial y diagnosticó el problema subyacente con una claridad visionaria: el tratamiento automatizado de datos personales creaba una asimetría de poder sin precedentes históricos. Su pregunta revolucionaria cambiaría todo el paradigma: **"¿De qué sirve una ley si solo actúa después de que el daño ya ocurrió?"**[16]

[14] Papakonstantinou, Vagelis. "Spiros Simitis–his legacy: Europeanisation and Internationalisation." *Spiros Simitis–sein Vermächtnis*. Nomos Verlagsgesellschaft mbH & Co. KG, 2024.
[15] https://www.datenschutzzentrum.de/artikel/940-Interview-mit-Prof.-Dr.-Dr.h.c.-Spiros-Simitis.html
[16] Ibid.

1.2.3. La Revolución Conceptual: Del Control Externo a la Supervisión Interna

Hasta ese momento histórico, la protección de datos dependía exclusivamente de autoridades externas que revisaban los ficheros después de su creación. Un modelo inherentemente reactivo, burocrático y, sobre todo, tardío. Cuando un abuso se descubría, invariablemente ya era demasiado tarde para prevenir el daño.

La propuesta de Simitis fue verdaderamente radical para su época:

"No basta con el control desde afuera. Debemos tener a alguien dentro de cada organización, independiente, con conocimiento especializado y autoridad real, que vigile todos los días cómo se utilizan los datos, que pueda decir NO antes de que ocurra el abuso".[17]

Esta visión transformadora se materializó en la **Ley de Protección de Datos de Hesse de 1970**, la primera legislación de su clase en el mundo. En sus visionarios 17 artículos, esta ley pionera estableció no solo los fundamentos conceptuales que hoy estructuran el RGPD, sino que creó una figura revolucionaria: el **funcionario de protección de datos** (*Datenschutzbeauftragter*), obligatorio en cada organismo público.[18]

1.2.4. Las Funciones Fundacionales del Primer DPO

La misión del funcionario de protección de datos, tal como fue concebida originalmente, estableció los pilares que perduran hasta hoy:[19]

- **Supervisar sistemáticamente** cómo se gestionaban y procesaban los datos dentro de la organización.
- **Advertir proactivamente** sobre riesgos potenciales antes de que se transformaran en vulneraciones o escándalos.
- **Servir como puente estratégico** entre los ciudadanos, los directivos organizacionales y la autoridad de control.
- **Garantizar la independencia funcional** para poder actuar sin presiones ni conflictos de interés.

Este modelo transformó completamente la lógica de la protección de datos: **dejó de ser exclusivamente un trámite legal post-facto y se convirtió en una responsabilidad viva, continua y proactiva dentro de la organización**. Por primera vez en la historia, existía alguien independiente operando desde el interior, vigilando las decisiones y defendiendo los derechos fundamentales desde el centro mismo de la acción organizacional.

---

[17] Ibid.
[18] Schneider, Daniel. "Data Protection in Germany: Historical Overview, its Legal Interest and the Brisance of Biobanking." *Trust in Biobanking: Dealing with Ethical, Legal and Social Issues in an Emerging Field of Biotechnology*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012. 169-187.
[19] Ibid.

1.2.5. El Fundamento Filosófico: Autodeterminación Informativa como Pilar Democrático

El mayor legado intelectual de Simitis fue dotar a esta nueva disciplina de una robusta base filosófica y constitucional. Sostenía convincentemente que la protección de datos no constituía un derecho individualista ni un obstáculo burocrático, sino una condición indispensable para la existencia y el funcionamiento de una sociedad democrática libre.

En el corazón de su pensamiento se encuentra el concepto de **autodeterminación informativa**, un principio que posteriormente sería consagrado por el Tribunal Constitucional alemán en su histórica "sentencia del censo" (*Volkszählungsurteil*) de 1983. Este derecho fundamental garantiza al individuo la potestad de decidir, en principio, quién conoce qué información sobre él, cuándo y en qué contexto específico.[20]

Simitis advirtió con extraordinaria clarividencia que un ciudadano que se siente constantemente observado, inseguro de si sus comportamientos "desviados" están siendo registrados y almacenados, inevitablemente tenderá a la autocensura y al conformismo social. Un individuo así no puede ejercer plenamente sus libertades fundamentales y, por tanto, no puede ser un participante genuinamente activo en la vida democrática.

1.2.6. De Hesse a Europa: La Expansión Global de un Modelo

El modelo alemán pionero —innovador en los años 70— inspiró progresivamente las legislaciones de protección de datos en todo el mundo. Su influencia fue determinante en:

- **Nivel Internacional (década de 1980)**: Las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, y especialmente el Convenio 108 del Consejo de Europa, el primer tratado internacional vinculante en la materia.
- **Nivel Europeo (década de 1990)**: La Directiva 95/46/CE, que armonizó por primera vez las legislaciones nacionales de los Estados miembros y estableció la figura del responsable de protección de datos como una opción recomendada.
- **La Consolidación Global (2016)**: El Reglamento General de Protección de Datos (RGPD), que elevó al Delegado de Protección de Datos a una figura obligatoria para determinadas organizaciones, consolidando definitivamente su rol como pilar fundamental de la gobernanza de datos.

1.2.7. El Legado Permanente: Del Funcionario de Hesse al DPO Global

Hoy, más de cinco décadas después de aquella primera ley en Hesse, el Delegado de Protección de Datos continúa teniendo la misma misión fundamental: **ser el contrapeso interno que asegura que la tecnología sirva a las personas y no al revés**. Su existencia representa la materialización institucional de las lecciones históricas más dolorosas del siglo XX y la determinación colectiva de que nunca más los datos personales se conviertan en instrumentos de opresión.

---

[20] Yaegashi, João Gabriel, Cleber Sanfelici Otero, and Robson Borges Maia. "A influência da Volkszählungsurteil no ordenamento jurídico brasileiro: um norte para a construção do direito à proteção de dados pessoais para a tutela da personalidade." *Opinión Jurídica* 23.49 (2024).

El DPO moderno no es simplemente un requisito legal; es el heredero de una tradición jurídica y filosófica que sitúa la protección de la información personal en el corazón mismo de la libertad y la democracia. Es, en última instancia, el custodio de un principio constitucional fundamental, un actor clave en la mediación de las tensiones entre la tecnología, la economía y los derechos fundamentales en el siglo XXI.

1.3. Estándares Internacionales y Marcos de Referencia: El Compás del DPO

- Reglamento General de Protección de Datos (GDPR - Reglamento UE 2016/679): Es el marco de referencia principal que define la figura, posición y funciones del DPO.[21]

- Comentarios Legales Especializados: Textos como los de *von dem Bussche,*[22] *Plath,*[23] o *Gola*[24] ofrecen interpretaciones doctrinales detalladas sobre la aplicación del GDPR, siendo fundamentales para un análisis jurídico profundo.

- Directrices del Comité Europeo de Protección de Datos (CEPD): Documentos como las directrices sobre los DPOs[25] o sobre los conceptos de responsable y encargado del tratamiento son de obligado cumplimiento interpretativo.

- Ley Chilena N° 19.628 con su nueva reforma: Es la normativa local que articula los derechos de los titulares y las obligaciones de los responsables en Chile, incluyendo las atribuciones de la futura Agencia de Protección de Datos.[26]

- Estándares de Seguridad de la Información (BSI, ISO): El Compendio *IT-Grundschutz* del BSI alemán[27] o las normas ISO/IEC 27001/27701[28] proporcionan los marcos técnicos y organizativos para implementar las medidas de seguridad que la ley de protección de datos exige, pero no detalla. El DPO debe conocerlos para poder evaluar la adecuación de las medidas adoptadas.

- Documentos de Autoridades de Control (CNIL, AEPD, LfDI BW): Publicaciones como las bases de conocimiento para DPIAs de la CNIL[29] o las guías prácticas del LfDI de

---

[21] Art. 37-39 GDPR.

[22] Voigt, Paul, and Axel von dem Bussche. "Cooperation with Supervisory Authorities." *The EU General Data Protection Regulation (GDPR) A Practical Guide*. Cham: Springer Nature Switzerland, 2024. 261-273.

[23] Voigt, Paul, and Axel Von dem Bussche. "The eu general data protection regulation (gdpr)." *A practical guide, 1st ed., Cham: Springer International Publishing* 10.3152676 (2017): 10-5555.

[24] Voigt, Paul, and Axel von dem Bussche. "Enforcement and fines under the GDPR." *The EU General Data Protection Regulation (GDPR) A Practical Guide*. Cham: Springer Nature Switzerland, 2024. 275-299.

[25] Directrices del Grupo de Trabajo del Artículo 29 sobre los Delegados de Protección de Datos (WP 243 rev.01), adoptadas el 13 de diciembre de 2016 y revisadas el 5 de abril de 2017

[26] https://www.bcn.cl/leychile/navegar?idNorma=141599&idVersion=2026-12-01

[27] Mathew, Delin, Simon Hacks, and Horst Lichter. "Developing a semantic mapping between TOGAF and BSI-IT-Grundschutz." Multikonferenz Wirtschaftsinformatik (MKWI) 2018. Leuphana Universität Lüneburg, 2018.

[28] Lachaud, Eric. "ISO/IEC 27701 standard: Threats and opportunities for GDPR certification." Eur. Data Prot. L. Rev. 6 (2020): 194.

[29] Commission Nationale de l'Informatique et des Libertés (CNIL). (2018). Privacy Impact Assessment (PIA). CNIL

Baden-Württemberg[30] ofrecen orientaciones prácticas y criterios aplicables a situaciones concretas.

1.4. Pilares Fundamentales del Rol del DPO

La función del DPO se sostiene sobre tres pilares interconectados, como lo detallan las principales guías de las autoridades europeas y las mejores prácticas internacionales:

1.4.1. Cualidades profesionales y conocimiento

El DPO debe ser designado sobre la base de sus cualidades profesionales y, en particular, de sus conocimientos especializados del Derecho y la práctica en materia de protección de datos.[31] Este conocimiento debe ser proporcional a la complejidad, sensibilidad y escala de los datos tratados por la organización. Las competencias clave incluyen:[32]

- Experiencia jurídica: Un conocimiento profundo de las leyes y prácticas de protección de datos, tanto nacionales como europeas.
- Comprensión técnica: Entendimiento de las operaciones de tratamiento, las tecnologías de la información y la seguridad de los datos.
- Conocimiento profundo del negocio: Familiaridad con el sector empresarial y la estructura organizacional.

- Habilidad de liderazgo: Capacidad para promover una cultura de protección de datos dentro de la organización.

1.4.2. Autonomía e Independencia: El Escudo de la Objetividad

Este es el pilar más protegido por las normas de protección de datos personales. La independencia del DPO, esencial para la objetividad de su supervisión, se garantiza principalmente a través de tres mecanismos cruciales:

- No recibe instrucciones sobre el desempeño de sus funciones. No se le puede indicar cómo ejercer sus funciones, qué resultado alcanzar en una investigación o si debe consultar a la autoridad. Su juicio debe ser libre.
- Reporta directamente al más alto nivel jerárquico de la organización para asegurar que sus advertencias sean escuchadas. Para asegurar que sus advertencias sean escuchadas; Informa directamente a la "máxima autoridad directiva o administrativa", asegurando que sus advertencias y recomendaciones lleguen sin filtros ni intermediarios al centro del poder decisorio.

---

[30] Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V., Berufsbild des Datenschutzbeauftragten (DSB) / Professional Profile of the Data Protection Officer (DPO), 4.ª ed. (Berlín: Berufsverband der Datenschutzbeauftragten Deutschlands, 2019), p. 12,

[31] Ver Art. 37.5 del GDPR.

[32] Article 29 Data Protection Working Party. (2017). Guidelines on Data Protection Officers ('DPOs') (WP 243 rev.01). European Commission.».

- Está protegido contra represalias, no pudiendo ser destituido ni sancionado por el ejercicio de sus tareas. Lo anterior está expresamente descrito en el artículo 38. Por su parte, el artículo 50 de la reformada Ley 19.628, que entrará en vigencia el 1 de diciembre de 2026, mandata que el Delegado "deberá contar con autonomía respecto de la administración" y que el responsable debe garantizar que no existan "conflictos de interés".[33]

Esta independencia no es una opción, sino una condición sine qua non para que su supervisión sea creíble y eficaz.

[33] Artículo 50.- Atribuciones del delegado. El responsable de datos podrá designar un delegado de protección de datos personales.

El delegado de protección de datos deberá ser designado por la máxima autoridad directiva o administrativa del responsable de datos. Se considerará como la máxima autoridad directiva o administrativa al directorio, un socio administrador o a la máxima autoridad de la empresa o servicio, según corresponda.

El delegado de protección de datos deberá contar con autonomía respecto de la administración, en las materias relacionadas con esta ley. En las micro, pequeñas y medianas empresas, el dueño o sus máximas autoridades podrán asumir personalmente las tareas de delegado de protección de datos.

El delegado de protección de datos podrá desempeñar otras funciones y cometidos, procurando mantener la independencia en su función. El responsable garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

Las sociedades o entidades que pertenezcan a un mismo grupo empresarial, empresas relacionadas o sujetas a un mismo controlador en los términos previstos en la Ley de Mercado de Valores, podrán designar un único delegado de protección de datos, siempre que todas ellas operen bajo los mismos estándares y políticas en materia de tratamiento de datos personales, y el delegado sea accesible para todas las entidades y establecimientos.

La designación del delegado de protección de datos debe recaer en una persona que reúna los requisitos de idoneidad, capacidad y conocimientos específicos para el ejercicio de sus funciones.

Los titulares de datos podrán ponerse en contacto con el delegado de protección de datos en lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo de esta ley.

El delegado de protección de datos estará obligado a mantener estricto secreto o confidencialidad de los datos personales que conociere en ejercicio de su cargo. Los funcionarios públicos que desempeñen estas funciones e infrinjan este deber de secreto o confidencialidad, serán sancionados de conformidad a lo que se prescribe en los artículos 246 a 247 bis del Código Penal. El responsable se hará cargo por las infracciones al deber de secreto o confidencialidad que debía cumplir su encargado de prevención o delegado de protección, sin perjuicio de las acciones de repetición que pueda ejercer contra éste.

El responsable de datos deberá disponer que el delegado cuente con los medios y facultades suficientes para el desempeño de sus funciones, debiendo otorgarle los recursos materiales necesarios para realizar adecuadamente sus labores, en consideración al tamaño y capacidad económica de la entidad.

Sin perjuicio de las demás funciones que se le puedan asignar, el delegado de protección de datos tendrá las siguientes funciones:

a) Informar y asesorar al responsable de datos, a los terceros encargados o mandatarios y a los dependientes del responsable, respecto de las disposiciones legales y reglamentarias relativas al derecho a la protección de los datos personales y a la regulación de su tratamiento.

b) Promover y participar en la política que dicte el responsable de datos respecto de la protección y el tratamiento de los datos personales.

c) Supervisar el cumplimiento de la presente ley y de la política que dicte el responsable, dentro del ámbito de su competencia.

d) Preocuparse de la formación permanente de las personas que participan en las operaciones de tratamiento de datos.

e) Asistir a los miembros de la organización en la identificación de los riesgos asociados a la actividad de tratamiento y las medidas a adoptar para resguardar los derechos de los titulares de datos personales.

f) Desarrollar un plan anual de trabajo y rendir cuenta de sus resultados.

g) Absolver las consultas y solicitudes de los titulares de datos.

h) Cooperar y actuar como punto de contacto de la Agencia.

1.4.3. Misión Basada en el Riesgo

Aunque no se detalla explícitamente en el artículo 50, el enfoque de riesgo es un principio transversal en la Ley. Así, por ejemplo, el artículo 15 ter (Evaluación de impacto) y el artículo 14 quinquies (Medidas de seguridad) exigen una evaluación basada en los riesgos para los derechos de los titulares. El Delegado debe, por tanto, priorizar su actuación en función de dichos riesgos. Este enfoque implica:

a) **Pragmatismo y selectividad:** Debe priorizar sus actividades, dedicando la mayor parte de su tiempo y recursos a los asuntos que presentan mayores riesgos.

b) **Proporcionalidad:** El nivel de escrutinio y las medidas que propone deben ser proporcionales a la sensibilidad, complejidad y escala de los datos tratados.

En resumen, el Delegado es mucho más que un requisito legal. Es un actor estratégico, un facilitador del cumplimiento y un custodio de la confianza digital, cuya eficacia depende directamente de su pericia, su independencia y los recursos que la organización le asigne para cumplir su crítica misión.

1.5. ¿Es obligatorio contar con un DPO en Chile?

Para responder a esta pregunta, es fundamental examinar lo que establece el Artículo 49 de la Ley N° 19.628, el cual regula los "Modelos de prevención de infracciones".

El inicio de este artículo es claro al señalar que la adopción de dicho modelo por parte del responsable de datos es una acción voluntaria:

"Los responsables de datos podrán voluntariamente adoptar un modelo de prevención de infracciones consistente en un programa de cumplimiento".

Esto significa que ninguna organización está obligada de manera general a implementar un "Modelo de prevención de infracciones" según la ley.

Sin embargo, el mismo Artículo 49 continúa especificando qué debe incluir este modelo si el responsable decide adoptarlo. Establece que "El programa de cumplimiento deberá contener, al menos, los siguientes elementos". Aquí es donde surge la obligación específica en relación con el DPO.

Dentro de la lista de elementos que obligatoriamente deben conformar este modelo (si se opta por él), el Artículo 49, letra a), menciona explícitamente:

"a) La designación de un delegado de protección de datos personales."

Adicionalmente, la letra b) refuerza la importancia de esta figura dentro del modelo al requerir la definición de sus "medios y facultades".

En consecuencia:

- La decisión de adoptar un "Modelo de prevención de infracciones" según el Artículo 49 es voluntaria para el responsable de datos.
- Pero, si el responsable decide adoptar este modelo, entonces la designación de un Delegado de Protección de Datos (DPO) deja de ser opcional y se convierte en un requisito obligatorio como componente esencial de ese modelo de cumplimiento específico.
- Por lo tanto, un DPO no es una figura universalmente obligatoria para todos los responsables en Chile, sino que su obligatoriedad está condicionada a la decisión del responsable de implementar el mecanismo de "Modelo de prevención de infracciones" contemplado en el Artículo 49 de la ley.[34]

1.6. El Rol Estratégico del Delegado de Protección de Datos (DPO)

El Delegado de Protección de Datos asume un rol que trasciende el cumplimiento para convertirse en una pieza clave de la estrategia corporativa. Su relevancia se manifiesta en la capacidad de la organización para navegar la complejidad del entorno digital y construir una base sólida de confianza, operando en el delicado equilibrio entre los objetivos legítimos del negocio y la protección de los derechos fundamentales.[35]

En este contexto, el DPO asume un rol especialmente crítico y estratégico en las organizaciones por múltiples razones interconectadas. Entre estas, se encuentra la propia complejidad de las actividades de tratamientos de datos que pueden ser particularmente desafiantes en diversos sectores, pues muchas actividades empresariales implican procesos que abarcan interacciones prolongadas con los clientes o empleados y que incluyen tratamientos sofisticados. Pensemos, por ejemplo, en el perfilado para la segmentación de mercado, las evaluaciones automatizadas de riesgo crediticio, el análisis de comportamiento para personalizar servicios y prevenir el abandono de clientes (churn), o la gestión de datos de salud ocupacional en el ámbito de los recursos humanos.

Precisamente, el DPO aporta una mirada especializada para evaluar estos procesos desde la perspectiva de la protección de datos, identificando riesgos específicos —como la discriminación algorítmica o la exclusión financiera— y proponiendo medidas de mitigación adaptadas al contexto operacional. Adicionalmente, la sensibilidad de la información gestionada por muchas empresas requiere un enfoque particularmente cuidadoso. La organización maneja información que a menudo es confidencial y, en algunos casos, especialmente sensible para la vida económica o personal de los individuos.

[34] Los "Modelos de prevención de infracciones" regulados en el Artículo 49 de la Ley N° 19.628 son voluntarios para los responsables. Sin embargo, su adopción y certificación (Art. 51) pueden ser consideradas como una circunstancia atenuante de responsabilidad en caso de infracción (Art. 36), incentivando su implementación.
[35] Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V., Das berufliche Leitbild der Datenschutzbeauftragten, 46.

Dicha información puede incluir datos financieros detallados, historiales de transacciones, información laboral sensible, y en ciertos contextos, datos de salud, afiliación sindical, o incluso datos biométricos para la verificación de identidad.[36]

En consecuencia, el DPO actúa como un guardián de estos datos sensibles, velando por que reciban el nivel de protección técnica y organizativa que merecen y que se implementen garantías adecuadas para prevenir usos indebidos o accesos no autorizados, conforme a los más altos estándares de seguridad.[37]

1.7. Contribución a la Gestión de Marcos Regulatorio Duales y complejos

En entornos con una regulación dual, donde coexisten leyes de protección de datos generales y normativas sectoriales específicas, el Delegado de Protección de Datos (DPO) juega un papel crucial. Su función es armonizar el cumplimiento de estos múltiples marcos, aportando su conocimiento especializado en Protección de Datos Personales complementado con una profunda comprensión del contexto sectorial. Esto le permite desarrollar soluciones integradas y eficientes que cumplen con todas las exigencias aplicables.
Un ejemplo claro de esta armonización se da en el sector financiero. Una entidad debe cumplir no solo con la ley de protección de datos, sino también con normativas sobre prevención de blanqueo de capitales que la obligan a retener ciertos datos por un período prolongado. Aquí, el DPO debe asesorar sobre cómo cumplir ambas obligaciones, por ejemplo, bloqueando los datos para que solo sean accesibles para el fin de prevención del blanqueo una vez que la finalidad comercial original haya expirado, aplicando así el principio de limitación de la finalidad.

Asimismo, mientras una normativa sectorial puede exigir la conservación de datos durante un largo período para fines de auditoría, la ley de protección de datos exige minimizar la retención. En esta situación, el DPO asesoraría sobre cómo cumplir *ambas* obligaciones, como por ejemplo, mediante el bloqueo de los datos una vez finalizada la finalidad principal, manteniéndolos disponibles únicamente para la autoridad sectorial competente, aplicando así de forma práctica los principios de limitación de la finalidad y del plazo de conservación.[38]

1.8. Aporte a la Gestión de Riesgos y la Innovación

En el ámbito de la gestión de riesgos, el Delegado de Protección de Datos (DPO) aporta metodologías específicas de evaluación y gestión de riesgos de protección de datos que complementan y enriquecen las evaluaciones de riesgo operacional o de ciberseguridad convencionales. Su enfoque, centrado en los "derechos y libertades de las personas físicas", permite identificar vulnerabilidades y consecuencias potenciales —como la angustia emocional, la discriminación o la pérdida de oportunidades— que podrían pasar desapercibidas en análisis

[36] La Ley chilena N° 19.628, en su Artículo 2°, define los datos sensibles, incluyendo estados de salud, ideología, opiniones políticas, entre otros. El GDPR hace lo propio en su Artículo 9.
[37] Véase el *IT-Grundschutz-Kompendium* (BSI, 2023) o las normas ISO/IEC 27001, que proporcionan marcos detallados para las medidas técnicas y organizativas (TOMs) que el DPO debe supervisar.
[38] Kneuper, R. (2021). *Datenschutz für Softwareentwicklung und IT*. Discute los principios generales del GDPR, como la limitación del plazo de conservación, en un contexto práctico.

de riesgos tradicionales. Esto contribuye así a una gestión más integral y efectiva, tal como lo exige una Evaluación de Impacto relativa a la Protección de Datos (EIPD o DPIA).[39]

Esta gestión de riesgos, particularmente a través del enfoque de DPIA, se vincula intrínsecamente con la innovación. La competitividad en muchos sectores exige continua innovación tecnológica, desde mejoras en interfaces digitales hasta el uso de inteligencia artificial para asesoramiento personalizado. En este contexto, el DPO no es un freno, sino que facilita que esta innovación se desarrolle de manera responsable. Lo logra incorporando la Protección de datos personales desde el Diseño y por Defecto[40] en nuevos productos y servicios, permitiendo a la organización aprovechar el potencial de los datos mientras se respetan los derechos fundamentales de los titulares y se construye una ventaja competitiva basada en la confianza..

1.9. Construcción de Confianza y Alcance de Responsabilidad

Finalmente, en cualquier sector donde la confianza es el pilar fundamental de la relación con los clientes, contar con un Delegado de Protección de Datos (DPO) visible y accesible demuestra el compromiso institucional con la protección de datos. Esto ofrece a los titulares de datos (clientes, empleados, etc.) un canal especializado y cualificado para consultas o reclamaciones relacionadas con el tratamiento de su información personal. Esta transparencia y accesibilidad contribuyen significativamente a construir y mantener la confianza de los titulares de datos en la gestión ética de su información.

Dicho esto, es importante destacar que, a pesar de su rol central en la gobernanza de datos, el DPO no es personalmente responsable del incumplimiento normativo en materia de protección de datos. Esa responsabilidad recae íntegramente en la organización como Responsable del Tratamiento.[41]

En línea con esta distinción, el DPO asesora, supervisa e informa, pero no decide ni implementa por sí mismo las medidas de protección. La decisión final sobre si asumir un riesgo o cómo implementar un control operativo recae en la dirección o en las áreas de negocio correspondientes. Este punto es crucial para entender correctamente el alcance de sus funciones, preservar su independencia y evitar conflictos de interés, como se detallará en los siguientes apartados de esta guía.

[39] Friedewald, M., et al. *White Paper DATENSCHUTZ-FOLGENABSCHÄTZUNG*. Este documento profundiza en la DPIA como herramienta para identificar y mitigar riesgos para los derechos y libertades.
[40] Euroepan, Data Protection Board. "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default."
[41] Esta distinción es explícitamente aclarada en las Directrices WP 243 rev.01, p. 19. La responsabilidad final siempre es del responsable o del encargado del tratamiento.

1.10. Roles Afines: Data Protection Manager Y Otras Figuras Relacionadas

1.10.1. Data Protection Manager (DPM)

El Data Protection Manager (DPM)[42] o Gerente de Protección de Datos es una figura que, a diferencia del DPO, no está explícitamente definida en marcos regulatorios como el GDPR, sino que ha surgido como respuesta organizativa a la necesidad de gestionar operativamente los programas de protección de datos. Mientras el DPO tiene un enfoque predominantemente supervisor, consultivo e independiente, el DPM tiene generalmente un carácter más ejecutivo y operacional.

El DPM suele ser responsable de implementar y gestionar diariamente las políticas y procedimientos de protección de datos, coordinar las actividades relacionadas con el cumplimiento de la Protección de Datos Personales—como mantener el Registro de Actividades de Tratamiento (RoPA)— y ejecutar los planes de acción derivados de las recomendaciones del DPO.

La diferencia fundamental radica en que el DPM no requiere la independencia formal que caracteriza al DPO, pudiendo estar integrado en la cadena jerárquica convencional y recibir instrucciones directas sobre su actividad. En organizaciones grandes, el DPM puede actuar como complemento operativo al DPO, ejecutando e implementando lo que el DPO asesora y supervisa, creando así una sinergia eficaz entre supervisión independiente y ejecución operativa.

1.10.2. Chief Privacy Officer (CPO)

El Chief Privacy Officer (CPO)[43] o Director de Privacidad es otra figura relevante, especialmente común en corporaciones multinacionales de origen norteamericano. El CPO suele tener un perfil ejecutivo de alto nivel, con responsabilidad directa sobre la estrategia de privacidad de la organización y autoridad para tomar decisiones e implementarlas.

A diferencia del DPO, que mantiene una posición independiente y consultiva, el CPO es típicamente parte del equipo directivo y tiene responsabilidad ejecutiva sobre programas y políticas de privacidad.
En algunas organizaciones, estas funciones pueden solaparse, pero conceptualmente responden a enfoques distintos: mientras el DPO es un supervisor independiente establecido por regulación, el CPO es un ejecutivo con autoridad decisoria establecida por la organización.

[42] Kneuper, Ralf. "Foundations of Data Protection According to GDPR." *Data Protection for Software Development and IT: A Practical Introduction*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2024. 21-65.
[43] Bantan, May, and Mazen Shawosh. "Chief Privacy Officer: A Systematic Literature Review and Future Research Directions." *Communications of the Association for Information Systems* 54.1 (2024): 792-814.

1.10.3. Privacy Champion

El Privacy Champion[44] o Campeón (Embajador) de Privacidad es un rol menos formal pero cada vez más utilizado en programas de privacidad maduros. Se trata de personas dentro de diferentes áreas de la organización (no dedicadas exclusivamente a privacidad) que actúan como puntos focales y promotores de buenas prácticas en sus respectivos departamentos.

Estos "campeones" reciben formación específica en protección de datos y sirven como multiplicadores de la cultura de privacidad, enlaces con el DPO, y facilitadores de la implementación de medidas en sus áreas.
En una organización, establecer una red de Privacy Champions en departamentos clave como TI, Marketing, Operaciones, Recursos Humanos y Atención al Cliente podría complementar eficazmente la labor del DPO, extendiendo su alcance y eficacia.

1.10.4. Data Governance Manager

Finalmente, el Data Governance Manager[45] o Responsable de Gobernanza de Datos tiene un enfoque más amplio sobre la gestión de todos los activos de información de la organización, no solo datos personales. Este rol se enfoca en la calidad, integridad, accesibilidad y utilidad de los datos para la organización, independientemente de su carácter personal.

Mientras el DPO se centra en el cumplimiento normativo y la protección de derechos, el Data Governance Manager busca maximizar el valor de los datos como activo organizacional. En una organización, ambos roles podrían colaborar estrechamente para asegurar que las iniciativas de gobernanza de datos incorporen adecuadamente los requisitos de protección de datos desde sus fases iniciales.

1.10.5. Modelo Recomendado para la realidad chilena

Considerando las distintas figuras y enfoques analizados, y en el contexto organizacional general, especialmente para empresas de cierta envergadura, es recomendable implementar un modelo que considere un DPO como figura central de supervisión independiente. Este rol se complementaría potencialmente con un Data Protection Manager para aspectos operativos, si el volumen de trabajo lo justifica, y con una red de Privacy Champions en departamentos clave. Esta estructura permitiría equilibrar efectivamente la independencia supervisora con la capacidad operativa de implementación, maximizando así la efectividad y la resiliencia del programa de protección de datos de la organización.

[44] Tahaei, Mohammad, Alisa Frik, and Kami Vaniea. "Privacy champions in software teams: Understanding their motivations, strategies, and challenges." *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 2021.
[45] Plotkin, David. *Data stewardship: an actionable guide to effective data management and data governance*. Academic press, 2020.

Capítulo 2: El Mandato del DPO

Funciones y Responsabilidades en la Organización

2.1 Información y Asesoramiento

Conocimiento actualizado
- Seguimiento normativo y jurisprudencial
- Informes periódicos y alertas
- Sesiones informativas adaptadas

Asesoramiento en tratamientos
- Base legal más adecuada
- Minimización y limitación de finalidad
- Transparencia con titulares
- Medidas técnicas y organizativas

Consultoría por departamento
- Marketing: campañas y captación
- TI: privacidad desde el diseño
- RRHH: datos de empleados
- Legal: contratos comerciales

2.2 Supervisión del Cumplimiento

Auditorías periódicas
- Conformidad con principios GDPR
- Calidad de información
- Implementación de TOMs
- Políticas internas

Monitorización continua
- KPIs de consentimientos
- Tiempos respuesta ARSOP
- Actualización RoPA
- Medidas datos sensibles

Gestión y reporting
- Informes trimestrales/semestrales
- Registro de no conformidades
- Planes de remediación
- Seguimiento correctivo

2.3 Cultura de Protección de Datos

Programa formativo
- Formación básica obligatoria
- Especializada por áreas
- Ejecutiva para dirección
- Actualizaciones periódicas

Materiales y herramientas
- Guías prácticas por proceso
- Checklists estandarizados
- FAQs y glosario
- Protocolos de actuación

Comunicación interna
- Hub de Privacidad intranet
- Boletines informativos
- Email semanalmente
- Sesiones Q&A abiertas

2.4 Cooperación con Autoridad de Control

Punto de contacto
- Interlocutor oficial designado
- Datos censo/contacto formalizados
- Comunicación centralizada

Gestión de inspecciones
- Coordinación solicitudes info
- Facilitación de accesos
- Trazación requerimientos
- Seguimiento comunicaciones

Consultas y notificaciones
- Consultas preventivas
- Notificación de brechas
- Dudas interpretativas
- Cumplimiento plazos legales

2.5 Evaluaciones de Impacto (DPIAs)

Determinación necesidad
- Nuevas tecnologías (IA, biometría)
- Perfilado sistemático
- Datos sensibles a gran escala
- Vigilancia zonas públicas

Metodología DPIA
- Fases y etapas template
- Herramientas de análisis
- Criterios valoración riesgos
- Plantillas documentación

Revisión y supervisión
- Análisis proporcionalidad
- Valoración de riesgos
- Medidas de mitigación
- Dictamen formal

2.6 Punto de Contacto Titulares

Canales dedicados
- Email específico DPO
- Formulario web privacidad
- Teléfono directo
- Reuniones presenciales

Gestión derechos ARSOP
- Identificación segura
- Respuesta en plazo legal
- Formato comprensible
- Trazabilidad completa

Mediación y educación
- Resolución conflictos
- Materiales informativos
- Lenguaje accesible
- Ejemplos prácticos

Asesor Experto | Supervisor | Educador | Enlace Regulador | Evaluador Riesgos | Defensor Datos

Figura 1 - El Mandato Completo del DPO: Funciones y Responsabilidades

2. El Mandato del DPO: Funciones y Responsabilidades

El DPO en una organización debe asumir una serie de funciones específicas. Estas funciones representan el núcleo de su actividad profesional y constituyen su aportación distintiva a la gobernanza de datos personales en la institución.

2.1. Función de Información y Asesoramiento

Esta función,[46] implica que el DPO debe informar y asesorar a la dirección y a sus empleados sobre las obligaciones derivadas de la normativa de protección de datos. En el contexto de una organización, esta función se concreta en:

2.1.1. Mantenimiento de conocimiento actualizado

La función de información y asesoramiento, implica que el DPO debe informar y asesorar a la dirección y a sus empleados sobre las obligaciones derivadas de la normativa de protección de datos. Esta función se concreta en diversas actividades continuadas y sistemáticas.

En primer lugar, el DPO debe mantener un conocimiento actualizado y profundo sobre la evolución normativa en materia de protección de datos, incluyendo el seguimiento detallado de la tramitación del proyecto de ley chileno, nuevas regulaciones sectoriales con impacto en privacidad, jurisprudencia relevante nacional e internacional, y tendencias globales aplicables al sector.

Este conocimiento actualizado no debe permanecer como un activo individual del DPO, sino que debe ser comunicado periódicamente a las áreas relevantes de la organización mediante informes periódicos, alertas específicas sobre cambios significativos, o sesiones informativas adaptadas a diferentes audiencias dentro de la organización.

2.1.2. Asesoramiento sobre nuevos tratamientos de datos

Un aspecto crucial de esta función consiste en proporcionar asesoramiento específico y oportuno sobre nuevos tratamientos de datos.

Cuando la organización planee implementar nuevos procesos que impliquen tratamiento de datos personales, como nuevas aplicaciones móviles para clientes, sistemas de autenticación biométrica, programas de fidelización o personalización, o herramientas de analítica avanzada para segmentación de clientes, el DPO debe proporcionar un asesoramiento integral.

Este asesoramiento abarca aspectos como:

- La legitimidad del tratamiento y base legal aplicable, asegurando que exista un fundamento jurídico adecuado para cada operación.

[46] Smolle, Michael. "Datenschutzkontrolle und Aufsicht." *Datenschutz in der Kommunalverwaltung*. Erich Schmidt Verlag GmbH & Co. KG, Berlin, 2023. 717-739.

- La aplicación de los principios de minimización de datos y limitación de finalidad, garantizando que solo se recojan los datos estrictamente necesarios para los fines especificados.

- Los requisitos de transparencia e información a los titulares de datos, asegurando que las comunicaciones sean claras, accesibles y completas.

- Las medidas técnicas y organizativas adecuadas para proteger los datos, siguiendo un enfoque basado en riesgo.

