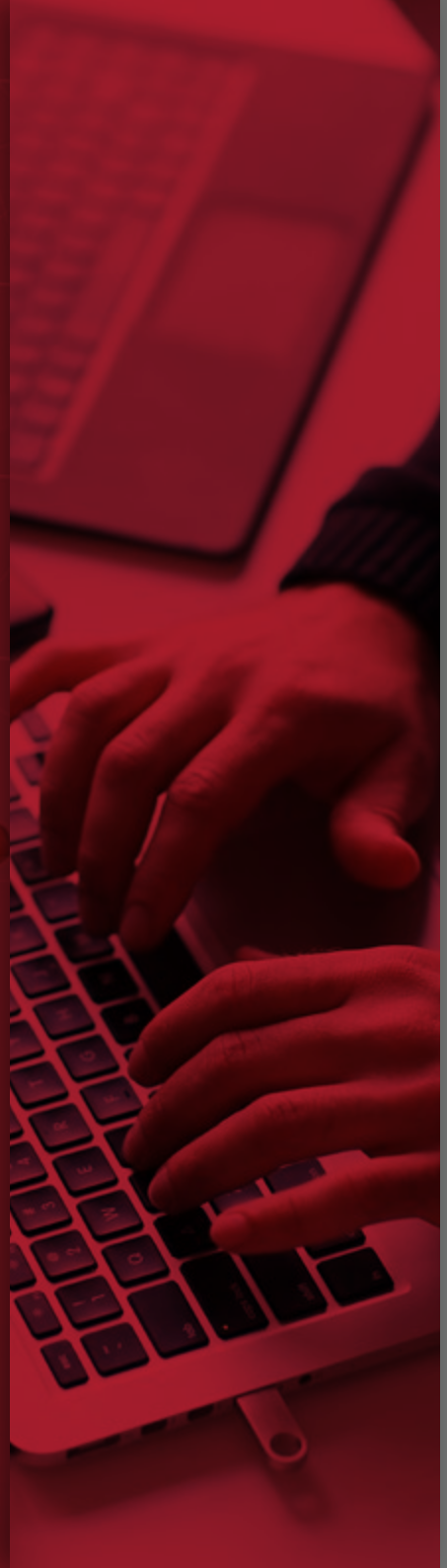
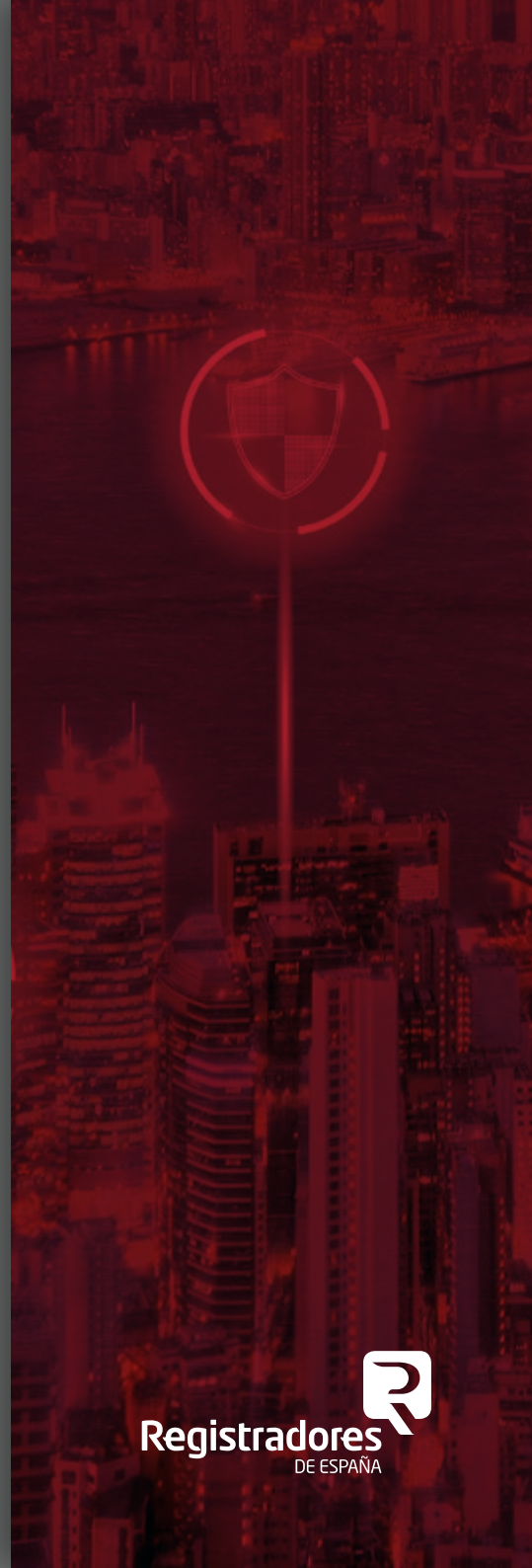


Guía de buenas prácticas

para el cumplimiento del RGPD en organismos descentralizados



En colaboración con
Unión Profesional

Registradores
DE ESPAÑA

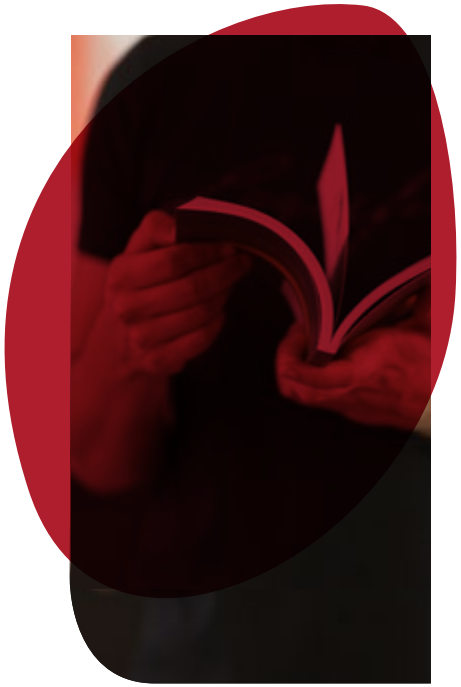
Índice

Introducción

La presente guía tiene por objeto **servir de ayuda a la implantación o mejora de un Servicio centralizado de protección de datos**. Entendemos Servicio centralizado de protección de datos (en adelante, Servicio centralizado) como un Servicio prestado por un organismo público o privado a un conjunto de Responsables de Tratamiento, para ayudarles a cubrir todos o la mayor parte de los requisitos de cumplimiento de la normativa de protección de datos estatal y europea (LOPDGDD, RGPD) así como los dictámenes, guías y resoluciones de las Autoridades de Control competentes.

Esta guía se compone fundamentalmente de las buenas prácticas necesarias para la implantación de un **modelo de servicio centralizado, robusto y eficiente de cumplimiento** en materia de protección datos, que permita optimizar esfuerzos, mejorar los sistemas de cumplimiento y reducir costes de implantación a los Responsables de Tratamiento, a la vez que garantizar los derechos de los ciudadanos en materia de protección de datos.

Es importante resaltar que esta guía no persigue medir el grado de cumplimiento de las organizaciones en materia de protección de datos, ni establecer un diagnóstico sobre dicho grado, sino establecer las pautas necesarias para implantar un modelo organizativo de cumplimiento centralizado óptimo, que pueda ser aprovechado por otros organismos descentralizados, estos sí responsables del cumplimiento de la normativa.



Organismos candidatos a adoptar el modelo

El diseño del modelo de Servicio centralizado permite ser enormemente eficiente en términos de cumplimiento, coste y esfuerzo a la hora de ser consumido por los clientes (Responsables de Tratamiento). No obstante, **este modelo alcanza las máximas cotas de rendimiento cuando los Responsables de Tratamiento objetivo cumplen las siguientes condiciones**:

- Formar parte de un colectivo con tratamientos de datos personales similares y bajo la misma legislación de aplicación.
- Estar bajo el amparo de un organismo centralizado con medios para dotar de un marco de cumplimiento homogéneo.
- Ser proclive a la normalización de los procesos de cumplimiento normativo.
- Contar con un marco previo de cultura de compliance para abordar de forma integral la gestión de los riesgos asociados a su funcionamiento en otras áreas.
- Estar poco especializado en la función de protección de datos y sin elevados medios para poder contratar este servicio en el mercado (pequeñas o medianas organizaciones).
- Requerir disponer de un Delegado de Protección de Datos, y que pueda ser prestado por una figura común al colectivo.