- La evaluación sobre la necesidad de realizar evaluaciones de impacto, identificando aquellos tratamientos que podrían suponer un alto riesgo para los derechos y libertades de los titulares de datos.

2.1.3. Consultoría interna especializada

El DPO debe también establecerse como un consultor interno especializado disponible para las diferentes áreas de la organización, adaptando su asesoramiento a las necesidades específicas de cada departamento.

- Para el departamento de Marketing, por ejemplo, el DPO revisará campañas publicitarias, formularios de captación de datos y políticas de comunicación con clientes, asegurando que se respeten las preferencias de Protección de Datos Personales y se utilicen adecuadamente las bases de legitimación.

- Para el área de Tecnología, proporcionará asesoramiento sobre la implementación de los principios de Protección de Datos Personales desde el diseño y por defecto en nuevos desarrollos, ayudando a integrar salvaguardas de Protección de Datos Personales desde las fases iniciales de los proyectos.

- Para el departamento de Atención al Cliente, ofrecerá orientación específica sobre la gestión de derechos ARSOP de los titulares de datos, asegurando respuestas adecuadas y dentro de los plazos establecidos.

- Para Recursos Humanos, atenderá consultas sobre el tratamiento de datos de empleados, un ámbito con características y requisitos propios.

- Para el departamento Legal, proporcionará apoyo especializado en la redacción de cláusulas de Protección de Datos Personales en contratos con proveedores, asegurando que se establezcan garantías adecuadas cuando se compartan datos personales con terceros.

2.1.4. Emisión de recomendaciones formales

Como parte de esta función asesora, el DPO debe además emitir recomendaciones formales sobre aspectos críticos en materia de protección de datos personales. Estas recomendaciones, dirigidas a la alta dirección o a los responsables de área correspondientes, representan la opinión

técnica oficial en materia de Protección de Datos Personales deben documentarse adecuadamente para demostrar la diligencia de la organización (accountability).

Las recomendaciones deben ser claras, fundamentadas en la normativa aplicable, y orientadas a soluciones prácticas que equilibren el cumplimiento con las necesidades operativas de la organización.

2.2. Función de Supervisión del Cumplimiento

El DPO debe supervisar el cumplimiento de la normativa de protección de datos y de las políticas internas en esta materia. En una organización, esto implica:

2.2.1. Auditorías periódicas de cumplimiento

Para ejercer eficazmente esta función supervisora, el DPO debe desarrollar y ejecutar un programa estructurado de auditoría interna sobre los procesos, sistemas y departamentos que impliquen tratamiento de datos personales. Estas auditorías no deben ser vistas como un ejercicio punitivo, sino como una herramienta colaborativa para identificar debilidades y fortalecer la postura de cumplimiento de la organización. Siguiendo una estrategia de auditoría bien definida,[47] estas evaluaciones deben abarcar aspectos fundamentales como:

- La conformidad con los principios básicos de protección de datos (licitud, lealtad, transparencia, minimización, exactitud, etc.), verificando su aplicación práctica en las operaciones diarias. Por ejemplo, una auditoría podría revisar si los datos recogidos en un formulario de marketing son realmente los mínimos necesarios para la finalidad declarada.

- La existencia y calidad de la información proporcionada a los titulares de datos, comprobando que sea completa, fácilmente comprensible y accesible, tal como exigen las guías de las autoridades de protección de datos.

- La implementación efectiva de las medidas técnicas y organizativas de seguridad, asegurando que no queden solo en políticas escritas, sino que se traduzcan en prácticas reales y verificables. Esto implica, por ejemplo, revisar la configuración de los controles de acceso a las bases de datos[84], la efectividad de las políticas de contraseñas o los procedimientos de eliminación segura de soportes de datos, siempre desde la perspectiva de la normativa de protección de datos personales.

- El cumplimiento general de políticas y procedimientos internos de protección de datos, verificando la coherencia entre lo que la organización ha documentado en su marco normativo interno y lo que realmente se practica en el día a día.

La auditoría debe ser un proceso integral que revise la organización, la infraestructura y la documentación relevante, incluyendo conceptos, políticas, registros y evaluaciones de Impacto.

[47] Behrendt, H. (2024). *Der Datenschutzbeauftragte*. Describe una estrategia de auditoría que incluye revisión de listas de verificación, análisis documental e inspecciones.

2.2.2. Verificación de conformidad de nuevos productos y servicios

Complementariamente a las auditorías periódicas, el DPO debe ejercer una labor de verificación previa de la conformidad (*ex ante*) de nuevos productos y servicios con la normativa de protección de datos. Cuando la organización desarrolle nuevas ofertas, ya sean aplicaciones tecnológicas, servicios de asesoría personalizada basados en algoritmos, o nuevos canales de comunicación con los clientes, el DPO debe evaluarlos antes de su lanzamiento al mercado. Esta evaluación debe culminar con la emisión de un dictamen técnico específico, que puede incluir recomendaciones de mejora de carácter vinculante para el área promotora.

Esta intervención temprana, un pilar de la metodología de Protección de Datos Personales desde el Diseño,[48] permite identificar y resolver problemas potenciales antes de que los productos o servicios lleguen al mercado. Actuar de esta forma proactiva no solo es una exigencia de la responsabilidad proactiva, sino que también evita costosas modificaciones posteriores, reduce el riesgo de sanciones y previene daños reputacionales.

[48] Barezzani, Sergio. "Data Protection by Design and by Default (DPbDD)." Encyclopedia of Cryptography, Security and Privacy. Cham: Springer Nature Switzerland, 2025. 577-579.

Privacy Gates en el Ciclo de Desarrollo

Puntos de Control Obligatorios - Privacy by Design

Metodología Waterfall | Metodología Agile/Scrum

IDEACIÓN
Concepto inicial

G1 Privacy Gate 1: Viabilidad — OBLIGATORIO

- ✓ Identificar datos personales necesarios
- ✓ Evaluar base legal preliminar
- ✓ Análisis de proporcionalidad inicial
- ✓ Decisión: ¿Requiere DPIA?

DISEÑO
Arquitectura

G2 Privacy Gate 2: Arquitectura — OBLIGATORIO

- ✓ Validar principio de minimización
- ✓ Definir medidas de seguridad (TOMs)
- ✓ Revisar flujos de datos
- ✓ Aprobar diseño de consentimientos

DESARROLLO
Construcción

G3 Privacy Gate 3: Implementación — RECOMENDADO

- ✓ Verificar implementación de controles
- ✓ Revisar APIs de derechos ARSOP
- ✓ Validar cifrado y anonimización
- ✓ Auditar logs y trazabilidad

PRUEBAS
QA/Testing

G4 Privacy Gate 4: Validación — OBLIGATORIO

- ✓ Confirmar uso de datos de prueba
- ✓ Testing de funciones de privacidad
- ✓ Validar políticas de privacidad
- ✓ Pruebas de portabilidad y borrado

LANZAMIENTO
Go-Live

G5 Privacy Gate 5: Go/No-Go — OBLIGATORIO

- ✓ Certificado de conformidad DPO
- ✓ DPIA finalizada (si aplica)
- ✓ Avisos de privacidad actualizados
- ✓ Plan de respuesta a incidentes

Privacy Gates en Metodología Ágil (Por Sprint)

Sprint Planning	Sprint Design	Sprint Review	Definition of Done
DPO revisa backlog Identifica user stories con impacto privacy	Validación de arquitectura privacy por incremento	Demo incluye features privacy Feedback DPO	Checklist privacy como criterio de aceptación

Figura 2 - Privacy Gates en el Ciclo deDesarrdlo - Privacy by Design Operativo

2.2.3. Monitorización continua

La supervisión del cumplimiento no puede limitarse a fotografías puntuales en el tiempo, como son las auditorías. Para una supervisión efectiva y dinámica, el DPO debe establecer mecanismos de monitorización continua sobre aspectos clave de la protección de datos, utilizando indicadores de rendimiento (KPIs) y de riesgo (KRIs) desde una perspectiva sistémica dentro de un sistema de gestión de datos personales propiamente tal. Estos mecanismos incluirán, entre otros:

- Indicadores y sistemas de seguimiento sobre la gestión y trazabilidad de consentimientos, asegurando que se registren adecuadamente, se respeten las preferencias expresadas por los titulares y que sea posible demostrar su validez en cualquier momento.[49]

- La atención a solicitudes de derechos ARSOP (o los derechos equivalentes según la ley aplicable) dentro de los plazos legalmente establecidos, monitorizando los tiempos medios de respuesta y la calidad y completitud de las mismas, tal como exigen normativas como la Ley N° 19.628.[50]

- La calidad y actualización periódica de los registros de actividades de tratamiento (RoPA), verificando que reflejen con exactitud la realidad de las operaciones de la organización, un requisito central tanto del GDPR como de la nueva normativa chilena.

- El cumplimiento de medidas de seguridad específicamente diseñadas para datos sensibles, atendiendo a su particular criticidad y a los mayores riesgos asociados a su tratamiento.

Esta monitorización puede apoyarse en reuniones periódicas con los responsables de los procesos, tal como hacen otras instituciones para asegurar el cumplimiento.

2.2.4. Informes periódicos de cumplimiento

Como parte integral de su función supervisora, y como principal vehículo para rendir cuentas ante la alta dirección, el DPO debe elaborar informes periódicos (por ejemplo, trimestrales o semestrales) sobre el estado general de cumplimiento en materia de protección de datos. Estos informes deben ser estratégicos, yendo más allá de una simple lista de hallazgos. Deben identificar fortalezas, debilidades, riesgos emergentes y áreas de mejora, proporcionando una visión integral y ejecutiva del nivel de madurez en Protección de Datos Personales de la organización.

Los informes se presentarán a la alta dirección y, en su caso, al Comité de Riesgos o al Directorio, siguiendo las rutas de comunicación y notificación establecidas. Esto garantiza que las cuestiones de Protección de Datos Personales reciban atención al más alto nivel organizativo y que la dirección disponga de la información necesaria para tomar decisiones informadas y asignar recursos de manera adecuada.

---

[49] Gradow, L., & Greiner, R. (2021). *Quick Guide Consent-Management*. Se discute el marco TCF de IAB como un ejemplo de sistema de gestión de consentimiento.

[50] Ley N° 19.628, que en su versión modificada establece la gratuidad y periodicidad del ejercicio de derechos.

2.2.5. Gestión de no conformidades

Adicionalmente, cuando el DPO detecte incumplimientos o no conformidades a través de sus actividades de supervisión, su función no termina con la mera identificación. Debe documentarlos formalmente en un registro, proponer medidas correctivas específicas y viables, y realizar un seguimiento riguroso del plan de remediación hasta su resolución completa. Este seguimiento implica verificar la efectividad de las soluciones implementadas y asegurarse de que el problema subyacente ha sido corregido para prevenir su recurrencia. Esta gestión de no conformidades es un componente esencial del ciclo de mejora continua que un programa de protección de datos maduro debe tener.[51]

2.3. Función de Promoción de Cultura de Protección de Datos Personales

Una de las funciones más trascendentales y, a menudo, más desafiantes del DPO es la de ser un arquitecto y promotor de una cultura de la protección de datos personales.[52] La normativa considera esta capacidad como parte intrínseca de la "capacidad para cumplir sus funciones" del DPO.

Un marco normativo robusto y las medidas técnicas más avanzadas resultan insuficientes si los empleados no comprenden su importancia y su rol en la protección de los datos. Por ello, esta función cultural y educativa es fundamental para lograr un cumplimiento que sea sostenible, proactivo y que forme parte del ADN de la organización. Esta misión se concreta en diversas actividades continuadas que el DPO debe liderar e impulsar en toda la empresa.

2.3.1. Programa de formación y sensibilización

El pilar de la construcción cultural es la formación. El DPO debe diseñar e implementar un programa estructurado y continuo de formación en protección de datos, el cual debe ser diferenciado por niveles y perfiles para maximizar su relevancia y eficacia. No se trata de un único curso genérico, sino de un plan de aprendizaje adaptado:

- Formación básica obligatoria para todos los empleados: Una sesión inicial (onboarding) y recordatorios anuales para establecer una línea de base común de conocimiento sobre los principios fundamentales, las políticas internas y las responsabilidades individuales.

- Formación especializada para áreas de alto riesgo: Talleres prácticos y detallados para los equipos que tratan intensivamente datos personales, como TI (sobre desarrollo seguro de software[136]), Marketing (sobre gestión de consentimientos y cookies[246]), y Atención al Cliente (sobre la gestión de los derechos de los titulares).

[51] Hanschke, I. (2020). *Informationssicherheit und Datenschutz....* Describe los componentes de un sistema de gestión integrado, que incluye la gestión de no conformidades y la mejora continua.
[52] Oikonomidis, Y., et al. "Data Privacy, Ethical, GDPR & Regulatory Compliance V1."

- Sesiones específicas para la alta dirección: Formación ejecutiva centrada en la responsabilidad estratégica, la gestión de riesgos de privacidad, el impacto de las brechas de datos y el valor de la confianza digital como ventaja competitiva.

- Actualización periódica sobre nuevas amenazas o requisitos: Cápsulas informativas o talleres sobre temas emergentes, como nuevas técnicas de ingeniería social, vulnerabilidades en software o cambios normativos relevantes.

La existencia de materiales de capacitación es, en sí misma, una medida organizativa auditable y un componente clave de la diligencia debida.[53]

2.3.2. Desarrollo de guías y materiales

Para que la formación se traduzca en práctica diaria, el DPO debe crear y mantener un repositorio de herramientas y materiales de consulta prácticos y accesibles. El objetivo es desmitificar la complejidad de la normativa y ofrecer orientación clara y aplicable:

- Guías prácticas sobre cómo aplicar los principios de protección de datos en procesos cotidianos, como la gestión de datos de candidatos en RRHH o el tratamiento de datos en eventos corporativos.

- Listas de verificación (*checklists*) para procesos estandarizados, como el lanzamiento de una nueva campaña de marketing o la contratación de un nuevo proveedor que tratará datos personales.

- Protocolos de actuación para situaciones específicas, como la respuesta a una solicitud de derechos o la identificación y escalamiento inicial de un posible incidente de seguridad.

- FAQs (Preguntas Frecuentes) sobre protección de datos en el contexto específico de la organización, que den respuesta a las dudas más comunes de los empleados.

- Un glosario de términos unificado para asegurar que todos en la organización, desde TI hasta Legal, hablen el mismo idioma y entiendan conceptos clave de la misma manera.[54]

2.3.3. Canales de comunicación interna

La cultura no se crea con un único evento, sino a través de una comunicación constante y multicanal. El DPO debe establecer y gestionar canales efectivos para difundir conocimiento, celebrar las buenas prácticas y mantener la Protección de Datos Personales en la mente de todos:

---

[53] *Criteria-Catalogue-for-Processor_Scope-DE_v3_0.pdf*. La existencia de materiales de capacitación para empleados es un elemento verificable.

[54] Kneuper, R. (2021). *Datenschutz für Softwareentwicklung und IT*.

- Una sección específica en la intranet corporativa, que funcione como un "Hub de Privacidad" o "Plataforma de Privacidad",[55] centralizando políticas, guías, contactos y noticias.

- Boletines periódicos sobre protección de datos y privacidad, que informen sobre novedades normativas, consejos prácticos o resúmenes de incidentes de seguridad (anonimizados) para fomentar el aprendizaje.

- Foros de discusión o canales en plataformas colaborativas sobre casos prácticos, donde los empleados puedan compartir experiencias y resolver dudas de forma colectiva.
- Sesiones abiertas de consulta, un formato muy eficaz donde cualquier empleado puede plantear dudas específicas directamente al DPO o su equipo en un entorno seguro y de confianza, fomentando una comunicación transparente que construye confianza.[56]

2.3.4. Promoción de Protección de Datos Personales desde el diseño y por defecto

Un aspecto particularmente importante de esta función cultural, y que representa el nivel más alto de madurez, es la promoción activa del enfoque de Protección de Datos Personales desde el Diseño y por Defecto.[57] El DPO debe trabajar estrechamente y de forma colaborativa con las áreas de desarrollo de productos, servicios e innovación para asegurar que los principios de protección de datos se integren desde las fases más tempranas de conceptualización de cualquier proyecto.

Esto significa participar en las reuniones de diseño, revisar los requisitos funcionales, y ayudar a los equipos a pensar en la Protección de Datos Personales no como un obstáculo final, sino como una característica de calidad esencial. Este enfoque preventivo y proactivo, además de ser una obligación legal (Art. 25 GDPR), reduce significativamente los costes y riesgos asociados a modificaciones posteriores, creando así una sinergia positiva entre cumplimiento, eficiencia e innovación. Es la manifestación más clara de una cultura donde la Protección de Datos Personales no es una ocurrencia tardía, sino un valor fundamental.[58]

---

[55] *SAK2024_IB09_Modulare_Dokumentation_Pecher.pdf*. Menciona la "Plataforma de Privacidad" de un ministerio como ejemplo de recurso centralizado.
[56] Cheimonidis, Pavlos. "The responsibilities of the DPO according to the GDPR." (2019).
[57] En el ámbito de la protección de datos, especialmente bajo el Reglamento General de Protección de Datos (RGPD), los conceptos de "protección de datos desde el diseño" (Data Protection by Design) y "privacidad desde el diseño" (Privacy by Design), junto con sus contrapartes "por defecto" (by Default), son a menudo utilizados de manera intercambiable. Históricamente, "Privacy" ha tendido a enfocarse más en la confidencialidad técnica, mientras que "Data Protection" se percibe de forma más amplia, incluyendo los derechos de los interesados. Sin embargo, el RGPD los considera como los mismos requisitos fundamentales, especialmente en su Artículo 25. El concepto de "Privacy by Design" fue desarrollado originalmente por la Dra. Ann Cavoukian, ex Comisionada de Información y Privacidad de Ontario, Canadá, y se basa en 7 principios fundacionales.
[58] Drev, Matjaž, and Boštjan Delak. "Conceptual model of privacy by design." *Journal of Computer Information Systems* 62.5 (2022): 888-895.

Protocolo de Privacy Champions

Marco Estratégico de Multiplicadores de Cultura de Privacidad

ARQUITECTURA DEL PROGRAMA CHAMPIONS

Red distribuida de expertise y evangelización en protección de datos

1:50	12m	4h	20h
RATIO ÓPTIMO	COMPROMISO	DEDICACIÓN/MES	FORMACIÓN BASE

CRITERIOS DE SELECCIÓN

REQUISITOS FUNDAMENTALES

- ✓ Antigüedad mínima 12 meses
- ✓ Posición de influencia demostrada
- ✓ Disponibilidad 10% tiempo laboral
- ✓ Endorsement directo del manager

COMPETENCIAS TÉCNICAS

- ✓ Comunicación efectiva multidisciplinar
- ✓ Interés genuino en protección datos
- ✓ Capacidad de simplificación conceptual
- ✓ Ausencia de conflictos de interés

PERFIL DE COMPETENCIAS

Liderazgo de Influencia
Capacidad de generar cambio sin autoridad formal

Facilitación Natural
Habilidad para guiar conversaciones complejas

Pensamiento Sistémico
Visión holística del impacto organizacional

Orientación al Servicio
Motivación intrínseca de apoyo a colegas

Adaptabilidad Cognitiva
Capacidad de traducir entre contextos

MATRIZ OPERACIONAL DE RESPONSABILIDADES

Distribución de actividades por frecuencia y criticidad

DIARIAS

- → Consultas ad-hoc del equipo
- → Observación de prácticas
- → Modelado de comportamiento
- → Microformaciones informales

SEMANALES

- → Sincronización con DPO
- → Revisión proyectos área
- → Actualización registro issues
- → Tips semanales al equipo

MENSUALES

- → Reunión red Champions
- → Reporte métricas actividad
- → Sesión formativa área
- → Auditoría de procesos

TRIMESTRALES

- → Evaluación de desempeño
- → Actualización competencias
- → Propuestas de mejora
- → Reconocimiento formal

RUTA DE DESARROLLO Y CERTIFICACIÓN

1 FUNDAMENTOS
Mes 1
Marco normativo Ley 19.628
Principios GDPR aplicables
Políticas internas organización

2 APLICACIÓN
Mes 2-3
Casos prácticos simulados
Role playing situacional
Shadowing con DPO

3 ESPECIALIZACIÓN
Mes 4-5
Focus área específica
Proyectos reales supervisados
Mentoring a nuevos champions

4 CERTIFICACIÓN
Mes 6
Evaluación competencias
Proyecto capstone
Badge digital oficial

ECOSISTEMA DE SOPORTE

- **Knowledge Base** — Wiki colaborativo con FAQs
- **Canal Dedicado** — #privacy-champions
- **Newsletter** — Updates exclusivos mensuales
- **Video Library** — Webinars y casos grabados
- **Templates** — Checklists y formularios
- **Hotline DPO** — Escalamiento directo

PROGRAMA DE RECONOCIMIENTO Y PROGRESIÓN

CHAMPION BRONCE
3 meses activo | Formación básica completada | 5+ consultas resueltas exitosamente

CHAMPION PLATA
6 meses activo | Proyecto implementado con impacto medible | Mentoring activo

CHAMPION ORO
12 meses activo | Liderazgo demostrado | Impacto organizacional documentado

Figura 3 Protocolo Privacy Champions - Marco de Multiplicadores de Cultura de Privacidad - Versión Ejecutiva 2025

2.4. Función de Cooperación con la Autoridad de Control

El DPO tiene el mandato expreso de cooperar con la autoridad de control y actuar como punto de contacto principal para esta en todas las cuestiones relativas al tratamiento de datos personales. Esta no es una función meramente reactiva o pasiva; un DPO eficaz gestiona esta relación de forma proactiva, transparente y colaborativa, posicionando a la organización como un actor diligente y responsable. Esta función es crítica, ya que la autoridad de control (en el caso de Chile, la futura Agencia de Protección de Datos)[59] es el organismo con la potestad de fiscalizar, investigar e imponer sanciones. En el contexto de una organización, esto se materializa en varias responsabilidades clave.

2.4.1. Punto de contacto oficial

El DPO será el interlocutor designado y cualificado ante la futura Agencia de Protección de Datos chilena para todas las cuestiones relacionadas con el tratamiento de datos personales. Sus datos de contacto (nombre, cargo, correo electrónico, teléfono) deben ser comunicados formalmente a la autoridad una vez que ésta se constituya.

Esta designación centraliza la comunicación, asegurando que las interacciones con el regulador sean gestionadas por un experto que comprende tanto la normativa como la operativa interna de la organización. Esto evita respuestas descoordinadas o incompletas que podrían generar desconfianza o dar lugar a investigaciones más profundas. La autoridad debe saber que tiene una contraparte fiable y competente a la que dirigirse.[60]

2.4.2. Facilitación de inspecciones

En caso de que la organización sea objeto de una inspección, una auditoría programada o una investigación formal por parte de la autoridad de control, el DPO actuará como el coordinador interno y facilitador principal del proceso. Su rol es asegurar una cooperación fluida y eficaz, lo que implica:

- Gestionar y centralizar las solicitudes de información, asegurando que se proporcione la documentación solicitada —como políticas, registros de actividades de tratamiento (RoPA), Evaluaciones de Impacto (DPIAs) o contratos con encargados— de manera completa, precisa y oportuna.

- Facilitar el acceso a documentación, personal e instalaciones cuando sea requerido, coordinando las entrevistas con los empleados pertinentes y las visitas a las instalaciones (como centros de datos o archivos físicos) de forma ordenada.

- Actuar como "traductor" entre la autoridad y las áreas internas, ayudando a la organización a comprender correctamente el alcance y la finalidad de la inspección, y a la autoridad a entender el contexto operativo de los tratamientos de datos.

[59] Ley N° 19.628, en su versión modificada, que establece las funciones y atribuciones de la Agencia de Protección de Datos.
[60] Directrices del Grupo de Trabajo del Artículo 29 sobre los DPOs (WP 243 rev.01). Abordan la designación y el rol del DPO como punto de contacto con la autoridad supervisora.

- Asegurar que las recomendaciones o requerimientos resultantes de la inspección se comprendan, se distribuyan a los responsables y se implementen adecuadamente, realizando un seguimiento posterior de su cumplimiento.

2.4.3. Consultas a la autoridad

El DPO también puede —y debe— ejercer un papel proactivo en la relación con la autoridad. La normativa prevé la posibilidad de realizar consultas previas a la autoridad de control[61] cuando una Evaluación de Impacto (DPIA) revela un alto riesgo residual que la organización no puede mitigar por sí misma. Sin embargo, la cooperación va más allá. El DPO puede consultar de manera preventiva cuando existan dudas interpretativas significativas sobre la aplicación de la normativa a situaciones específicas y novedosas del sector, que no estén claras en la ley o en guías existentes.

Esta capacidad de consulta anticipada es particularmente valiosa en sectores altamente regulados o en la implementación de tecnologías emergentes. El DPO actuará como canal formal para estas consultas, asegurando que se planteen de manera técnicamente correcta y jurídicamente fundamentada, y que las respuestas obtenidas se implementen adecuadamente en la organización. Esta proactividad demuestra buena fe y un compromiso genuino con el cumplimiento.

2.4.4. Notificación de brechas de seguridad

Aunque la decisión final de notificar una brecha de seguridad a la autoridad recae en el responsable del tratamiento, el DPO desempeña un papel central en este proceso. Asesorará sobre si el incidente cumple los criterios para ser notificado, supervisará la recopilación de la información necesaria para la notificación y, habitualmente, será el encargado de realizar la comunicación formal con la autoridad, asegurando que se cumplan los estrictos plazos legales.[62] Su experiencia es crucial para gestionar una de las situaciones más críticas y de mayor exposición para la organización.

En resumen, la cooperación con la autoridad de control no es una mera formalidad. Es una función estratégica que, bien gestionada, puede mitigar riesgos, resolver incertidumbres y construir una reputación de organización confiable y transparente ante los ojos del regulador.

2.5. Función de Asesoramiento en Evaluaciones de Impacto (DPIAs)

El DPO debe asesorar sobre la evaluación de impacto relativa a la protección de datos (EIPD o DPIA, por sus siglas en inglés) y supervisar su aplicación. Las evaluaciones de impacto constituyen una herramienta fundamental del enfoque preventivo y basado en riesgo que caracteriza a los marcos modernos de protección de datos, como el GDPR.

---

[61] Art. 36 GDPR.

[62] El Artículo 33(1) del GDPR establece que la notificación a la autoridad de control debe realizarse "sin dilación indebida y, de ser posible, dentro de las 72 horas siguientes a que haya tenido constancia de ella".

Son un ejercicio de responsabilidad proactiva (*accountability*) en acción, que obliga a la organización a analizar y mitigar sistemáticamente los riesgos de un tratamiento de datos *antes* de que este se inicie. El DPO juega un papel central, aunque no de ejecución, en su adecuada implementación en una organización. Su función es la de un asesor experto y un supervisor objetivo.[63]

2.5.1. Asesoramiento sobre la necesidad de DPIA

Una primera responsabilidad clave consiste en determinar qué operaciones de tratamiento requieren una evaluación de impacto, basándose en criterios objetivos establecidos por la normativa y las mejores prácticas, por ejemplo:

- El DPO analizará aspectos como el uso de nuevas tecnologías con potencial impacto en Protección de Datos Personales(inteligencia artificial, biometría, geolocalización).

- La realización de evaluaciones sistemáticas de aspectos personales, incluida la elaboración de perfiles para predecir comportamientos o preferencias de clientes.

- El tratamiento a gran escala de categorías especiales de datos, como los datos de salud sensibles;

- La vigilancia sistemática de zonas de acceso público, como los sistemas de videovigilancia en sucursales. Este análisis permitirá identificar aquellos tratamientos que, por su naturaleza, alcance, contexto o finalidades, podrían entrañar un alto riesgo para los derechos y libertades de los titulares de datos, requiriendo por tanto una evaluación formal de impacto.

2.5.2. Metodología para DPIAs

El DPO debe desarrollar y mantener una metodología específica para realizar evaluaciones de impacto adaptada al contexto de la organización, que incluya:

- Fases y cronograma del proceso.

- Cuestionarios y herramientas de análisis.

- Criterios de valoración de riesgos.

- Plantillas para documentación.

[63] Grütter, Bodo Jeremy, and Bettina Schneider. "Data protection impact assessment guidelines in the context of the general data protection regulation." (2019).

2.5.3. Revisión de DPIAs

Cuando se realice una evaluación de impacto, ya sea para un nuevo tratamiento o para uno existente que experimente cambios significativos, el DPO debe revisar diversos aspectos críticos:

- Examinará el análisis de necesidad y proporcionalidad del tratamiento, verificando que se hayan considerado alternativas menos intrusivas y que el alcance del tratamiento sea el mínimo necesario para lograr los fines legítimos perseguidos.

- Evaluará la identificación y valoración de riesgos realizada, asegurando que se hayan considerado todos los impactos potenciales sobre los derechos y libertades de los titulares de datos personales.

- Verificará la adecuación de las medidas de mitigación propuestas, analizando si son suficientes para reducir los riesgos a un nivel aceptable.

- Emitirá un dictamen formal sobre la DPIA que exprese su opinión profesional sobre la viabilidad del tratamiento desde la perspectiva de protección de datos.

2.5.4. Supervisión de la implementación

El DPO debe verificar que las medidas de mitigación identificadas en las DPIAs se implementan efectivamente y establecer mecanismos de seguimiento para garantizar su continuidad.

2.5.5. Función como Punto de Contacto para Titulares de Datos

Según el artículo 38(4) del GDPR, los interesados pueden contactar con el DPO por lo que respecta a todas las cuestiones relacionadas con el tratamiento de sus datos personales y el ejercicio de sus derechos. Esto se concreta en:

2.5.6. Canal específico de contacto

Para facilitar esta comunicación directa, el DPO debe contar con canales dedicados y fácilmente accesibles para que los titulares de datos puedan realizar consultas o reclamaciones sobre protección de datos. Estos canales incluirán:

- Un correo electrónico específico y claramente identificado como perteneciente al DPO, diferenciado de las direcciones generales de atención al cliente.

- Un formulario web de contacto específico para cuestiones de privacidad, accesible desde la sección de Protección de Datos Personales del sitio web de la organización.

- Un teléfono directo o extensión específica que permita la comunicación inmediata cuando sea necesario.

- La posibilidad de concertar reuniones presenciales previa cita para asuntos que requieran una interacción más directa o compleja.

La existencia y forma de acceso a estos canales debe comunicarse claramente a todos los titulares de datos como parte de la política de privacidad y en otros materiales informativos relevantes.

2.6. Coordinación de atención a derechos ARSOP

Una responsabilidad clave del DPO en este ámbito consiste en establecer procedimientos claros y eficientes para la gestión de los derechos ARSOP ampliados (acceso, rectificación, supresión, oposición, portabilidad, bloqueo).

Estos procedimientos deben garantizar la identificación adecuada y segura del solicitante, evitando tanto la exposición indebida de datos a terceros como la imposición de barreras excesivas que dificulten el ejercicio de derechos; la respuesta dentro del plazo legal establecido; la presentación de la información solicitada en un formato comprensible, estructurado y adaptado a las características del solicitante; y la completa trazabilidad de la gestión, documentando cada paso del proceso para demostrar el cumplimiento.

2.6.1. Mediación en casos de conflicto

Cuando un cliente no esté satisfecho con la respuesta recibida a una solicitud relacionada con sus datos, el DPO debe actuar como mediador imparcial entre el área de negocio responsable y el titular, buscando una resolución satisfactoria que equilibre los intereses legítimos de ambas partes.

Esta función mediadora requiere una posición de independencia y objetividad, evaluando la situación desde la perspectiva de la normativa de protección de datos y no exclusivamente desde la conveniencia operativa o comercial de la organización.

2.6.2. Información y educación

Complementariamente, el DPO debe desarrollar materiales informativos específicos para los titulares de datos sobre sus derechos en materia de protección de datos y los procedimientos para ejercerlos.

Estos materiales deben utilizar un lenguaje claro, accesible y libre de tecnicismos innecesarios, adaptado al perfil general de los titulares de datos de la organización; incluir ejemplos concretos y relevantes que ilustran el ejercicio de derechos en situaciones habituales del ámbito operativo; explicar los plazos, formatos y posibles resultados de las diferentes solicitudes; y estar disponibles en múltiples formatos y canales para garantizar su accesibilidad a todos los titulares de datos.

2.7. Funciones Específicas según el Contexto Operacional

Además de las funciones generales y transversales mencionadas, el DPO de una organización debe asumir funciones específicas que se derivan del contexto operacional, sectorial y tecnológico particular de la empresa. Su asesoramiento y supervisión deben estar anclados en la realidad del negocio para ser verdaderamente eficaces. Estas funciones adaptativas demuestran la capacidad del DPO para traducir los principios abstractos de la ley en soluciones concretas para los desafíos específicos de su organización.

2.7.1. Armonización normativa

En sectores altamente regulados como la banca, los seguros, las telecomunicaciones o la salud, el DPO debe analizar y asesorar sobre la compleja interrelación entre la normativa general de protección de datos y la regulación sectorial aplicable. Su función es ser un intérprete experto capaz de navegar este entorno normativo complejo,[64] identificando:

- Posibles contradicciones y cómo resolverlas, por ejemplo, entre el derecho al olvido y las obligaciones de conservación de registros con fines de prevención de blanqueo de capitales.

- Requisitos acumulativos que deben cumplirse, donde la normativa sectorial impone obligaciones de seguridad o confidencialidad adicionales a las de la ley de protección de datos.

- Especificidades del tratamiento de datos en el ámbito operacional, como los requisitos para el tratamiento de datos de salud en investigación médica como, por ejemplo, bajo el GDPR[65] o la gestión de datos de tráfico en telecomunicaciones.

El DPO debe ser capaz de desarrollar guías internas y criterios de actuación que armonicen estas diferentes capas regulatorias, proporcionando seguridad jurídica a la organización.

2.7.2. Protocolos especiales para datos sensibles

Dada la naturaleza de muchas operaciones comerciales, es probable que se traten datos especialmente sensibles que requieren un nivel de protección reforzado. El DPO debe liderar el desarrollo de protocolos específicos para el tratamiento de estas categorías de datos, asegurando la implementación de medidas técnicas y organizativas robustas. Esto incluye:

- Datos de salud sensibles: Definir protocolos para su recogida, almacenamiento seguro (p. ej., cifrado robusto), control de acceso estrictamente limitado bajo el principio de "necesidad de conocer" y su uso con fines de investigación.

- Datos biométricos para verificación de identidad: Asesorar sobre la proporcionalidad de su uso, las garantías contra la suplantación y la gestión segura de las plantillas biométricas.

---

[64] *Manejo de Entorno Regulatorio Complejo* (del Anexo), y Schrader, L. F. (2022). *Datenschutz im Gesundheitswesen.* Ambas fuentes apuntan a la necesidad de que el DPO domine el marco regulatorio dual y específico de su sector.

[65] Schrader, L. F. (2022). *Op. cit*. Un ejemplo claro de la especialización requerida para sectores como el de la salud.

- Datos de menores de edad: Establecer procedimientos para la verificación de la edad y la obtención del consentimiento de los padres o tutores cuando sea aplicable.

- Información financiera detallada: Supervisar las medidas de seguridad para proteger los datos de transacciones, cuentas y perfiles de riesgo crediticio contra el fraude y el acceso no autorizado.

2.7.3. Estrategias de anonimización

Para permitir análisis estadísticos, desarrollo de modelos actuariales, investigación o mejora de servicios sin comprometer la Protección de Datos Personales de los individuos, el DPO debe asesorar sobre técnicas de anonimización y seudonimización.[66] Su rol no es implementar técnicamente estas soluciones, sino:

- Evaluar si una técnica propuesta alcanza una anonimización real (donde la reidentificación es razonablemente imposible) o si se trata de una seudonimización (donde la reidentificación sigue siendo posible con información adicional).

- Asesorar sobre la técnica más adecuada para cada caso de uso, como la microagregación para la divulgación estadística[67] o el uso de *hashes* para la seudonimización de identificadores.

- Garantizar que los datos seudonimizados sigan siendo tratados como datos personales, con las salvaguardas correspondientes, y que la información que permite la reidentificación se almacene de forma segura y separada.

2.7.4. Gestión de transferencias internacionales

En un entorno de negocio globalizado, el DPO debe supervisar y asesorar sobre los flujos internacionales de datos[68] que puedan producirse en el contexto de la organización, que a menudo son complejos y conllevan riesgos significativos. Esto incluye:

- Uso de servicios en la nube (*cloud*) cuyos servidores están ubicados fuera de las fronteras nacionales.[69]

- Tratamiento de datos de titulares que residen en el extranjero.

- Colaboraciones y acuerdos con socios internacionales que impliquen el intercambio de datos personales.

---

[66] Ribeiro, Sérgio Luís, and Emilio Tissato Nakamura. "Privacy protection with pseudonymization and anonymization in a health IoT system: results from ocariot." *2019 IEEE 19th International Conference on Bioinformatics and Bioengineering (BIBE)*. IEEE, 2019.

[67] Kneuper, R. (2021). *Datenschutz für Softwareentwicklung und IT*.

[68] Marelli, Massimo. "Transferring personal data to international organizations under the GDPR: an analysis of the transfer mechanisms." *International Data Privacy Law* 14.1 (2024): 19-36.

[69] Blume, Joshua. "A Contextual Extraterritoriality Analysis of the DPIA and DPO Provisions in the GDPR." *Geo. J. Int'l L.* 49 (2017): 1425.

El DPO debe evaluar la existencia de una base legal para la transferencia, como una decisión de adecuación de la autoridad competente, la firma de Cláusulas Contractuales Tipo (CCTs), o la implementación de Normas Corporativas Vinculantes (BCRs), y asesorar sobre las garantías adicionales que puedan ser necesarias.[70]

2.7.5. Asesoría sobre comunicaciones con titulares de datos

Finalmente, el DPO debe establecer criterios claros y un marco de gobernanza sobre las comunicaciones con los titulares, ayudando a la organización a encontrar el equilibrio adecuado entre sus objetivos y el respeto a la privacidad. Esto implica asesorar sobre:

- La distinción entre comunicaciones operativas y comunicaciones comerciales, y la base legal apropiada para cada una (p. ej., ejecución de contrato vs. consentimiento).

- Los requisitos para obtener un consentimiento válido para fines de marketing,[71][72] que debe ser libre, específico, informado e inequívoco.

- La personalización de servicios y ofertas, asegurando que se realice de forma transparente y no discriminatoria, y que los titulares puedan oponerse a dicho perfilado.

- El cumplimiento de las obligaciones de información sectorial que puedan existir, integrándolas de forma coherente con los requisitos de transparencia de la ley de protección de datos.

[70] Tras la sentencia del Tribunal de Justicia de la Unión Europea en el caso C-311/18 ("Schrems II"), las transferencias basadas en Cláusulas Contractuales Tipo (CCTs) requieren una evaluación caso por caso (Transfer Impact Assessment - TIA) por parte del exportador de datos para verificar si la legislación del país de destino garantiza un nivel de protección sustancialmente equivalente al de la UE. El DPO juega un rol crucial en asesorar sobre estas complejas evaluaciones.
[71] Dubé, Jean-Pierre, et al. "The intended and unintended consequences of privacy regulation for consumer marketing." (2025).
[72] Gradow, L., & Greiner, R. (2021). *Quick Guide Consent-Management*.

Funciones que NO corresponden al DPO

Delimitación clara de responsabilidades para preservar la independencia

Definición de Políticas y Estrategias

NO

El DPO NO debe:

- ✗ Determinar fines y medios del tratamiento
- ✗ Aprobar políticas y procedimientos
- ✗ Decidir sobre legitimidad de tratamientos
- ✗ Establecer bases legales
- ✗ Definir periodos de conservación

→ Alta Dirección y Gestión

Implementación Técnica y Operativa

NO

El DPO NO debe:

- ✗ Desarrollar soluciones técnicas
- ✗ Gestionar infraestructura tecnológica
- ✗ Ejecutar derechos ARSOP operativamente
- ✗ Administrar controles de acceso
- ✗ Implementar medidas de seguridad

→ TI y Seguridad

Representación Legal y Defensa

NO

El DPO NO debe:

- ✗ Representar ante tribunales
- ✗ Defender ante autoridades
- ✗ Negociar acuerdos o sanciones
- ✗ Firmar documentos legales

→ Departamento Legal

Ejecución de DPIAs

NO

El DPO NO debe:

- ✗ Realizar DPIAs completas
- ✗ Diseñar las TOMs específicas
- ✗ Implementar mitigaciones
- ✗ Aprobar ejecución final
- ✗ Análisis técnicos especializados

→ Áreas de Negocio

Auditoría y Control Interno General

NO

El DPO NO debe:

- ✗ Auditoría interna general
- ✗ Implementar controles internos
- ✗ Certificar cumplimiento formal
- ✗ Auditorías técnicas de seguridad
- ✗ Supervisión disciplinaria

→ Auditoría Interna

Decisiones sobre Brechas

NO

El DPO NO debe:

- ✗ Decidir sobre notificación
- ✗ Aprobar contenido comunicaciones
- ✗ Liderar respuesta técnica
- ✗ Decisiones disciplinarias
- ✗ Comunicación externa

→ Comité de Crisis

Gestión Operativa de Datos

NO

El DPO NO debe:

- ✗ Administrar bases de datos
- ✗ Gestionar procesos masivos de datos
- ✗ Gestión operativa de consentimientos
- ✗ Diseño de formularios y documentos
- ✗ Gestión de calidad de datos
- ✗ Ejecutar transferencias de datos

→ Áreas Operativas y TI

Principios Fundamentales para la Exclusión de Funciones

Evitar Conflictos de Interés | Preservar Función Supervisora | Mantener Independencia | Claridad de Responsabilidades | Proteger Objetividad

Figura 4 - Funciones que NO Corresponden al DPO Completo

3. Delimitación del Rol: Funciones que NO Corresponden al DPO

Para garantizar la independencia funcional, la efectividad supervisora y el correcto posicionamiento organizacional del DPO, es tan esencial definir lo que hace como establecer con claridad meridiana qué funciones NO deben asignársele.

Esta delimitación no solo protege la integridad de la función del DPO, evitando conflictos de interés inherentes, sino que también clarifica las responsabilidades dentro de la organización. Asignar al DPO tareas incompatibles con su rol supervisor no solo contraviene el espíritu y la letra de la normativa, sino que diluye la responsabilidad donde realmente debe recaer: en la dirección y las áreas de negocio como responsables del tratamiento.

3.1. Definición de Políticas y Estrategias de Tratamiento de Datos

El DPO asesora sobre la estrategia de datos, pero no la define. La responsabilidad de determinar los fines y los medios del tratamiento es la definición misma de "responsable del tratamiento". Por tanto, el DPO NO debe asumir las siguientes funciones:[73][74]

3.1.1. Determinación de fines y medios del tratamiento de datos personales

El DPO no debe decidir qué datos personales se recogerán para un nuevo producto, para qué finalidades específicas se utilizarán (p. ej., para marketing, para análisis de riesgo, etc.), durante cuánto tiempo se conservarán, o mediante qué sistemas o tecnologías se procesarán. Estas son decisiones estratégicas y operativas que corresponden a las áreas de negocio (p. ej., Marketing, Producto) y a la alta dirección, quienes deben asumirlas con plena responsabilidad. El DPO debe cuestionar, evaluar y asesorar sobre la legitimidad y conformidad de estas decisiones, pero nunca tomarlas.

3.1.2. Aprobación formal de políticas y procedimientos

Igualmente, la aprobación final y formal de políticas y procedimientos corporativos no es competencia del DPO. Las políticas de privacidad, los procedimientos de seguridad de la información, los protocolos de respuesta a incidentes y otros documentos normativos internos deben ser aprobados por los órganos de gobierno corporativo con capacidad decisoria (Directorio, Comités específicos, Gerencia General).

[73] Article 29 Data Protection Working Party. (2017). *Guidelines on Data Protection Officers ('DPOs')* (WP 243 rev.01). La guía es taxativa al señalar que la organización "garantizará que dichas funciones y cometidos no den lugar a conflictos de intereses".
[74] Comité Europeo de Protección de Datos (SEPD) (2021). *Directrices del SEPD sobre los conceptos de controlador, encargado del tratamiento y control conjunto en virtud del Reglamento (UE) 2018/1725*.

El DPO debe participar activamente en su elaboración, revisión y actualización, aportando su conocimiento especializado y asegurando su alineación con la ley, pero la firma que les confiere carácter vinculante dentro de la organización es responsabilidad de la dirección.[75]

3.1.3. Decisiones sobre la legitimidad de tratamientos

Las decisiones finales sobre la base legal que legitima un tratamiento específico tampoco corresponden al DPO. Si bien éste debe asesorar sobre la conformidad de un tratamiento, la idoneidad de una base legal sobre otra (p. ej., usar consentimiento vs. interés legítimo) o emitir un informe y recomendaciones al respecto, la decisión final sobre su realización corresponde a los órganos de gestión como Responsables del Tratamiento.

Cuando un tratamiento presenta riesgos significativos, la decisión de proceder o no, asumiendo los riesgos residuales, es una responsabilidad corporativa que no puede ni debe delegarse en el DPO.[76]

3.1.4. Establecimiento de las bases legales

Íntimamente ligado a lo anterior, la elección y el establecimiento formal de la base legal específica que legitimará cada tratamiento (consentimiento, interés legítimo, obligación legal, contrato, etc.) tampoco es competencia exclusiva del DPO.

Aunque debe asesorar sobre las opciones disponibles y su adecuación al caso concreto, la decisión final sobre qué base legal utilizar implica una valoración estratégica y de riesgo que corresponde a los órganos de gestión.

3.1.5. Definición de los periodos de conservación de datos

Finalmente, la definición de los periodos de conservación de datos es otra decisión que, si bien debe considerar el asesoramiento experto del DPO, debe tomar en cuenta múltiples factores adicionales como requisitos regulatorios sectoriales, necesidades operativas, plazos de prescripción legal y la estrategia general de gestión de información. Por tanto, esta definición corresponde igualmente a los órganos de gestión de la organización, con el DPO actuando como supervisor de su razonabilidad y cumplimiento.

[75] Hanschke, I. (2020). *Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten: Eine kompakte Einführung in die Praxis*. Springer Vieweg.
[76] Reglamento (UE) 2016/679, Artículo 4(7). Define al "responsable del tratamiento" como la persona física o jurídica que "sola o junto con otros, determine los fines y medios del tratamiento".

Fundamentos de estas exclusiones

Estas exclusiones de funciones se fundamentan en varios principios esenciales

1

Conflicto directo con función supervisora

Existe un conflicto directo con la función supervisora del DPO, pues si participa en definir los tratamientos que luego debe supervisar, se compromete seriamente su independencia. El DPO no puede ocupar un cargo que le lleve a determinar los fines y medios del tratamiento, precisamente para preservar su capacidad supervisora independiente.

2

Responsabilidad legal definida

Adicionalmente, la responsabilidad de determinar los fines y medios del tratamiento corresponde al Responsable, no al DPO. Es importante separar el rol asesor del DPO de la responsabilidad decisoria del Responsable del Tratamiento.

3

Separación de responsabilidades

Desde una perspectiva práctica, el DPO no puede evaluar imparcialmente la conformidad de tratamientos que él mismo ha definido o aprobado, pues se convertiría en "juez y parte", comprometiendo la objetividad de su supervisión.

4

Dilución de responsabilidad

Finalmente, si el DPO asumiera estas funciones decisorias, podría diluirse la responsabilidad que la alta dirección y las áreas de negocio deben mantener sobre la protección de datos, cuando el objetivo es precisamente que esta responsabilidad sea compartida y asumida por toda la organización.

¿Quién debe asumir estas funciones?

- **Gerencia General**
- **Directorio**
- **Jefes de Departamento**
- **Comités específicos (Riesgos, Nuevos Productos)**

***Todas estas decisiones deben tomarse, eso sí, con el asesoramiento previo del DPO**, que aportará la perspectiva de protección de datos a la toma de decisiones estratégicas y operativas.*

Figura 5- Fundamentos de exclusiones con roles de responsable

3.2. Implementación Técnica y Operativa de Medidas

El DPO tampoco debe encargarse de funciones de implementación técnica y operativa directa. Su rol es asesorar sobre qué controles son necesarios y por qué, y luego supervisar su correcta implementación y eficacia, pero no debe ser quien los ejecute materialmente. Estas tareas corresponden a perfiles y departamentos con la especialización técnica, los recursos y la responsabilidad operativa para llevarlas a cabo. Esta separación es fundamental para mantener la capacidad supervisora independiente del DPO y evitar la dilución de sus recursos en actividades ejecutivas que no le competen.[77] [78]

3.2.1. Desarrollo e implementación de soluciones técnicas

El desarrollo e implementación de soluciones técnicas de seguridad o privacidad no es una función que corresponda al DPO. Esto implica que el DPO no debe programar, configurar ni implementar directamente sistemas técnicos como controles de acceso a datos, herramientas de cifrado o seudonimización, mecanismos de borrado seguro o sistemas de monitorización de accesos.

Por consiguiente, la ejecución de estas tareas recae en los equipos de Tecnologías de la Información (TI) o Seguridad de la Información (Ciberseguridad), ya que requieren conocimientos técnicos especializados. El papel del DPO, en este ámbito, consiste en especificar los requisitos que estas soluciones deben cumplir desde la perspectiva de protección de datos (por ejemplo, "el sistema debe permitir el cifrado de datos en reposo y en tránsito") y verificar posteriormente su adecuación, sin participar en la implementación directa.

3.2.2. Gestión de la infraestructura tecnológica

Igualmente, la gestión diaria de la infraestructura tecnológica que alberga o procesa datos personales no es responsabilidad del DPO. Este no debe administrar directamente servidores, bases de datos, redes, sistemas de comunicación, dispositivos de almacenamiento o sistemas de backup.

Estas tareas operativas corresponden a perfiles técnicos especializados (administradores de sistemas, DBAs, ingenieros de redes) dentro del área de TI, que actúan siguiendo políticas y procedimientos previamente definidos con el asesoramiento del DPO cuando sea relevante.

3.2.3. Ejecución operativa de los derechos de los titulares

La ejecución operativa de las solicitudes de derechos de los titulares (ARSOP) tampoco debe recaer en el DPO. Aunque este supervisa el proceso general y asesora sobre casos complejos, las tareas operativas específicas como la extracción de datos de un CRM para responder a una solicitud de acceso, la modificación directa de registros en una base de datos para atender una

[77] Eggl, Barbara. "Learning to walk a tightrope: Challenges DPOs face in the day-to-day exercise of their responsibilities." *Journal of Data Protection & Privacy* 3.1 (2019): 69-81.
[78] Feng, Duanyu, et al. "Towards analyzing and understanding the limitations of dpo: A theoretical perspective." *arXiv preprint arXiv:2404.04626* (2024).

rectificación, o la eliminación técnica de datos para cumplir una supresión, deben ser ejecutadas por los equipos operativos responsables de los sistemas y datos correspondientes (p. ej., Atención al Cliente, RRHH, TI).

3.2.4. Administración de controles de acceso

La administración diaria de los controles de acceso a sistemas que procesan datos personales no forma parte de las responsabilidades del DPO. La creación o eliminación de usuarios, la asignación de perfiles y permisos específicos, la revisión operativa de logs de acceso o la gestión de contraseñas son tareas que corresponden típicamente a los administradores de sistemas o al equipo de seguridad de la información.

Por su parte, el DPO tiene la función de asegurar la existencia y adecuación de políticas de control de acceso que se fundamenten en los principios de mínimo privilegio y necesidad de conocer. No obstante, la ejecución operativa de dichas políticas queda fuera de su ámbito de acción.

3.2.5. Implementación de medidas de seguridad generales

Finalmente, la implementación de medidas técnicas de seguridad generales tampoco es competencia del DPO.

Estas tareas de implementación técnica, tales como la instalación de parches de seguridad, la configuración de cortafuegos (firewalls)[79], la implementación de sistemas antimalware o la gestión operativa de la seguridad perimetral, son responsabilidades del departamento de TI o del equipo de seguridad de la información. El papel del DPO, en este sentido, es verificar que existan procesos adecuados para la realización de estas tareas (p. ej., un plan de gestión de vulnerabilidades) y que se ejecuten con la frecuencia y diligencia necesarias, sin que él las realice personalmente.

[79] Witt, B. C. *Datenschutz kompakt und verständlich*. La mención de "Firewall" en su índice destaca que, si bien el DPO debe entender su propósito, no es responsable de su configuración.

Fundamentos de esta exclusión

Por qué el DPO no debe ejecutar funciones técnicas de TI y seguridad

1

Necesidad de expertise técnico especializado

Estas tareas requieren conocimientos y habilidades técnicas específicas que corresponden a perfiles de TI y seguridad, diferentes del perfil jurídico-organizacional típico del DPO.

2

Separación entre asesoramiento y ejecución

Para preservar la capacidad supervisora, debe existir una clara separación entre quien asesora sobre las medidas necesarias y quien las implementa. Si el DPO implementara los controles, no podría luego auditarlos de manera objetiva.

3

Recursos limitados del DPO

El tiempo y los recursos del DPO, que suelen ser limitados, deben concentrarse en sus funciones esenciales de asesoramiento, supervisión y coordinación, y no dispersarse en tareas técnicas operativas que pueden ser realizadas más eficientemente por especialistas dedicados.

4

Riesgo de autoevaluación

Si el DPO implementara estas medidas, se vería obligado posteriormente a supervisar su propia implementación, lo que comprometería la objetividad de su evaluación y generaría un claro conflicto de interés.

5

Foco estratégico vs. operativo

El DPO debe mantener una visión estratégica y global sobre la protección de datos en toda la organización. Involucrarse excesivamente en detalles técnicos operativos cotidianos podría hacerle perder esta perspectiva esencial.

¿Quién debe asumir estas funciones?

- **Departamento de TI**
- **Seguridad de la Información**
- **Departamento de Operaciones**
- **Áreas de negocio**

Todos estos departamentos deben actuar siguiendo las recomendaciones y bajo la supervisión del DPO, quien verificará que las implementaciones cumplan efectivamente con los requisitos de protección de datos.

Figura 6- Fundamentos de exclusión Roles TI

3.3. Representación Legal y Defensa Jurídica

Existen funciones relacionadas con la representación legal y la defensa jurídica que resultan incompatibles con el rol del DPO, pues comprometería seriamente su independencia y objetividad. Esta incompatibilidad es especialmente relevante en asuntos relacionados con protección de datos, donde el DPO debe mantener una posición imparcial y orientada a la conformidad normativa, no a la defensa de intereses particulares de la organización.[80]

3.3.1. Representación ante tribunales

El DPO no debe actuar como representante legal en procesos judiciales relacionados con protección de datos. Esto incluye demandas presentadas por titulares de datos personales por presunta vulneración de sus derechos en materia de datos personales, recursos judiciales contra resoluciones administrativas de la autoridad de control, litigios derivados de brechas de seguridad que hayan afectado a datos personales, o procesos de hábeas data iniciados por titulares insatisfechos con la respuesta a sus solicitudes.

En todos estos casos la representación debe corresponder a otros abogados del departamento legal o a asesores externos especializados en litigios, manteniendo al DPO en su rol consultivo e independiente.

3.3.2. Defensa ante autoridades

Igualmente, el DPO no debe ejercer como defensor de la organización ante la autoridad de protección de datos. En procedimientos sancionadores iniciados por presuntos incumplimientos, investigaciones formales sobre posibles infracciones, o requerimientos de información con carácter coercitivo, el DPO debe mantener su rol de facilitador y punto de contacto, no de defensor corporativo.

Actuar como defensor comprometería seriamente su credibilidad como interlocutor imparcial ante la autoridad y generaría un conflicto directo con su obligación de cooperar establecida en el artículo 50 (h) de la LPDP.[81]

3.3.3. Negociación de acuerdos o sanciones

El DPO tampoco debe ser quien negocie acuerdos o sanciones con autoridades reguladoras en caso de infracciones. La negociación del importe o condiciones de posibles sanciones, el establecimiento de compromisos formales de cumplimiento con autoridades supervisoras, la representación de la organización en acuerdos transaccionales, o la asunción de responsabilidades institucionales en nombre de la organización, son funciones que corresponden a representantes corporativos con mandato específico, no al DPO que debe mantener su independencia.[82]

---

[80] Cheimonidis, Pavlos. "The responsibilities of the DPO according to the GDPR." (2019).

[81] Esta prohibición previene un conflicto de interés fundamental. El DPO debe poder cooperar de forma transparente con la autoridad de control, lo que sería incompatible con el papel de defensor de la organización en un litigio contra esa misma autoridad. Grupo de Trabajo del Artículo 29, *Directrices sobre los DPO*, 15-16.

[82] Ibid.

3.3.4. Formalización de documentos legales

Finalmente, el DPO no debe ser el firmante principal de documentos legales en representación de su organización. Esto incluye contratos con encargados de tratamiento donde la empresa actúa como responsable, compromisos formales ante autoridades reguladoras, declaraciones oficiales sobre cumplimiento normativo, o garantías contractuales de cumplimiento frente a terceros.

Estos documentos, que implican la asunción de obligaciones jurídicas para la organización, deben ser firmados por representantes corporativos con poderes específicos, tras el correspondiente asesoramiento del DPO sobre los aspectos de protección de datos.

Caso de uso 2: Litigios con Titulares de Datos

Separación del DPO en procesos legales de protección de datos personales

Matriz de Responsabilidades en Litigios

Preservación de la independencia del DPO en disputas legales

Exclusión de Estrategia Procesal

Cuando un titular de datos inicia acciones legales contra la organización, el DPO debe quedar completamente al margen de la definición y ejecución de la estrategia de defensa procesal. No debe participar en discusiones de tácticas legales, redactar argumentos de defensa, ni interactuar con abogados litigantes como representante de la empresa. Su rol se limita a velar por que se respeten los derechos del demandante durante el proceso.

Designación de Abogados Diferentes

La organización debe asignar la representación legal a profesionales claramente diferenciados del DPO. Si el litigio lo lleva el departamento legal interno, se encarga un abogado que no sea el DPO (idealmente del área contenciosa). Mejor aún, contratar un despacho externo. Incluso dentro del mismo departamento, otro abogado podría reportar al Director Legal para ese litigio, mientras el DPO mantiene su reporte funcional separado.

Separación de Documentación

Debe diferenciarse claramente entre documentación de opiniones técnicas del DPO (informes sobre cumplimiento en el caso que originó el litigio) y documentos de estrategia legal de defensa (contestación de demanda, comunicaciones con abogado del demandante). El DPO no accede a escritos de defensa que podrían comprometer su objetividad, y los abogados defensores no interfieren en análisis post-mortem de cumplimiento del DPO.

Asesoría Legal Externa Independiente

En litigios de especial relevancia o complejidad, es recomendable evaluar recurrir a asesores legales externos especializados en protección de datos. Esto aporta expertise y elimina conflictos internos: un abogado externo puede contradecir la postura del DPO sin tensiones jerárquicas internas, y el DPO puede interactuar proporcionando información transparentemente. El externo funciona como "cortafuegos" entre el DPO y la defensa.

DPO	Abogado Interno (Contencioso)	Despacho Externo Especializado	Director Legal
✔ Análisis técnico post-mortem	✔ Estrategia procesal de defensa	✔ Representación legal externa	✔ Supervisión de estrategia general
✔ Velar por derechos del demandante	✔ Redacción de argumentos legales	✔ Expertise en protección de datos	✔ Coordinación entre equipos
✔ Cooperar con información si la corte lo solicita	✔ Coordinación con despachos externos	✔ Independencia de jerarquías internas	✔ Decisiones sobre asesoría externa
✔ Mantener independencia funcional	✔ Gestión de documentación legal	✔ Análisis de responsabilidades	✔ Gestión de reportes separados
✔ Supervisión de cumplimiento continuo	✔ Comunicación con demandantes	✔ Estrategia de litigios complejos	✔ Autorización de recursos legales

Figura 7 - Matriz de Responsabilidades en Litigios

3.4. Ejecución de Evaluaciones de Impacto (DPIAs)

El DPO debe mantener también una separación clara respecto a la ejecución completa de evaluaciones de impacto en protección de datos (DPIAs). Esta separación es fundamental para preservar su capacidad de supervisión objetiva y evitar situaciones donde debería evaluar su propio trabajo.[83]

3.4.1. Realización completa de DPIAs

El DPO no debe ejecutar por sí mismo la totalidad de una evaluación de impacto. Específicamente, no debe responsabilizarse de realizar la descripción sistemática y detallada de las operaciones de tratamiento previstas, tarea que corresponde a los equipos que diseñan e implementarán el tratamiento; la evaluación exhaustiva de la necesidad y proporcionalidad del tratamiento en relación con su finalidad, que implica una valoración de alternativas y opciones operativas; la identificación y análisis completo de todos los riesgos potenciales, que requiere un conocimiento profundo de la operativa del tratamiento; ni la determinación detallada de todas las medidas de mitigación necesarias, que implica decisiones técnicas y organizativas específicas.

Todas estas actividades corresponden principalmente a los responsables del tratamiento, propietarios de procesos y a los equipos técnicos y operativos, con el asesoramiento del DPO.

3.4.2. Decisión final tras DPIA negativa

El DPO tampoco debe ser quien determine si un tratamiento con alto riesgo residual puede seguir adelante. Esta decisión estratégica, que implica asumir un riesgo corporativo, corresponde a la alta dirección de la organización. [84]

Igualmente, el DPO no debe decidir unilateralmente si es necesaria la consulta previa a la autoridad de control en casos de alto riesgo residual, si los riesgos identificados son aceptables para la organización desde una perspectiva corporativa, o si las medidas de mitigación propuestas son suficientes considerando la tolerancia al riesgo de la organización.

Todas estas valoraciones estratégicas sobre asunción de riesgos corresponden a los órganos de gobierno y gestión, con el asesoramiento del DPO pero no bajo su responsabilidad directa.

3.4.3. Implementación de mitigaciones

La implementación de las medidas de mitigación identificadas en una DPIA tampoco corresponde al DPO. Este no debe responsabilizarse de implementar técnicamente las medidas de seguridad identificadas como necesarias, desarrollar los controles organizativos requeridos para mitigar riesgos, modificar procesos operativos según los resultados de la evaluación, ni ejecutar directamente los cambios en sistemas o aplicaciones derivados de la DPIA.

---

[83] Reglamento (UE) 2016/679, Artículo 35(1) establece que "el responsable del tratamiento efectuará [...] una evaluación del impacto", mientras que el Artículo 39(1)(c) indica que el DPO "asesorará [...] en relación con la evaluación de impacto".

[84] Article 29 Data Protection Working Party. (2017). *Guidelines on Data Protection Officers ('DPOs')* (WP 243 rev.01). La guía aclara que la decisión de implementar o no las recomendaciones del DPO recae en el responsable, quien debe poder justificar su decisión.

Estas tareas de implementación corresponden a los departamentos técnicos y operativo, bajo la responsabilidad de sus respectivos directores.

3.4.4. Aprobación de la adecuación

El DPO no debe ser quien apruebe o valide formalmente la DPIA como suficiente desde una perspectiva corporativa. No le corresponde certificar la conformidad final del tratamiento tras la evaluación, declarar oficialmente la adecuación de las medidas implementadas, ni asumir la responsabilidad final sobre los riesgos residuales que puedan persistir tras la implementación de medidas mitigadoras.

Estas funciones de aprobación y asunción de responsabilidad corresponden a los responsables del tratamiento y a la dirección de la empresa.

3.4.5. Análisis técnicos especializados

Finalmente, el DPO no debe realizar personalmente análisis técnicos especializados que formen parte de la DPIA.

Esto incluye pruebas técnicas de seguridad en sistemas que procesarán los datos, análisis de vulnerabilidades en aplicaciones vinculadas al tratamiento, evaluaciones técnicas detalladas de algoritmos o código utilizados para el procesamiento, o verificaciones de cumplimiento técnico específico. Estas tareas requieren especialización técnica y corresponden a profesionales de TI, seguridad o analistas de sistemas.

Los fundamentos para esta exclusión son:

3.4. Ejecución de Evaluaciones de Impacto (DPIAs)

1

Conflicto directo con función cooperativa

Existe un conflicto directo con la función cooperativa, pues el DPO debe cooperar con la autoridad de control, lo que resulta incompatible con defender a la organización frente a ésta en procedimientos adversariales.

2

Compromiso de la objetividad

Si el DPO actuara como defensor de la organización, difícilmente podría mantener la imparcialidad necesaria para evaluar objetivamente la situación y asesorar sobre el cumplimiento, comprometiendo su credibilidad interna y externa.

3

Confusión ante terceros

Adicionalmente, esta función generaría confusión ante terceros sobre si el DPO actúa como figura independiente y objetiva o como representante de los intereses corporativos, diluyendo la claridad de su posicionamiento.

4

Contradicción con deber de confidencialidad

Finalmente, el DPO está sometido a confidencialidad en el ejercicio de sus funciones, pero necesita libertad para evaluar y comunicar internamente posibles incumplimientos, lo que podría verse comprometido si simultáneamente debiera defender la posición de la organización ante terceros.

¿Quién debe asumir estas funciones?

Departamento Legal

Estas funciones de representación legal y defensa jurídica deben ser asumidas por otros abogados del Departamento Legal no vinculados a la función de DPO

Asesores Legales Externos

O por asesores legales externos especializados en litigios. El DPO puede asesorar a estos profesionales sobre aspectos más técnicos de protección de datos, pero debe mantenerse al margen de la estrategia de defensa propiamente dicha.

Estas funciones de representación legal y defensa jurídica deben ser asumidas por otros abogados del Departamento Legal no vinculados a la función de DPO, o por asesores legales externos especializados en litigios. El DPO puede asesorar a estos profesionales sobre aspectos más técnicos de protección de datos, pero debe mantenerse al margen de la estrategia de defensa propiamente dicha.

Figura 8 -Fundamentos de Exclusión Elaboración DPIAs

3.5. Auditoría y Control Interno General: La Necesaria Segregación de Funciones

Una de las áreas donde el conflicto de interés puede manifestarse de forma más sutil, pero igualmente perjudicial, es en la intersección con las funciones de auditoría y control interno general. Para preservar su independencia y objetividad, es imperativo que el Delegado de Protección de Datos (DPO) no asuma responsabilidades que le obliguen a supervisar su propio trabajo o a tomar decisiones operativas sobre la implementación de controles. Asumir tales funciones comprometería su capacidad para realizar una supervisión imparcial, un pilar fundamental de su mandato según el GDPR.[85]

3.5.1. Distinción con la Auditoría Interna General

El DPO no debe confundirse con la figura del Auditor Interno. Aunque ambas funciones implican supervisión y evaluación, sus alcances, metodologías y, sobre todo, su enfoque, son fundamentalmente distintos. El rol del Auditor Interno es proporcionar una seguridad objetiva e independiente sobre la eficacia de los procesos de gobernanza, gestión de riesgos y control de *toda* la organización, abarcando áreas financieras, operativas y de cumplimiento general.[86]

Por tanto, el DPO no debe actuar como auditor interno en aspectos no relacionados con la protección de datos. Esto incluye, de manera explícita:

- Auditorías financieras o contables: La revisión de estados financieros o la contabilidad de la empresa está completamente fuera de su competencia.
- Auditorías de cumplimiento normativo general: No le corresponde auditar el cumplimiento de normativas no relacionadas con la privacidad, como las leyes antimonopolio, medioambientales o de prevención del lavado de activos.
- Auditorías de procesos operativos o de sistemas: No debe auditar la eficiencia de una línea de producción o la configuración de sistemas de TI que no procesen datos personales de manera significativa.

La función del DPO es ser auditado por la Auditoría Interna en lo que respecta a la eficacia del programa de Protección de Datos Personales que él supervisa, pero no ser el ejecutor de la auditoría general.

---

[85] Grupo de Trabajo del Artículo 29. (2017). Directrices sobre los delegados de protección de datos («DPD») (WP 243 rev.01), p. 15-16. Se subraya que el DPO no puede ocupar un puesto que implique la determinación de los fines y medios del tratamiento, lo que por extensión incluye la implementación final de controles.

[86] The Institute of Internal Auditors (IIA). (2017). *Marco Internacional para la Práctica Profesional de la Auditoría Interna (MIPP)*. Define el alcance y la misión de la auditoría interna, dejando clara su distinción con funciones de cumplimiento operativo como la del DPO.

3.5.2. Prohibición de Diseñar o Implementar Controles Internos

La responsabilidad de diseñar, implementar y mantener un sistema de control interno recae inequívocamente en la dirección de la empresa y en las áreas operativas. El DPO asesora sobre *qué* controles de Protección de Datos Personales son necesarios, pero no sobre *cómo* implementarlos en detalle ni ejecutarlos. Asignarle al DPO la tarea de implementar controles crearía un conflicto insalvable: estaría supervisando la eficacia de los mismos mecanismos que él ha diseñado y puesto en marcha.

En consecuencia, el DPO no debe diseñar el sistema general de control interno: Esta es una función de la alta dirección y, a menudo, de los departamentos de finanzas y operaciones. Tampoco debe implementar controles financieros u operativos: No es su responsabilidad configurar aprobaciones en un sistema ERP o definir procedimientos de control de inventario ni desarrollar matrices de control para procesos generales: La creación de matrices de Riesgo y Control (RCM) para áreas como compras o logística corresponde a los dueños de esos procesos y a la función de control interno.

3.5.3. Incompatibilidad con la Certificación Formal de Cumplimiento

El DPO es un asesor y supervisor interno, no una entidad certificadora. No puede emitir juicios formales y vinculantes que acrediten el cumplimiento de la organización ante terceros o incluso internamente. Esta función comprometería su objetividad, ya que pasaría de ser un evaluador crítico a un defensor del estado actual de la empresa.

Por ello, el DPO no debe:

- Emitir certificaciones formales de cumplimiento normativo general.
- Firmar declaraciones de conformidad para reguladores sectoriales que impliquen una aserción formal en nombre de la empresa.
- Acreditar oficialmente el cumplimiento ante auditorías externas. Su rol es facilitar la auditoría, proporcionar evidencia y explicar el programa de privacidad, pero la afirmación final de cumplimiento la debe hacer la dirección.
- Certificar la efectividad del sistema de control interno. Esta es, nuevamente, una conclusión que corresponde a la función de auditoría.

3.5.4. Delimitación frente a las Auditorías Técnicas de Seguridad

El DPO requiere un conocimiento profundo de seguridad para supervisar el cumplimiento de la normativa sobre protección de datos, pero su rol no es el de un ejecutor técnico. Esto significa que no debe realizar personalmente pruebas de penetración, análisis de vulnerabilidades, auditorías técnicas de configuración o ejercicios de red teaming. Tales tareas exigen especialización técnica y son responsabilidad del equipo de Ciberseguridad o proveedores externos. Asignar estas funciones al DPO minaría su independencia para evaluar objetivamente si las medidas implementadas son suficientes para proteger los datos personales.

3.5.5. Exclusión de la Supervisión Disciplinaria

Finalmente, el DPO no es parte del sistema disciplinario o de Recursos Humanos de la organización. Su rol es promover una cultura de Protección de Datos Personales supervisar el cumplimiento, no investigar o sancionar a los empleados. Asumir un rol disciplinario lo colocaría en una posición de conflicto directo, especialmente si tuviera que investigar a un empleado con quien previamente colaboró en un proyecto o a quien asesoró.

Por consiguiente, el DPO no debe asumir funciones disciplinarias ni de control formal sobre los empleados, lo que implica no actuar como órgano disciplinario, investigar conductas inapropiadas más allá de la identificación inicial de incidentes de datos, proponer o aplicar sanciones, ni gestionar el régimen disciplinario interno (tarea exclusiva de Recursos Humanos y la gerencia). Mantener al DPO alejado de estas funciones es esencial para proteger su independencia, evitar conflictos de interés y asegurar su rol de supervisor crítico, un valor clave para la gobernanza de la organización.

Los fundamentos para esta exclusión son:

3.5. Auditoría y Control Interno General: La Necesaria Segregación de Funciones

1

Asignación legal específica

La responsabilidad de realizar las DPIAs es del Responsable del Tratamiento, mientras que el DPO posee una función consultiva, estableciendo una clara distinción de roles.