Es necesario recalcar que este modelo de servicios es apto y **muestra fortalezas incluso ante problemáticas complejas** que se pueden dar en el colectivo al que se presta servicio, como por ejemplo: tratamientos a gran escala y/o de categorías especiales, dispersión geográfica de los Responsables de Tratamiento, alta heterogeneidad en los sistemas de información que realizan los tratamientos, diferentes niveles de madurez en el cumplimiento, diferentes grados de autonomía en la gestión, etc.

Por tanto, serían ejemplos válidos de organismos candidatos a prestar el Servicio centralizado todos aquellos organismos públicos o privados con capacidad de centralizar servicios de centenares o miles de entidades independientes, descentralizadas y autónomas en su gestión, tales como colegios profesionales, federaciones, agrupaciones, asociaciones, etc.

Beneficios obtenidos al adoptar el modelo

En base a la experiencia atesorada, **se pueden establecer tres grandes bloques de beneficios para las organizaciones que adoptan el modelo**:

BENEFICIOS PARA LOS RESPONSABLES DEL TRATAMIENTO:

- **Cumplimiento** optimizado y adaptativo del RGPD / LOPDGDD en las entidades.
- Cobertura de la figura del **Delegado de Protección de Datos** atendiendo a todos los requisitos legales en aquellos colectivos obligados o implantación de un servicio especializado en aquellos que no estén obligado estrictamente a disponer de DPD.
- **Minimización drástica de los costes** debido a la optimización de recursos y las economías de escala, gestionando los riesgos de forma proporcional a las funciones realizadas.
- Dotación de los elementos necesarios para establecer un **modelo organizativo y de gestión** que gobierne y opere la privacidad en la organización.
- Mejora de los sistemas de *compliance* corporativo, en el ámbito de la privacidad, así como un **mayor rendimiento de un modelo de prevención de riesgos** integral que contemple otras materias.
- Mejora, incremento o restitución de un nivel de **reputación** deseable para el Responsable, producto de la gestión más efectiva, adecuada y proporcional de la normativa sobre privacidad.

BENEFICIOS PARA EL CIUDADANO:

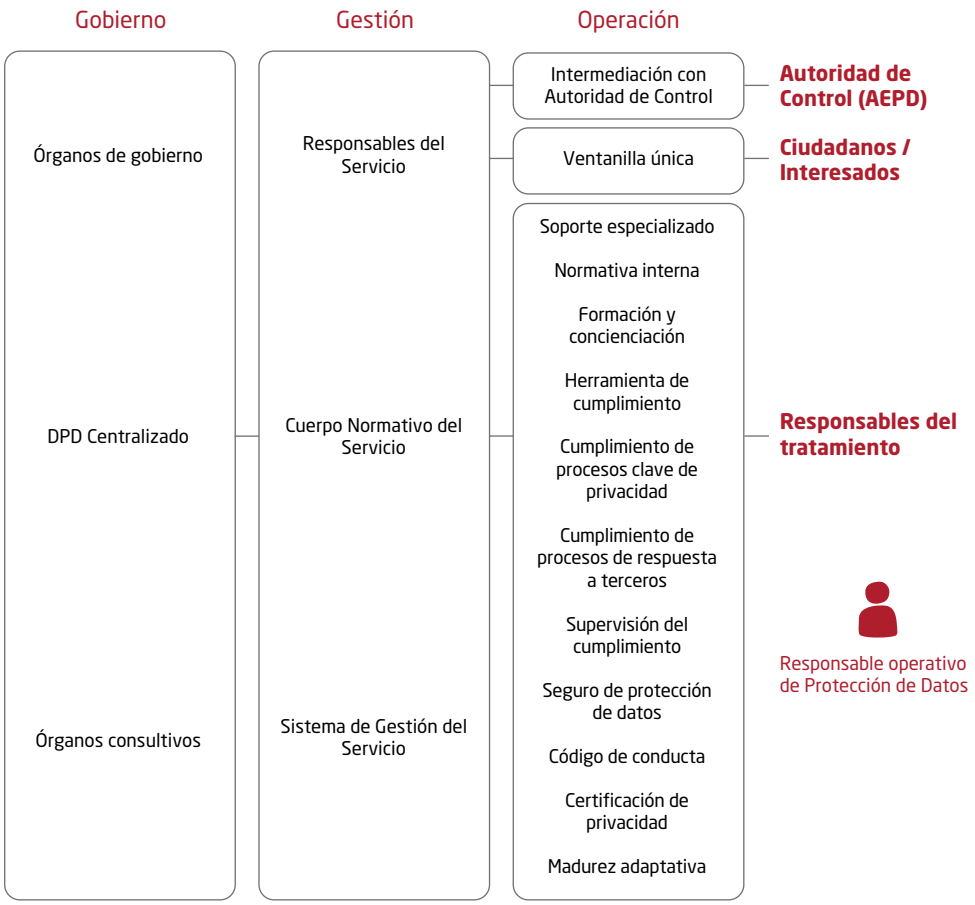
- **Garantías de privacidad homogéneas** por colectivos basadas en el establecimiento de criterios comunes por parte del servicio centralizado, que evitan en la mayor medida de lo posible respuestas dispares ante solicitudes idénticas.
- **Canales ágiles** de comunicación y resolución de dudas respecto de la privacidad de sus datos personales (ventanilla única, servicio especializado de resolución de consultas).
- Servicios ágiles de **intermediación** entre el DPD o servicio especializado y la AEPD, que reduzca los costes operativos para el ciudadano asociados a una reclamación.
- **Transparencia** de los elementos del modelo que tengan una especial relevancia sobre las garantías de privacidad de sus datos personales.

BENEFICIOS PARA LA AUTORIDAD DE CONTROL:

- Disponer de un **punto único de contacto** con todo el colectivo adherido.
- Disponer de un punto único para la **colaboración con la autoridad** de control en foros de trabajo o eventualmente para el lanzamiento de iniciativas conjuntas (formación, etc.). dirigidas a colectivos específicos a través de sus propios órganos de gobierno o asociaciones de las que participan directamente.
- **Reducción de costes** internos al reducir las reclamaciones directas ante la autoridad de control por disponer de elementos ágiles de mediación entre el ciudadano y el responsable del tratamiento.

Arquitectura del modelo de servicio

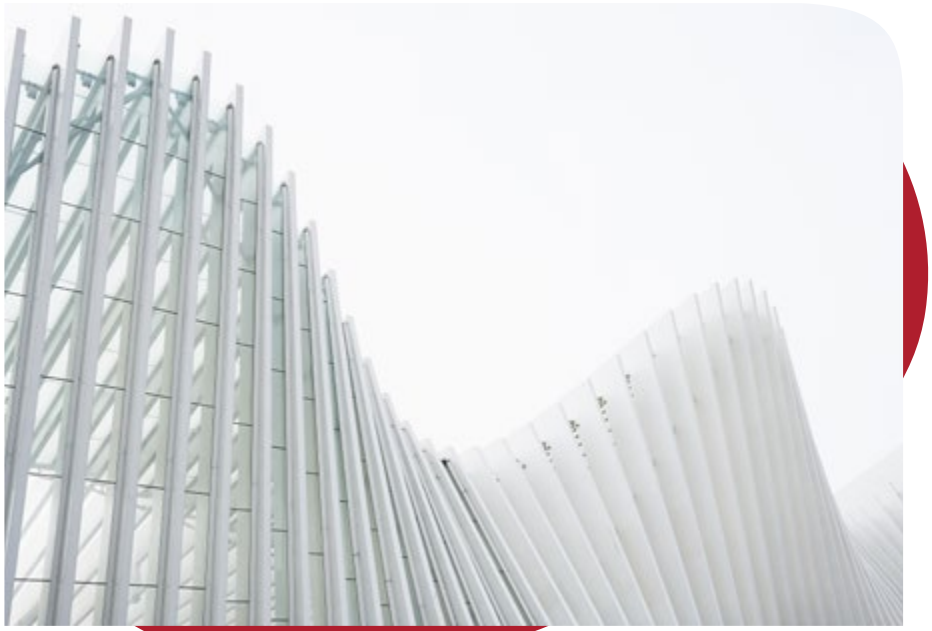
El modelo de Servicio centralizado se fundamenta en tres capas (Gobierno, Gestión y Operación), compuestas por una serie de elementos que se entrelazan e interactúan entre sí, con el objetivo común de **prestar un servicio ágil, robusto y eficiente**. Estos elementos se organizan a alto nivel a través de la siguiente arquitectura:



Para mejorar el despliegue y consumo del Servicio centralizado en los Responsables de Tratamiento, **se recomienda asignar en cada uno de ellos la figura de Responsable operativo de Protección de Datos**, cuyas funciones se detallarán en los apartados posteriores.