2

Preservación de la función supervisora

Delegar la realización completa de la DPIA al DPO crearía un conflicto directo con su rol supervisor y revisor, pues estaría examinando la integridad de su propio trabajo.

3

Conocimiento operativo del proceso

Adicionalmente, las áreas de negocio que proponen el tratamiento tienen un conocimiento más profundo y detallado de su funcionamiento, necesario para una descripción completa y precisa, por lo que están mejor posicionadas para aportar esta información esencial.

4

Responsabilidad clara sobre el riesgo

Si el DPO realizara la DPIA completa, podría diluirse la responsabilidad del Responsable sobre los riesgos identificados y las decisiones tomadas, cuando el objetivo es precisamente reforzar esta responsabilidad.

5

Separación entre asesoramiento y decisión

Finalmente, el DPO debe mantener la capacidad de cuestionar aspectos de la DPIA y de la decisión final, lo que sería imposible o poco creíble si fuera el mismo quien la realiza íntegramente y decide sobre ella.

¿Quién debe asumir estas funciones?

- **Áreas de Negocio**
- **Área de Riesgos**
- **Compliance**
- **DPO (Asesor)**

Estas funciones deben ser asumidas por: las áreas de negocio que proponen el tratamiento, con apoyo metodológico del área de Riesgos o Compliance cuando sea necesario, y siempre con el asesoramiento del DPO durante todo el proceso. El DPO debe participar activamente como asesor y supervisor, pero no como ejecutor principal de la evaluación.

Figura 9.- Fundamentos de Exclusión Auditoría y Control interno

3.6. Decisiones Ejecutivas sobre Brechas de Seguridad

Las brechas de seguridad que afectan a datos personales representan situaciones críticas donde la distinción de roles resulta particularmente importante. El DPO debe mantener su función asesora y supervisora, pero no asumir responsabilidades ejecutivas que corresponden a la dirección de la organización.[87]

3.6.1. Decisión sobre notificación

El DPO no debe ser quien decida si una brecha de datos debe notificarse a la autoridad de control. Esta decisión estratégica, que implica una valoración de riesgos legales, reputacionales y operativos, corresponde al órgano de gestión de la empresa como Responsable del Tratamiento, típicamente a través de un Comité de Crisis o la alta dirección.[88]

3.6.2. Aprobación del contenido de notificaciones

Igualmente, el DPO no debe decidir unilateralmente si es necesario informar a los titulares de datos personales afectados, cuál es el momento exacto más adecuado para realizar estas notificaciones teniendo en cuenta consideraciones estratégicas, o si un incidente de seguridad alcanza el umbral necesario para ser considerado una "brecha de datos personales" en términos regulatorios. Todas estas son decisiones corporativas que deben tomarse con el asesoramiento del DPO pero bajo la responsabilidad final de la dirección.

El DPO tampoco debe aprobar formalmente el contenido final de las comunicaciones sobre brechas de seguridad. No debe ser el responsable final de aprobar el texto de las notificaciones a la autoridad de control, los comunicados dirigidos a titulares de datos personales afectados, las respuestas a solicitudes de información adicional por parte de reguladores, o las comunicaciones a medios de comunicación o público general. Estos contenidos, que comprometen oficialmente a la organización, deben ser aprobados por la dirección con el asesoramiento del DPO y los departamentos de Legal y Comunicación.

3.6.3. Liderazgo técnico en respuesta a incidentes

El liderazgo técnico en la respuesta a incidentes tampoco corresponde al DPO. Este no debe dirigir técnicamente la contención del incidente para evitar que la brecha continúe o se expanda, coordinar operativamente al equipo técnico de respuesta, ejecutar personalmente las medidas técnicas de mitigación, ni liderar la recuperación de sistemas afectados. Estas funciones técnicas y operativas corresponden al departamento de TI, al equipo de Seguridad de la Información o a especialistas en respuesta a incidentes, según la estructura de la organización.

3.6.4. Decisiones disciplinarias

[87] Reglamento (UE) 2016/679, Artículo 33. La obligación de notificar la violación de seguridad a la autoridad recae explícitamente en el "responsable del tratamiento", no en el DPO.

[88] Article 29 Data Protection Working Party. (2017). *Guidelines on Data Protection Officers ('DPOs')* (WP 243 rev.01). La decisión final sobre si notificar, y sobre qué comunicar a los interesados, es del responsable del tratamiento, quien debe tener en cuenta el asesoramiento del DPO.

El DPO no debe determinar responsabilidades personales en la causa de la brecha ni establecer sanciones por negligencia o incumplimiento.

No le corresponde decidir qué medidas disciplinarias deben aplicarse contra empleados que hayan podido contribuir a la brecha por negligencia o incumplimiento de políticas, ni determinar las consecuencias contractuales para proveedores que hayan incumplido sus obligaciones de seguridad. Estas decisiones corresponden a Recursos Humanos, al departamento Legal o a la dirección de la empresa, según la naturaleza específica del caso.

3.6.5. Decisiones sobre medidas correctivas

El DPO tampoco debe decidir qué medidas técnicas específicas implementar tras la brecha para prevenir incidentes similares futuros, qué cambios organizativos son necesarios como respuesta estructural al incidente, qué recursos deben asignarse a las acciones correctivas, o qué soluciones tecnológicas deben adquirirse o desarrollarse para reforzar la seguridad.

Estas decisiones ejecutivas sobre asignación de recursos y cambios organizativos corresponden a la dirección de la empresa y a los responsables de los departamentos afectados.

3.6.6. Comunicación externa institucional

Finalmente, el DPO no debe actuar como portavoz oficial de la organización ante medios de comunicación en relación con brechas de seguridad. No debe decidir la estrategia comunicativa corporativa para gestionar la crisis reputacional, aprobar comunicados de prensa, ni representar públicamente a la organización en explicaciones sobre el incidente. Estas funciones comunicativas corresponden al departamento de Comunicación o portavoces oficiales designados específicamente.

Los fundamentos para esta exclusión son:

Decisiones sobre Brechas de Seguridad

1

Responsabilidad legal definida

La ley asigna explícitamente al Responsable del Tratamiento, no al DPO, la obligación de notificar las violaciones de seguridad, estableciendo una clara distinción de responsabilidades. El Responsable decide sobre la notificación, aunque debe consultar al DPO para informar su decisión.

2

Naturaleza estratégica de la decisión

La decisión de notificar una brecha implica consideraciones estratégicas, reputacionales y legales complejas que corresponden al nivel de alta dirección, no a una función de asesoramiento como el DPO.

3

Preservación del rol asesor

Si el DPO tomara estas decisiones ejecutivas perdería su capacidad para asesorar imparcialmente sobre ellas y para cuestionar posteriormente su adecuación si fuera necesario.

4

Separación de responsabilidades

La decisión final debe recaer en quien asume las consecuencias legales y reputacionales de la misma, es decir, la alta dirección de la organización como Responsable del Tratamiento.

5

Expertise técnico especializado

Adicionalmente, la respuesta técnica a incidentes requiere conocimientos específicos en ciberseguridad y gestión de crisis que normalmente exceden el perfil típico del DPO, que tiene un enfoque más orientado al cumplimiento normativo y protección de derechos.

¿Quién debe asumir estas funciones?

Comité de Crisis o Gestión de Incidentes

Con participación de Dirección General, Legal, Comunicación, TI y Seguridad

Asesoramiento del DPO

El DPO asesora sobre el riesgo normativo, pero no decide

Estas funciones deben ser asumidas por: un Comité de Crisis o Gestión de Incidentes (con participación de Dirección General, Legal, Comunicación, TI y Seguridad), con el asesoramiento del DPO.

Figura .10- Fundamentos de Exclusión Decisiones sobre Brechas de Seguridad

3.7. Gestión Operativa General de los Datos

Finalmente, el DPO debe mantener una clara separación respecto a funciones operativas relacionadas con la gestión diaria de datos personales. Estas funciones operativas, aunque implican tratamiento de datos y por tanto están sujetas a supervisión, corresponden a los equipos y sistemas especializados que mantienen y procesan la información en la empresa.[89]

3.7.1. Administración de bases de datos de titulares de datos personales

El DPO no debe administrar técnicamente las bases de datos de titulares de datos personales. No debe responsabilizarse de la administración de los sistemas de gestión de bases de datos, la gestión de la estructura o modelo de datos, la creación o modificación de tablas o campos en las bases de datos, ni el mantenimiento técnico de las bases de datos que almacenan información de titulares de datos personales.

Estas son funciones técnicas especializadas que corresponden a los administradores de bases de datos y al equipo de TI.

3.7.2. Gestión de procesos masivos de datos

Igualmente, el DPO no debe ejecutar procesos masivos relacionados con datos personales. No debe responsabilizarse de procesos de carga masiva de datos (como incorporación de nuevos titulares de datos personales), actualizaciones masivas de registros (como modificaciones en datos de contacto), procesos de migración de datos entre sistemas, o cruces e interconexiones de bases de datos con información externa. Estos procesos operativos corresponden a las áreas de negocio o TI según la naturaleza específica de cada operación.

3.7.3. Gestión operativa de consentimientos

La gestión operativa de consentimientos tampoco corresponde al DPO. Si bien debe supervisar el sistema general, no debe implementar técnicamente los mecanismos de recogida de consentimiento, gestionar directamente los registros de consentimientos en sistemas operativos, ejecutar procesos de actualización de preferencias cuando los titulares de datos personales las modifican, ni realizar verificaciones técnicas rutinarias de trazabilidad de consentimientos. Estas funciones operativas corresponden a los sistemas y equipos que gestionan la relación con titulares de datos personales.

3.7.4. Diseño técnico de formularios y documentos

El DPO no debe responsabilizarse del diseño técnico de formularios físicos o digitales, el desarrollo de interfaces de usuario para recopilación de información, la creación de plantillas

[89] Feng, D., et al. (2024). "Towards analyzing and understanding the limitations of dpo: A theoretical perspective." La implicación excesiva en tareas operativas es un factor que limita la capacidad del DPO para mantener una visión estratégica y supervisora.

operativas de documentos, ni la implementación de campos y validaciones en sistemas. Estas tareas de diseño e implementación corresponden a los equipos de Experiencia de Usuario, Desarrollo o áreas de negocio según el caso específico.

3.7.5. Gestión de calidad de datos

La gestión operativa de la calidad de datos no es responsabilidad del DPO. No debe realizar verificaciones técnicas rutinarias de calidad de datos, procesos de limpieza o normalización de información, duplicación de registros, ni correcciones masivas de datos.

Estas tareas de calidad de datos corresponden a los administradores de datos o a equipos especializados en Data Quality Management.

3.7.6. Gestión de transferencias de datos

Finalmente, el DPO no debe ejecutar operativamente transferencias de datos a terceros. No debe implementar técnicamente interfaces de intercambio de información con otras entidades, gestionar operativamente extracciones periódicas de datos para envío a terceros autorizados, ni configurar técnicamente los canales seguros para estas transferencias. Estas operaciones técnicas corresponden a los equipos de TI o Integraciones de Sistemas.

Los fundamentos para esta exclusión son:

Gestión de transferencias de datos

1

Separación entre gestión y supervisión

Existe una necesaria separación entre la gestión operativa de los datos y su supervisión desde la perspectiva del cumplimiento, quien gestiona directamente los datos no puede supervisar con objetividad el cumplimiento normativo de ese mismo tratamiento.

2

Especialización técnica requerida

Las funciones operativas descritas requieren habilidades técnicas y conocimientos específicos propios de perfiles de TI, administración de datos o áreas de negocio, diferentes a las competencias típicas del DPO, que se enfocan más en aspectos legales, de cumplimiento y supervisión.

3

Recursos limitados del DPO

El DPO debe concentrar sus recursos y tiempo en sus funciones estratégicas de asesoramiento, supervisión y coordinación.

4

Riesgo de operativización excesiva

Un DPO excesivamente involucrado en tareas operativas perdería inevitablemente la visión estratégica y la perspectiva global necesarias para evaluar adecuadamente los riesgos y cumplimiento.

5

Preservación de la independencia funcional

La carga operativa comprometería la disponibilidad del DPO para el análisis, asesoramiento y supervisión independientes.

6

Evitar la dilución de responsabilidades

Cada área operativa debe mantener la responsabilidad sobre la correcta gestión de los datos que trata.

¿Quién debe asumir estas funciones?

Operaciones	**Atención al Cliente** **TI**	**DPO (Asesor/Supervisor)**

Estas funciones deben ser asumidas por: las áreas operativas específicas (Operaciones, Atención al cliente, TI) con el asesoramiento y bajo la supervisión del DPO.

Figura 11.- Fundamentos de Exclusión Gestión de Transferencias de Datos

4. Gobernanza, Posicionamiento e Independencia del DPO

La designación de un Delegado de Protección de Datos (DPO) es el punto de partida, no el destino. La eficacia real de esta figura, su capacidad para mitigar riesgos y su rol como catalizador de la confianza digital dependen críticamente de su correcta arquitectura dentro del gobierno corporativo. Un DPO aislado, sin recursos o sin poder real, es un riesgo en sí mismo. Por el contrario, un DPO correctamente posicionado se convierte en un activo estratégico invaluable.

Este capítulo detalla la estructura de gobernanza indispensable para el DPO, desglosando los principios, la arquitectura organizacional, las interfaces operativas y los recursos que, en conjunto, materializan los mandatos de la legislación chilena y se alinean con los más altos estándares internacionales.

4.1. Principios Fundamentales: La Doble Garantía de Independencia y Ausencia de Conflicto de Interés

Estos dos principios son inseparables y constituyen el fundamento de la credibilidad y efectividad del DPO. La ley no los sugiere, los exige.

4.1.1. La Independencia como Mandato Funcional

La autonomía del Delegado de Protección de Datos (DPO) no es un mero detalle operativo; es la condición fundamental que le permite actuar con la objetividad e imparcialidad necesarias. Sin autonomía, su capacidad para evaluar críticamente los tratamientos de datos, identificar riesgos y reportar incumplimientos carecería de credibilidad tanto interna (ante la dirección y empleados) como externa (ante los titulares de datos y la autoridad de control). La legislación chilena, consciente de esta necesidad, establece explícitamente que "el delegado de protección de datos deberá contar con autonomía respecto de la administración. Esta garantía legal es crucial y se manifiesta en tres niveles clave.[90]

a) Independencia Funcional

Esta dimensión asegura que el DPO es libre de determinar el alcance, la metodología y el enfoque para llevar a cabo sus tareas principales de asesoramiento y supervisión. En la práctica, esto significa que el DPO no debe recibir instrucciones vinculantes sobre cómo realizar una investigación interna (qué personas entrevistar, qué documentos revisar), qué contenido incluir en sus informes a la dirección, o qué conclusiones emitir en sus dictámenes sobre tratamientos de datos. La organización debe respetar su criterio profesional en el ejercicio de estas funciones sustantivas.[91]

---

[90]

[91] Article 29 Data Protection Working Party (2017). *Guidelines on Data Protection Officers ('DPOs')* (WP 243 rev.01), p. 15. Este documento es el estándar interpretativo global sobre la figura del DPO.

b) Independencia Decisoria

Complementando la independencia funcional, la independencia decisoria garantiza que el DPO es autónomo en la toma de ciertas decisiones clave relacionadas con el cumplimiento. Esto implica que no se le puede coaccionar para que alcance un resultado predeterminado en una evaluación de impacto (por ejemplo, declarar un tratamiento como de bajo riesgo si considera lo contrario), ni obligarle a consultar (o abstenerse de consultar) a la Agencia de Protección de Datos cuando, según su propio criterio, lo considere necesario. Su juicio profesional y su obligación legal prevalecen sobre las directivas internas en estos casos.

4.1.2. La Prohibición de Conflicto de Interés: La Regla de "No ser Juez y Parte"

El principio más crítico y a menudo más difícil de implementar es la ausencia de conflicto de interés. La ley es explícita: el responsable "garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses".[92]

Este conflicto se materializa cuando una misma persona tiene la responsabilidad de decidir sobre los fines y medios del tratamiento de datos y, a la vez, supervisar la legalidad de esas mismas decisiones. Es una autoevaluación carente de objetividad.

Por ello, es fundamental reconocer que existen ciertos roles dentro de una organización que, por su naturaleza, presentan un conflicto de intereses intrínseco e insalvable con la función de supervisión independiente del DPO. Estos incluyen:

a) Alta Dirección (C-Suite):

- Director General (CEO), Director de Operaciones (COO), Director Financiero (CFO): Estos roles tienen la responsabilidad última sobre los resultados del negocio. Sus decisiones están inherentemente orientadas a objetivos comerciales, lo que puede entrar en colisión directa con los principios de protección de datos, como la minimización de datos o la limitación de la finalidad.

b) Jefaturas de Áreas Operativas Clave:

- Director de Tecnologías de la Información (CIO) o Jefe de TI: Determina qué sistemas se utilizan, cómo se configuran y qué datos se procesan, es decir, define los "medios" del tratamiento.
- Director de Marketing: Decide los fines y medios para la captación de clientes, el perfilado, la publicidad dirigida y el uso de cookies, actividades de alto riesgo para la privacidad.

[92] Ley N° 19.628, Artículo 50, inciso 4.

- Director de Recursos Humanos: Determina los fines y medios del tratamiento de los datos de empleados y candidatos, una categoría de datos especialmente sensible.
- Director de Riesgos o de Auditoría Interna: Aunque parezcan roles afines, también pueden generar conflictos. Un Auditor Interno evalúa controles, pero el DPO tiene una función de asesoramiento continuo y supervisión que debe poder ser auditada de forma independiente.

4.2. Arquitectura Organizacional: El Modelo de Doble Reporte como Solución Estructural

La legislación establece los principios de independencia y reporte al más alto nivel, pero no prescribe una estructura organizacional única. Sin embargo, la experiencia global y las directrices de las autoridades de control europeas han consolidado al modelo de doble reporte como la arquitectura de gobierno corporativo más robusta y defendible.

Esta estructura no es una complicación burocrática, sino la solución estructural a la paradoja fundamental del DPO: la necesidad de estar integrado en la operativa para entenderla y ser efectivo, y al mismo tiempo, de estar separado de ella para poder supervisarla con objetividad crítica.

4.2.1. El Fundamento Legal: El Principio de Jerarquía

La ley chilena es explícita al exigir que el DPO "deberá ser designado por la máxima autoridad directiva o administrativa del responsable de datos".[93]Esta disposición va más allá del mero acto de nombramiento; implica el establecimiento de una relación directa y continua con el vértice estratégico.

Se trata de un canal de comunicación funcional que asegura que las advertencias y el asesoramiento del DPO lleguen, sin filtros ni intermediarios, a quienes asumen la responsabilidad final por el cumplimiento.
Para materializar este principio en la práctica, el modelo de doble reporte divide la dependencia del DPO en dos líneas distintas, cada una con un propósito, un alcance y una jerarquía claramente definidos.
Para materializar este principio en la práctica, el modelo de doble reporte divide la dependencia del DPO en dos líneas distintas, cada una con un propósito, un alcance y una jerarquía claramente definidos.

4.2.2. La Línea de Reporte Funcional: La Brújula Estratégica y el Canal de Independencia

Esta es la línea de reporte más importante y la que consagra la verdadera autonomía funcional del Delegado de Protección de Datos (DPO). Es su canal directo al poder decisorio y el mecanismo que garantiza que su voz sea escuchada en el más alto nivel.[94]

c) Propósito Fundamental

- Su fin principal es materializar la independencia, asegurar que la alta dirección sea directamente informada sobre los riesgos de Protección de Datos Personales

[93] Conforme a las funciones listadas en el Artículo 50, letras a) a h), de la Ley N° 19.628.
[94] Las directrices del WP 243 (rev. 01) establecen que "el DPO debe informar directamente al más alto nivel de la dirección". La prevalencia de la línea funcional sobre la administrativa es la única forma de dar efectividad a este mandato.

(*accountability*), y proteger el juicio profesional del DPO de cualquier tipo de interferencia, presión o veto por parte de mandos intermedios.

d) ¿A Quién Reporta? (El Destinatario Estratégico)

A la "máxima autoridad", que en la práctica se traduce en el Directorio. La mejor práctica internacional es que el reporte se realice a un comité del directorio, preferentemente el Comité de Auditoría o el Comité de Riesgos, por las siguientes razones:

- Expertise: Estos comités ya están familiarizados con la supervisión de riesgos y metodologías de control.
- Independencia: Operan con un alto grado de independencia respecto de la gestión ejecutiva.
- Influencia: Sus informes y recomendaciones tienen un peso determinante en las decisiones del Directorio. Anclar al DPO en este nivel le otorga una plataforma de influencia y credibilidad inigualable.

e) Otras Opciones Viables:

- El Directorio en pleno: Garantiza la máxima visibilidad, pero puede ser menos ágil para un seguimiento continuo y detallado

- El Gerente General (CEO): Es una opción posible en organizaciones con una cultura de gobierno corporativo muy madura. Sin embargo, siempre debe existir un mecanismo de escalada directo y formalizado para que el DPO pueda acceder al Directorio si lo considera necesario.

f) ¿Sobre Qué Reporta? (El Contenido Sustantivo)

Este reporte se centra exclusivamente en el núcleo de las funciones del DPO[95] e incluye:

- Informe Periódico de Cumplimiento y Madurez: Un reporte formal (ej. trimestral) que presenta el estado del programa de privacidad, el nivel de cumplimiento normativo, las brechas identificadas y el progreso en la mitigación de riesgos, utilizando indicadores clave (KPIs).
- Análisis de Riesgos Críticos: Comunicación proactiva de los riesgos más significativos para los derechos de las personas y para la reputación de la organización.
- Dictámenes sobre Proyectos Estratégicos: Presentación de los resultados de Evaluaciones de Impacto (DPIA)[96] para nuevos productos, tecnologías o procesos de alto riesgo.

[95] Conforme a las funciones listadas en el Artículo 50, letras a) a h), de la Ley N° 19.628.
[96] Requeridas por el Artículo 15 ter de la Ley N° 19.628.

- Alertas sobre Brechas de Seguridad Significativas: Informe inmediato y sin filtros sobre cualquier incidente de seguridad grave, incluyendo la recomendación formal sobre la necesidad de notificar a la autoridad y a los afectados.[97]
- Escalada de Desacuerdos Materiales: Informar formalmente cuando una recomendación crítica del DPO no haya sido atendida, presentando tanto su postura como la de la gerencia.

g) ¿Cómo Reporta? (El Formato y la Cadencia)

A través de informes escritos formales, presentaciones en las sesiones del Comité, *dashboards* con métricas de privacidad, y comunicaciones *ad-hoc* e inmediatas para asuntos urgentes.

4.2.3. La Línea de Reporte Administrativo: El Anclaje Operativo y el Motor de Integración

Esta línea asegura que el DPO no sea una figura aislada e inoperante. Lo conecta con la estructura diaria de la organización, le provee de soporte y facilita las sinergias con otras funciones de control.

A diferencia de la línea funcional, esta línea de reporte asegura que el DPO no sea una figura aislada e inoperante. Lo conecta con la estructura diaria de la organización, le provee de soporte y facilita las sinergias con otras funciones de control.

a) Propósito Fundamental

Su fin es facilitar la integración operativa del DPO, asegurar que reciba el apoyo logístico y de gestión necesario para funcionar eficientemente, y fomentar la colaboración con áreas afines.

b) ¿A Quién Reporta? (El Destinatario Operativo)

Reporta a un director de una función de control o legal. Las opciones más lógicas y comunes son:

- Director(a) del Departamento Legal.
- Director(a) de Cumplimiento (Compliance Officer).
- Director(a) de Riesgos.

La elección de este superior administrativo dependerá de la estructura de la organización, pero en todos los casos, debe ser un área con afinidad cultural por el cumplimiento y la gestión de riesgos.

[97] Conforme a las obligaciones del Artículo 14 sexies de la Ley N° 19.628.

c) ¿Sobre Qué Reporta? (El Contenido - Estrictamente Acotado)

El alcance de este reporte debe estar rigurosamente limitado a cuestiones administrativas y logísticas. En ningún caso puede versar sobre el fondo, contenido, conclusiones o recomendaciones sustantivas de la función de DPO.

- Incluido en el reporte administrativo:
  - Gestión de Presupuesto: Discusión y ejecución del presupuesto asignado (gastos de formación, herramientas, etc.).
  - Gestión de Personas (si aplica): Coordinación del equipo de apoyo, evaluaciones de desempeño sobre competencias transversales (no técnicas), planificación de vacaciones y permisos.
  - Soporte Logístico: Requerimientos de equipamiento, espacio físico, soporte informático.
  - Coordinación Departamental: Planificación de iniciativas conjuntas que no comprometan la independencia (ej. un proyecto de formación general del área legal).
- Excluido del reporte administrativo:
  - La aprobación previa de los informes que se enviarán a la línea funcional.
  - La discusión sobre la severidad de un hallazgo de auditoría de privacidad.
  - La decisión de si un riesgo debe ser escalado o no.
  - Cualquier instrucción que limite o dirija el juicio profesional del DPO.

d) ¿Cómo Reporta? (El Formato y la Cadencia)

A través de reuniones de equipo regulares (semanales o quincenales), conversaciones uno a uno, correos electrónicos y los procesos de gestión corporativos estándar (sistemas de RRHH, plataformas de gestión de proyectos, etc.).

Líneas de Reporte del DPO

La Brújula Estratégica y el Canal de Independencia

Línea de Reporte Funcional

Canal de Independencia

¿A Quién Reporta?

Máxima Autoridad: Directorio
Nivel Ejecutivo: Gerente o Comité
✔ Comité de Auditoría
✔ Comité de Riesgos

¿Sobre Qué Reporta?

- Informe de Cumplimiento y Madurez (90%)
- Análisis de Riesgos Críticos
- Dictámenes de Evaluaciones de Impacto (DPIAs)
- Alertas sobre Brechas de Seguridad Graves
- Escalada de Desacuerdos Materiales

Propósito Fundamental

• Independencia: Proteger el juicio profesional del DPO de interferencias o vetos
• Accountability: Asegurar que la alta dirección sea informada directamente sobre los riesgos
• Canal Directo: Materializar la autonomía y la influencia en el máximo órgano

¿Cómo Reporta?

A través de informes escritos formales, presentaciones en las sesiones del Comité, dashboards con métricas de privacidad, y comunicaciones ad-hoc e inmediatas para asuntos urgentes.

Línea de Reporte Administrativo

Anclaje Operativo

¿A Quién Reporta?

Director de área de Control
✔ Director(a) Legal
✔ Dir. de Cumplimiento
✔ Director(a) de Riesgos

Alcance del Reporte: Límites Estrictos

- ✔ Gestión de Presupuesto
- ✔ Gestión de Personas
- ✔ Soporte Logístico
- ✔ Coordinación Departamental

Excluido (Sustantivo)

- ✗ Aprobación previa de informes
- ✗ Discusión de severidad de riesgos
- ✗ Decisión sobre escalamiento
- ✗ Cualquier instrucción o veto

Propósito y Formato

Propósito: Facilitar la integración operativa, proveer soporte logístico y fomentar la colaboración con áreas afines sin comprometer la independencia.

¿Cómo reporta?: A través de reuniones regulares, 1-a-1, correos y sistemas de gestión corporativos (RRHH, Proyectos, etc.).

Delegado de Protección de Datos (DPO)

Directorio / Comité
Reporte Funcional

←

DPO
Punto de Origen del Reporte

→

Director Legal/Compliance
Reporte Administrativo

Figura 12- Líneas de Reporte

4.2.4. El Principio de Prevalencia: La Regla de Oro en Caso de Conflicto

Para asegurar la efectividad del modelo de doble reporte, debe existir una regla de oro explícita y documentada: en caso de conflicto entre la línea de reporte administrativa y la línea de reporte funcional, esta última siempre prevalece.

Ejemplo Práctico: El superior administrativo del DPO (ej. Gerente Legal) le indica que debe reducir el presupuesto para formación en Protección de Datos Personales para cumplir con una meta de ahorro del departamento. Simultáneamente, el DPO identifica una necesidad crítica de capacitar al equipo de Marketing sobre una nueva normativa de cookies.

Aplicación del Principio: El DPO tiene el deber y el derecho de escalar esta situación a su línea funcional (ej. al Comité de Riesgos), argumentando que el recorte presupuestario pone en riesgo el cumplimiento normativo. La decisión del Comité de Riesgos prevalecerá sobre la instrucción del Gerente Legal.

Característica	Línea Administrativa (El Anclaje)	Línea Funcional (La Brújula)
Propósito	Integración, soporte, logística.	Independencia, supervisión, influencia estratégica.
Reporta a	Jefe de departamento (Legal, Compliance).	Comité del Directorio (Riesgos, Auditoría), Directorio.
Frecuencia	Continua, según necesidad operativa.	Periódica (trimestral) e inmediata (en caso de crisis).
Contenido	Presupuesto, vacaciones, coordinación.	Riesgos, cumplimiento, brechas, estrategia.
Naturaleza	Operativa.	Estratégica y de Supervisión.
Prevalencia	Subordinada.	Siempre Prevalente.

4.3. Salvaguardas para la Independencia del DPO

Aunque el DPO pueda estar **integrado orgánicamente** en el Departamento Legal u otro, es crucial establecer salvaguardas específicas que garanticen su independencia funcional, conforme lo exige la normativa de protección de datos.[98] Estas salvaguardas deben ser explícitas y formales para evitar interferencias indebidas en el ejercicio de sus funciones. Las principales son:

[98] Kneuper, Ralf. *Datenschutz für Softwareentwicklung und IT*. Berlin: Springer Vieweg, 2021.

4.3.1. Pilares Documentales: La Consagración del Estatuto del DPO

La base de la armadura jurídica reside en documentos corporativos clave, que deben ser precisos, explícitos y aprobados por las más altas instancias.[99]

a) La Política Integral de Protección de Datos Personales

Este es el documento fundacional de la protección de datos personales en la organización. Debe ir más allá de una declaración de principios abstractos y contener un capítulo específico y detallado que consagre el estatuto del DPO. Este capítulo deberá establecer inequívocamente:

- Misión y Alcance Detallados: Una descripción exhaustiva del rol del DPO como supervisor independiente del cumplimiento normativo y asesor de la alta dirección, incluyendo explícitamente sus funciones conforme al Artículo 50 de la Ley N° 19.628 (ej. informar, asesorar, supervisar, cooperar con la Agencia).

- Posición Jerárquica y Modelo de Reporte: La descripción explícita del modelo de doble reporte (funcional y administrativo), identificando los cargos o comités específicos a los que reporta en cada línea. Esto incluye el acceso directo a la "máxima autoridad directiva o administrativa".[100]

- Principio de Autonomía: Una cláusula robusta que prohíba expresamente a cualquier miembro de la organización, sin importar su rango o área, dar instrucciones al DPO sobre el desempeño sustantivo de sus funciones (ej. cómo investigar una queja, qué conclusión debe alcanzar, si debe consultar a la autoridad).

- Protección contra represalias: Una declaración firme de que el DPO no será objeto de despido, sanción o perjuicio por el correcto y diligente desempeño de sus tareas, incluso si sus conclusiones o recomendaciones son incómodas o contrarias a intereses comerciales inmediatos de la organización². Esta protección es un disuasivo clave contra la censura.

b) El Acta de Nombramiento del Directorio (o del Máximo Órgano de Gobierno)

El nombramiento del DPO no debe ser un mero trámite administrativo de recursos humanos. Debe ser formalizado mediante un acuerdo y acta específica del Directorio (o del máximo órgano de gobierno). [101]Este acto tiene un profundo significado:

Legitimidad y Respaldo: Otorga al DPO el respaldo explícito y visible del nivel más alto de la organización, enviando un mensaje claro a toda la estructura sobre la seriedad e importancia de su función.

---

[99] Roßnagel, Alexander. *Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung*. Springer Fachmedien Wiesbaden, 2017.
[100] Eggl, Barbara. "Learning to walk a tightrope: Challenges DPOs face in the day-to-day exercise of their responsibilities." *Journal of Data Protection & Privacy* 3.1 (2019): 69-81.
[101]Ibid.

Vinculación Formal: El acta debe reflejar no solo el nombramiento, sino también el reconocimiento y compromiso del Directorio con los principios de independencia, acceso directo y provisión de recursos suficientes.

c) La Descripción del Cargo del DPO

Este documento es el "contrato" operativo del DPO. Debe ser un reflejo fiel de lo establecido en la política y el acta de nombramiento, traduciendo los principios a responsabilidades y derechos concretos. Debe detallar:[102]

- Las funciones y responsabilidades del DPO, diferenciando claramente las de carácter consultivo/supervisor de cualquier otra tarea asignada.
- La clara definición de su doble línea de reporte.
- Las garantías de no conflicto de interés y no recepción de instrucciones.
- Los recursos a su disposición (tiempo, personal de apoyo, herramientas).
- La obligatoriedad de su participación en determinados procesos (ej. DPIAs, revisión de contratos clave).

d) Cláusulas en Contratos de Trabajo o Servicios (DPO Interno/Externo)

Para el DPO interno, su contrato laboral debe incluir una cláusula específica que refuerce su independencia, la prohibición de instrucciones y la protección contra represalias por el ejercicio de sus funciones como DPO.[103] Para un DPO externo, estas garantías deben ser explícitas y detalladas en el contrato de servicios, incluyendo acuerdos de nivel de servicio (SLAs) para los tiempos de respuesta.[104]

e) Reglamento Interno de Orden, Higiene y Seguridad (RIOHS) o Código de Conducta

Para una formalización completa y un arraigo cultural de la protección de datos personales, es recomendable incluir menciones al rol del DPO y a las obligaciones de colaboración de todos los empleados.

- Deber de Colaboración: Establecer la obligación de todos los trabajadores de colaborar con el DPO, proporcionándole la información y el acceso que requiera para el desempeño de sus funciones.
- Confidencialidad: Reforzar la obligación de confidencialidad de todos los empleados respecto de la información a la que accedan, incluidos los datos personales.

[102] Cheimonidis, Pavlos. "The responsibilities of the DPO according to the GDPR." (2019).
[103] Lambert, Paul. *The Data Protection Officer: Profession, Rules, and Role*. CRC Press, 2016.
[104] Los SLAs deben especificar no solo tiempos de respuesta, sino también el nivel de involucramiento esperado en procesos clave como DPIAs, diseño de nuevos productos y gestión de incidentes, para evitar un rol meramente superficial.

4.4. Protocolos Operativos de Interacción y Escalada

Si los documentos son la estructura estática, los protocolos son los mecanismos dinámicos que dan vida a la autonomía en el día a día.

4.4.1. Protocolo de Consulta Obligatoria (Gatekeeping Preventivo):

Este protocolo define los "disparadores" (triggers) que activan la participación preceptiva y temprana del DPO. Su objetivo es asegurar la aplicación del principio de "Protección de Datos Personales desde el Diseño". Los disparadores deben incluir, como mínimo:

- El inicio de cualquier nuevo proyecto que implique tratamiento de datos personales.
- La contratación de nuevos proveedores tecnológicos (IaaS, PaaS, SaaS) que vayan a procesar datos.
- La implementación de nuevas tecnologías (ej. biometría, inteligencia artificial, geolocalización masiva).
- Modificaciones sustanciales en procesos de tratamiento de datos existentes.
- Procesos de fusión o adquisición de empresas (due diligence de privacidad).

4.4.2. Protocolo de Resolución de Conflictos y Escalada Formal:

Este es el mecanismo más crítico para proteger la independencia del DPO cuando su criterio choca con el de un área de negocio. Un DPO sin un canal de escalada formal es un DPO sin poder real. El protocolo debe definir un proceso claro:

- Documentación del Disenso: Si un área de negocio decide no seguir una recomendación crítica del DPO, este último debe documentar formalmente por escrito su recomendación, los riesgos asociados a no seguirla, y solicitar al área que documente su contraargumento y decisión final.
- Escalada Directa a la Línea Funcional: El DPO debe tener el derecho y el deber de elevar este disenso documentado directamente a su línea de reporte funcional (ej. Presidente del Comité de Riesgos), eludiendo la línea administrativa.
- Decisión Final Informada y Asunción de Riesgo: El órgano superior escucha a ambas partes y toma una decisión final. Si decide apartarse de la recomendación del DPO, lo hace de manera informada y asume formalmente la responsabilidad por el riesgo residual.

4.4.3. Protocolo de Acceso Directo al Directorio:

Se debe formalizar el derecho del DPO a solicitar una audiencia directa con el Directorio en pleno, sin necesidad de autorización previa, en circunstancias excepcionales y graves. Esto puede incluir:

- La detección de un riesgo gravísimo para la protección de datos personales que no está siendo atendido.
- El incumplimiento sistemático de sus recomendaciones por parte de la administración.
- Situaciones que comprometan gravemente la independencia de su función.

4.5. Protocolos Operativos: Mecanismos para la Gestión y Resolución de Conflictos[105]

La documentación es la base, pero los protocolos son los mecanismos dinámicos que dan vida a la independencia en el día a día, especialmente cuando surgen fricciones.

4.5.1. Procedimiento de Identificación y Registro de Conflictos de Interés:

h) Registro Centralizado

Establecer un "Registro de Conflictos de Interés" formal (ej. en una base de datos o sistema GRC) donde se documente cada situación de conflicto potencial o real identificada. Debe incluir fecha, circunstancias, partes involucradas, y el principio del rol del DPO que podría verse comprometido (independencia, confidencialidad, objetividad).

i) Análisis de Impacto

Por cada conflicto registrado, se debe evaluar su impacto potencial en la independencia real o percibida del DPO, así como los riesgos para la organización y los titulares de datos.

Notificación Formal: Una vez documentado, el conflicto debe comunicarse de manera transparente a todos los stakeholders internos pertinentes (alta dirección, Comité de Auditoría/Riesgos, áreas operativas involucradas).

j) Medidas de Mitigación Escalables según la Gravedad

Los protocolos deben prever una gradación de acciones según la seriedad del conflicto:

- Conflictos Menores: Puede bastar con la documentación transparente del desacuerdo y la justificación por escrito de la decisión final de la dirección.

- Conflictos Moderados: Requerir una segregación temporal de responsabilidades (ej. asignar un abogado diferente del Departamento Legal para un proyecto específico si el DPO

[105] Grosmann, Patrick. *Die Interessenkonflikte Der Betrieblichen und Behördlichen Datenschutzbeauftragten*. 2024.

tiene una opinión divergente), o la obtención de una segunda opinión de un asesor externo independiente.

- Conflictos Graves: Proceder a la abstención formal del DPO en el asunto, con la designación de un sustituto (interno sin conflicto o externo). Esto es crítico en procesos sancionadores o litigios donde el DPO no puede actuar como "abogado defensor" de la compañía.

k) Procedimiento Formal de Escalada y Resolución de Desacuerdos

- Activación: El DPO debe tener el derecho y el deber de activar el procedimiento de escalada si sus recomendaciones críticas no son atendidas o si percibe interferencias.

- Cadena de Escalada Clara: Definir la ruta exacta (ej. DPO → Comité de Riesgos → Directorio) y los plazos máximos para cada nivel.

- Documentación del Disenso: Si la alta dirección decide apartarse de la recomendación del DPO, esta decisión y sus motivos deben quedar registrados por escrito en las actas del comité o Directorio, junto con la recomendación original del DPO. Esto crea una trazabilidad auditable y protege al DPO.

l) Supervisión y Aprendizaje Continuo

- Revisión Periódica del Registro de Conflictos: Analizar anualmente el registro para identificar patrones recurrentes, áreas problemáticas o tendencias.

- Actualización de Procedimientos: Incorporar las lecciones aprendidas para mejorar continuamente los protocolos de gestión de conflictos.

- Formación Basada en Casos Reales: Utilizar ejemplos de conflictos (anonimizados) en programas de capacitación para la alta dirección y gerencias.

Al establecer y mantener esta "armadura jurídica", la organización no solo cumple con las exigencias legales de autonomía y no conflicto de interés, sino que también construye una cultura de accountability y transparencia que refuerza la confianza interna y externa.

4.6. Habilitadores del Rol: Recursos Adecuados y Suficientes

Un Delegado de Protección de Datos con independencia formal pero sin los recursos para ejercerla es, en la práctica, una figura inoperante. La Ley N° 19.628 es clara y establece una obligación de resultado para la organización: debe disponer que el delegado "cuente con los medios y facultades suficientes para el desempeño de sus funciones, debiendo otorgarle los recursos materiales necesarios para realizar adecuadamente sus labores"[1].

La "suficiencia" de estos recursos no es un concepto estático, sino una medida proporcional y dinámica que debe estar alineada con la escala, complejidad y perfil de riesgo de las operaciones

de tratamiento de datos de la organización. Un DPO sin los recursos adecuados no solo es una oportunidad estratégica desperdiciada, sino que constituye un incumplimiento directo de la ley. Estos recursos deben entenderse en un sentido holístico, abarcando capital humano, presupuesto, herramientas tecnológicas y acceso al conocimiento.

4.6.1. Capital Humano y Estructura de Apoyo: El Ecosistema del DPO[106]

La eficacia del DPO no depende únicamente de su pericia individual, sino del ecosistema de soporte que la organización construye a su alrededor.

m) Tiempo Protegido y Dedicado del DPO

Un escenario común, aunque **riesgoso**, es que el DPO desempeñe otras funciones. **Para mitigar este riesgo**, es crucial que la organización defina y formalice por escrito un **porcentaje de tiempo mínimo protegido y dedicado** a sus tareas de protección de datos (ej. un mínimo del 80%), **evitando que** las urgencias de su otro rol canalicen sus responsabilidades. **Más allá de este porcentaje**, una **salvaguarda fundamental** es establecer una **política de prevalencia**: en caso de conflicto de agenda o prioridades, las funciones de DPO **siempre prevalecerán**. **Para las organizaciones de gran tamaño o con tratamientos de datos complejos**, esta dedicación efectiva **suele requerir** que el rol sea a tiempo completo y con dedicación exclusiva.[107]

n) Equipo de Soporte Directo (si aplica):

En contextos de alta complejidad, un solo individuo no puede abarcar todas las funciones del DPO. Se debe contemplar una estructura de apoyo con roles definidos, que reporten al DPO:

- Analistas de Privacidad: Para llevar a cabo tareas operativas de supervisión, como realizar Evaluaciones de Impacto (DPIA), mantener actualizado el Registro de Actividades de Tratamiento (RAT), y monitorear el cumplimiento de políticas.

- Abogados de Protección de Datos Personales Junior: Para apoyar en la revisión de contratos, el análisis de nueva normativa y la gestión de la respuesta a solicitudes de derechos de los titulares.

- Soporte Administrativo: Para la gestión logística, coordinación de reuniones, seguimiento de planes de acción y administración del presupuesto.

o) Red de "Privacy Champions" (Embajadores de Privacidad)

Este es un modelo de gobernanza distribuida altamente eficaz para escalar el alcance del DPO sin necesidad de un gran equipo centralizado. Consiste en un programa formal para:

---

[106] Jaksch, Christian, and Gerrit von Daacke. "Datenschutzbeauftragter und Datenschutz-Organisation unter der DSGVO." *Datenschutz und Datensicherheit-DuD* 42.12 (2018): 758-763.

[107] Eggl, Barbara. "Learning to walk a tightrope: Challenges DPOs face in the day-to-day exercise of their responsibilities." Journal of Data Protection & Privacy 3.1 (2019): 69-81.

- Identificar y Nombrar: Designar formalmente a un "Privacy Champion" en cada área de negocio o unidad funcional crítica (ej. TI, Ciberseguridad, Marketing, RRHH, Operaciones, Desarrollo de Productos).

- Definir Roles y Responsabilidades: Actúan como el primer punto de contacto para consultas de Protección de Datos Personales en su área, ayudan a implementar las directrices del DPO, promueven la cultura de Protección de Datos Personales y son los primeros en reportar nuevos proyectos o riesgos al DPO.

- Capacitar y Empoderar: El DPO debe proporcionarles formación específica y avanzada, así como acceso a recursos y plantillas, convirtiéndolos en su extensión operativa en el terreno.

- Coordinar y Sincronizar: Establecer un "Foro de Privacy Champions" con reuniones periódicas (ej. mensuales o trimestrales) para alinear estrategias, compartir conocimientos y discutir desafíos.

4.6.2. Recursos Financieros

El DPO debe contar con un presupuesto propio, específico y anual, que no esté sujeto a la discrecionalidad de otras áreas. La mejor práctica para garantizar su independencia es que este presupuesto sea aprobado directamente por la línea de reporte funcional (ej. el Comité de Auditoría) y no por su superior administrativo, evitando así conflictos de interés. Este presupuesto debe cubrir, como mínimo:

4.6.3. Formación, Certificaciones y Desarrollo Profesional

Un componente esencial de los recursos es el desarrollo profesional. Se deben asignar partidas para cursos de actualización, preparación y mantenimiento de certificaciones reconocidas internacionalmente (ej. CIPP/E, CIPM, CDPSE de la IAPP; CISA, CRISC de ISACA), y asistencia a congresos y seminarios nacionales e internacionales para mantenerse al día con las tendencias.

4.6.4. Asesoría Externa Especializada

Para situaciones que requieran *expertise* específico o una perspectiva externa, es fundamental contar con fondos para contratar consultores, peritos técnicos o bufetes de abogados externos. Esto es crucial para obtener segundas opiniones en casos complejos, realizar auditorías independientes, o gestionar situaciones de alta complejidad (ej. una brecha de seguridad masiva, un litigio complejo, un proyecto de IA con alto impacto).

4.6.5. Suscripciones y Acceso a Conocimiento

Pago de membresías en asociaciones profesionales (IAPP, ISACA), suscripciones a publicaciones especializadas, bases de datos jurídicas y servicios de inteligencia sobre amenazas a la privacidad.

4.6.6. Recursos Tecnológicos y Materiales: Las Herramientas del Oficio

En la era digital, la gestión de la Protección de Datos Personales es inmanejable sin el apoyo de la tecnología adecuada. El DPO debe tener la autoridad para proponer y el presupuesto para adquirir las herramientas necesarias.

a) Software Especializado de Gobernanza de Protección de Datos Personales(Plataformas P-GRC)

Adquisición de herramientas que permitan automatizar y gestionar eficientemente:

- Registro de Actividades de Tratamiento (RoPA/RAT): Inventarios de datos dinámicos.

- Gestión de Evaluaciones de Impacto (DPIA/EIPD): Flujos de trabajo para su realización y seguimiento, cumpliendo con el Artículo 15 ter.

- Gestión del Consentimiento: Plataformas para recabar y administrar los consentimientos de los usuarios de forma granular.

- Gestión de Solicitudes de Derechos (DSAR): Portales y sistemas para recibir, tramitar y responder a las solicitudes de los titulares (acceso, rectificación, supresión, etc.).

- Gestión de Incidentes y Brechas: Herramientas para registrar, evaluar y gestionar brechas de seguridad.

4.6.7. El Recurso Intangible: Acceso Irrestricto a la Información y al Conocimiento

Más allá de los recursos tangibles y económicos, el acceso irrestricto a la información y al conocimiento es un recurso fundamental y no negociable para el DPO. Este recurso se compone de dos elementos clave, esenciales para su capacidad de asesoramiento y supervisión efectiva:

- Acceso a la Información y a los Procesos Internos: Debe estar garantizado por política interna que el DPO tiene el derecho a acceder, sin demoras indebidas, a todas las operaciones de tratamiento, documentos, sistemas, informes de auditoría y bases de datos necesarios para su labor. La confidencialidad interna no puede ser invocada como barrera para impedir el acceso del DPO. Esta garantía es vital para poder comprender la realidad operativa de la organización.

- Acceso al Conocimiento Externo y Benchmarking: Además del acceso interno, la organización debe facilitar y financiar la participación del DPO en foros sectoriales y comunidades de profesionales de la privacidad, así como cubrir suscripciones especializadas y bases de datos. Esto permite el *benchmarking*, el intercambio de buenas

prácticas y mantenerse al tanto de las tendencias y amenazas emergentes, asegurando que su asesoramiento esté actualizado y sea pertinente.

Mapa de Calor - Riesgos de Privacidad por Área

Evaluación Q4 2024 - Priorización de Esfuerzos DPO

Crítico (9-10) Alto (7-8) Medio (5-6) Bajo (3-4) Mínimo (1-2)

Marketing Digital — 9.2

Volumen: Alto
Sensibilidad: Alta

- ⚠ Perfilado extensivo
- ⚠ Cookies terceros
- ⚠ Consentimientos débiles

Recursos Humanos — 7.8

Volumen: Medio
Sensibilidad: Muy Alta

- ⚠ Datos salud/sindicales
- ⚠ Monitoreo empleados
- ⚠ Retención excesiva

Ventas/CRM — 7.5

Volumen: Alto
Sensibilidad: Media

- ⚠ Compartir con terceros
- ⚠ Bases desactualizadas
- ⚠ Cross-selling agresivo

IT/Sistemas — 6.3

Volumen: Alto
Sensibilidad: Baja

- ⚠ Logs excesivos
- ⚠ Accesos privilegiados
- ⚠ Shadow IT

Finanzas — 5.8

Volumen: Medio
Sensibilidad: Alta

- ⚠ Datos bancarios
- ⚠ Scoring crediticio
- ⚠ Retención legal

Servicio Cliente — 5.5

Volumen: Alto
Sensibilidad: Baja

- ⚠ Grabación llamadas
- ⚠ Gestión quejas
- ⚠ Derechos ARSOP

Operaciones — 4.2

Volumen: Bajo
Sensibilidad: Media

- ⚠ Videovigilancia
- ⚠ Control accesos
- ⚠ Proveedores

Legal — 2.8

Volumen: Bajo
Sensibilidad: Baja

- ⚠ Contratos
- ⚠ Litigios
- ⚠ Poderes

Métricas Consolidadas de Riesgo

6.1	3	45%	12
Riesgo Promedio	Áreas Críticas	Mejora vs Q3	DPIAs Requeridas

Prioridades de Acción Inmediata

1. Auditoría urgente en Marketing Digital
2. Revisar retención datos RRHH
3. Actualizar consentimientos CRM
4. Formación intensiva áreas críticas

Figura 13 - Mapa de Calor de Riesgos de Privacidad - Evaluación por Área Organizacional

4.7. Proceso de Evaluación Periódica de la Suficiencia de Recursos

Complementando la provisión de recursos, la adecuación de los recursos del DPO no es estática. El entorno normativo evoluciona, las operaciones cambian y el volumen de datos aumenta, lo que afecta las necesidades del rol. Por ello, la organización debe implementar un proceso formal de revisión anual (liderado por el DPO y presentado a su línea de reporte funcional) para evaluar si los recursos asignados (incluidos los intangibles, humanos, financieros y tecnológicos) siguen siendo suficientes. Este proceso es crucial para asegurar la adaptabilidad del rol a las necesidades cambiantes de la organización y el entorno, garantizando así su sostenibilidad a largo plazo.

4.8. Protección contra represalias en la práctica

Deben establecerse garantías explícitas contra el despido o sanción del DPO por el cumplimiento diligente de sus funciones. Incluso si sus opiniones o informes resultan incómodos o contrarios a intereses inmediatos de algunos directivos, el DPO no debe ser penalizado por ello.

En Europa, esta garantía suele recogerse en el artículo 38(3) del GDPR y debe trasladarse internamente, por ejemplo mediante una cláusula específica en el contrato del DPO que refuerce la prohibición de represalias, o en la política antes mencionada.[108]

Adicionalmente, es aconsejable implementar un procedimiento específico y transparente para que el DPO pueda elevar cualquier preocupación sobre intentos de interferencia en su labor. Por ejemplo, identificar uno o más miembros del Directorio (o un Comité de Auditoría) como interlocutores de alto nivel responsables de velar por su independencia, ante quienes el DPO pueda reportar confidencialmente si percibe presiones indebidas.

Debe proveerse al DPO un canal seguro de denuncia interna para reportar cualquier intento de comprometer su independencia o influir indebidamente en sus evaluaciones técnicas, sin miedo a repercusiones negativas. La existencia de este protocolo y el compromiso de la alta dirección con el mismo sirven como elemento disuasorio frente a posibles presiones.

4.9. Separación física y lógica cuando sea necesaria

Finalmente, en algunos casos puede requerirse implementar medidas de separación física o lógica adicionales para reforzar la autonomía del DPO.

Por ejemplo, el DPO debería disponer de un espacio de trabajo que garantice la confidencialidad de sus comunicaciones cuando sea preciso (una oficina donde pueda tener conversaciones privadas con responsables de áreas, con interesados o con la autoridad de control durante una visita).

---

[108] "El delegado de protección de datos no será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o del encargado."

Asimismo, debe establecerse un control de acceso diferenciado a cierta documentación especialmente sensible relacionada con protección de datos: por ejemplo, si existen investigaciones internas vinculadas a protección de datos personales o comunicaciones confidenciales con la autoridad, estas podrían mantenerse en archivos restringidos donde solo el DPO (y quizá algunos directivos) tengan acceso, evitando que otros abogados de la empresa las consulten libremente.

Es recomendable mantener archivos y registros separados para las actividades propias del DPO (p. ej., registro de actividades de tratamiento, evaluaciones de impacto, comunicaciones con la autoridad) frente a otros archivos legales, preservando así la integridad de la información y evitando que se mezclen con expedientes litigiosos u operativos.

Adicionalmente, debe garantizarse la posibilidad de que el DPO celebre reuniones confidenciales con personal interno u organizaciones externas (incluida la autoridad de protección de datos) cuando la naturaleza del asunto lo requiera, sin que participen ni tengan visibilidad otros miembros del departamento legal. Estas medidas de separación, aplicadas caso a caso, ofrecen una capa extra de seguridad para que el DPO pueda ejercer su función sin interferencias, especialmente en situaciones delicadas.

4.10. Mecanismos Formales de Interacción: La Arquitectura del Proceso Colaborativo

La buena voluntad no es una estrategia de gobernanza. La colaboración debe estar cimentada en procesos formales que garanticen la consistencia, la transparencia y la trazabilidad.

4.10.1. Reuniones Periódicas de Coordinación (Comité de Control)

Establecer una reunión formal y periódica (ej. mensual) entre los líderes de DPO, Legal, Compliance y, preferiblemente, Ciberseguridad. La agenda debe incluir:

- Revisión del pipeline de nuevos proyectos y tecnologías.
- Análisis de novedades regulatorias y jurisprudenciales.
- Revisión de incidentes y reclamaciones recientes (lessons learned).
- Planificación de campañas de formación y sensibilización.
- Protocolo de Consulta Mutua y Gatekeeping: Crear un procedimiento documentado que defina los "disparadores" que activan la consulta obligatoria al DPO. Esto asegura su participación temprana (Privacy by Design).

.

- Diferenciación de Entregables: Para mantener la claridad de roles, las opiniones deben documentarse por separado. El Departamento Legal emite un "Informe Legal" o "Opinión Jurídica". El DPO emite un "Dictamen del DPO" o "Informe de Privacidad". Si ambos se

integran en un único documento para la alta dirección, deben ser secciones claramente diferenciadas y firmadas por cada responsable, preservando la integridad y la autoría de cada análisis.

Al implementar esta arquitectura de proceso, la organización transforma la potencial fricción entre las funciones de control en una poderosa sinergia, asegurando una visión de 360 grados sobre el riesgo y el cumplimiento, y fortaleciendo la defensa de la compañía y la protección de sus clientes.

4.11. Salvaguardas Específicas para Áreas de Alto Riesgo

Existen ciertas áreas o situaciones donde el riesgo de conflicto de interés para el DPO es particularmente elevado. En estos casos, además de las medidas generales ya expuestas, se deben implementar salvaguardas reforzadas, dada la sensibilidad del asunto y su potencial impacto en la independencia del DPO. Destacamos a continuación algunas de esas áreas críticas y las salvaguardas especiales pertinentes:

4.11.1. Procesos sancionadores o investigaciones oficiales en materia de datos

Segregación total de roles en procedimientos formales ante la autoridad: Si la organización enfrenta un procedimiento sancionador o una investigación oficial por parte de la autoridad de protección de datos, el DPO no debe participar en modo alguno en la defensa legal de la organización. Su papel debe limitarse a la cooperación requerida con la autoridad (proveyendo información, facilitando inspecciones, etc.), pero la estrategia de defensa debe llevarla exclusivamente el equipo legal litigante. Esta separación absoluta mantiene intacta la imparcialidad y credibilidad del DPO frente a la autoridad.

4.11.2. Designación preventiva de abogados dedicados para la defensa

Es aconsejable identificar por anticipado (en el plan de contingencia ante brechas, por ejemplo) qué profesionales legales asumirán la representación y defensa de la empresa en caso de un procedimiento de esta naturaleza. Debe establecerse que serán abogados diferentes del DPO –idealmente externos o de otra área–, detallando sus responsabilidades. De este modo, cuando ocurre el evento, no hay dudas de quién defiende y quién coopera.

4.11.3. Canales de comunicación completamente separados

Deben existir líneas de comunicación diferenciadas para tratar con la autoridad en estos casos: un canal para la cooperación del DPO (p. ej., comunicaciones formales sobre brecha de seguridad, respuesta a requerimientos de información factual) y otro para la defensa legal (presentación de alegaciones, recursos, negociaciones de sanción). Esto evita interferencias o mensajes cruzados. La autoridad percibirá claramente cuándo habla con el DPO en su rol garante y cuándo con los representantes legales defensores.

4.11.4. Documentación rigurosa de todas las interacciones

Se debe documentar con sumo detalle todas las comunicaciones, reuniones y actuaciones realizadas durante el procedimiento, delimitando quién intervino y en qué capacidad. Por ejemplo: acta de reunión con la autoridad tal día – asistió el DPO (cooperación) y el abogado X (defensa). Esta claridad documental no solo ordena internamente el proceso sino que sirve como evidencia ante la autoridad de que se respetaron los roles (evitando sospechas de que el DPO actuó de abogado defensor encubierto, por ejemplo).

5. El DPO como Socio Estratégico y Catalizador de la Innovación Responsable

5.1. Introducción: La Transformación del Rol del DPO en la Era Digital

Dentro del contexto actual donde los datos se han convertido en el activo más valioso y la confianza en la piedra angular de la competitividad, el Delegado de Protección de Datos (DPO) emerge como una figura transformadora. La evolución de este rol representa uno de los cambios más significativos en la gobernanza corporativa moderna: el tránsito desde una función reactiva y centrada en el cumplimiento hacia un rol proactivo como arquitecto de la innovación responsable y socio estratégico indispensable.

Esta transformación no es meramente semántica ni aspiracional; es una necesidad operativa y estratégica. De hecho, las organizaciones que continúan percibiendo al DPO como un "policía del cumplimiento" o un "freno a la innovación" están desperdiciando una oportunidad única de diferenciación competitiva y asumiendo riesgos innecesarios.

En contraste, aquellas que han comprendido el verdadero potencial del rol están cosechando beneficios tangibles: mayor velocidad de lanzamiento al mercado, reducción de costos por rediseños, fortalecimiento de la confianza del consumidor y creación de ventajas competitivas sostenibles basadas en la Protección de Datos Personales como valor diferenciador.

Cosechar estos beneficios tangibles requiere que el DPO moderno adopte una mentalidad diferente. Ya no pregunta "¿podemos hacer esto legalmente?", sino "¿cómo podemos hacer esto de manera innovadora mientras maximizamos la protección de datos y generamos valor para todas las partes interesadas?". Esta mentalidad transformadora requiere una integración profunda y sistemática con las áreas clave de la organización, convirtiéndose en un facilitador que elimina obstáculos, anticipa riesgos y co-crea soluciones que antes parecían imposibles.

5.2. La Arquitectura de la Integración Estratégica: Un Modelo de Madurez

5.2.1. Nivel 1: Del Aislamiento Reactivo a la Presencia Operativa

En organizaciones con modelos de Protección de Datos Personales inmaduros, el DPO opera en un silo funcional, respondiendo a consultas puntuales y actuando como un "bombero" que apaga incendios normativos. Este modelo reactivo se caracteriza por:

- Intervenciones tardías: El DPO es consultado cuando el producto ya está desarrollado, los contratos firmados o las campañas en marcha, limitando su capacidad de influencia a medidas correctivas costosas.

- Comunicación unidireccional: La información fluye hacia el DPO solo cuando surge un problema, sin canales establecidos para el asesoramiento preventivo.

- Percepción negativa: El DPO es visto como un obstáculo que retrasa proyectos y aumenta costos, generando resistencia organizacional.

La transición hacia la presencia operativa requiere establecer puntos de contacto sistemáticos en los procesos críticos de la organización. Esto no significa simplemente "invitar al DPO a más reuniones", sino rediseñar los procesos para incorporar la perspectiva de protección de datos personales como un elemento constitutivo, no accesorio.

5.2.2. Nivel 2: De la Presencia Operativa a la Influencia Estratégica

En este nivel, el DPO trasciende el rol de asesor técnico para convertirse en un influenciador de las decisiones estratégicas. La organización reconoce que la protección de datos personales no es solo un requisito legal, sino un habilitador de oportunidades de negocio. Las características de este nivel incluyen:

- Participación en la planificación estratégica: El DPO contribuye activamente en la definición de la estrategia de datos de la organización, identificando oportunidades donde la Protección de Datos Personales puede ser un diferenciador competitivo.

- Rol consultivo en innovación: Antes de descartar ideas por consideraciones de privacidad, el DPO trabaja con los equipos para encontrar formas creativas de implementarlas respetando los principios de protección de datos.

- Métricas de valor: La contribución del DPO se mide no solo en términos de cumplimiento, sino en valor agregado: tiempo de comercialización reducido, nuevos modelos de negocio habilitados, confianza del cliente incrementada.

5.2.3. Nivel 3: La Simbiosis Estratégica - El DPO como Co-Creador de Valor

En el nivel más alto de madurez, el DPO se convierte en un co-creador integral del valor corporativo. La protección de datos personales está embebida en el ADN organizacional y el DPO es reconocido como un ejecutivo estratégico cuya perspectiva es indispensable para la toma de decisiones críticas. Este nivel se caracteriza por:

- Liderazgo en la transformación digital responsable: El DPO no solo asesora sobre proyectos existentes, sino que propone e impulsa iniciativas innovadoras basadas en el uso ético y responsable de los datos.

- Influencia en el modelo de negocio: La organización desarrolla productos y servicios donde la protección de datos personales es una característica central de la propuesta de valor, no un añadido.

- Embajador de la confianza digital: El DPO representa a la organización en foros externos, construyendo reputación y posicionando a la empresa como líder en innovación responsable.

5.3. Pilar 1 de la Integración Estratégica del DPO

Este es el pilar de la prevención. Asegura que la protección de datos personales se incorpora desde el inicio, reduciendo costes, riesgos y la necesidad de rediseños costosos.

5.3.1. La Operacionalización de la "Privacidad desde el Diseño y por Defecto" (Privacy by Design & by Default)

Este principio, consagrado en el Artículo 14 quáter de la Ley N° 19.628, no es una recomendación, sino un mandato legal. Para cumplirlo, la participación del DPO debe ser temprana, continua y obligatoria. Se deben establecer mecanismos formales para:

p) Involucramiento en la Fase de Ideación

El DPO debe participar en las etapas conceptuales de nuevos productos o servicios para identificar posibles riesgos de Protección de Datos Personales antes de que se inviertan recursos significativos.

Un primer ejemplo práctico de esta intervención temprana ocurre cuando una empresa financiera planea lanzar una aplicación móvil de scoring crediticio basada en IA. El DPO debe estar presente desde las primeras reuniones de diseño conceptual, y no esperar a que el producto esté desarrollado. En esta fase inicial, su aporte es crucial para la aplicación de la "Privacidad desde el Diseño" (Privacy by Design), permitiendo identificar que el uso de datos de geolocalización para evaluar solvencia podría ser desproporcionado y sugerir alternativas menos invasivas que se integren directamente en la arquitectura inicial del sistema.
La Realización de Evaluaciones de Impacto (PIA/DPIA) es un proceso fundamental dentro de este enfoque preventivo, especialmente para proyectos que impliquen un tratamiento de datos personales de alto riesgo. Se debe implementar un proceso formal donde cualquier proyecto que cumpla este criterio deba someterse a una Evaluación de Impacto en la Protección de Datos, dirigida o supervisada por el DPO, para analizar sistemáticamente los riesgos y definir las medidas adecuadas.

Otro ejemplo práctico que ilustra la aplicación de este principio se ve en una cadena de retail que implementa sistemas de cámaras. Si bien podría considerarse el reconocimiento facial, el DPO guía la DPIA para evaluar alternativas que prioricen la privacidad desde el diseño y, cuando aplique, por defecto. Esto podría llevar a la implementación de sistemas de conteo anónimo (un enfoque de 'Privacy by Design' menos invasivo) o, si el reconocimiento es necesario, a configurar el sistema para minimizar la recolección de datos y establecer periodos de conservación por defecto ('Privacy by Default'), así como configuraciones de privacidad más estrictas habilitadas por defecto para el usuario. El DPO supervisa que estas consideraciones se integren efectivamente en la solución final.

q) Puntos de Control de Protección de Datos Personales Obligatorios (Privacy Gates) en las Metodologías de Desarrollo

La organización debe integrar "puertas de privacidad" en sus metodologías de gestión de proyectos (ej. Waterfall, Agile, Scrum). La validación del DPO se convierte en un requisito para pasar de una fase a la siguiente.

r) Fase de Diseño/Arquitectura

El DPO valida que la arquitectura del sistema y los flujos de datos minimizan la recolección de datos (principio de minimización) y contemplan medidas de seguridad adecuadas.

Ejemplo práctico: En el desarrollo de una plataforma de telemedicina, el DPO revisa los diagramas de arquitectura y detecta que el sistema propuesto almacena historiales médicos completos cuando solo necesita datos específicos de cada consulta. Propone una arquitectura de datos segregada donde solo se accede a la información necesaria para cada interacción médica.

s) Fase de Desarrollo

El DPO asesora sobre técnicas de seudonimización, anonimización y sobre cómo implementar la gestión de consentimientos y los derechos de los titulares.

Ejemplo práctico: **Durante el desarrollo de un sistema CRM, el DPO trabaja con los desarrolladores para implementar:**

- **Campos de datos con fechas de expiración automática**
- **APIs específicas para el ejercicio de derechos ARCO**
- **Logs de auditoría que registran quién accede a qué datos y cuándo**
- **Mecanismos de exportación de datos en formatos portables (JSON, XML)**

t) Fase de Pruebas (QA)

El DPO verifica que las pruebas se realicen con datos de prueba (no reales) o datos debidamente anonimizados y que los mecanismos de protección de datos personales funcionen como se diseñó.

Ejemplo práctico: En una empresa de seguros, el equipo de QA tradicionalmente usaba copias de la base de datos de producción para pruebas. El DPO implementa un proceso donde:

- ***Se crean datos sintéticos que mantienen las características estadísticas pero no son rastreables a personas reales***
- ***Se establecen ambientes de prueba con datos anonimizados mediante técnicas de k-anonimidad***
- ***Se verifican los mecanismos de consentimiento con casos de prueba específicos***
- ***Fase de Lanzamiento: Se requiere una validación final del DPO ("Go/No-Go" desde la perspectiva de la privacidad) antes de que el producto o servicio sea lanzado al mercado.***

Ejemplo práctico: Antes del lanzamiento de una app de fitness que recopila datos de salud:

- *El DPO realiza una revisión final del cumplimiento*
- *Verifica que las políticas de protección de datos personales estén actualizadas y sean claras*
- *Confirma que los mecanismos de consentimiento funcionan correctamente*
- *Valida que las medidas de seguridad estén implementadas*
- *Emite un certificado de conformidad de protección de datos personales que es requisito para el lanzamiento*

5.4. Pilar 2: Participación Activa en Órganos Colegiados de Gobernanza (La Influencia Estratégica)

La presencia del DPO en los comités clave le proporciona una visión holística de la organización, le permite anticipar riesgos y asegura que la protección de datos personales sea una variable constante en la toma de decisiones estratégicas.

5.4.1. Comité de Seguridad de la Información (CSI)

Naturaleza de la Participación: Permanente, con voz y voto.

Aporte Estratégico del DPO: Asegura que la estrategia de ciberseguridad no solo proteja los activos de la empresa, sino también los derechos y libertades de las personas. Traduce los requisitos legales de seguridad en controles técnicos y organizativos específicos.

Ejemplo práctico: En una reunión del CSI donde se discute la implementación de un nuevo sistema de monitoreo de empleados:

- *El CISO propone un sistema que registra todas las teclas presionadas para prevenir fugas de información*
- *El DPO interviene señalando que esto sería desproporcionado y viola el principio de minimización*
- *Juntos diseñan una solución que detecta patrones anómalos sin registrar el contenido específico*
- *El DPO documenta la evaluación de proporcionalidad y las salvaguardas implementadas.*

5.4.2. Comité de Riesgos y/o Auditoría

Naturaleza de la Participación: Permanente, con reporte funcional directo.

Aporte Estratégico del DPO: Integra el riesgo de protección de datos personales en la matriz de riesgos corporativos. Permite que la alta dirección tenga una visión completa de los riesgos legales, financieros y reputacionales asociados al tratamiento de datos.

Ejemplo práctico: El DPO presenta trimestralmente un "Privacy Risk Dashboard" que incluye:

- ***Mapa de calor de riesgos de protección de datos personales por área de negocio***
- ***Indicadores de madurez del programa de Protección de Datos Personales(escala 1-5)***
- ***Riesgos emergentes (nuevas tecnologías, cambios regulatorios)***
- ***Impacto financiero potencial de cada riesgo (multas, litigios, pérdida de clientes)***
- ***Estado de las medidas de mitigación en curso***

5.4.3. Comité de Nuevos Productos/Servicios

Naturaleza de la Participación: Permanente o recurrente obligatorio.

Aporte Estratégico del DPO: Es el foro natural para la aplicación de la "Protección de Datos Personales desde el Diseño". Evalúa el impacto de las innovaciones en la Protección de Datos Personales desde su concepción, evitando costosos rediseños y asegurando un lanzamiento al mercado responsable.

Ejemplo práctico: En el desarrollo de un servicio de asesoría financiera automatizada:

- ***Marketing presenta la idea de usar IA para analizar patrones de gasto y ofrecer consejos personalizados***
- ***El DPO plantea preguntas clave: ¿Qué datos necesitamos realmente? ¿Podemos lograr el mismo resultado con datos agregados? ¿Cómo garantizamos transparencia en las decisiones de la IA?***
- ***Se establece un grupo de trabajo DPO-Producto-Legal para diseñar el servicio***
- ***El resultado: un servicio que usa datos agregados y anonimizados para tendencias generales, solicitando consentimiento específico solo para personalización avanzada***

5.4.4. Comité de Crisis / Gestión de Incidentes

Naturaleza de la Participación: Participación esencial y de liderazgo en caso de brecha.

Aporte Estratégico del DPO: En caso de una brecha de datos, el DPO es el asesor principal sobre las obligaciones legales de notificación a la autoridad y a los titulares, la gestión de la comunicación y la mitigación del impacto para los afectados.

Ejemplo práctico: **Durante una brecha que expone datos de 50,000 clientes:**

- **Hora 0-2: El DPO activa el protocolo de respuesta, evalúa la naturaleza de los datos comprometidos**
- **Hora 2-6: Determina el riesgo para los derechos y libertades (alto: incluye datos financieros)**
- **Hora 6-24: Prepara la notificación a la autoridad con todos los elementos requeridos**

- **Hora 24-48: Diseña la comunicación a los afectados (clara, sin tecnicismos, con acciones concretas)**
- **Hora 48-72: Coordina con legal y comunicaciones para mensajes consistentes**
- **Post-incidente: Lidera el análisis post-mortem y la actualización de protocolos**

5.4.5. Comité de Tecnología y Arquitectura

Naturaleza de la Participación: Participación recurrente o como consultor clave.

Aporte Estratégico del DPO: Asesora sobre la selección de tecnologías y arquitecturas que sean respetuosas con la privacidad (Privacy-Enhancing Technologies - PETs) y evalúa los riesgos de protección de datos personales de las nuevas plataformas tecnológicas.