De forma general, todos los elementos del Servicio centralizado han sido diseñados en base a **buenas prácticas y con criterios de proactividad** en el cumplimiento por parte de los Responsables de Tratamiento que lo consumen, y poseen ciertas características de autogestión, uniformidad, escalabilidad, automatización y salvaguarda de los derechos de los interesados. Este diseño unido a la última capa de personalización realizadas por los Responsables de Tratamiento permite ofrecer un **servicio muy potente, escalable y perfectamente adaptado al colectivo objetivo**.

A continuación, se procederá a detallar cada uno de los elementos del modelo, y la propuesta de buenas prácticas asociadas.



Órganos de gobierno

Descripción y objetivo

Los **órganos de gobierno** cumplen una función primordial en el modelo de servicio, ya que son la base sobre la que asienta el Servicio centralizado, y los máximos responsables de **fomentar la cultura de privacidad, tomar las decisiones y alinear el servicio a los objetivos de los clientes** (Responsables de Tratamiento) e interesados (ej: ciudadanos).

Buena práctica

Se deberían confeccionar órganos internos que permitan realizar un adecuado **gobierno de la privacidad y la seguridad** en la organización que presta el Servicio centralizado, de cara a que los objetivos del Servicio se encuentren alineados con las necesidades de los Responsables de Tratamiento (RT), a la vez que permitan **garantizar los derechos y libertades** de los ciudadanos alcanzados. La definición de estos órganos se debería asentar sobre los siguientes requisitos:

- Formalizar los órganos ejecutivos, compuestos por perfiles de dirección, con capacidad de establecer los objetivos y estrategia del Servicio centralizado, dotar de los recursos necesarios para llevarlos a cabo, tomar decisiones acerca de cuestiones relevantes que afecten al Servicio o los RT en materia de privacidad y monitorizar periódicamente su estado.
- Formalizar los órganos operativos, compuestos por personal clave de las áreas relacionadas con la privacidad y la seguridad, con las capacidades técnicas necesarias para llevar a cabo las decisiones tomadas por los órganos ejecutivos, y servir de apoyo a los órganos ejecutivos en la resolución o análisis de las cuestiones que, por su especificidad, quedan fuera su alcance.
- Definir y aprobar formalmente las funciones de cada uno de los órganos, así como los mecanismos de interactuación entre ellos y el Servicio centralizado.
- Aprobar formalmente la composición de cada uno de los órganos, junto con los procedimientos de alta, baja o sustitución de miembros en cada órgano.
- Garantizar la independencia entre la organización prestadora y los órganos internos del Servicio centralizado, en el ejercicio de las funciones de DPD centralizado.
- Formalizar la periodicidad de las convocatorias ordinarias de cada uno de los órganos, junto con el procedimiento de convocatorias extraordinarias.
- Llevar a cabo activamente las convocatorias según la planificación estipulada.

Ejemplos de implantación

Los órganos de gobierno pueden diferir en función del tamaño y la naturaleza de la organización, pero como ejemplo de implantación se podrían plantear los siguientes:

- **Comité ejecutivo**, compuesto por un conjunto de miembros de alta dirección que representen a negocio, sistemas, legal y protección de datos, con las siguientes funciones (entre otras): aprobar el presupuesto y cuota del Servicio centralizado, aprobar el Cuerpo Normativo del Servicio, impulsar el Sistema de Gestión del Servicio, velar por el cumplimiento de los objetivos, tomar decisiones relevantes en el ámbito de notificación de brechas y aceptación de riesgos, revisar indicadores y el estado del Servicio, etc.
- **Comité técnico**, compuesto por los responsables de áreas técnicas, legal, recursos humanos, calidad, seguridad y protección de datos, con las siguientes funciones (entre otras): revisar los cuerpos normativos antes de su elevación al Comité ejecutivo, apoyar en la implantación y mantenimiento del Sistema de Gestión del Servicio, actuar en segunda instancia frente a desviaciones de los indicadores del servicio, facilitar la prestación del Servicio y el cumplimiento de plazos en el ámbito de sus responsabilidades, etc.

Guías, herramientas, enlaces, documentación

Guía de Seguridad de las TIC - Responsabilidades y Funciones (CCN)

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/501-ccn-stic-801-responsibilidades-y-funciones-en-el-ens/file.html

ISO/IEC 38500:2015 - Gobernanza corporativa de la Tecnología de la Información

https://www.iso.org/standard/62816.html

COBIT (ISACA)

https://www.isaca.org/resources/cobit

Delegado de Protección de Datos Centralizado

Descripción y objetivo

Existen Responsables de Tratamiento (RT) que, por su naturaleza, están obligados a designar un **Delegado de Protección de Datos** (DPD). En función del tamaño y tipo de organización, la contratación de un DPD puede suponer un coste proporcionalmente elevado. El objetivo de esta buena práctica se focaliza en **asegurar el cumplimiento de las funciones del DPD**, mediante procesos que optimizan su funcionamiento y los costes de llevarlo a cabo, a través de la centralización de su figura en el organismo que proporciona el Servicio centralizado.

Buena práctica

La normativa de protección de datos es clara respecto de las **funciones asociadas a la figura del DPD**, y además fija las condiciones e independencia necesaria para desempeñarlas. Debido a que la propia normativa permite la externalización de esta figura, el hacerlo en el organismo que presta el Servicio centralizado de protección **permite establecer numerosas sinergias que optimizan, economizan y facilitan el cumplimiento** de la normativa de protección de datos en los RT adheridos. Para llevar a cabo este planteamiento, se deberían tener en cuenta los siguientes requisitos:

- Plasmar las funciones a llevar a cabo por el DPD centralizado en un contrato entre el RT y organismo que presta el Servicio centralizado (también puede formar parte del contrato del Servicio).
- Formalizar los procesos de adhesión, firma y desestimación del contrato por los RT.
- Gestionar los procesos de comunicación del DPD (altas, bajas y modificaciones) a la Autoridad de Control a través del Servicio centralizado, estableciendo como vía de contacto la Ventanilla única.
- Cubrir las funciones asociadas al DPD centralizado mediante los diferentes elementos que forman parte del servicio prestado a los RT.
- Documentar, formalizar y aprobar por los máximos órganos de gobierno una normativa de independencia y conflicto de intereses, para garantizar que los intereses (en materia de privacidad) de los RT están salvaguardados frente a los intereses del organismo que gestiona el Servicio centralizado.
- Que, como recomendación, se designe una figura en los RT con funciones operativas de protección de datos, de forma complementaria o no a sus funciones normales de trabajo, con el objetivo de servir de enlace entre el RT y el Servicio centralizado, a la par de ser la figura referente dentro de su organización para la toma de decisiones operativas que impacten en la privacidad y la seguridad.