Ejemplo práctico: En la selección de una nueva plataforma de analytics:

- ***IT propone tres opciones de proveedores***
- ***El DPO evalúa cada una considerando:***
- ***Ubicación de los servidores y transferencias internacionales***
- ***Capacidades de anonimización y agregación***
- ***Controles de acceso y segregación de datos***
- ***Certificaciones de seguridad y privacidad***
- ***Términos del DPA (Data Processing Agreement)***
- ***Recomienda la opción que ofrece procesamiento local y anonimización en origen***
- ***Trabaja con IT para definir la arquitectura de implementación que minimice riesgos.***

5.4.6. Comité de Ética y Cumplimiento

Naturaleza de la Participación: Permanente.

Aporte Estratégico del DPO: Aporta la perspectiva de la ética de los datos, asegurando que el uso de la información no solo sea legal, sino también justo, transparente y alineado con los valores de la organización y las expectativas de la sociedad.

Ejemplo práctico: En la discusión sobre el uso de IA para decisiones de contratación:

- ***RRHH propone usar IA para filtrar CVs y predecir el desempeño de candidatos***
- ***El DPO plantea consideraciones éticas:***
- ***Riesgo de sesgo algorítmico y discriminación***
- ***Transparencia en los criterios de decisión***
- ***Derecho de los candidatos a intervención humana***
- ***Se establece un marco ético que incluye:***
- ***Auditorías regulares del algoritmo para detectar sesgos***
- ***Explicación clara a candidatos sobre el uso de IA***
- ***Derecho a solicitar revisión humana***
- ***Métricas de equidad y diversidad en los resultados.***

5.5. Pilar 3: Integración Transversal con Áreas Funcionales Clave (La Colaboración Operativa)

5.5.1. Integración con el Departamento Legal: De la Tensión Funcional a la Complementariedad Estratégica

a) La Reconceptualización de la Relación

La relación entre el Delegado de Protección de Datos (DPO) y el Departamento Legal puede presentar tensiones funcionales, debido a sus diferentes mandatos y perspectivas. Sin embargo, esta relación puede estructurarse para operar como una colaboración efectiva dentro de la organización. La clave está en reconocer que la diferencia de perspectivas puede ser funcional, creando un sistema de contrapesos (checks and balances) que beneficia a la organización.

El Departamento Legal aporta conocimiento sobre el riesgo jurídico general, experiencia en la negociación de acuerdos complejos, y comprensión del contexto regulatorio amplio.

El DPO, por su parte, aporta conocimiento especializado en privacidad, una perspectiva centrada en los derechos de los individuos, y un enfoque preventivo para identificar riesgos en las fases iniciales.

La colaboración entre estas perspectivas distintas genera un asesoramiento que integra los aspectos legales generales y los de privacidad. Esto resulta en un análisis más completo y alineado con las necesidades de la organización y las expectativas relevantes (stakeholders).

b) Mecanismos de Colaboración Avanzada

- El Modelo de "Legal Privacy Partner"

En lugar de operar en silos paralelos, las organizaciones más avanzadas están implementando un modelo donde cada abogado del departamento legal tiene asignado un "privacy partner" del equipo del DPO. Este modelo funciona de manera similar a como los despachos de abogados asignan asociados a socios senior, pero con un enfoque de colaboración horizontal:

- Revisión conjunta de contratos complejos

Cuando llega un nuevo contrato que involucra procesamiento de datos, el abogado principal y su privacy partner lo revisan simultáneamente. El abogado se enfoca en los términos comerciales, limitaciones de responsabilidad y cláusulas generales, mientras el privacy partner analiza los flujos de datos, las bases legales, las medidas de seguridad y los mecanismos de cumplimiento de derechos. Ambos consolidan sus observaciones en un documento único que presenta una visión integral.

- Desarrollo de cláusulas estándar innovadoras

En lugar de utilizar cláusulas de protección de datos genéricas, los equipos colaboran para desarrollar cláusulas que no solo cumplan con la normativa, sino que también agreguen valor comercial. Por ejemplo, una cláusula que no solo establezca obligaciones de seguridad, sino que también cree un framework para compartir mejores prácticas de seguridad entre las partes, convirtiendo el cumplimiento en una oportunidad de aprendizaje mutuo.

c) El "Privacy Deal Team" para Transacciones Estratégicas

En fusiones, adquisiciones, joint ventures y otras transacciones estratégicas, se forma un "Privacy Deal Team" integrado que trabaja desde el inicio del proceso:

- Due Diligence integrada: Durante la fase de due diligence, mientras el equipo legal revisa contratos y litigios, el componente de protección de datos personales del equipo realiza una evaluación profunda de los activos de datos, identificando no solo riesgos sino también oportunidades. Por ejemplo, identificar bases de datos que, con el consentimiento adecuado, podrían utilizarse para nuevos productos o servicios post-fusión.

- Estructuración creativa de transacciones: El equipo conjunto puede proponer estructuras innovadoras que maximicen el valor mientras minimizan el riesgo de privacidad. Por ejemplo, en lugar de una transferencia directa de datos en una adquisición, podrían estructurar un período de transición donde la empresa adquirida continúa como encargada del tratamiento mientras se obtienen los consentimientos necesarios para la transferencia.

d) Laboratorio de Innovación Legal-Privacidad

Las organizaciones vanguardistas están creando espacios de innovación conjunta donde Legal y Protección de Datos Personales experimentan con nuevos modelos:

- Sandbox regulatorio interno: Antes de proponer nuevos productos o servicios al mercado, los equipos crean un "sandbox" interno donde prueban diferentes aproximaciones legales y de privacidad. Esto permite identificar y resolver problemas potenciales antes de involucrar a reguladores externos.

- Desarrollo de nuevos modelos de negocio: El laboratorio explora activamente cómo la Protección de Datos Personales puede habilitar nuevos modelos de negocio. Por ejemplo, desarrollar servicios premium basados en mayor privacidad, o crear ecosistemas de datos donde el control granular del usuario sobre sus datos se convierte en la propuesta de valor central.

🛍️ Caso 1: Campaña de Marketing Global Multicanal

5.6. Ejemplos Prácticos de Sinergia Legal-DPO

1 Conceptualización Colaborativa

IDEACIÓN

Legal

Revisión de regulaciones de marketing digital y requisitos contractuales con proveedores

DPO

Propuestas innovadoras para Privacy Dashboard y personalización ética

💡 **Innovación Conjunta**

Privacy Dashboard donde usuarios ven en tiempo real qué datos se usan para personalizar su experiencia y ajustan preferencias granularmente

2 Arquitectura Legal-Privacidad Integrada

DISEÑO

Legal

Co-diseño de Privacy Framework Agreement con estándares consistentes para todos proveedores

DPO

Definición de controles de privacidad y mecanismos de auditoría integrados

✔ **Resultado Innovador**

Contratos unificados que simplifican gestión y mejoran coherencia, reemplazando múltiples acuerdos separados

3 Modelo de Consentimiento Dinámico

INNOVACIÓN

Legal

Estructuración legal de consentimientos temporales, condicionales y colaborativos

DPO

Diseño de experiencia de usuario diferenciadora que convierte cumplimiento en ventaja competitiva

🎯 **Diferenciación de Mercado**

Consentimientos temporales ("solo durante Black Friday"), condicionales ("solo si descuentos >30%") y colaborativos ("comparte insights si me muestras aprendizajes")

Figura 14 - Caso de uso 1: Sinergia Lega y DPO

Caso 2: Plataforma de Salud Digital

Innovación en protección de datos de salud

1 Privacy-by-Design Colaborativo

ARQUITECTURA

Legal

Análisis de múltiples regulaciones de salud y diseño de estructura adaptable a futuras normativas

DPO

Diseño de Privacy Modules que se activan/desactivan según jurisdicción y cambios regulatorios

Arquitectura Adaptable

Sistema modular que no solo cumple regulaciones actuales sino que es adaptable a futuras normativas mediante Privacy Modules configurables

2 Modelo de Gobernanza Innovador

GOBERNANZA

Legal

Estructuración jurídicamente ejecutable de Data Governance Charter co-creado con pacientes

DPO

Diseño de mecanismos de auditoría, transparencia y principios éticos más allá del cumplimiento mínimo

Ética Ejecutable

Reemplazo de términos de servicio tradicionales por Data Governance Charter que establece compromisos éticos jurídicamente ejecutables

3 Monetización Ética de Datos

MONETIZACIÓN

Legal

Estructuración de acuerdos justos y ejecutables para beneficios tangibles a pacientes

DPO

Garantía de anonimización robusta y protección integral de derechos de pacientes

Valor Compartido

Datos anonimizados para investigación con beneficios tangibles: descuentos en servicios, acceso prioritario a tratamientos, contribución a causas elegidas por pacientes

Figura 15 - Caso 2 Legal y Sinergia DPO

5.6.1. Integración con Compliance: Creando un Ecosistema de Integridad Corporativa

a) La Evolución de la Relación Compliance-DPO

La relación entre el DPO y la función de Compliance ha evolucionado significativamente. Mientras que inicialmente se veía como una relación problemática debido a potenciales conflictos de interés, las organizaciones maduras han descubierto cómo estructurar esta relación para crear sinergias poderosas mientras mantienen la independencia necesaria.

La clave está en reconocer que mientras Compliance tiene un rol ejecutivo en el diseño e implementación de controles, el DPO puede actuar como un asesor especializado y un multiplicador de fuerza que eleva la efectividad del programa de compliance general. Esta colaboración se manifiesta en múltiples dimensiones:

b) Integración de Protección de Datos Personales en el Sistema de Gestión de Compliance

En lugar de crear sistemas paralelos, las organizaciones avanzadas integran la protección de datos personales como un componente core de su sistema de gestión de compliance:

- Risk Assessment Unificado: Compliance y el DPO colaboran para crear una metodología de evaluación de riesgos que capture tanto los riesgos tradicionales de compliance como los específicos de privacidad. Por ejemplo, al evaluar el riesgo de un nuevo proveedor, no solo se considera el riesgo de corrupción o sanciones, sino también su madurez en protección de datos y su capacidad de responder a incidentes de privacidad.

- Taxonomía de Controles Integrada: Desarrollan conjuntamente una taxonomía de controles donde cada control se mapea tanto a requisitos de compliance general como a principios de privacidad. Un control de "segregación de funciones" no solo previene fraude, sino que también implementa el principio de minimización de datos al limitar el acceso a información personal.

- Indicadores Compuestos: Crean KPIs que reflejan la intersección entre compliance y privacidad. Por ejemplo, un indicador de "Integridad de Datos de Terceros" que mida simultáneamente el cumplimiento de políticas anti-corrupción en la selección de proveedores y la robustez de sus prácticas de privacidad.

- El Modelo de "Privacy Champions" Integrado en la Red de Compliance

Las organizaciones están integrando los Privacy Champions dentro de la red más amplia de Compliance Champions, creando sinergias operativas:

- Formación Cruzada: Los Compliance Champions reciben formación en protección de datos personales y los Privacy Champions en compliance general. Esto crea embajadores

multifuncionales que pueden identificar y escalar tanto riesgos de protección de datos personales como de compliance en sus áreas.

- Reuniones de Coordinación Regional: En organizaciones globales, las reuniones regionales de Champions incluyen tanto temas de compliance como de privacidad, permitiendo identificar patrones y tendencias que afectan ambas áreas. Por ejemplo, un cambio regulatorio en una jurisdicción puede tener implicaciones tanto en anticorrupción como en transferencias internacionales de datos.

- Sistema de Escalamiento Unificado: Se establece un protocolo donde ciertos tipos de consultas o incidentes se escalan conjuntamente a Compliance y al DPO, evitando duplicación de esfuerzos y asegurando respuestas coherentes.

c) Programas de Ética y Cultura Conjuntos

La protección de datos personales y el compliance comparten un fundamento común en la ética corporativa. Las organizaciones líderes están creando programas conjuntos que refuerzan ambos:

- Narrativa Integrada de Integridad: En lugar de mensajes separados sobre "cumplir las reglas" y "proteger los datos", desarrollan una narrativa unificada sobre "hacer lo correcto". Por ejemplo, explican cómo proteger los datos de los clientes y rechazar sobornos son ambas manifestaciones del mismo valor corporativo de integridad.

- Casos de Estudio Multidimensionales: En las sesiones de formación, utilizan casos que involucran tanto aspectos de compliance como de privacidad. Por ejemplo, un caso sobre un empleado que descubre que un proveedor está sobrefacturando y además está manejando inadecuadamente datos personales, enseñando cómo ambos issues deben ser reportados y gestionados.

- Reconocimiento y Recompensas Integradas: Los programas de reconocimiento celebran comportamientos que demuestran excelencia tanto en compliance como en privacidad, reforzando que ambos son igualmente valorados por la organización.

🔍 Caso 1: Investigación Interna por Sospecha de Fraude

5.7. Casos Prácticos de Colaboración Compliance-DPO

1 Protocolo de Investigación Conjunto PROTOCOLO

Compliance

Lidera la investigación definiendo alcance, metodología y cronograma. Establece estrategia de recopilación de evidencia

DPO

Integrado desde el inicio para asegurar respeto a derechos de privacidad de empleados durante la investigación

Protocolo Integral

Desarrollo conjunto especificando exactamente qué datos revisar, tiempo de retención y procedimientos de destrucción para evidencia no relevante

2 Comunicación Transparente a Empleados COMUNICACIÓN

Compliance

Asegura que mensajes no comprometan integridad de la investigación. Define límites de información compartida

DPO

Verifica información adecuada sobre tratamiento de datos personales y derechos de los empleados afectados

Equilibrio Comunicacional

Diseño conjunto de comunicaciones que mantienen la efectividad investigativa mientras garantizan transparencia sobre el tratamiento de datos personales

3 Documentación Dual-Purpose DOCUMENTACIÓN

Compliance

Documentación que demuestra integridad de la investigación y cumplimiento con estándares de compliance corporativo

DPO

Evidencia cumplimiento con principios de protección de datos y respeto a derechos de privacidad durante proceso

Valor Dual

Documentación que sirve tanto para evidenciar integridad investigativa como cumplimiento de protección de datos, invaluable ante cuestionamientos legales o regulatorios

Intervención de Rescate (6 semanas)

Semanas 1-3: Análisis

- Firma de crisis contratada
- Mediador en campeonado
- Protocolo establecido
- Análisis forense

Semanas 4-6: Rediseño

- Tiger Team con poderes
- Co-liderado DPO + CTO
- Arquitectura privacy-first
- Enfoque colaborativo

Renacimiento del Consentimiento
73% adopción

Arquitectura Federada
Datos en origen

Ethics Board con Poder
Veto sobre funciones invasivas

✔ Resultados

• Lanzamiento exitoso (+3 meses)
• NPS superior a competidores
• DPO promovido a C-suite
• Caso de estudio en la industria

Lecciones Críticas

• Mega-conflictos requieren mediación externa
• Excluir al DPO es más costoso que incluirlo
• Transparencia radical = oportunidad de mercado
• Privacy-by-design no es opcional

Figura 16 - CASO 1: Sinergia DPO y Compliance

📣 Caso 2: Sistema Global de Whistleblowing

Colaboración Compliance-DPO en canales de denuncia

1 Diseño de Arquitectura Flexible

ARQUITECTURA

Compliance

Define requisitos funcionales: tipos de denuncias, flujos de escalamiento, plazos de investigación y cumplimiento anticorrupción

DPO

Diseña arquitectura de privacidad para múltiples jurisdicciones usando almacenamiento regional y técnicas de seudonimización

Sistema Adaptable

Arquitectura que cumple regulaciones de múltiples jurisdicciones con almacenamiento regional pero acceso global para investigaciones, usando seudonimización avanzada

2 Modelo de Consentimiento Contextual

CONSENTIMIENTO

Compliance

Establece criterios de gravedad de denuncias y requisitos de información según tipo de alegación y riesgos asociados

DPO

Diseña niveles de anonimato variables según contexto, siempre dando control al denunciante sobre qué información compartir

Flexibilidad Contextual

Sistema donde el nivel de información requerida varía según gravedad: mayor anonimato para denuncias menores, más información para alegaciones graves con explicación clara del por qué

3 Métricas de Efectividad Integral

MÉTRICAS

Compliance

Mide efectividad del canal: casos substantivos identificados, tiempo de resolución, impacto en cultura ética organizacional

DPO

Evalúa efectividad de privacidad: confianza en anonimato, ausencia de brechas de confidencialidad, satisfacción de denunciantes

Medición Holística

Métricas integradas que evalúan tanto efectividad investigativa como protección de privacidad, creando un sistema verdaderamente balanceado y confiable

Métricas de Compliance

- Casos substantivos: 18% del total
- Tiempo promedio resolución: 32 días
- Reducción incidentes éticos: 47%
- ROI del programa: 4.2x

Métricas de Privacidad

- Confianza en anonimato: 87%
- Brechas de confidencialidad: 0
- Satisfacción denunciantes: 8.3/10
- Adopción del canal: +65% YoY

Figura 17 - Caso 2:Sinergia DPO y Compliance

5.7.1. Integración con el CISO: La Alianza Tecnológica para la Protección Integral

a) Redefiniendo la Colaboración CISO-DPO

La relación entre el Chief Information Security Officer (CISO) y el DPO representa una de las alianzas más críticas en la protección de datos moderna. Mientras que tradicionalmente se ha enfocado en evitar conflictos de interés al mantener estos roles separados, las organizaciones líderes están descubriendo cómo crear una colaboración que multiplica la efectividad de ambas funciones sin comprometer la independencia.
Esta colaboración se basa en el reconocimiento de que la seguridad y la privacidad, aunque distintas, son interdependientes.

La seguridad sin protección de datos personales puede resultar en sistemas técnicamente robustos pero intrusivos. La protección de datos personales sin seguridad es una promesa vacía. La verdadera protección de datos emerge de la síntesis de ambas perspectivas.

b) Modelos Avanzados de Colaboración

El Concepto de "Security-Privacy by Design" Las organizaciones están evolucionando del "Security by Design" y "Privacy by Design" separados hacia un enfoque integrado:

- Equipos de Diseño Conjuntos: Para cada nuevo sistema o aplicación significativa, se forma un equipo de diseño que incluye arquitectos de seguridad del equipo del CISO y especialistas en protección de datos personales del equipo del DPO. Este equipo trabaja de manera iterativa, donde cada decisión de arquitectura se evalúa simultáneamente desde ambas perspectivas.

- Threat Modeling Expandido: El proceso tradicional de threat modeling liderado por seguridad se expande para incluir "Privacy Threat Modeling". Por ejemplo, al evaluar amenazas a un sistema de analytics, no solo se consideran ataques externos, sino también riesgos de re-identificación, inferencias no autorizadas, o usos secundarios no previstos de los datos.

- Catálogo de Patrones Conjunto: CISO y DPO co-desarrollan un catálogo de patrones arquitectónicos que son tanto seguros como respetuosos con la privacidad. Por ejemplo, un patrón para "Analytics Seguros y Privados" que especifica cómo implementar capacidades analíticas usando técnicas como computación multipartita segura o privacidad diferencial.

c) Centro de Excelencia en Tecnologías de Mejora de la Privacidad (PETs)

Las organizaciones avanzadas están creando centros de excelencia conjuntos enfocados en Privacy Enhancing Technologies:

- Laboratorio de Innovación PETs: CISO y DPO co-lideran un laboratorio donde se prueban y validan nuevas tecnologías como homomorphic encryption, secure multi-party computation, y federated learning. El CISO evalúa la robustez técnica y la integración con la

infraestructura existente, mientras el DPO valida que efectivamente mejoren la privacidad y cumplan con principios regulatorios.

- Pilots y Proof of Concepts: Ejecutan pilots conjuntos donde nuevas tecnologías se prueban en casos de uso reales. Por ejemplo, implementar federated learning para entrenar modelos de machine learning sin centralizar datos sensibles, con el CISO asegurando la integridad del proceso y el DPO verificando la minimización de datos.

- Programa de Certificación Interna: Desarrollan un programa donde las soluciones tecnológicas reciben una "certificación PET" interna que valida tanto su seguridad como su mejora de privacidad, creando un estándar interno más alto que el mero cumplimiento.

d) Gestión Integrada de Incidentes y Brechas

La respuesta a incidentes es un área donde la colaboración CISO-DPO es absolutamente crítica:

- War Room Conjunto: Durante un incidente significativo, CISO y DPO co-lideran el war room, con roles claramente definidos pero complementarios. El CISO lidera la contención técnica y la investigación forense, mientras el DPO evalúa en tiempo real el impacto en los derechos de los afectados y las obligaciones de notificación.

- Playbooks Integrados: Desarrollan playbooks que integran las perspectivas de seguridad y protección de datos personales para diferentes tipos de incidentes. Por ejemplo, el playbook para "Ransomware con Exfiltración de Datos" incluye pasos técnicos de contención y recuperación junto con árboles de decisión para determinar obligaciones de notificación basados en el tipo y sensibilidad de los datos potencialmente afectados.

- Simulacros Conjuntos: Realizan ejercicios de mesa y simulacros donde los equipos practican la respuesta a escenarios complejos. Por ejemplo, un escenario donde un insider malicioso ha estado exfiltrando datos durante meses requiere coordinación perfecta entre la investigación forense (CISO) y la evaluación de impacto en Protección de Datos Personales(DPO).

👁️ Caso 1: Sistema de Monitoreo de Empleados para Seguridad

5.8. Casos Prácticos de Sinergia CISO-DPO

1 Diseño Proporcional de Capacidades

DISEÑO

CISO

Propone capacidades técnicas necesarias: monitoreo de USB, análisis de patrones de acceso, detección de anomalías para amenazas internas

DPO

Asegura que cada capacidad sea proporcional al riesgo, evaluando impacto en derechos de privacidad de empleados

⚖️ **Sistema Escalonado**

Diseño conjunto de sistema donde el nivel de monitoreo aumenta solo cuando se detectan indicadores de riesgo específicos, balanceando seguridad y privacidad

2 Transparencia Innovadora

TRANSPARENCIA

CISO

Define algoritmos de detección y alertas automáticas para patrones anómalos y amenazas de seguridad

DPO

Diseña mecanismos de transparencia y notificación que respetan principios de información y participación del empleado

📊 **Security & Privacy Dashboard**

Dashboard para empleados donde ven qué monitoreo está activo y por qué. Si se detecta anomalía, reciben notificación con oportunidad de explicar actividad legítima antes de escalar

3 Salvaguardas Técnicas y Procedimentales

SALVAGUARDAS

CISO

Implementa controles técnicos como algoritmos que anonimizan datos personales no relevantes para la seguridad

DPO

Establece controles procedimentales como comité de revisión con representación de empleados y procesos de escalamiento

🔍 **Controles Integrados**

Combinación de salvaguardas técnicas (anonimización automática) y procedimentales (comité de revisión) diseñadas conjuntamente para máxima efectividad

Figura 18 -Caso 1: Sinergia CISO y DPO

☁️ Caso 2: Migración a la Nube con Datos Sensibles

Colaboración CISO-DPO en transformación cloud

1 Evaluación de Proveedores 360° EVALUACIÓN

CISO

Conduce pruebas técnicas de seguridad: penetration testing, revisión de arquitectura, evaluación de certificaciones

DPO

Evalúa capacidades de privacidad: herramientas de gestión de consentimiento, portabilidad de datos, transparencia en sub-procesadores

Framework de Evaluación Integral

Desarrollo conjunto de framework que va más allá de certificaciones estándar, combinando evaluación técnica de seguridad con capacidades avanzadas de privacidad

2 Arquitectura de Datos Estratificada ARQUITECTURA

CISO

Clasifica datos por criticidad de negocio y seguridad, define controles de encryption y gestión de keys

DPO

Clasifica datos por sensibilidad de privacidad, establece requisitos de localización y controles de acceso

Estratificación Dual

Arquitectura donde datos se clasifican tanto por criticidad de seguridad como sensibilidad de privacidad. Datos altamente sensibles en on-premise o con encryption controlada, otros aprovechan eficiencias del cloud público

3 Modelo de Responsabilidad Compartida Expandido RESPONSABILIDAD

CISO

Define responsabilidades de seguridad entre organización y proveedor cloud, establece controles de monitoreo

DPO

Expande modelo para incluir responsabilidades de privacidad, documenta controles de cumplimiento compartidos

Responsabilidad Integral

Expansión del modelo tradicional de responsabilidad compartida para incluir tanto seguridad como privacidad, documentando claramente qué controles son responsabilidad del proveedor, de la organización, o requieren colaboración

Figura 19- Caso 2: Sinergia CISO y DPO

5.8.1. Integración con el Directorio: Elevando la Protección de Datos Personales al Nivel Estratégico

a) La Transformación del Diálogo con el Directorio

La relación entre el DPO y el Directorio representa la culminación de la transformación del rol hacia un verdadero socio estratégico. Esta relación debe evolucionar desde reportes de cumplimiento periódicos hacia un diálogo estratégico continuo sobre cómo la protección de datos personales puede impulsar el valor corporativo y la ventaja competitiva.

El Directorio moderno debe ver al DPO no como un reportador de riesgos, sino como un estratega que puede identificar oportunidades donde otros ven solo restricciones. Esta transformación requiere que tanto el Directorio como el DPO adopten nuevas formas de pensar y comunicarse.

b) Elementos de una Relación Estratégica Madura

La evolución en la naturaleza de las interacciones es fundamental:

- Sesiones de Estrategia de Datos: Además de los reportes regulares, el DPO participa en sesiones estratégicas del Directorio donde se discuten oportunidades de negocio basadas en datos. El DPO no solo señala restricciones, sino que propone modelos innovadores. Por ejemplo, cuando el Directorio considera entrar en un nuevo mercado, el DPO puede proponer cómo las fortalezas en protección de datos personales de la empresa pueden ser un diferenciador en ese mercado.

- Análisis de Competencia en Privacidad: El DPO presenta análisis sobre cómo los competidores están abordando la privacidad, identificando tanto riesgos de quedarse atrás como oportunidades de liderazgo. Por ejemplo, mostrar cómo un competidor ganó participación de mercado después de un incidente de protección de datos personales de otro rival, o cómo empresas están creando nuevas líneas de negocio basadas en protección de datos personales premium.

- Escenarios de Futuro: El DPO facilita ejercicios de planificación de escenarios con el Directorio, explorando cómo diferentes futuros regulatorios o tecnológicos podrían impactar el negocio. Por ejemplo, explorar las implicaciones de tecnologías emergentes como computación cuántica en la privacidad, o cómo cambios geopolíticos podrían afectar las transferencias internacionales de datos.

c) El DPO como Consejero Estratégico del Directorio

El rol evoluciona hacia una función consultiva de alto nivel:

- Asesor en Transacciones Estratégicas: En M&As, el DPO no solo realiza due diligence de cumplimiento, sino que asesora sobre el valor estratégico de los activos de datos y cómo la integración post-fusión puede maximizar este valor mientras respeta la privacidad. Por ejemplo,

identificar sinergias de datos que serían posibles con las estructuras de consentimiento adecuadas.

- Facilitador de Innovación Responsable: Cuando el Directorio considera nuevas tecnologías disruptivas como IA generativa o Internet de las Cosas, el DPO actúa como un "innovation enabler", mostrando cómo implementar estas tecnologías de manera que generen confianza y cumplan con principios éticos más allá del mero cumplimiento legal.

- Voz en Decisiones de Inversión: El DPO participa en evaluaciones de inversiones tecnológicas significativas, no como un gatekeeper sino como un asesor que ayuda a maximizar el ROI considerando la dimensión de privacidad. Por ejemplo, al evaluar una plataforma de Customer Data Platform (CDP), el DPO puede mostrar cómo características adicionales de protección de datos personales pueden abrir nuevos casos de uso y mercados.

d) Creación de Valor a través de la protección de datos

El diálogo con el Directorio se centra en cómo la Protección de Datos Personales genera valor tangible:

- Métricas de Valor de Privacidad: El DPO desarrolla y presenta métricas que conectan la Protección de Datos Personales con resultados de negocio. Por ejemplo:

    - Trust Index: Correlación entre las inversiones en protección de datos personales y los índices de confianza del consumidor
    - Privacy Premium: Análisis de cuánto más están dispuestos a pagar los clientes por servicios con mejores garantías de privacidad
    - Velocidad de Innovación: Cómo un framework robusto de Protección de Datos Personales acelera el time-to-market al reducir rediseños y problemas regulatorios
    - Costo de Incidentes Evitados: Cuantificación del valor de incidentes prevenidos gracias a medidas proactivas de privacidad

- Casos de Negocio para Inversiones en Privacidad: El DPO presenta casos de negocio completos para inversiones en protección de datos personales que van más allá del cumplimiento. Por ejemplo, proponer una inversión en una plataforma de gestión de consentimiento no solo como una necesidad de cumplimiento, sino mostrando cómo puede habilitar personalización más granular, mejorar las tasas de conversión y abrir oportunidades de monetización ética de datos.

- Protección de Datos Personales como Ventaja Competitiva: Ejemplos concretos de cómo la empresa puede usar la protección de datos personales para ganar mercado. Por ejemplo, lanzar una campaña de marketing destacando las prácticas de protección de datos personales superiores, o crear alianzas estratégicas basadas en estándares compartidos de privacidad.

e) Estructuras de Gobernanza Innovadoras

- El Comité de Innovación y protección de datos personales del Directorio: Algunas organizaciones están creando sub-comités del Directorio específicamente enfocados en la intersección de innovación y privacidad:

    - Composición Multidisciplinaria: Incluye directores con experiencia en tecnología, legal, y negocio, creando un foro donde la protección de datos personales se discute desde múltiples perspectivas estratégicas.

    - Agenda Proactiva: En lugar de reaccionar a issues, el comité proactivamente explora oportunidades. Por ejemplo, sesiones sobre "¿Cómo podemos usar synthetic data para acelerar la innovación?" o "¿Qué nuevos modelos de negocio habilita el federated learning?"

    - Conexión con Innovación Externa: El comité invita a expertos externos, startups, y académicos para explorar el futuro de la protección de datos personales y sus implicaciones estratégicas.

- El Privacy Board Advisory Council: Establecer un consejo asesor que reporta al Directorio, compuesto por:

    - Expertos Externos: Líderes de pensamiento en privacidad, tecnología y ética que aportan perspectivas externas
    - Representantes de Stakeholders: Incluyendo clientes, empleados, y sociedad civil
    - El DPO como Secretario Ejecutivo: Facilitando el diálogo entre el consejo y la organización
    - Este consejo eleva el nivel del diálogo sobre protección de datos personales y ayuda al Directorio a anticipar tendencias y expectativas sociales.

🏢 Caso 1: Transformación del Modelo de Negocio Basada en Privacidad

Casos Transformadores de Interacción DPO-Directorio

1 Análisis Estratégico de Mercado

ANÁLISIS

Contribución DPO

Presenta análisis mostrando preocupación creciente de consumidores por privacidad. Identifica segmento "privacy-conscious consumers" sub-atendido por el mercado

Respuesta Directorio

Reconoce oportunidad estratégica en datos presentados. Autoriza exploración de nuevo posicionamiento competitivo basado en privacidad

Insight Estratégico

Identificación de oportunidad de mercado basada en análisis de tendencias de privacidad y comportamiento del consumidor, respaldado con datos de mercado y tendencias regulatorias

2 Modelo "Privacy-First Retail"

PROPUESTA

Contribución DPO

Diseña modelo innovador: app con control total de datos, programa de lealtad "data dividends", marketplace donde clientes monetizan sus datos

Respuesta Directorio

Evalúa viabilidad financiera y estratégica del modelo propuesto. Aprueba desarrollo de prototipo y estudios de factibilidad

Modelo Disruptivo

Transformación completa del modelo de negocio donde los clientes tienen control total de sus datos, reciben beneficios tangibles por compartirlos, y pueden monetizarlos directamente con marcas

3 Roadmap de Implementación de 3 Años

ROADMAP

Roadmap de Implementación

Año 1

Desarrollo roadmap detallado con hitos, inversiones requeridas, retornos esperados y métricas de éxito en privacidad y confianza

Año 2

Aprueba inversión y transformación gradual. Establece governance y supervisa implementación y ajustes estratégicos

Año 3

Expansión del modelo y consolidación del liderazgo en retail ético y privacidad como ventaja competitiva

✔ Transformación Exitosa

La empresa captura nuevo segmento de mercado, aumenta lealtad del cliente, se posiciona como líder en retail ético, y convierte cumplimiento en ventaja competitiva

Figura 20 - Caso 1: Sinergia Directorio y DPO

🤖 Caso 2: Decisión de Inversión en IA con Implicaciones de Privacidad

Equilibrio entre innovación tecnológica y protección de datos

1 Framework de Evaluación Holística

FRAMEWORK

Contribución DPO

Desarrolla framework que evalúa ROI tradicional, riesgo regulatorio a 5 años, impacto en confianza del cliente y oportunidades de diferenciación

Respuesta Directorio

Adopta framework expandido para decisiones de inversión en tecnología. Reconoce valor de evaluación integral más allá de métricas financieras

📈 **Evaluación Integral**

Framework que considera no solo ROI tradicional sino también riesgo regulatorio futuro, impacto en confianza del cliente y oportunidades de diferenciación por privacidad superior

2 Diseño de Alternativas Innovadoras

ALTERNATIVAS

Contribución DPO

Propone federated learning, explainable AI con control del cliente, y AI Ethics Board con participación externa para uso responsable

Respuesta Directorio

Evalúa alternativas propuestas. Considera balance entre innovación y responsabilidad. Aprueba enfoque que fortalece diferenciación

💡 **Innovación Responsable**

En lugar de aprobar/rechazar, el DPO propone alternativas innovadoras: federated learning, explainable AI y governance ético que permiten capturar valor manteniendo principios

3 Piloto con Métricas Expandidas

PILOTO

Contribución DPO

Diseña piloto que mide métricas de negocio tradicionales más niveles de confort del cliente, tasas de opt-in voluntario y impacto en NPS

Respuesta Directorio

Aprueba inversión con salvaguardas propuestas. Establece métricas de éxito que incluyen tanto rendimiento como responsabilidad

✔ **Éxito Integral**

Implementación exitosa comercialmente que fortalece reputación de la empresa, midiendo no solo ROI sino confort del cliente, participación voluntaria y satisfacción general

Figura 21 - Caso 2: Sinergia Directorio y DPO

6. Gestión de Conflictos de Interés del DPO - Marco Operativo y Casos Prácticos

6.1. Introducción: La Naturaleza Inherente de los Conflictos de Interés en la Función del DPO

La gestión de conflictos de interés constituye uno de los desafíos más complejos y críticos en la operativa del Delegado de Protección de Datos. A diferencia de otros roles corporativos donde los conflictos son excepcionales, en la función del DPO estos son prácticamente inherentes debido a la dualidad fundamental de su mandato: servir a la organización mientras protege los derechos de los individuos cuyos datos trata esa misma organización.

Esta tensión estructural no es un defecto del diseño regulatorio, sino una característica deliberada que busca crear un sistema de equilibrios y contrapesos internos. Sin embargo, para que este sistema funcione efectivamente, requiere de mecanismos sofisticados de identificación, prevención y gestión de conflictos que permitan al DPO navegar estas aguas turbulentas manteniendo su independencia, credibilidad y efectividad, conforme a su obligación de garantizar que sus funciones no den lugar a conflicto de intereses.[109]

La complejidad se multiplica cuando el DPO está integrado en estructuras corporativas existentes, particularmente en el Departamento Legal, donde las sinergias operativas pueden verse opacadas por conflictos funcionales profundos. Este capítulo proporciona un marco integral para gestionar estos conflictos, ilustrado con casos prácticos que demuestran cómo las tensiones teóricas se manifiestan en la realidad operativa de las organizaciones.[110]

6.2. Taxonomía de Conflictos de Interés

Para gestionar los conflictos, primero hay que entenderlos. A continuación, se presenta una taxonomía de los tipos de conflictos más comunes que enfrenta un DPO.

- Naturaleza del Conflicto: Surge cuando la organización enfrenta procedimientos administrativos o judiciales relacionados con protección de datos, y el DPO se encuentra atrapado entre su deber de cooperación con las autoridades y la estrategia defensiva de la empresa.