Ejemplos de implantación

Como ejemplo de implantación, los RT externalizarían mediante un contrato de encargado de tratamiento todas las funciones del DPD en el organismo que presta el Servicio centralizado. Desde el Servicio centralizado se cubrirían las funciones y responsabilidades asociadas al DPD, mediante el despliegue de los elementos necesarios que se describen en la Capa de Operación, junto con los elementos de la Capa de Gobierno y Capa de Gestión que permitan operar el Servicio con las garantías e independencia necesaria. Para facilitar el despliegue del Servicio centralizado y, por tanto, el cumplimiento de la normativa de protección de datos en los RT, se propondría a estos la asignación a alguien de su plantilla del siguiente rol: "Responsable operativo de Protección de Datos", con las funciones de contacto principal entre su organización y el servicio, estar formado en los diferentes elementos del servicio, tener nociones básicas de privacidad, coordinar la implantación de medidas a nivel interno, requerir su cumplimiento en los proveedores y servir de contacto operativo en caso de que el Servicio requiera contactar con el RT.

Guías, herramientas, enlaces, documentación

Guía para los DPDs en los sectores públicos y semi-públicos (AEPD)

https://www.aepd.es/sites/default/files/2019-12/El%20Manual%20del%20DPD%20-%20KORFFGEORGES%20-%20ESP.pdf

Directrices del Delegado de Protección de Datos (GT del Articulo 29, May 2018)

https://ec.europa.eu/newsroom/article29/items/612048/en

Guía rápida de comunicación del Delegado de Protección de Datos (AEPD)

https://www.aepd.es/sites/default/files/2019-12/guia-rapida-dpd.pdf

Órganos consultivos

Descripción y objetivo

La normativa de protección de datos debe ser aplicada por los Responsables de Tratamiento (RT), pero no debemos olvidar que esta normativa se ve afectada de forma complementaria (o suplementaria) por otras normativas o legislaciones sectoriales, regionales, estatales y europeas. Pese a que los expertos en protección de datos pueden realizar una primera adaptación de la normativa de protección de datos a la realidad de los RT, a lo largo del ciclo de vida de los tratamientos se requerirá de **órganos consultivos que sean capaces de resolver conflictos entre varias normativas, o bien resolver dudas** a la hora de realizar ciertas operativas que cumplan todas las normativas y legislación aplicables.

Buena práctica

Como buena práctica en este aspecto, se deberían cumplir los siguientes requisitos:

- Reflejar en su composición los perfiles necesarios para adaptar con éxito la normativa de protección de datos a la realidad de los RT y contar, como mínimo, con: expertos en la operativa de los RT, expertos en protección de datos y expertos en la legislación ajena a protección de datos aplicable.
- Definir y aprobar formalmente las funciones de cada uno de los órganos, así como los mecanismos de interacción entre ellos y el Servicio centralizado.
- Aprobar formalmente la composición de cada uno de los órganos, junto con los procedimientos de alta, baja o sustitución de miembros en cada órgano.
- Formalizar la periodicidad de las convocatorias ordinarias de cada uno de los órganos, junto con el procedimiento de convocatorias extraordinarias.
- Llevar a cabo activamente las convocatorias según la planificación estipulada.
- Implicar a los órganos consultivos en iniciativas relevantes de protección de datos que afecten a la operativa de los RT.

Ejemplos de implantación

Los órganos consultivos pueden diferir en función de los sectores cubiertos por el Servicio centralizado, pero como ejemplo sencillo de implantación se podría plantear el siguiente órgano:

- **Comité mixto de protección de datos**, compuesto por un conjunto de Responsables de Tratamiento expertos en operativas de negocio, asesores legales expertos en normativa sectorial y territorial, conjunto de Responsables del Servicio centralizado en su calidad de expertos en seguridad y protección de datos. Este órgano tendría las siguientes funciones (entre otras): revisión y mejora de la Normativa Interna de aplicación a los RT, resolución de conflictos normativos, resolución de dudas no cubiertas por la normativa interna, revisión y propuesta de actividades de supervisión, colaboración en iniciativas y campañas a desplegar en los RT, etc.

Guías, herramientas, enlaces, documentación

COBIT (ISACA)

https://www.isaca.org/resources/cobit

Responsables del servicio

Descripción y objetivo

Para dar cobertura a las funciones y obligaciones del Servicio centralizado, se debería **disponer de una estructura organizativa interna formada por personal cualificado** que dé respuesta a todos los elementos desplegados, y que esta estructura se encuentre especialmente **diseñada y dimensionada para cubrir la demanda del propio servicio**, utilizando criterios que permitan optimizar esfuerzos y escalar recursos.

Buena práctica

Como en cualquier otro servicio, **una de las piezas clave de éxito es el personal** que lo conforma. En orden a que el Servicio centralizado se preste en las condiciones acordadas, se deberían tener en cuenta los siguientes requisitos:

- Contar con perfiles cualificados y formados en todos los elementos del Servicio centralizado, y que como mínimo cubran adecuadamente los principales aspectos técnicos y legales, junto con los perfiles de gestión para mantener el servicio.
- Contar con que el personal responsable ostente certificaciones adecuadas a las tareas desempeñadas, con especial recomendación de contar con algún perfil certificado según el esquema de DPD.
- Dimensionar adecuadamente el personal, atendiendo al número de Responsables de Tratamiento que consumen el Servicio y a los indicadores de la demanda.

Ejemplos de implantación

La composición del servicio se encuentra íntimamente ligada a los elementos que lo conforman, pero como mínimo se podrían plantear contar con los siguientes perfiles:

- **Director del servicio**: Persona con formación en protección de datos y experiencia en gestión y dirección de equipos, con las funciones de garantizar que los objetivos fijados por los órganos de gobierno se cumplen, gestionar el equipo, presupuesto y los problemas del día a día en el servicio, así como elevar a los órganos correspondientes las cuestiones que no se puedan resolver a su nivel.
- **Responsable legal de cumplimiento**: Persona con estudios de derecho y formación experta en protección de datos (deseable certificación DPD), con las funciones de asesoramiento experto en protección de datos, elaboración de normativas, resolución de cuestiones complejas de protección de datos, etc.
- **Responsable de gestión de riesgos**: Persona con estudios técnicos y formación en privacidad y seguridad (deseable certificación CISM, CRISC o similar), con las funciones de asesoramiento técnico en seguridad y privacidad, análisis y gestión de riesgos, EIPD, marcos de control, etc.
- **Responsable de supervisión del cumplimiento**: Persona con formación en protección de datos y seguridad (deseable certificación CISA o similar), con las funciones de realizar las actividades de supervisión y verificación del cumplimiento, revisión de evidencias, coordinación de auditorías, etc.).
- **Responsable de Soporte (atención al cliente)**: Persona con formación en protección de datos (deseable certificación ITIL o similar), con las funciones de coordinación y supervisión del equipo de Soporte Especializado a Responsables de Tratamiento, gestión de la demanda, coordinación del lanzamiento de campañas, etc.
- **Equipo de Soporte**: En función de los niveles de Soporte establecidos, personal cualificado de atención telefónica y *backoffice*, dimensionado acorde a la gestión de la demanda.
- **Personal de apoyo**: En función de la gestión de la demanda y la carga de trabajo, personal de apoyo a los responsables anteriores y a la gestión del servicio.

Guías, herramientas, enlaces, documentación

Guía de Seguridad de las TIC - Responsabilidades y Funciones (CCN)

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/501-ccn-stic-801-responsibilidades-y-funciones-en-el-ens/file.html

ISO/IEC 38500:2015 - Gobernanza corporativa de la Tecnología de la Información

https://www.iso.org/standard/62816.html

COBIT (ISACA)

https://www.isaca.org/resources/cobit

ISO/IEC 27701:2019 – Extensión de la ISO/IEC 27001 y de la ISO /IEC 27002 para la gestión de la privacidad de la información

https://www.iso.org/standard/71670.html

ISO/IEC 27001:2013 – Sistemas de Gestión de Seguridad de la Información

https://www.iso.org/isoiec-27001-information-security.html

Esquema de certificación AEPD-DPD

https://www.aepd.es/sites/default/files/2020-07/esquema-aepd-dpd.pdf

Cuerpo normativo del servicio

Descripción y objetivo

Como parte de cualquier Servicio, **los procesos y procedimientos que lo rigen deben encontrarse documentados, formalizados y actualizados**. El objetivo de este elemento es el de disponer de una estructura de documentos que permita establecer las directrices para la gestión de los procesos normalizados que forman parte del Servicio, los procedimientos de obligado cumplimiento interno y las evidencias que demuestren la efectividad de los mismos en procesos de supervisión interna y externa.

Buena práctica

Un elemento imprescindible a la hora de diseñar, poner en marcha y mantener el Servicio, es el de plasmar documentalmente la forma de proceder para prestarlo. Para ello, se deberían tener en cuenta los siguientes requisitos:

- Definir la estructura del Cuerpo Normativo, alineándolo en su caso a los procesos de gestión documental existentes en la organización.
- Documentar todas las políticas, normativas, procedimientos, instrucciones, manuales, etc. necesarios para el adecuado funcionamiento del Servicio.
- Aprobar el Cuerpo Normativo del Servicio por los órganos de gobierno, y distribuir a todo el personal afectado.
- Revisar, actualizar y publicar periódicamente el Cuerpo Normativo, incorporando las mejoras y correcciones necesarias.
- Realizar formaciones periódicas sobre el Cuerpo Normativo al personal afectado.

Ejemplos de implantación

Como ejemplo de implantación, se podría elaborar un Cuerpo Normativo con la siguiente estructura:

- **Política**: Documento de nivel estratégico en el que se incluyen las directrices emitidas por la legislación y normativa vigente, así como los objetivos establecidos por los órganos de gobierno.
- **Normativas**: Documentos de nivel táctico en el que se establecen las normas que definen las pautas genéricas a seguir dentro del Servicio por el personal que lo conforma, atendiendo a los objetivos marcados.
- **Procedimientos**: Documentos de nivel operativo, en el que se desarrollan los procedimientos e instrucciones técnicas, detallándose las actividades a realizar para gestionar cada uno de los elementos del Servicio centralizado.

Estos documentos, elaborados por los diferentes Responsables del Servicio, conformarían el Cuerpo Normativo del Servicio, que sería elevado a los diferentes comités de gobierno para su aprobación. Una vez aprobado se difundiría y publicaría en un repositorio interno a disposición del personal del Servicio. De forma anual, cada Responsable debería revisar los documentos elaborados a fin de aplicar mejoras y correcciones, que serían nuevamente elevadas para su aprobación, difusión y posterior publicación.

Guías, herramientas, enlaces, documentación

ISO/IEC 27701:2019 – Extensión de la ISO/IEC 27001 y de la ISO /IEC 27002 para la gestión de la privacidad de la información

https://www.iso.org/standard/71670.html

ISO/IEC 27001:2013 – Sistemas de Gestión de Seguridad de la Información

https://www.iso.org/isoiec-27001-information-security.html

ISO/IEC 20000-1:2018 - Requisitos del Sistema de Gestión de Servicios (SGS)

https://www.iso.org/standard/70636.html

Sistema de gestión del servicio

Descripción y objetivo

El Servicio centralizado **debería operar siempre al máximo nivel de calidad, efectividad y eficiencia**, Para ello, es necesario establecer las fases, modelo y requerimientos mínimos a las que debe atender el sistema de gestión del Servicio en los procesos de **mejora continua** internos, tomando como referencia las buenas prácticas y estándares internacionales del sector.

Buena práctica

Para una adecuada gestión del servicio, no es suficiente contar con personal capacitado y normativa formalizada, ya que **debe mantenerse a través de todo el ciclo de mejora continua**. Para implantar y mantener un Sistema de Gestión, se deberían tener en cuenta los siguientes requisitos:

- Analizar los estándares de sistemas de gestión más adecuados a implementar, de cara a tener en cuenta los requisitos necesarios.
- Definir el alcance y objetivos cubiertos por el Sistema de Gestión.
- Diseñar e implementar los elementos de las Capas de Gobierno, Gestión y Operación para que se alineen con los requisitos del Sistema de Gestión.
- Contar con la colaboración y el compromiso de la alta dirección, Órganos de Gobierno y todas las áreas implicadas por el Sistema de Gestión.
- Obtener la certificación del Sistema de Gestión, bajo los estándares seleccionados, por organismos acreditados.

Ejemplos de implantación

De cara a la implantación de un Sistema de Gestión, se deberían considerar estándares como ISO 9001 de calidad, ISO 27001 de seguridad, ISO 27701 de privacidad y/o ISO 20000 de calidad de los servicios, ya que todos ellos cubren las fases más comunes del ciclo de vida del servicio (ciclo de Deming o PDCA):

- **Planificar (*Plan*)**: Esta fase busca asegurar el compromiso de la Dirección en la implantación y desarrollo del Sistema de Gestión, y dotar de los medios y del personal que conformará el mismo, una vez identificado su alcance y recopilada la documentación necesaria. En esta fase se establece la política, objetivos, procesos y procedimientos pertinentes a la gestión de riesgos y los procedimientos que permitan obtener resultados de acuerdo con las políticas y objetivos generales de la organización.
- **Implementar (*Do*)**: Implementar y operar la política, controles, procesos y procedimientos del Sistema de Gestión.
- **Medir (*Check*)**: Evaluar y, donde sea aplicable, medir el rendimiento del proceso contra la política, sus objetivos y líneas de referencia, e informar de los resultados.
- **Mejorar (*Act*)**: Tomar acciones correctivas y preventivas basadas en los resultados de indicadores, auditorías, u otra información relevante, para lograr la mejora continua del Servicio.

Guías, herramientas, enlaces, documentación

ISO/IEC 27701:2019 – Extensión de la ISO/IEC 27001 y de la ISO /IEC 27002 para la gestión de la privacidad de la información

https://www.iso.org/standard/71670.html

ISO/IEC 27001:2013 – Sistemas de Gestión de Seguridad de la Información

https://www.iso.org/isoiec-27001-information-security.html

ISO/IEC 20000-1:2018 - Requisitos del Sistema de Gestión de Servicios (SGS)

https://www.iso.org/standard/70636.html

ISO/IEC 9001:2015 - Sistemas de gestión de la calidad

https://www.iso.org/standard/62085.html

Normativa interna de protección de datos

Descripción y objetivo

La normativa interna de protección de datos permite a los Responsables de Tratamiento (RT) disponer del **soporte documental y procedimental necesario para un adecuado cumplimiento de la normativa de protección de datos**. El objetivo de esta normativa interna es servir de referencia para que los RT puedan implantar los procesos propios de privacidad y seguridad derivados, así como cubrir que todos los procesos de negocio que traten datos de carácter personal estén convenientemente **adaptados a la normativa de protección de datos**, respetando la legislación sectorial que le aplique al RT.

Buena práctica

La normativa interna de protección de datos es y debe ser el **pilar bajo el cual se vertebra el cumplimiento de privacidad** en la organización del RT. Adicionalmente, debería ser la principal referencia para Soporte Especializado, por lo que cuanto más completa sea ésta, más eficiente será la resolución de consultas. Esta normativa, para que sea útil, completa y efectiva, debería cumplir los siguientes requisitos:

- Contemplar todos los requisitos que apliquen en el ámbito de protección de datos: Normativa europea, normativa estatal y local; dictámenes y guías de las autoridades de control, etc.
- Contemplar todos los requisitos que apliquen en el ámbito sectorial de la organización: legislación específica europea, estatal y local; dictámenes y guías de los organismos superiores, etc.
- Asegurar que sea común y homogénea a cada tipología de organización a la que le afecte las mismas normativas de protección de datos y sectoriales.
- Adaptar los preceptos normativos de protección de datos a la realidad de la organización del RT, de tal forma que permita a la organización cumplir con la normativa de protección en la operativa diaria.
- Aprobar la normativa interna por los Órganos de Gobierno y Órganos Consultivos, con el aval de los comités técnicos involucrados.
- Asegurar que, una vez distribuida a las organizaciones, sea avalada y difundida por el RT, quedando fácilmente accesible para todo el personal implicado.
- Revisar y mejorar regularmente la normativa para actualizar el contenido en base a las novedades normativas, aclaración de interpretaciones, criterios de cumplimiento, resolución de conflictos entre normativa de protección de datos y normativa sectorial, etc.