6.2.1. Caso Práctico - Industria Retail: "La Investigación del Black Friday"

- ***Escenario: Una cadena de tiendas implementó un sistema de tracking avanzado para el Black Friday que capturaba el comportamiento de los clientes mediante WiFi y cámaras con reconocimiento facial. Un exempleado denunció ante la autoridad de protección de datos que el sistema operaba sin base legal adecuada.***

[109]Bock, K., & Meissner, S. (2012, junio). Datenschutz-Schutzziele im Recht. Datenschutz und Datensicherheit (DuD), 36(6), 425–431

[110] Ciclosi, F., & Massacci, F. (2023). The Data Protection Officer: A Ubiquitous Role That

- *Desarrollo del Conflicto: La autoridad inicia una investigación formal y solicita documentación extensa. El Departamento Legal adopta una estrategia de "divulgación mínima", argumentando que debe protegerse información comercial sensible. El DPO, quien había expresado reservas sobre el sistema pero fue ignorado, ahora debe decidir qué información proporcionar.*

- *Manifestación del Conflicto: En la reunión de estrategia, Legal propone responder solo a las preguntas explícitas de la autoridad, interpretándolas restrictivamente. La posición del DPO es que debe revelarse que existieron advertencias internas no atendidas sobre la legalidad del sistema. La tensión resultante es clara: si el DPO insiste en la transparencia total, podría ser visto como "traidor" interno; si calla, compromete su integridad profesional y su deber de cooperar con la autoridad.*

- *Resolución Estructurada: Se activa inmediatamente el protocolo de segregación: el DPO se abstiene de participar en la estrategia de defensa. Se contrata a un asesor externo para manejar la interlocución con la autoridad. El DPO documenta por separado su análisis técnico del incumplimiento, y la alta dirección recibe ambas perspectivas para tomar una decisión informada.*

6.2.2. Caso Práctico - Sector Salud: "Los Datos del Ensayo Clínico"

- *Escenario: Un hospital universitario que condujo ensayos clínicos enfrenta una demanda colectiva de pacientes que alegan uso no autorizado de sus datos genéticos para investigación comercial.*

- *Complejidad Adicional: Los datos involucran información genética extremadamente sensible; existen contratos con farmacéuticas que podrían verse afectados; y el DPO participó en la revisión inicial de los consentimientos hace tres años.*

- *Gestión del Conflicto Multicapa: Se presenta un conflicto personal (el DPO debe evaluar un proceso en el que participó), un conflicto institucional (reputación científica vs. derechos de pacientes) y un conflicto de intereses externos (presión de las farmacéuticas).*

- *Protocolo de Resolución: Se designa un "Shadow DPO" externo específicamente para este caso, se crea un comité de crisis con representación de pacientes, se desarrolla una estrategia de comunicación transparente pero legalmente prudente, y se realiza una revisión completa de todos los consentimientos por un panel independiente.*

6.2.3. Caso Práctico - Sector Financiero: "La Auditoría Sorpresa"

- *Escenario: Un banco recibe una inspección no anunciada de la autoridad de protección de datos. Los inspectores solicitan acceso inmediato y descubren que el banco ha estado recopilando datos de redes sociales para scoring crediticio sin*

informar a los clientes. El equipo legal quiere invocar secreto bancario para limitar el acceso.

- *Conflicto en Tiempo Real: A las 10:00 AM, llegan los inspectores y Legal instruye a todos a "no ofrecer información no solicitada". A las 10:30, el DPO debe decidir si menciona un informe interno que alertaba sobre los riesgos. A las 11:00, los inspectores preguntan por las evaluaciones de impacto, y Legal sugiere decir que "se están preparando", pero el DPO sabe que debieron hacerse hace 18 meses.*

- *Decisiones Críticas y Protocolo: El DPO activa el procedimiento de escalamiento inmediato al CEO. Se establece un "war room" con segregación clara de funciones: Legal maneja los aspectos procedimentales, el DPO proporciona información técnica, y Compliance coordina la respuesta. Se designa un único portavoz.*

- *Resultado y Aprendizajes: La transparencia selectiva del DPO generó credibilidad. La autoridad apreció la cooperación como atenuante, y se implementó un protocolo permanente para futuras inspecciones.*

6.2.4. Caso Práctico - Industria Tecnológica: "El Algoritmo de Recomendación"

- *El Dilema: Una plataforma de streaming quiere implementar un nuevo algoritmo de IA que predice el estado emocional del usuario para ajustar las recomendaciones. La innovación promete aumentar el engagement un 40%. Legal argumenta que es posible bajo "interés legítimo", pero el DPO considera que inferir estados emocionales sin consentimiento explícito es invasivo y arriesgado.*

- *Desarrollo y Resolución: Ante la presión del CEO por una implementación rápida, el DPO documenta formalmente sus objeciones. En lugar de una confrontación binaria (sí/no), se desarrolla una solución creativa de "Progressive Consent": el usuario puede optar por diferentes niveles de personalización, recibiendo beneficios premium a cambio de un consentimiento explícito para las recomendaciones emocionales. Además, se implementa un "Mood Dashboard" donde los usuarios ven qué infiere el sistema y pueden corregirlo, dándoles el control.*

6.2.5. Caso Práctico - Sector Logístico: "El Monitoreo de Conductores"

- **Contexto del Conflicto: Una empresa de logística quiere implementar un sistema de monitoreo de su flota con GPS, cámaras y sensores biométricos, justificado por seguridad y requisitos de clientes. El sindicato alerta sobre vigilancia excesiva.**

- **Proceso de Resolución Multicapa: Se crea un comité multidisciplinario que incluye representantes sindicales y un experto externo en Protección de Datos Personales laboral. Se realiza un análisis diferenciado por componente: el GPS es aceptable con políticas claras; las cámaras solo se activan por eventos (frenado brusco); y los**

biométricos se implementan como un piloto voluntario con incentivos. Un comité paritario revisa mensualmente el uso de los datos.

6.2.6. Caso Práctico - E-commerce: "El Dilema del Carrito Abandonado"

- ***El Conflicto Fundamental: Marketing quiere implementar una estrategia agresiva de recuperación de carritos abandonados, incluyendo compartir datos con marcas para ofertas directas. El DPO señala que no hay base legal clara para esto, mientras que Legal argumenta que se podría usar el interés legítimo.***

- ***Desarrollo y Resolución: Se forma una task force que, tras un análisis profundo de riesgos y el modelado del impacto de las restricciones, diseña una solución innovadora: se crea un "Shopping Assistant" con IA. Los usuarios pueden activar la "ayuda para completar la compra", consintiendo específicamente en el remarketing. Los datos se comparten con las marcas solo en modo anonimizado/agregado, y se implementa una atribución respetuosa con la Protección de Datos Personales para medir la efectividad.***

6.2.7. Caso Práctico - SaaS B2B: "El Cliente Enterprise Inflexible"

- ***Contexto de Presión: Una empresa de software está cerrando su contrato más grande del año. El cliente insiste en cláusulas problemáticas (transferencia irrestricta de datos, uso de subprocesadores sin notificación, etc.). El equipo de ventas presiona para cerrar el trato a final de trimestre.***

- ***Evolución del Conflicto: Legal marca las cláusulas como "agresivas pero negociables", mientras que el DPO las califica como "incompatibles con GDPR". La negociación se tensa y el CEO presiona.***

- ***Solución Estructurada: Ante el riesgo de perder el contrato, se diseña una solución compleja: se crea una entidad legal separada para este cliente con una arquitectura técnica que garantiza la residencia de los datos; se incluyen cláusulas sunset (revisión obligatoria en 12 meses); se contrata un seguro de ciberseguridad específico para este contrato; y se designa a un DPO externo solo para supervisar esta cuenta. El contrato se firma con salvaguardas, el DPO mantiene su independencia y el modelo se vuelve replicable.***

6.2.8. Caso Práctico - Sector Educativo: "La Plataforma de Aprendizaje Global"

- ***Conflicto Multidimensional: Una universidad contrata una plataforma de e-learning que procesará datos sensibles de 50,000 estudiantes. El proveedor insiste en hosting en un país sin adecuación y en cláusulas de responsabilidad limitada. El conflicto tiene dimensiones académicas (la mejor herramienta), legales (contratos estándar del***

sector), de Protección de Datos Personales(múltiples red flags) y financieras (presupuesto aprobado solo para esta solución).

- *Proceso de Resolución: Se forma un comité especial con representantes estudiantiles y un experto en EdTech privacy. Se negocia un "Privacy Addendum" específico que incluye localización de datos sensibles y opt-in para el uso de datos en la mejora de la IA. La implementación se realiza en fases, con un piloto voluntario y la designación de un Student Privacy Officer.*

6.2.9. Caso Práctico - Industria Hotelera: "El Sistema de Fidelización Evolutivo"

- *Contexto del Conflicto: Una cadena hotelera quiere expandir su programa de fidelización (en cuyo diseño original participó el DPO) para incluir reconocimiento facial y análisis predictivo. Ahora, el DPO debe auditar la expansión, lo que implica una auto-supervisión de su trabajo previo.*

- *Gestión del Conflicto de Auto-Supervisión: El DPO declara inmediatamente su participación previa y solicita una revisión independiente. Se establece una estructura de doble revisión donde un auditor externo revisa los elementos nuevos, y el DPO solo revisa las recomendaciones del auditor. Un comité de Protección de Datos Personales valida todo el proceso.*

6.2.10. Caso Práctico - Sector Público: "La Base de Datos de Servicios Sociales"

- *Conflicto Ético-Legal: Un municipio quiere cruzar su base de datos de beneficiarios de servicios sociales con registros de empleo, salud y policiales para una intervención integral. El objetivo es ayudar a familias vulnerables, pero el DPO y la sociedad civil alertan sobre los enormes riesgos de discriminación y estigmatización.*

- *Protocolo de Gestión: Se realiza no solo una DPIA, sino una Evaluación de Impacto Social con consulta a los grupos afectados. Se diseñan salvaguardas extraordinarias, como la prohibición de decisiones automatizadas y el derecho a un "nuevo comienzo" (fresh start). La supervisión es continua, con un comité ciudadano de oversight y auditorías públicas.*

6.3. Marco Avanzado de Gestión de Conflictos

Una gestión de conflictos de clase mundial no se basa en la intuición, sino en un sistema proactivo y estructurado. Este marco avanzado se compone de tres elementos: un sistema de detección temprana, protocolos de resolución adaptativa y salvaguardas institucionales.[111][112]

El objetivo es identificar los conflictos antes de que escalen, permitiendo una intervención preventiva.

6.3.1. Herramienta: Conflict Risk Score (CRS)

Se puede desarrollar un sistema de puntuación que evalúe automáticamente el riesgo de conflicto inherente a cada nuevo proyecto o decisión, basándose en una fórmula ponderada:[113]

CRS = (Impacto_Financiero × Sensibilidad_Datos × Presión_Temporal × Divergencia_Inicial) / Salvaguardas_Existentes)

Aplicación Práctica - Caso Farmacéutico:

Proyecto: Una aplicación de seguimiento de medicación con datos compartidos para investigación.
Cálculo CRS:

- Impacto Financiero: 8/10 (*partnership* multimillonario).
- Sensibilidad Datos: 10/10 (datos de salud).
- Presión Temporal: 7/10 (lanzamiento en 3 meses).
- Divergencia Inicial: 6/10 (DPO y Legal difieren en la base legal).
- Salvaguardas Existentes: 3/10 (políticas genéricas).
- Resultado: Un CRS de 186.7 (Alto Riesgo) activa automáticamente acciones predefinidas, como la notificación al Comité de Riesgos, la asignación de un facilitador neutral, y el requisito de una revisión por parte de un *Privacy Board*.

6.3.2. Gestión Proactiva: Implementación de Indicadores Clave de Riesgo (KRIs) de Privacidad

En una organización madura, la gestión de la privacidad trasciende el cumplimiento reactivo para convertirse en una función estratégica de gestión de riesgos. Para ello, es fundamental implementar un sistema de Indicadores Clave de Riesgo (KRIs), que actúan como un sistema de alerta temprana. Al igual que un canario en una mina, estos KRIs señalan la degradación de la cultura de privacidad antes de que se materialice un incidente o un conflicto grave, permitiendo una intervención proactiva.

A continuación, se describen cuatro KRIs de privacidad fundamentales:

[111] Hansen, M., & Kreutzer, M. (Eds.). (2022). Selbstbestimmung, Privatheit und Datenschutz. Springer Vieweg
[112] Ury, William L., Jeanne M. Brett, and Stephen B. Goldberg. *Getting disputes resolved: Designing systems to cut the costs of conflict*. Jossey-bass, 1988.
[113] National Institute of Standards and Technology (NIST). (2020). NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0.

- KRI 1: Degradación de la Colaboración y el Lenguaje. Se manifiesta cuando la función del DPO pasa de ser vista como un socio estratégico a un obstáculo. Esto se detecta en comunicaciones internas que hablan de "manejar" o "gestionar al DPO", o en la exclusión sistemática del DPO de reuniones clave de estrategia y desarrollo de productos. Señala un riesgo de que las decisiones se tomen sin una evaluación de privacidad adecuada.
- KRI 2: Compresión de Plazos de Análisis. Ocurre cuando los plazos para realizar Evaluaciones de Impacto en la Protección de Datos (EIPD) se acortan de manera repetida e injustificada. Este indicador revela que la organización está trivializando la rigurosidad del análisis de riesgos, priorizando la velocidad sobre la debida diligencia y aumentando la probabilidad de lanzar productos o servicios no conformes.
- KRI 3: Evasión de los Canales de Gobernanza. Este KRI se activa cuando los problemas de privacidad son escalados directamente a la alta dirección o al departamento legal, "saltándose" al DPO. Este comportamiento indica una ruptura en el marco de gobernanza establecido y un riesgo de que las decisiones se tomen basadas en una perspectiva puramente legal o comercial, ignorando el análisis técnico y ético del experto en privacidad.
- KRI 4: Deterioro de la Trazabilidad. Se evidencia por una disminución en la calidad, frecuencia o existencia de la documentación que respalda las decisiones de privacidad. La falta de actas, informes de riesgo o registros de decisiones formales crea un riesgo significativo de auditoría y dificulta la rendición de cuentas en caso de una investigación regulatoria.

a) Modelo Escalonado de Resolución de Conflictos

La detección de un KRI debe activar un protocolo de respuesta. Un marco de gobernanza eficaz utiliza un modelo de resolución por capas, adaptando la intervención a la intensidad del conflicto.

- **Capa 1: Resolución Colaborativa (~80% de los casos)**

Corresponde a conflictos de baja intensidad donde la comunicación sigue siendo posible. El objetivo es realinear a las partes mediante el diálogo estructurado antes de que el desacuerdo se enquiste.

- **Ejemplo Aplicado (Startup Fintech):**
  El equipo de producto propuso lanzar un innovador modelo de *credit scoring* utilizando datos transaccionales de los usuarios para mejorar la precisión. El DPO se opuso, argumentando que la centralización y el análisis de dichos datos sin un propósito explícito violaban el principio de minimización. En una sesión colaborativa facilitada, se descubrió que el verdadero obstáculo era un malentendido sobre las alternativas tecnológicas. La solución fue adoptar *federated learning*, una técnica que permite entrenar el modelo de IA en los datos locales del dispositivo del usuario sin necesidad de centralizarlos. De esta forma, el equipo de producto logró su objetivo de innovación y el DPO validó una solución que protegía la privacidad desde el diseño.
- **Capa 2: Mediación Estructurada (~15% de los casos)**

Se activa ante conflictos de alta intensidad donde la comunicación se ha roto. Requiere la intervención de un tercero neutral para reconstruir puentes y encontrar un terreno común.

Ejemplo Aplicado (Empresa de Seguros). Surgió un choque frontal entre el área de negocio y el DPO respecto al uso de datos de dispositivos IoT (wearables) para la tarificación dinámica de pólizas de vida. Negocio argumentaba que era clave para la competitividad, mientras que el DPO advertía sobre un riesgo reputacional y regulatorio masivo por la percepción de vigilancia. Un mediador externo, experto en InsurTech, facilitó un taller de co-creación. El resultado fue un innovador modelo

de consentimiento granular y dinámico, donde los clientes podían elegir qué tipo de datos compartir (pasos, sueño, frecuencia cardíaca) a cambio de beneficios y descuentos claros y tangibles. La solución no solo resolvió el conflicto, sino que se convirtió en un diferenciador competitivo basado en la transparencia y la confianza.

- **Capa 3: Arbitraje Ejecutivo (~5% de los casos)**

Reservada para conflictos críticos e irresolubles con un impacto estratégico significativo. El proceso se formaliza para que la alta dirección tome una decisión final informada y documentada.

Ejemplo Aplicado (Retailer Global). El conflicto más crítico surgió cuando el área de marketing propuso implementar "IA emocional" en las tiendas físicas para analizar las reacciones de los clientes a los productos y campañas, proyectando un aumento del 20% en las ventas. El DPO se opuso firmemente, calificándolo de desproporcionado, invasivo y éticamente cuestionable. Ante el *impasse*, el caso fue elevado al Directorio. El DPO presentó un "Informe de Impacto y Riesgo de Privacidad" y el área de negocio un "Caso de Negocio y Proyección Estratégica". Tras deliberar, el Directorio tomó una decisión de riesgo controlado: autorizar un piloto limitado a dos tiendas en una única región, condicionado a (1) señalización clara y consentimiento explícito reforzado a la entrada, y (2) una auditoría ética externa e independiente con resultados públicos cada trimestre.

6.3.3. Sistema "Black Box" para Conflictos

Similar a las cajas negras de los aviones, se implementa un sistema que captura toda la información relevante de un conflicto para su análisis posterior, incluyendo correos electrónicos, minutas de reuniones, diferentes versiones de documentos y una línea de tiempo automática.[114][115]

Ejemplo - Multinacional de Consumo: Un conflicto sobre el lanzamiento de una app con geolocalización precisa fue analizado a través de su "caja negra". El análisis de 47 emails, 6 versiones del privacy assessment y 3 opiniones legales divergentes reveló que la causa raíz era la falta de claridad en los roles decisorios y la presión de tiempo artificial. Como resultado, se implementó una matriz RACI específica, criterios de proporcionalidad y un tiempo de revisión de Protección de Datos Personales obligatorio. Para fortalecer aún más el sistema, se pueden crear estructuras y roles específicos.

6.3.4. El Modelo de "Privacy Chambers"

Creación de espacios seguros y confidenciales para la discusión de conflictos, con reglas claras, un facilitador neutral permanente y garantía de no represalias.[116]

Ejemplo: Se estableció una "Privacy Chamber" mensual de 2 horas con la participación del DPO, Head Legal, CTO, CISO y un representante de negocio rotativo, facilitada por un ex-regulador. En su primer año, el 89% de los 47 conflictos potenciales se resolvieron en esta instancia, y el 11% restante se escaló con una recomendación unánime.

---

[114] European Data Protection Board (EDPB). (2020). Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Aunque no es sobre resolución de conflictos, las guías del EDPB enfatizan la necesidad de "documentar" las decisiones y la base de las mismas. El sistema "Black Box" y la documentación requerida en la "Capa 3: Arbitraje Ejecutivo" son una manifestación de este principio de rendición de cuentas (accountability).

[115] Project Management Institute (PMI). A Guide to the Project Management Body of Knowledge (PMBOK® Guide).

[116] IAPP (International Association of Privacy Professionals). (2019). Establishing a Privacy Office: A Practical Guide.

6.3.5. Sistema de "Privacy Advocates"

Designación de un grupo rotativo de altos directivos entrenados para actuar como "abogados del DPO" en situaciones de conflicto.[117]

Ejemplo - Tech Unicorn: Ante un conflicto sobre el uso de reconocimiento facial, el CFO fue designado como Privacy Advocate trimestral. Estudió el caso desde la perspectiva de la Protección de Datos Personales y representó la posición del DPO en las reuniones del C-suite, negociando una solución equilibrada. Este modelo permite al DPO mantener su independencia, mientras que la perspectiva de la Protección de Datos Personales gana un poderoso aliado interno.

6.3.6. Casos Complejos de Gestión Integrada

Los conflictos rara vez ocurren en un vacío. A menudo, múltiples dimensiones de tensión convergen en un único proyecto de alta presión. Aquí es donde un marco de gestión robusto se pone a prueba.

Caso Comprehensivo - Conglomerado de Medios: "La Plataforma de Contenido Personalizado"

- **Contexto: Una empresa tradicional de medios inicia un proyecto de transformación digital de 500 millones de dólares para competir con plataformas como Netflix, involucrando los datos de 50 millones de usuarios existentes y con una presión extrema del Directorio para un lanzamiento en 6 meses.**

- **Elementos del Conflicto: El proyecto presenta un "mega-conflicto" con múltiples dimensiones:**
  Legal: Contratos de contenido que requieren compartir datos de consumo; licencias territoriales que complican los flujos de datos; litigios existentes por derechos digitales.
  Compliance: Regulaciones diferentes en 30 países, con edades de consentimiento variables y requisitos de localización de datos.
  CISO: Una arquitectura legacy incompatible con la Protección de Datos Personales desde el diseño; necesidad de integrar 15 sistemas distintos; riesgos de seguridad en APIs con terceros.
  DPO: Consentimientos originales insuficientes para los nuevos usos; perfilado extensivo que plantea riesgos; transferencias internacionales masivas requeridas.

[117] Ibid

Matriz de Roles Incompatibles con el DPO

Prevención de Conflictos de Interés – No Ser Juez y Parte

⚠ PRINCIPIO FUNDAMENTAL

El DPO NO puede ocupar ningún cargo que le lleve a determinar los FINES y MEDIOS del tratamiento de datos
Esto crearía un conflicto de interés insalvable con su función de supervisión independiente

Alta Dirección (C-Suite)

CEO - Director General
Define estrategia global y objetivos comerciales que pueden entrar en conflicto con minimización de datos

COO - Director de Operaciones
Determina procesos operativos y flujos de datos para eficiencia del negocio

CFO - Director Financiero
Presión por resultados financieros puede comprometer decisiones de privacidad

Áreas Operativas Clave

CMO - Director de Marketing
Define fines de captación, perfilado y uso de datos para publicidad dirigida

CHRO - Director de RRHH
Determina tratamiento de datos sensibles de empleados y candidatos

Director de Ventas
Presión comercial puede llevar a uso extensivo de datos de clientes

Funciones de Control

Director de Auditoría Interna
El DPO debe ser auditado, no puede auditar y ser auditado simultáneamente

Director de Riesgos
Define apetito de riesgo corporativo que puede diferir del riesgo de privacidad

Compliance Officer (si decide medios)
Si implementa controles directamente, no puede supervisarlos objetivamente

Tecnología y Sistemas

CIO/CTO - Director de TI
Determina arquitecturas y sistemas (medios) para el procesamiento de datos

CISO - Director de Seguridad
Puede priorizar seguridad sobre privacidad (ej: monitoreo excesivo)

Director de Transformación Digital
Impulsa innovación tecnológica que puede maximizar uso de datos

Test Rápido de Conflicto de Interés

¿El rol decide QUÉ datos recoger?
SÍ = CONFLICTO | NO = OK

¿Define PARA QUÉ usar los datos?
SÍ = CONFLICTO | NO = OK

¿Determina CÓMO procesarlos?
SÍ = CONFLICTO | NO = OK

¿Tiene objetivos de negocio directos?
SÍ = CONFLICTO | NO = OK

Figura 22 - Matriz de Roles Incompatibles con el DPO - Art. 50 Ley 19.628 y Art. 38 GDPR

6.4. Conclusiones y Mejores Prácticas en la Gestión de Conflictos del DPO

La gestión de conflictos no es un aspecto secundario de la función del DPO; es su corazón palpitante, el crisol donde su independencia, pericia e influencia se forjan y se demuestran. Lejos de ser una señal de fracaso, los conflictos son un indicador de madurez y relevancia. Su ausencia no denota armonía, sino el silencio de una función de protección de datos personales que ha dejado de ser escuchada o, peor aún, de hablar.

Por tanto, la meta no es un entorno estéril libre de conflictos, sino la construcción de un ecosistema de gobernanza vibrante que los canalice hacia el progreso. Una gestión de clase mundial es un acto de alquimia organizacional: transforma la tensión en tracción, el desacuerdo en diálogo y el riesgo en resiliencia y reputación.

Este ecosistema se nutre de principios que van más allá de las meras políticas:

- Una transparencia radical que ilumina en lugar de acusar.
- Una intervención temprana que actúa como brújula, no como ancla.
- Un respeto profundo por la legitimidad de cada mandato, reconociendo que la tensión entre negocio y Protección de Datos Personales no es una batalla, sino un diálogo entre ambiciones necesarias.
- Un foco incesante en las soluciones, preguntando siempre "¿cómo podemos?" en lugar de explicar "por qué no".

Y, sobre todo, un aprendizaje sistémico, viendo cada conflicto como una clase magistral gratuita para fortalecer a toda la organización.

El futuro de esta disciplina es dinámico y apasionante. La IA nos ayudará a anticipar y los estándares globales a unificar el lenguaje. Pero la evolución final, la más poderosa, es ver los conflictos no como un problema a gestionar, sino como el principal motor de la innovación del mañana. Cada conflicto es una pregunta que empuja a la organización a encontrar nuevas formas de crear valor para sus clientes de una manera más ética, elegante y humana.

En definitiva, la gestión efectiva de conflictos trasciende el cumplimiento y la gestión de riesgos; es el arte de construir organizaciones que innovan con conciencia y lideran con confianza. Los conflictos, navegados con maestría, no son obstáculos, sino los catalizadores que pulen las decisiones, fortalecen los procesos y elevan la madurez organizacional.

El DPO que domina este arte no solo protege a la organización; la eleva. No es un guardián que evita caídas, sino un guía que muestra cómo escalar más alto. Cada conflicto bien resuelto no es una cicatriz, sino un peldaño más en el ascenso de la empresa hacia un liderazgo ético y una ventaja competitiva sostenible en la era digital.

7. Conclusión: El DPO, la Llave Maestra para la Confianza en la Era Digital

A lo largo de este texto, hemos trascendido la visión del Delegado de Protección de Datos (DPO) como un mero requisito normativo. Hemos demostrado que el DPO no es simplemente *una* clave para el cumplimiento, sino la **llave maestra** que abre la puerta a un nuevo paradigma de gobernanza de datos, confianza y valor estratégico.

Hemos desglosado el **"QUÉ"** hace el DPO: sus funciones de supervisión, asesoramiento y promoción cultural, delimitando con precisión quirúrgica las responsabilidades que no le corresponden para preservar su independencia. Hemos definido el **"DÓNDE"** y el **"CÓMO"** opera: en el vértice de la organización, habilitado por un modelo de doble reporte y protegido por una robusta armadura jurídica y de recursos. Y, finalmente, hemos delineado el **"QUIÉN"** debe ser: un profesional híbrido, un estratega que combina la agudeza jurídica con la visión de negocio y la fluidez tecnológica.

La conclusión es inequívoca: designar a un DPO es solo el primer movimiento en una partida estratégica. Una organización que se limita a nombrar a una persona para "cumplir con la ley", sin dotarla de la posición, la independencia y los recursos adecuados, no solo está malinterpretando el espíritu de la norma, sino que está aceptando un riesgo inmanejable. **Un DPO sin poder real es un escudo de cartón ante la inevitabilidad de una brecha o una investigación.**

Por el contrario, una organización que abraza plenamente el rol del DPO realiza una inversión estratégica. Transforma la protección de datos de un centro de costos a un generador de confianza. Un DPO verdaderamente empoderado no es un freno para la innovación, sino su catalizador, asegurando que el desarrollo de nuevos productos y servicios se construya sobre una base de confianza con los clientes, un diferenciador competitivo clave en la economía digital.

En última instancia, el éxito del DPO es el reflejo directo del compromiso de la alta dirección. Cuando el Directorio entiende y ejerce su rol de habilitador, la protección de datos deja de ser un apéndice para convertirse en lo que realmente es: un pilar fundamental de la ética corporativa, la resiliencia organizacional y la sostenibilidad del negocio en el siglo XXI. El éxito de la protección de datos no se medirá por la ausencia de multas, sino por la presencia de una confianza duradera con clientes, empleados y la sociedad en su conjunto. Esa confianza es la verdadera clave, y el DPO es quien la forja.

1. Anexo: El Perfil del Delegado de Protección de Datos (DPO): Competencias para la Confianza Digital

La eficacia de la función del DPO no solo depende de una correcta arquitectura de gobernanza, sino también, y de manera crucial, de las cualidades y competencias de la persona que ocupa el cargo. La Ley N° 19.628 establece que la designación "debe recaer en una persona que reúna los requisitos de idoneidad, capacidad y conocimientos específicos para el ejercicio de sus funciones".[118] De forma análoga, el Artículo 37(5) del GDPR exige que el DPO sea designado "atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39".[119]

Este anexo detalla el perfil del DPO moderno, un profesional híbrido que combina pericia jurídica, entendimiento técnico, visión de negocio y habilidades interpersonales para actuar como el arquitecto de la confianza digital en la organización.

7.1. El Triángulo de Competencias: La Sinergia Indispensable

El DPO eficaz no es un especialista aislado, sino un profesional que integra tres dominios de conocimiento interconectados. La ausencia o debilidad en uno de los vértices compromete la totalidad de su función.

1. **Conocimiento Jurídico-Regulatorio (El Fundamento):** Es la base indispensable. Un profundo dominio del marco normativo aplicable (Ley N° 19.628 y sus reglamentos) y de los estándares internacionales que lo informan, principalmente el GDPR. Esto va más allá de la mera memorización de artículos; implica una comprensión doctrinal de los principios (Art. 5 GDPR), los derechos de los interesados (Arts. 12-22 GDPR), las bases de legitimación (Art. 6 GDPR), las condiciones para el tratamiento de categorías especiales de datos (Art. 9 GDPR) y las obligaciones del responsable y del encargado (Capítulo IV GDPR).
2. **Pericia Técnica y de Seguridad de la Información (El Puente):** Es la capacidad de traducir los requisitos legales en salvaguardas operativas. El DPO debe dialogar con fluidez con los equipos de TI, Ciberseguridad y Desarrollo sobre arquitecturas de sistemas, cifrado, seudonimización, controles de acceso (RBAC), seguridad desde el diseño y por defecto (Art. 25 GDPR) y la gestión de la seguridad del tratamiento (Art. 32 GDPR). No necesita ser un programador, pero sí debe entender la lógica y las implicaciones de las tecnologías utilizadas.
3. **Visión de Negocio y Contextual (El Catalizador):** Es la habilidad de alinear la Protección de Datos Personales con la estrategia corporativa. Esto requiere una comprensión íntima del sector, los procesos de negocio, los objetivos estratégicos y los flujos de datos que los sustentan. Permite que el asesoramiento del DPO sea pragmático, orientado a soluciones y percibido como un habilitador de negocio responsable, en lugar de un obstáculo.

1.2. Cuadro Detallado de Requisitos y Competencias

La selección de un DPO debe ser un proceso riguroso que evalúe cualificaciones, experiencia y habilidades blandas. El nivel de exigencia debe ser proporcional a la complejidad, escala y sensibilidad de los tratamientos de datos de la organización.[120]

---

[118] [1] Ley N° 19.628, Sobre Protección de los Datos Personales (actualizada por Ley 21.719), Artículo 50, inciso 5.
[119] Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos - GDPR), Artículo 37(5).
[120] *Este principio de proporcionalidad se deriva directamente del enfoque basado en el riesgo que impregna todo el GDPR. Organizaciones que realizan tratamientos a gran escala de datos sensibles (p.ej., un hospital) o*

Categoría	Requisitos Básicos (Nivel de Cumplimiento)	Requisitos Optimizados (Nivel Estratégico)	Justificación (Vinculación con GDPR/Ley)
1. Formación Académica	• Título universitario en Derecho, Ingeniería Informática, o afines.	• **Postgrado especializado** en Derecho de las TIC, Protección de Datos, Ciberseguridad o Gobernanza de Datos. • **Formación continua demostrable** en normativas sectoriales y tecnologías emergentes.	Un perfil optimizado trasciende la formación base, demostrando una dedicación especializada que asegura la "capacidad para desempeñar sus funciones" (Art. 37.5 GDPR) en un entorno regulatorio y tecnológico en constante cambio.
2. Conocimientos Jurídicos	• Dominio de la ley de protección de datos local. •Conocimiento general del GDPR.	• **Dominio experto y comparado** de la ley local, el GDPR y otras regulaciones relevantes (p.ej., ePrivacy). • **Análisis profundo** de las bases de legitimación, especialmente el interés legítimo y el consentimiento • Expertise en **transferencias internacionales de datos** (incluyendo el impacto de *Schrems II*).	El DPO debe "informar y asesorar" (Art. 39.1.a GDPR). Esto exige un conocimiento que permita no solo aplicar la norma, sino interpretar sus zonas grises y navegar su complejidad, como las transferencias de datos (Capítulo V GDPR).
3. Conocimientos Técnicos	• Principios de seguridad de la información (Confidencialidad, Integridad, Disponibilidad). • Conocimiento de medidas técnicas y organizativas básicas.	• **Comprensión avanzada de arquitecturas de sistemas** y flujos de datos en la organización • Conocimiento de **Tecnologías de Mejora de la Privacidad (PETs)**, como la anonimización, seudonimización y el cifrado homomórfico. • Capacidad para evaluar la seguridad de **tecnologías emergentes** (IA, IoT, Biometría).	Esencial para supervisar el cumplimiento de la **seguridad del tratamiento** (Art. 32 GDPR) y la **Protección de Datos Personales desde el diseño y por defecto** (Art. 25 GDPR). El DPO debe poder cuestionar y validar las soluciones técnicas propuestas.
4. Experiencia Profesional	• 3-5 años en privacidad, cumplimiento o auditoría TI. • Participación en proyectos de cumplimiento.	• Mínimo 5 años con dedicación **principal a la protección de datos/privacidad** • Experiencia liderando la **implementación y gestión de un programa de Protección de Datos Personales**(basado en ISO 27701 o similar). • Experiencia directa en la **gestión de brechas de**	La "práctica en materia de protección de datos" (Art. 37.5 GDPR) es clave. La experiencia en situaciones de crisis (brechas) y en el diálogo con reguladores es un diferenciador crítico que demuestra madurez profesional.

perfilados complejos (p.ej., una entidad financiera) requieren un DPO con competencias significativamente más avanzadas que una PYME con tratamientos básicos.

		seguridad e interacción con **autoridades de control**.	
5. Habilidades Blandas	• Buena comunicación. • Integridad y ética. • Independencia.	• **Habilidad de comunicación estratégica:** Capacidad de traducir riesgos de Protección de Datos Personales en impacto de negocio para el Directorio. • **Liderazgo influyente:** Guiar a la organización hacia una cultura de Protección de Datos Personales sin autoridad jerárquica directa. • **Resiliencia y coraje:** Mantener una postura objetiva frente a presiones comerciales. • **Pensamiento orientado a soluciones:** Proponer alternativas viables en lugar de simplemente decir "no".	Estas habilidades son cruciales para superar la percepción del DPO como un "freno" y posicionarlo como un "socio estratégico". La capacidad de influencia es el motor de la "promoción de la cultura" (función implícita en Art. 39.1.b GDPR).
6. Certificaciones	• Se valoran certificaciones de privacidad (e.g., CIPP/E).	• **Combinación estratégica de certificaciones:** - **CIPP/E** (Normativa Europea, el estándar global) - **CIPM** (Gestión del Programa de Privacidad) - **CIPT** (Tecnología de la Privacidad) •Certificaciones complementarias en **Seguridad (CISSP, CISM)** o **Riesgos (CRISC)** son altamente deseables.	Las certificaciones no son obligatorias, pero sirven como evidencia objetiva de los "conocimientos especializados" requeridos. La combinación CIPM + CIPT demuestra el perfil híbrido (gestión + tecnología) ideal para un DPO estratégico.

1.3. Metodología de Evaluación: De la Teoría a la Práctica

La idoneidad de un DPO no se mide por su currículum, sino por su capacidad para actuar bajo presión y en contextos complejos. Se recomienda un proceso de selección multifacético.