Ejemplos de implantación

Supongamos que el organismo centralizado presta soporte a tres tipologías de entidades diferentes, es decir, por ejemplo, entidades de tres tipos a las que a cada una le aplica legislación sectorial diferente. En este caso, podría generar una normativa interna con la parte común que afecte a todos los tipos y una parte específica para cada tipo, donde se particularizara la adaptación de la normativa sectorial correspondiente a la normativa de protección de datos (si es que la normativa sectorial afecta en este sentido).

Cada una de las normativas específicas puede enriquecerse con casos resueltos que afecten a cada tipología, con el visto bueno de los Órganos Consultivos en caso de conflicto normativo.

El soporte normativo debería intentar adecuarse a los procesos de gestión documental de las entidades (todo concentrado en un solo documento, dividido en varios documentos, estructura en árbol, solo soporte web, etc.), si bien el objetivo principal es que se garantice que la normativa que queda accesible a los usuarios esté siempre actualizada, aprobada por los órganos de gobierno y avalada por los Responsables de los Tratamientos.

Guías, herramientas, enlaces, documentación

Decálogo de recursos (AEPD)

https://www.aepd.es/es/guias-y-herramientas/guias/decalogo-de-recursos-de-ayuda

Informes y dictámenes de la (AEPD)

https://www.aepd.es/es/informes-y-resoluciones/informes-juridicos

https://www.aepd.es/es/informes-y-resoluciones/normativa-y-circulares

Informes y dictámenes de la Comisión Europea (CEPD)

https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_es

Guías específicas de la AEPD (AEPD)

https://www.aepd.es/es/guias-y-herramientas/guias

Ventanilla única

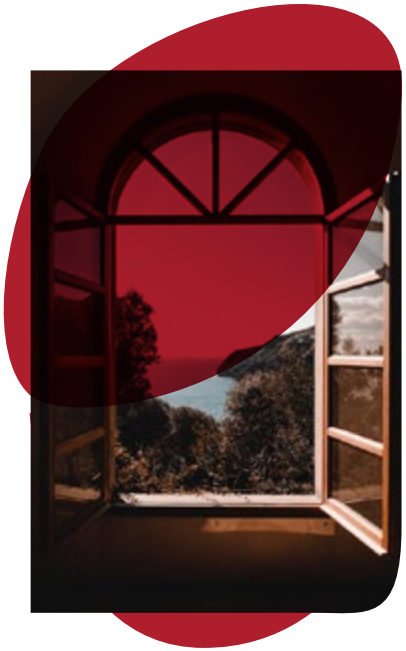
Descripción y objetivo

La ventanilla única se establece como el mecanismo unificado de entrada que permite establecer los **canales de comunicación centralizados** a disposición de los ciudadanos y otros interesados para contactar con el Delegado de Protección de Datos centralizado o con los Responsables del Tratamiento (RT) de las organizaciones adheridas al servicio. A nivel interno, se deberán gestionar, coordinar y encaminar las solicitudes y consultas de los interesados que se reciban a través de esta ventanilla **para la salvaguarda de los derechos y libertades** respecto de sus datos de carácter personal.

Buena práctica

La ventanilla única **permite unificar la entrada** de las comunicaciones dirigidas a las entidades bajo el servicio centralizado a través de un mismo mecanismo, lo que permite gestionar las solicitudes de principio a fin, **optimizando el proceso de atención y garantizando que las solicitudes se atienden en tiempo y forma**. Para ello, la ventanilla única debería cumplir los siguientes requisitos:

- Disponer de los principales canales de comunicación: teléfono, email, web, dirección postal, fax, etc.
- Publicar los canales y ponerlos a disposición del público objetivo.
- Cubrir todos o los principales idiomas utilizados por los usuarios, interesados y terceras empresas / organismos que puedan realizar solicitudes, consultas o reclamaciones a las organizaciones adheridas al Servicio.
- Utilizar herramientas automatizadas que permitan realizar un registro de la petición, redireccionarlas internamente a los destinatarios, alertar de los plazos y realizar seguimiento de la misma hasta que se tramite y envíe la respuesta.



Ejemplos de implantación

Un ejemplo de ventanilla única podría ser la creación de un teléfono y email específicos para gestionar todas las cuestiones de protección de datos de todas las entidades bajo el Servicio centralizado. Este teléfono y email podrían ser publicitados tanto desde el organismo centralizado como por los RT adheridos a través de sus respectivas Web, folletos, tablones de anuncios, etc.

Mediante su publicación, cualquier ciudadano, cliente o interesado que, en el ámbito de la protección de datos, necesite realizar alguna solicitud, consulta, reclamación, ejercicio de derechos, notificación de brecha, etc. ante cualquier entidad, utilizaría esta ventanilla. Si se permite, también se podría utilizar ante la autoridad de control, de cara a facilitar la interacción con la misma y centralizar sus requerimientos.

Los canales podrían ser atendidos y gestionados por el Servicio centralizado a través de personal de Soporte Especializado, con la ayuda de una herramienta automática de ticketing, donde se registrarían las peticiones y se encaminarían bien a los gestores especializados, bien a las respectivas entidades para que se proporcione respuesta. En caso de que la petición conlleve plazos (ejercicio de derechos, notificación de brecha, consulta de la autoridad de control), el Servicio centralizado debe garantizar que se cumplen, mediante avisos y un adecuado seguimiento.

Guías, herramientas, enlaces, documentación

ISO/IEC 20000-1:2018 - Requisitos del Sistema de Gestión de Servicios (SGS)

https://www.iso.org/standard/70636.html

ISO/IEC 9001:2015 - Sistemas de gestión de la calidad:

https://www.iso.org/standard/62085.html

Intermediación con la autoridad de control

Descripción y objetivo

El objetivo de este elemento es conferir al Servicio centralizado (en sus funciones derivadas por el DPD centralizado) de la capacidad de **intermediar con la Autoridad de Control** (AC) en nombre de los Responsables de Tratamiento (RT) para todas las cuestiones establecidas o no por vía normativa (reclamaciones, brechas, quejas, propuestas, consultas, etc.), garantizando el cumplimiento de plazos en aquellas que lo requieran.

Buena práctica

En determinadas circunstancias, **debe existir comunicación entre la Autoridad de Control y los Responsables de Tratamiento y viceversa**. Como parte de las funciones del Servicio centralizado, se podrían establecer labores de intermediación con la Autoridad de Control, lo cual optimizaría ciertos procesos y permitiría **garantizar el ejercicio de las competencias** de ambas partes. Para ello, sería necesario tener en cuenta los siguientes requisitos:

- Establecer formalmente el canal de comunicación que utilizará la Autoridad de Control para contactar con el DPD centralizado y los Responsables de Tratamiento, alineándolo si es posible con la Ventanilla Única.
- Definir las gestiones que se atenderán provenientes de la Autoridad de Control, previa autorización de los Órganos de Gobierno, implantando los procesos que soporten y garanticen el cumplimiento de los plazos establecidos.
- Fijar los mecanismos de interacción entre Servicio centralizado y RTs con la Autoridad de Control.

Ejemplos de implantación

La implantación de esta práctica podría regularizarse a través del contrato entre el Servicio centralizado y los RT, a través del cual se daría la capacidad al Servicio para intermediar con la Autoridad de Control en las siguientes gestiones:

- **Provenientes de la Autoridad de Control**: Registrar la dirección de la Ventanilla Única como dirección del DPD, de cara a que las notificaciones de la AC se canalicen a través del Servicio centralizado. Gestionar y canalizar las reclamaciones y requerimientos recibidos por la AC, garantizando los plazos. Coordinar, canalizar y gestionar los procesos de inspección y sanción a instancias de la AC.
- **Provenientes del Servicio o los RT**: Lanzar las consultas previas en caso de riesgo alto resultante del EIPD; notificar brechas de datos personales; presentar quejas, sugerencias, reclamaciones, preguntas parlamentarias, etc.; establecer convenios o acuerdos de colaboración entre el sector de los RT y la AC, etc.

Guías, herramientas, enlaces, documentación

Canal para la declaración, modificación o baja de los DPDs nombrados por las entidades (AEPD)

https://sedeagpd.gob.es/sede-electronica-web/vistas/formDelegadoProteccionDatos/procedimientoDelegadoProteccion.jsf

Canal de consulta de los DPDs ya declarados por las entidades (AEPD)

https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/consultaDPD.jsf

Canal del DPD (AEPD)

https://www.aepd.es/es/guias-y-herramientas/herramientas/canalDPD

Comunica-Brecha RGPD (AEPD)

https://www.aepd.es/es/guias-y-herramientas/herramientas/comunica-brecha-rgpd

Canal de prioritario de denuncia en caso de conocimiento de la publicación de fotografías, vídeos o audios de contenido sexual o violento en Internet sin el consentimiento de las personas afectadas (AEPD)

https://www.aepd.es/canalprioritario/

Soporte especializado

Descripción y objetivo

El equipo de soporte se debería componer de un grupo de personas con conocimientos específicos de protección de datos, que **permita dar respuestas o realizar los escalados oportunos** en tiempo real y en horario laboral a consultas, peticiones, reclamaciones, etc. que puedan llegar desde cualquier origen (ciudadanos, interesados, entidades bajo el servicio, autoridades de control u otros organismos) y canal (teléfono, web, email, etc.).

Buena práctica

El equipo de soporte **es uno de los elementos clave del modelo**, debido a que es el punto de contacto principal entre el Servicio centralizado y las entidades del Responsable de Tratamiento (RT) a las que se presta el servicio. Adicionalmente, de cara a optimizar los procesos, este equipo de soporte también podría desempeñar las labores de atención y gestión de la Ventanilla Única. Para configurar el Soporte especializado de forma óptima y eficaz, se deberían tener en cuenta los siguientes requisitos:

- Realizar el soporte a través de varios canales (teléfono, email, Web, etc.).
- Estratificar el equipo en varios niveles de soporte o escalado, desde el más básico y menos capacitado hasta el más avanzado y capacitado.
- Dimensionar adecuadamente cada nivel de soporte, atendiendo a indicadores de gestión de la demanda.
- Capacitar al personal en materia de protección de datos de forma adecuada y proporcional al nivel de soporte en el que se encuentre.
- Automatizar todo lo posible, a través de herramientas y procedimientos.
- Establecer y formalizar acuerdos de niveles de servicio (SLA) con tiempos de respuesta en función del tipo de peticiones o incidencias.

Ejemplos de implantación

Como ejemplo de implementación de este elemento, el equipo de soporte se podría organizar según los siguientes criterios:

- **Nivel 1**: Personal con formación básica en protección de datos, con las siguientes funciones:

  - Atención de ciudadanos e interesados a través de la ventanilla única (teléfono, email, web, dirección postal): Filtrado de peticiones de protección de datos respecto de las que no lo son. Registro de peticiones. Respuestas predefinidas de las peticiones más comunes. Solicitud de información adicional en caso de derechos, violaciones, etc. Redirección de peticiones a RT o Nivel 2 en caso requerido.

- **Nivel 2:** Personal especializado en protección de datos y en la Normativa Interna de los RT, con las siguientes funciones:

  - Atención de ciudadanos e interesados a través de la ventanilla única (derivados de Nivel 0): Ejecución de procedimientos predefinidos relacionados con ciudadanos e interesados. Redirección de peticiones a RT o Nivel 3 en caso requerido.

  - Atención a Responsables de Tratamiento (teléfono, email, web): Registro de peticiones. Resolución de dudas sobre protección de datos, operativa, normativa interna o cualquier otro elemento del servicio de protección de datos. Respuestas predefinidas a las peticiones / consultas más comunes. Solicitud de información adicional en caso de derechos, violaciones, etc. Redirección de peticiones a Nivel 3 en caso requerido. Realización de campañas de protección de datos a los RT.

- **Nivel 3**: Responsables de Servicio, con las funciones de ejecución de procedimientos complejos, resolución de problemas en la ejecución de procedimientos, resolución de dudas no documentadas, resolución de conflictos normativos junto con los órganos consultivos, diseño de campañas, etc.

Guías, herramientas, enlaces, documentación

ISO/IEC 20000-1:2018 - Requisitos del Sistema de Gestión de Servicios (SGS)

https://www.iso.org/standard/70636.html

ISO/IEC 9001:2015 - Sistemas de gestión de la calidad:

https://www.iso.org/standard/62085.html

Formación y concienciación

Descripción y objetivo

El objetivo de este elemento es el de poner a disposición de los Responsables de Tratamiento (RT) los **recursos necesarios** para la formación y concienciación en materia de protección de datos de su personal, a través de **herramientas y planes adaptados a sus funciones**.

Buena práctica

Uno de los pilares fundamentales para fomentar la **cultura de protección de datos**, son las acciones destinadas a la formación y concienciación del personal especializado y el resto del personal bajo el mando del RT. Las actividades de formación y concienciación deberían organizarse a través de un **plan** que tenga en cuenta, al menos, los siguientes requisitos:

- Identificar las necesidades y objetivos de formación en consonancia con los objetivos estratégicos perseguidos, tanto aquellas necesidades reactivas (que cubren problemas o deficiencias detectadas) como aquellas proactivas (que cubren futuras novedades o avances conocidos).
- Identificar los distintos colectivos que van a recibir la formación / concienciación, de cara a lanzar actividades segmentadas en función de las necesidades de cada colectivo.
- Seleccionar las actividades más adecuadas a cada colectivo para cumplir los objetivos, teniendo en cuenta para el diseño de las actividades, entre otras, las siguientes cuestiones: herramienta o formato más adecuado, modalidad presencial / online, duración, periodicidad, lugar de impartición, etc.
- Utilizar mecanismos de motivación o recompensa por parte del RT para que su personal realice la formación de forma continuada.

Ejemplos de implantación

Se podría elaborar un plan de formación y concienciación tomando como ejemplo los siguientes perfiles (colectivos) existentes en los RT:

- **Responsable de Tratamiento:**

  - Curso ejecutivo de protección de datos, focalizado en los puntos clave de la normativa, los riesgos a tener en cuenta y todo lo que el Servicio centralizado de Protección de Datos pone a su disposición.

- **Responsable de Seguridad:**

  - Curso focalizado en las medidas de seguridad a cumplir derivadas del cumplimiento de Protección de Datos.

- **Responsable en funciones de Protección de Datos:**

  - Itinerario formativo sobre todas las materias de protección de datos que les afectan.

  - Envío de píldoras con novedades que afecten al cumplimiento de protección de datos.

- **Responsables de negocio, proyectos y TI**

  -Curso focalizado en procesos clave de análisis de riesgos, privacidad desde el diseño y privacidad por defecto.

- **Resto de la plantilla**

  - Curso básico de protección de datos adaptado a su operativa.

  - Decálogo de buenas prácticas en privacidad.

  - Envío de píldoras periódicas sobre operativas diarias bien ejecutadas desde la perspectiva de protección de datos.