1.3.1. Evaluación de Conocimientos Técnicos y Jurídicos

- **Prueba técnica-jurídica:** Presentar un escenario complejo (p.ej., "Una empresa de e-commerce quiere usar una herramienta de IA de un proveedor estadounidense para analizar el comportamiento del cliente y predecir el abandono. Los datos incluyen historial de compras y geolocalización").
    - *Preguntas clave:* ¿Cuál sería la base de licitud principal? ¿Es necesaria una DPIA? ¿Qué riesgos de transferencia internacional existen y cómo los mitigaría? ¿Qué cláusulas contractuales exigiría al proveedor?

1.3.2. Evaluación de Habilidades Estratégicas y de Comunicación (Simulación)

- **Caso Práctico de Conflicto (Role-playing):** El candidato debe presentar al "Directorio" (interpretado por los entrevistadores) las conclusiones de la DPIA del caso anterior, que resulta en un alto riesgo residual. El "CEO" presiona para lanzar el producto rápidamente.

    - *Evaluación:* Se valora la capacidad del candidato para explicar riesgos complejos en lenguaje de negocio, su firmeza para defender los principios de privacidad, su habilidad para negociar salvaguardas y proponer alternativas (p.ej., un lanzamiento por fases con consentimiento granular) en lugar de un bloqueo total.
- **Simulación de Gestión de Brecha de Seguridad:** Informar al candidato de una brecha de datos (p.ej., "una base de datos de empleados con nombres, RUT y salarios ha sido exfiltrada").
    - *Evaluación:* Se valora su capacidad para mantener la calma, su metodología para evaluar el riesgo para los afectados, su claridad al delinear los plazos y contenidos de la notificación a la autoridad y su empatía al proponer la comunicación a los empleados.

Matriz RACI de Privacidad

Asignación de Responsabilidades en Protección de Datos

Leyenda RACI

R **Responsable:** Ejecuta la tarea A **Aprobador:** Autoriza y rinde cuentas C **Consultado:** Proporciona asesoría I **Informado:** Recibe información

Actividad / Proceso	DPO	Legal	IT/CISO	Negocio	RRHH	Dirección
Evaluación de Impacto (DPIA)	C	C	R	R	I	A
Gestión de Brechas de Seguridad	C	C	R	I	I	A
Atención Derechos ARSOP	C	C	R	R	R	I
Políticas de Privacidad	R	R	C	C	I	A
Formación y Cultura PDP	R	I	I	C	C	A
Auditoría de Cumplimiento	R	I	I	I	I	A
Contratos con Encargados	C	R	C	R	I	A
Transferencias Internacionales	C	R	C	R	I	A
Registro de Actividades (RoPA)	R	C	C	R	C	I
Cooperación con Autoridad	R	C	I	I	I	A

Puntos Clave de la Matriz RACI

- El DPO actúa principalmente como **Responsable (R)** en funciones de supervisión y cultura, y como **Consultado (C)** en decisiones operativas
- La Dirección mantiene la **Aprobación (A)** final en todas las decisiones críticas de privacidad
- Legal y Negocio comparten **Responsabilidad (R)** en la ejecución de muchos procesos
- IT/CISO lidera la **ejecución técnica (R)** de medidas de seguridad y gestión de incidentes
- La matriz garantiza segregación de funciones y evita conflictos de interés del DPO

Figura 23 - Matriz RACI de Privacidad - Asignación de Responsabilidades GDPR

Flujo de Supervisión del DPO

Proceso Continuo de Cumplimiento Normativo

1 RECOPILACIÓN Y ANÁLISIS

Recopilar Información

- ✓ Inventario de tratamientos
- ✓ Documentación de procesos
- ✓ Políticas y procedimientos
- ✓ Contratos con encargados

Analizar Conformidad

- ✓ Verificar bases legales
- ✓ Revisar medidas TOMs
- ✓ Evaluar principios GDPR
- ✓ Validar plazos conservación

2 EVALUACIÓN Y DOCUMENTACIÓN

Identificar Hallazgos

- ✓ Detectar no conformidades
- ✓ Clasificar por criticidad
- ✓ Evaluar riesgos asociados
- ✓ Priorizar acciones

Documentar Resultados

- ✓ Registrar conformidades
- ✓ Detallar incumplimientos
- ✓ Evidencias recopiladas
- ✓ Trazabilidad completa

3 RECOMENDACIONES Y SEGUIMIENTO

Emitir Recomendaciones

- ✓ Proponer medidas correctivas
- ✓ Definir plazos implementación
- ✓ Asignar responsables
- ✓ Estimar recursos necesarios

Realizar Seguimiento

- ✓ Monitorear avances
- ✓ Verificar implementación
- ✓ Actualizar estado acciones
- ✓ Escalar bloqueos

4 REPORTING Y MEJORA CONTINUA

Preparar Informes

- ✓ Consolidar resultados
- ✓ Métricas de cumplimiento
- ✓ Tendencias y patrones
- ✓ Recomendaciones estratégicas

Comunicar a Dirección

- ✓ Presentar al Comité
- ✓ Escalar riesgos críticos
- ✓ Obtener aprobaciones
- ✓ Asegurar recursos

TIPOS DE REPORTES DEL DPO

Reporte Trimestral

- Estado de cumplimiento
- KPIs de privacidad
- Avances del período

→ **Comité de Riesgos**

Reporte de Incidentes

- Brechas de seguridad
- Análisis de impacto
- Medidas adoptadas

→ **Dirección + Autoridad**

Reporte Anual

- Madurez del programa
- Benchmarking sectorial
- Plan estratégico

→ **Directorio**

Figura 24 - Flujo de Supervisión del DPO - Proceso de Cumplimiento Normativo GDPR

10. Anexo: Manual de Integración del DPO - Primeros 90 días

1. Resumen Ejecutivo y Objetivos Estratégicos

Este manual presenta un plan estructurado para la integración del Delegado de Protección de Datos (DPO) en la organización. Su propósito es acelerar la curva de aprendizaje, establecer las bases para una gobernanza de datos efectiva y posicionar el rol del DPO como un socio estratégico indispensable para el negocio.

Objetivos Clave del Período de Integración:

- **Comprensión:** Asimilar la estructura, cultura, operaciones y flujos de datos críticos de la organización.
- **Relacionamiento:** Establecer canales de comunicación y alianzas con los stakeholders clave en todas las áreas.
- **Diagnóstico:** Evaluar el nivel de madurez y cumplimiento actual en materia de protección de datos personales (PDP).
- **Planificación:** Diseñar un plan de acción estratégico a 12 meses, validado por la alta dirección.

Indicadores Clave de Éxito (KPIs) al Día 90:

- Diagnóstico de madurez de PDP completado para el 100% de las áreas críticas.
- Mapeo de stakeholders clave finalizado y canales de comunicación establecidos.
- Plan de Trabajo Anual de PDP aprobado por la dirección.
- Implementación de al menos tres iniciativas de impacto temprano (*quick wins*).

FASE 1: DÍAS 1-30 | INMERSIÓN Y DIAGNÓSTICO
Objetivo: Obtener una comprensión profunda del negocio y realizar una evaluación inicial del estado de la protección de datos.

Semana	Foco Principal	Actividades Clave
Semana 1	**Orientación Institucional**	• **Reunión de Alineación Estratégica:** Con CEO/Gerente General para entender el mandato, prioridades y modelo de reporte. • **Proceso de Onboarding:** Con RR.HH. para documentación, credenciales y políticas internas. • **Configuración Tecnológica:** Asegurar accesos a sistemas y un espacio de trabajo que garantice la confidencialidad.
Semana 2-3	**Diagnóstico del Estado Actual**	• **Análisis Documental:** Revisión de políticas de PDP, avisos de privacidad, contratos con encargados y Registro de Actividades de Tratamiento. • **Evaluación de Procesos:** Análisis de los procedimientos de gestión de derechos, brechas de seguridad y transferencias internacionales. • **Mapeo Tecnológico:** Inventario de sistemas que tratan datos personales y evaluación de las medidas de seguridad existentes.
Semana 4	**Mapeo de Stakeholders**	• **Reuniones Individuales:** Con directores de área para presentar el rol, entender sus necesidades y establecer líneas de comunicación

		directa. • **Presentación al Comité de Dirección:** Exponer el rol del DPO, las primeras observaciones y la propuesta de modelo de trabajo. • **Identificación de Aliados:** Mapeo de potenciales *Privacy Champions* en áreas clave.

Herramienta: Checklist de Áreas para Diagnóstico Inicial

Área	Puntos a Evaluar
Marketing y Ventas	Bases de datos de clientes/prospectos, campañas, segmentación, uso de cookies y tecnologías de seguimiento.
Recursos Humanos	Gestión de datos de empleados, procesos de reclutamiento, sistemas de vigilancia y monitoreo laboral.
IT y Seguridad	Controles de acceso lógico, políticas de respaldo y recuperación, logs de auditoría y monitoreo de seguridad.
Legal y Cumplimiento	Cláusulas de PDP en contratos, gestión de litigios relacionados, comunicaciones con la autoridad de control.
Operaciones y Servicio al Cliente	Gestión de solicitudes, grabación de llamadas, tratamiento de datos en procesos críticos de negocio.

FASE 2: DÍAS 31-60 | PLANIFICACIÓN ESTRATÉGICA E IMPLEMENTACIÓN INICIAL
Objetivo: Traducir el diagnóstico en un plan de acción concreto e implementar iniciativas de alto impacto y baja complejidad para demostrar valor rápidamente.

Semana	Foco Principal	Actividades Clave
Semana 5-6	**Desarrollo del Plan Estratégico**	• **Elaboración del Informe de Diagnóstico:** Documentar el nivel de madurez, brechas, riesgos y oportunidades. • **Priorización de Iniciativas:** Utilizar una matriz de impacto vs. esfuerzo para definir proyectos a corto, mediano y largo plazo. • **Redacción del Plan de Acción Anual de PDP:** Estructurar el documento para su presentación a la dirección.
Semana 7-8	**Implementación de Iniciativas de Impacto Inmediato**	Ejecutar proyectos seleccionados para generar resultados visibles y construir credibilidad. (Ver tabla abajo).

Iniciativas de Impacto Inmediato (Ejemplos)

Iniciativa	Objetivo Clave
Actualización de Avisos de Privacidad	Mejorar la transparencia y asegurar el cumplimiento normativo en los principales puntos de contacto con el titular de los datos.
Establecimiento del Canal Oficial del DPO	Centralizar y formalizar la comunicación (ej. dpo@empresa.com), definiendo SLAs de respuesta.
Protocolo Básico de Respuesta a Brechas	Crear un flujograma de acción y una plantilla de notificación para garantizar una respuesta inicial rápida y coordinada.
Sesión de Sensibilización General	Lanzar un webinar introductorio para toda la organización sobre la importancia de la privacidad y el rol del DPO.

FASE 3: DÍAS 61-90 | ESTABLECIMIENTO DE LA GOBERNANZA Y PROYECCIÓN
Objetivo: Formalizar las estructuras de gobernanza, establecer un sistema de medición y presentar un plan consolidado a la alta dirección.

Semana	Foco Principal	Actividades Clave

Semana 9-10	**Formalización de la Gobernanza**	• **Constitución del Comité de PDP:** Definir su carta constitutiva, miembros y calendario de reuniones. • **Lanzamiento de la Red de *Privacy Champions*:** Nombrar formalmente a los miembros y realizar la primera sesión de capacitación. • **Documentación de Procesos Clave:** Formalizar y publicar los procedimientos para la gestión de derechos, EIPD y brechas.
Semana 11-12	**Sistema de Métricas y Reporte Estratégico**	• **Definición de KPIs de PDP:** (Ej: Tiempo de respuesta a solicitudes, % de proyectos con EIPD, incidentes por mes). • **Diseño de un Dashboard de Privacidad:** Crear una herramienta visual para el seguimiento de métricas. • **Presentación del Informe de 90 Días:** Comunicar a la alta dirección los logros, el diagnóstico final y el plan de trabajo detallado.

Factores Críticos de Éxito y Recursos de Apoyo

Señales de Alerta a Monitorear:

- Falta de acceso a información o reuniones críticas.
- Resistencia cultural o burocrática sistemática por parte de un área.
- Incumplimiento en la asignación de recursos previamente acordados.
- Presiones que busquen comprometer la independencia del rol.

Mejores Prácticas para el DPO:

- **Documentar:** Mantener un registro de decisiones, reuniones y recomendaciones.
- **Construir Alianzas:** Invertir tiempo en relaciones interpersonales antes de que surjan los conflictos.
- **Comunicar el Valor:** Traducir los riesgos de privacidad en impacto para el negocio y celebrar los logros.
- **Aprendizaje Continuo:** Mantenerse actualizado y buscar mentoría externa.

Recursos Clave de Apoyo:

- **Internos:** Sponsor Ejecutivo, RR.HH. Business Partner, Soporte de IT.
- **Externos:** Asesoría legal especializada, consultores senior, comunidades profesionales de DPOs.

Timeline de Integración del DPO

Plan Estructurado de 90 Días

Días 1-30
INMERSIÓN Y DIAGNÓSTICO

Semana 1: Orientación
- Reunión con CEO/Dirección
- Onboarding con RRHH
- Setup tecnológico
- Accesos y credenciales

Semanas 2-3: Diagnóstico
- Análisis documental
- Evaluación procesos
- Mapeo tecnológico
- Inventario sistemas

Semana 4: Stakeholders
- Reuniones individuales
- Presentación Comité
- Identificar aliados
- Mapeo Privacy Champions

Días 31-60
PLANIFICACIÓN E IMPLEMENTACIÓ

Semanas 5-6: Plan Estratégico
- Informe diagnóstico
- Priorización iniciativas
- Plan anual PDP
- Presupuesto y recursos

Semana 7: Quick Wins
- Actualizar avisos privacidad
- Canal DPO oficial
- Protocolo brechas
- Template DPIAs

Semana 8: Formación
- Sesión sensibilización
- Material educativo
- Guías por área
- FAQ privacidad

Días 61-90
GOBERNANZA Y PROYECCIÓN

Semanas 9-10: Gobernanza
- Constituir Comité PDP
- Red Privacy Champions
- Procesos documentados
- Calendario reuniones

Semana 11: Métricas
- Definir KPIs PDP
- Dashboard privacidad
- Sistema reporting
- Baseline métricas

Semana 12: Consolidación
- Informe 90 días
- Presentación Directorio
- Roadmap año 1
- Compromisos recursos

KPIs de Éxito al Día 90

100%	3+	✓	100%
Áreas críticas diagnosticadas	Quick wins implementados	Plan anual aprobado	Stakeholders mapeados

Figura 25 - Timeline de Integración del DPO - Primeros 90 días

11. Anexo: El Delegado de Protección de Datos Externo: Una Alternativa Estratégica

El Reglamento General de Protección de Datos (GDPR) de la Unión Europea introdujo una flexibilidad clave que ha sido adoptada como estándar global: la posibilidad de que la función del DPO sea desempeñada por un proveedor de servicios externo en virtud de un contrato.[121] Esta modalidad, conocida como DPO como Servicio (DPOaaS), no es una solución de "segunda clase", sino una alternativa estratégica que, si se implementa correctamente, puede ofrecer beneficios considerables, especialmente para organizaciones que enfrentan desafíos de recursos, talento o complejidad interna.

Esta sección analiza en profundidad las ventajas, los desafíos inherentes y los factores críticos de éxito para la externalización de la función del DPO, proporcionando un marco para que las organizaciones tomen una decisión informada y gestionen la relación de manera eficaz.

Beneficios de contar con un DPO Externo

Optar por un DPO externo puede ofrecer beneficios que van más allá del simple cumplimiento.

1. Acceso Inmediato a Expertise de Alto Nivel

El mercado de profesionales de la Protección de Datos Personales es altamente competitivo y el talento es escaso y costoso. El modelo DPOaaS permite a las organizaciones, especialmente a las Pequeñas y Medianas Empresas (PYMES), *startups* y ONGs, acceder de inmediato a un nivel de conocimiento y experiencia que sería difícil y oneroso contratar internamente. Estos proveedores suelen contar con equipos multidisciplinarios (abogados, ingenieros, consultores) y certificaciones de primer nivel (CIPP/E, CIPM, CDPSE, etc.).

1. Mitigación Estructural de Conflictos de Interés

Como se ha discutido extensamente, el conflicto de interés es el mayor riesgo para la validez del nombramiento de un DPO interno. Un DPO externo, al no ser un empleado inmerso en la jerarquía, la política interna y los objetivos operativos de la organización, está estructuralmente mejor posicionado para mantener la objetividad. Su lealtad principal es hacia el cumplimiento del contrato de servicios y de la ley, no hacia un superior jerárquico interno, lo que facilita una supervisión más imparcial y la emisión de recomendaciones sin temor a represalias directas sobre su carrera dentro de la empresa.[122]

2. Eficiencia de Costos y Flexibilidad

Para muchas organizaciones, un DPO interno a tiempo completo puede no ser justificable en términos de costo-efectividad. El modelo externo permite una estructura de costos flexible (ej.

[121]

[122] Guidelines on Data Protection Officers (WP243 rev.01), Sección 3.5 "Conflictos de interés".

una tarifa mensual fija o un banco de horas), convirtiendo un costo fijo (salario) en un costo operativo variable (servicio). Esto proporciona "Protección de Datos Personales a escala", permitiendo a la empresa aumentar o disminuir el nivel de servicio según sus necesidades.

5.1.4. Acceso a Herramientas y Metodologías Consolidadas

Los proveedores de DPOaaS, al trabajar con múltiples clientes, desarrollan y refinan constantemente sus propias herramientas, plantillas y metodologías (ej. para DPIAs, gestión de brechas, programas de formación). El cliente se beneficia de este conocimiento acumulado y de estas mejores prácticas, acelerando la implementación de su programa de Protección de Datos Personales sin tener que "reinventar la rueda".

5.1.5 Perspectiva y Benchmarking Multisectorial

Un DPO externo aporta una visión más amplia, enriquecida por su experiencia con diferentes industrias y modelos de negocio. Puede ofrecer valiosos *insights* y *benchmarks* sobre cómo otras organizaciones están abordando desafíos similares, aportando una perspectiva fresca y soluciones innovadoras que un DPO interno, con una visión más endogámica, podría no tener.

5.1. Desafíos de contar con un DPO Externo

A pesar de sus ventajas, la externalización presenta desafíos significativos que deben ser gestionados proactivamente para evitar que el DPO se convierta en una figura distante e ineficaz.

5.1.1. El Dilema de la Proximidad vs. la Independencia

Un DPO eficaz necesita una "proximidad" íntima con la organización para entender su cultura, sus procesos de negocio y sus verdaderos flujos de datos. Un DPO externo que solo interactúa a través de llamadas trimestrales corre el riesgo de convertirse en un auditor superficial, incapaz de detectar riesgos ocultos.[123]

5.1.2. La independencia no debe confundirse con el distanciamiento.

El desafío es encontrar un proveedor que se comprometa a una integración profunda (participando en reuniones clave, conociendo al personal) sin perder su objetividad.

5.1.3. Disponibilidad y Tiempos de Respuesta

Un DPO externo atiende a múltiples clientes. En una situación de crisis, como una brecha de seguridad grave, la organización necesita acceso inmediato. Este riesgo debe ser mitigado a través de Acuerdos de Nivel de Servicio (SLAs) muy claros en el contrato.[124]

[123] Guidelines on Data Protection Officers (WP243 rev.01), Sección 2.2.
[124] ISO/IEC 27001:2022. Anexo A, Control 5.20 "Gestión de la seguridad de la información en la cadena de suministro".

5.1.4. Riesgo de Implicación Superficial en Organizaciones Complejas

En grandes empresas multinacionales, con operaciones y sistemas de datos muy complejos, es dudoso que un DPO externo con un compromiso de tiempo parcial pueda desarrollar el conocimiento profundo necesario para un desempeño eficaz. Su implicación limitada podría impedirle garantizar de forma plena el cumplimiento de obligaciones clave como la supervisión diaria o la integración de la *Privacy by Design*.

5.2.5 Integración Cultural y Confianza Interna

Un DPO externo debe hacer un esfuerzo consciente para no ser visto meramente como un "auditor" externo por los empleados. Debe construir relaciones de confianza y posicionarse como un "asesor de confianza" y un facilitador.

5.2. Dificultad en la Selección del Proveedor Adecuado

Elegir un proveedor de DPOaaS competente es un desafío. La organización debe realizar una diligencia debida rigurosa, verificando no solo las certificaciones, sino también la experiencia práctica relevante en su sector, las referencias de otros clientes, la metodología de trabajo y la solidez del equipo detrás del servicio.

La relación con un DPO externo debe estar cimentada en un contrato de servicios robusto y detallado. Este documento es la principal herramienta de gobernanza y debe especificar, como mínimo:

- Alcance Preciso de Tareas y Responsabilidades: El contrato debe detallar las actividades concretas que realizará el DPO (ej. "realizar dos DPIAs al año", "mantener el RAT actualizado mensualmente", "impartir formación anual").
- Garantías Explícitas de Independencia y Reporte: Debe estipular contractualmente la prohibición de recibir instrucciones y la obligación del DPO de reportar directamente al más alto nivel jerárquico, definiendo quién es este interlocutor.
- Asignación de Tiempo y Recursos (SLAs): Debe especificarse el tiempo asignado (ej. "un mínimo de 20 horas mensuales") y, fundamentalmente, los SLAs para los tiempos de respuesta (ej. respuesta en 24-48h para consultas rutinarias, disponibilidad inmediata para brechas de seguridad).
- Plan de Integración y Comunicación (*Onboarding*): El contrato debe detallar el plan de integración del DPO externo: a quién entrevistará, a qué reuniones asistirá y con qué frecuencia.
- Confidencialidad y Seguridad: Debe incluir una cláusula estricta de secreto profesional y especificar las medidas de seguridad que el propio proveedor de DPOaaS utiliza.
- Condiciones de Terminación y Transición: Definir claramente el proceso de transición y entrega de toda la documentación al finalizar la relación para garantizar la continuidad

En definitiva, el DPO externo es una opción viable y potente, pero exige una gestión activa de la relación por parte de la organización contratante. No se trata de "externalizar el problema", sino de integrar un socio estratégico en el ecosistema de gobernanza.

Test de Evaluación: DPO Interno vs Externo

Herramienta de Decisión Estratégica

Criterio de Evaluación	DPO Interno	DPO Externo
Costo Anual	Alto ($80K-150K + beneficios)	Variable ($30K-80K según demanda)
Conocimiento del Negocio	Profundo (Inmersión total)	Limitado (Curva aprendizaje)
Independencia	Riesgo (Presiones internas)	Alta (Sin conflictos)
Disponibilidad	24/7 (Dedicación exclusiva)	Limitada (Horas contratadas)
Expertise Especializado	Variable (Según perfil)	Alta (Multi-industria)
Tiempo Respuesta	Inmediato	SLA acordado

DPO Interno

Ventajas

- ✓ Conocimiento profundo cultura
- ✓ Integración con equipos
- ✓ Respuesta inmediata crisis
- ✓ Relaciones largo plazo
- ✓ Champion permanente

Desventajas

- × Costo fijo elevado
- × Difícil encontrar talento
- × Riesgo "captura" organizacional
- × Posible aislamiento
- × Única perspectiva

DPO Externo

Ventajas

- ✓ Independencia garantizada
- ✓ Expertise multi-sectorial
- ✓ Costo variable/escalable
- ✓ Red de conocimiento
- ✓ Perspectiva fresca

Desventajas

- × Menor conocimiento interno
- × Disponibilidad limitada
- × Rotación potencial
- × Menos integración cultural
- × Respuesta no inmediata

Test Rápido de Decisión - Responda estas preguntas

¿Volumen de datos procesados?
- >1M registros → Interno
- <1M registros → Externo

¿Presupuesto anual privacidad?
- >$100K → Interno
- <$100K → Externo

¿Complejidad operaciones?
- Alta/Multinacional → Interno
- Simple/Local → Externo

¿Datos sensibles (salud, menores)?
- Sí, volumen alto → Interno
- No/Mínimo → Externo

¿Frecuencia cambios normativos?
- Constante → Interno
- Estable → Externo

¿Cultura de privacidad actual?
- Inmadura → Interno
- Madura → Externo

Recomendaciones por Escenario

StartUp/PyME
DPO Externo
Flexibilidad y costo variable críticos en fase inicial

Empresa Mediana
Híbrido
Externo + Privacy Champion interno como enlace

Corporación
DPO Interno
Complejidad requiere dedicación exclusiva

Figura 26 - Test de Evaluación DPO Interno vs Externo - Herramienta de Decisión

Bibliografía

Article 29 Data Protection Working Party. (2017). *Guidelines on Data Protection Officers ('DPOs') (WP 243 rev.01)*. Comisión Europea.

Bantan, M., & Shawosh, M. (2024). Chief Privacy Officer: A Systematic Literature Review and Future Research Directions. *Communications of the Association for Information Systems*, 54(1), 792-814.

Barezzani, S. (2025). Data Protection by Design and by Default (DPbDD). En *Encyclopedia of Cryptography, Security and Privacy* (pp. 577-579). Cham, Suiza: Springer Nature.

Behrendt, H. (2024). *Der Datenschutzbeauftragte*. Alemania: Haufe.

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. (2019). *Berufsbild des Datenschutzbeauftragten (DSB) / Professional Profile of the Data Protection Officer (DPO)* (4.ª ed.). Berlín, Alemania: Autor.

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. (s.f.). *Das berufliche Leitbild der Datenschutzbeauftragten*.

Blume, J. (2017). A Contextual Extraterritoriality Analysis of the DPIA and DPO Provisions in the GDPR. *Georgetown Journal of International Law*, 49, 1425-1473.

Bock, K., & Meissner, S. (2012). Datenschutz-Schutzziele im Recht. *Datenschutz und Datensicherheit (DuD)*, 36(6), 425–431.

Cheimonidis, P. (2019). *The responsibilities of the DPO according to the GDPR*. (Tesis de maestría). Universidad Internacional Helénica, Tesalónica, Grecia.

Ciclosi, F., & Massacci, F. (2023). The Data Protection Officer: A Ubiquitous Role That No One Really Knows. *IEEE Security & Privacy*, 21(1), 60-69.

Comisión Nacional de Informática y Libertades (CNIL). (2018). *Privacy Impact Assessment (PIA)*. París, Francia: CNIL.

Comisión Nacional de Informática y Libertades (CNIL). (2021). *Practical guide GDPR: Data protection officers*. París, Francia: CNIL.

Comité Europeo de Protección de Datos (EDPB). (2021). *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*. Bruselas, Bélgica: EDPB.

Declaración Universal de Derechos Humanos. (1948). Adoptada por la Asamblea General de las Naciones Unidas.

Drev, M., & Delak, B. (2022). Conceptual model of privacy by design. *Journal of Computer Information Systems*, 62(5), 888-895.

Dubé, J. P., et al. (2025). The intended and unintended consequences of privacy regulation for consumer marketing. *Manuscrito en preparación*.

Eggl, B. (2019). Learning to walk a tightrope: Challenges DPOs face in the day-to-day exercise of their responsibilities. *Journal of Data Protection & Privacy*, 3(1), 69-81.

European Data Protection Board (EDPB). (2019). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. Bruselas, Bélgica: EDPB.

Feng, D., et al. (2024). Towards analyzing and understanding the limitations of dpo: A theoretical perspective. *arXiv preprint arXiv:2404.04626*.

fit4privacy. (2025, junio). *Look Back & Forward at 7 Years of EU GDPR* [Video]. YouTube. https://www.youtube.com/watch?v=-zIea6a49zc

Friedewald, M., et al. (2017). *White Paper DATENSCHUTZ-FOLGENABSCHÄTZUNG*. Stuttgart, Alemania: Fraunhofer IAO.

Gradow, L., & Greiner, R. (2021). *Quick Guide Consent-Management*. Hamburgo, Alemania: ePrivacy GmbH.

Grosmann, P. (2024). *Die Interessenkonflikte Der Betrieblichen und Behördlichen Datenschutzbeauftragten*. Hamburgo, Alemania: Diplomica Verlag.

Grütter, B. J., & Schneider, B. (2019). *Data protection impact assessment guidelines in the context of the general data protection regulation*. Documento de trabajo.

Hanschke, I. (2020). *Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten: Eine kompakte Einführung in die Praxis*. Wiesbaden, Alemania: Springer Vieweg.

Hansen, M., & Kreutzer, M. (Eds.). (2022). *Selbstbestimmung, Privatheit und Datenschutz*. Wiesbaden, Alemania: Springer Vieweg.

International Association of Privacy Professionals (IAPP). (2019). *Establishing a Privacy Office: A Practical Guide*.

International Organization for Standardization (ISO). (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.

Jaksch, C., & von Daacke, G. (2018). Datenschutzbeauftragter und Datenschutz-Organisation unter der DSGVO. *Datenschutz und Datensicherheit-DuD*, 42(12), 758-763.

Kneuper, R. (2021). *Datenschutz für Softwareentwicklung und IT*. Berlín, Alemania: Springer Vieweg.

Kneuper, R. (2024). Foundations of Data Protection According to GDPR. En *Data Protection for Software Development and IT: A Practical Introduction* (pp. 21-65). Berlín, Heidelberg: Springer.

Lachaud, E. (2020). ISO/IEC 27701 standard: Threats and opportunities for GDPR certification. *European Data Protection Law Review*, 6(2), 194-206.

Lambert, P. (2016). *The Data Protection Officer: Profession, Rules, and Role*. Boca Raton, FL: CRC Press.

Ley N° 19.628, Sobre Protección de los Datos Personales (actualizada por Ley 21.719). Congreso Nacional de Chile.

Marelli, M. (2024). Transferring personal data to international organizations under the GDPR: an analysis of the transfer mechanisms. *International Data Privacy Law*, 14(1), 19-36.

Mathew, D., Hacks, S., & Lichter, H. (2018). Developing a semantic mapping between TOGAF and BSI-IT-Grundschutz. *Proceedings of the Multikonferenz Wirtschaftsinformatik (MKWI) 2018*. Lüneburg, Alemania: Leuphana Universität Lüneburg.

National Institute of Standards and Technology (NIST). (2020). *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Version 1.0)*. Gaithersburg, MD: U.S. Department of Commerce.

Oikonomidis, Y., et al. (s.f.). *Data Privacy, Ethical, GDPR & Regulatory Compliance V1*. Documento de proyecto.

Papakonstantinou, V. (2024). Spiros Simitis–his legacy: Europeanisation and Internationalisation. En *Spiros Simitis–sein Vermächtnis*. Baden-Baden, Alemania: Nomos Verlagsgesellschaft.

Plotkin, D. (2020). *Data stewardship: an actionable guide to effective data management and data governance*. Cambridge, MA: Academic Press.

Project Management Institute (PMI). (2021). *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)* (7.ª ed.).

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Ribeiro, S. L., & Nakamura, E. T. (2019). Privacy protection with pseudonymization and anonymization in a health IoT system: results from ocariot. *Proceedings of the 2019 IEEE 19th International Conference on Bioinformatics and Bioengineering (BIBE)*. Atenas, Grecia: IEEE.

Roßnagel, A. (2017). *Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung*. Wiesbaden, Alemania: Springer Fachmedien.

Schneider, D. (2012). Data Protection in Germany: Historical Overview, its Legal Interest and the Brisance of Biobanking. En *Trust in Biobanking: Dealing with Ethical, Legal and Social Issues in an Emerging Field of Biotechnology* (pp. 169-187). Berlín, Heidelberg: Springer.

Schrader, L. F. (2022). *Datenschutz im Gesundheitswesen*. Heidelberg, Alemania: C.F. Müller Verlag.

Smolle, M. (2023). Datenschutzkontrolle und Aufsicht. En *Datenschutz in der Kommunalverwaltung* (pp. 717-739). Berlín, Alemania: Erich Schmidt Verlag.

Tahaei, M., Frik, A., & Vaniea, K. (2021). Privacy champions in software teams: Understanding their motivations, strategies, and challenges. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Yokohama, Japón: ACM.

The Institute of Internal Auditors (IIA). (2017). *Marco Internacional para la Práctica Profesional de la Auditoría Interna (MIPP)*. Lake Mary, FL: The IIA.

Ury, W. L., Brett, J. M., & Goldberg, S. B. (1988). *Getting disputes resolved: Designing systems to cut the costs of conflict*. San Francisco, CA: Jossey-Bass.

Voigt, P., & von dem Bussche, A. (2024). Cooperation with Supervisory Authorities. En *The EU General Data Protection Regulation (GDPR): A Practical Guide* (pp. 261-273). Cham, Suiza: Springer Nature.

Voigt, P., & von dem Bussche, A. (2024). Enforcement and fines under the GDPR. En *The EU General Data Protection Regulation (GDPR): A Practical Guide* (pp. 275-299). Cham, Suiza: Springer Nature.

Voigt, P., & von dem Bussche, A. (Eds.). (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide* (1.ª ed.). Cham, Suiza: Springer International Publishing.

Witt, B. C. (2022). *Datenschutz kompakt und verständlich*. Frechen, Alemania: mitp.

Yaegashi, J. G., Otero, C. S., & Maia, R. B. (2024). A influência da Volkszählungsurteil no ordenamento jurídico brasileiro: um norte para a construção do direito à proteção de dados pessoais para a tutela da personalidade. *Opinión Jurídica*, 23(49).

Soluciones Legales para un Mundo Digital

SOMOS IDÓNEA

Una consultora boutique **especializada en servicios legales en materia de datos personales, IA y ciberseguridad** y conformada por un equipo interdisciplinario de abogados, ingenieros y profesionales con experiencia en diversas áreas. Nos especializamos en ofrecer soluciones adaptadas a los retos y objetivos únicos de cada cliente, manteniendo una estructura de costos competitiva.

SELLO IDÓNEA

- Enfoque integral e interdisciplinario
- Soluciones end-to-end personalizadas y estratégicas
- Experiencia y especialización
- Metodologías exhaustivas para la operativización de obligaciones legales

SERVICIOS

IMPLEMENTACIÓN NUEVA LEY DE DATOS PERSONALES:
Sistema Gestión de Datos Personales

DELEGADO DE PROTECCIÓN DE DATOS (DPO) EXTERNO

MODULARES EN MATERIA DE DATOS PERSONALES:
- Asesoría legal continua
- Evaluaciones de impacto (DPIAs)
- Negociación y redacción de acuerdos críticos
- Capacitación
- Y más.

IMPLEMENTACIÓN LEY MARCO DE CIBERSEGURIDAD:
Programa Ciberseguridad

MODULARES EN CIBERSEGURIDAD:
- Asesoría legal continua
- Seguridad por diseño
- Respuesta y recuperación de incidentes
- Assessment cadena de suministro y riesgos sistémicos
- Protección infraestructura crítica
- Planes de recuperación y continuidad del negocio
- Capacitación
- Y más.

PROGRAMA DE CUMPLIMIENTO EN IA
En etapas de diseño, desarrollo e implementación

ASISTENCIA EN DESARROLLO Y COMERCIALIZACIÓN SISTEMAS DE IA

MODULARES EN IA
- Asesoría legal continua
- Evaluaciones de impacto IA en derechos humanos
- Programa de auditoría algorítmica
- Cadena de suministro
- Capacitación
- Y más.

Cuéntanos sobre ti

info@idonea.cl

Idónea Consultores

www.idonea.cl

Más allá del código y la ley, existen personas. Y la forma en que una organización gestiona sus datos es, en esencia, un reflejo de cómo valora a esas personas.

A menudo, la función del Delegado de Protección de Datos (DPO) queda atrapada en la burocracia del cumplimiento. Este libro la libera. Aquí, el DPO no es un obstáculo para el negocio, sino el arquitecto de su activo más frágil y poderoso: la confianza.

Catherine Muñoz Gutiérrez reconstruye el rol del DPO desde sus cimientos estratégicos. Con un análisis anclado en la realidad latinoamericana, esta guía va más allá de la teoría para ofrecer un marco de actuación: un puente entre la ambición del negocio, la ética y el complejo panorama regulatorio.

Este no es un libro sobre cómo evitar multas. Es un libro sobre cómo construir valor. Es una herramienta esencial para los directivos, juristas y tecnólogos que ya no se preguntan si deben proteger los datos, sino cómo pueden convertir ese deber en su más clara y honorable distinción.