Guías, herramientas, enlaces, documentación

ISO/IEC 27701:2019 – Extensión de la ISO/IEC 27001 y de la ISO /IEC 27002 para la gestión de la privacidad de la información [Punto 6.4.2.2]

https://www.iso.org/standard/71670.html

ISO/IEC 27001:2013 – Sistemas de Gestión de Seguridad de la Información [Punto 7.2]

https://www.iso.org/isoiec-27001-information-security.html

Herramientas Ángeles (CCNCert)

https://angeles.ccn-cert.cni.es/index.php/es/

Infografías de concienciación de la AEPD

https://www.aepd.es/es/guias-y-herramientas/infografias

Kit de Concienciación de INCIBE

https://www.incibe.es/protege-tu-empresa/kit-concienciacion

Plataforma de Formación de INCIBE

https://www.incibe.es/protege-tu-empresa/formacion

Herramienta de cumplimiento

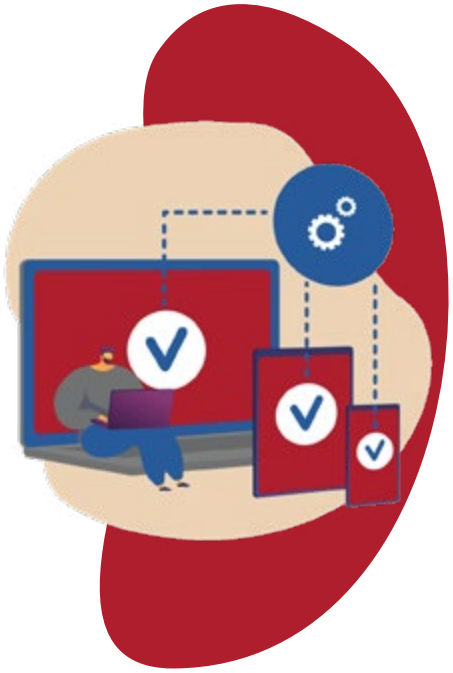
Descripción y objetivo

Al margen del soporte prestado por el Servicio centralizado, los Responsables del Tratamiento (RT) **deben ser capaces de gestionar la privacidad adecuadamente en el día a día**. Para ello, se hace indispensable poder contar con una herramienta que cubra adecuadamente todas las tareas que los RT deben llevar a cabo como parte de sus responsabilidades.

Buena práctica

Los Responsables de Tratamiento, como parte de su operativa, deben realizar gestiones derivadas de la normativa de protección de datos. **Para desempeñar esta labor de forma ágil y eficiente**, deberían contar con una herramienta que facilite su cumplimiento. La herramienta de cumplimiento de protección de datos debería tener en cuenta los siguientes requisitos:

- Ser multiplataforma y de fácil uso.
- Facilitar el cumplimiento de las funciones requeridas por la normativa de protección de datos y su seguimiento.
- Asegurar el mantenimiento actualizado con nuevas funciones o novedades derivadas de la normativa de protección de datos y los dictámenes, guías y recomendaciones de la autoridad de control.
- Alinear su estructura y funcionamiento con las funciones cubiertas por el Servicio centralizado.
- Alinear su contenido y funciones con el resto de elementos del modelo de servicio (normativa interna de protección de datos, procesos clave, procesos de respuesta, supervisión del cumplimiento, etc.).



Ejemplos de implantación

Como ejemplo de esta buena práctica, se podría desarrollar una herramienta de cumplimiento en formato SAAS (*Software As A Service*), de tal forma que estuviera disponible vía Web para todos los Responsables de Tratamiento (cada uno con su información) a través del navegador. Como parte de las funcionalidades a implementar, que facilitan la gestión de la privacidad, podrían ser:

- Inventario de los activos (personal, equipos, servidores, sistemas, aplicaciones, proveedores, soportes, locales, etc.) y registro de autorizaciones de su uso por parte del personal.
- Gestión de los Procesos Clave (Registro de Actividades de Tratamiento, Análisis de Riesgos y EIPDs, privacidad desde el diseño y por defecto), sobre los propuestos por defecto desde el Servicio centralizado.
- Gestión y registro de los Procesos de Respuesta (ejercicio de derechos, violaciones de seguridad, reclamaciones de la Autoridad de Control), en colaboración con el Servicio centralizado.
- Gestión de los procesos de Supervisión del Cumplimiento (auditorías, verificaciones, revisiones internas), junto con el almacenamiento de evidencias derivadas.
- Repositorio documental, donde gestionar, actualizar y publicar el material relativo a protección de datos (Normativa Interna, casos resueltos, preguntas frecuentes, cláusulas, plantillas, modelos, contratos, etc.).
- Cuadro de mandos e indicadores de cumplimiento.
- Plataforma de comunicación entre Servicio centralizado y Responsables de Tratamiento, para comunicar novedades, lanzamientos, avisos, etc. y viceversa, para comunicar dudas, sugerencias, incidencias, etc.

Guías, herramientas, enlaces, documentación

Facilita RGPD (AEPD)

https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd

Facilita EMPRENDE (AEPD)

https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-emprende

Gestiona EIPD (AEPD)

https://www.aepd.es/es/guias-y-herramientas/herramientas/gestiona-eipd

Aplicación para las EIPD (APDCAT)

https://apdcat.gencat.cat/es/documentacio/programari/aipd-programari/

Evalúa-Riesgo RGPD (AEPD)

https://www.aepd.es/es/guias-y-herramientas/herramientas/evalua-riesgo-rgpd

Comunica-Brecha RGPD (AEPD)

https://www.aepd.es/es/guias-y-herramientas/herramientas/comunica-brecha-rgpd

Cumplimiento de procesos clave de privacidad

Descripción y objetivo

La normativa de protección de datos **obliga a realizar ciertos procesos que pueden ser costosos** de implantar y mantener, como son los de Privacidad por defecto (PpD) y desde el diseño (PdD), análisis de riesgos (AARR) y evaluaciones de impacto (EIPD) o el registro de actividades de tratamiento (RAT). El objetivo del Servicio centralizado sería **optimizar esfuerzos** sobre los elementos comunes de los Responsables de Tratamiento (RT), con el fin de que estos minimicen los esfuerzos requeridos para su implantación.

Buena práctica

Teniendo en cuenta que una de las premisas iniciales es que el Servicio centralizado presta soporte a Responsables de Tratamiento con características similares o del mismo del sector, es de esperar que **compartan similitudes** en los tratamientos y operativa realizada. Partiendo de esa base, desde el Servicio centralizado se debería realizar el trabajo de **estandarizar la parte común de los procesos clave de privacidad mencionados, de tal forma que sea utilizable por defecto por la gran mayoría de los RT**, lo cual les facilitaría en gran medida su labor. Como parte de este trabajo de estandarización y cumplimiento de los procesos clave de privacidad, se deberían tener en cuenta los siguientes requisitos:

- Analizar todos los factores que existen en común en los RT, que afecten a los procesos clave.
- Analizar aquellos factores específicos que podrían variar entre diferentes RT.
- Diseñar soluciones estandarizadas, basadas en los factores comunes, válidas para todos o la gran parte de RTs.
- Elaborar procedimientos (e incluirlos en la normativa interna) que indiquen al RT como utilizar y complementar las soluciones estandarizadas en su organización.
- Diseñar, implementar y poner a disposición de los RT, las herramientas necesarias que permitan personalizar, complementar y/o adaptar las soluciones estandarizadas a sus características, si fuera el caso.
- Actualizar periódicamente las soluciones estandarizadas y las herramientas, para adecuarlas a la realidad normativa y operativa de los RT.

Ejemplos de implantación

Como ejemplo de esta buena práctica, se podrían realizar las siguientes labores de estandarización:

- **RAT**: Desde el Servicio centralizado se podría analizar los tratamientos que son comunes a cada tipología de RT, y elaborar y mantener un RAT que comparta los elementos comunes a cada una de estas tipologías (previa validación por los Órganos Consultivos y de Gobierno). Este RAT común se pondría directamente a disposición de los RT a través de la Herramienta de Cumplimiento, desde donde podrían añadir, eliminar o modificar los tratamientos, según sus necesidades o características propias.
- **Privacidad por defecto (PpD)**: Desde el Servicio centralizado se podría evaluar las medidas de seguridad y privacidad que afectan al RT, derivadas de: normativa de protección de datos, legislación general de aplicación (ej: ENS), legislación específica del sector, normativas internas, etc. Con el listado completo de medidas de seguridad y privacidad aplicables, se podría elaborar un marco de control, consolidando y unificando aquellas medidas similares, y adaptando las que sea posible a la realidad de los RT. Al margen de las medidas que, por defecto, sean necesarias cumplir en todos los tratamientos, el marco de control podría contemplar la segmentación del resto de medidas en relación al riesgo de privacidad (por ejemplo, en tres niveles: Bajo, Medio y Alto).
- **AARR y EIPD**: Una vez que existe un inventario común de tratamientos, se podría realizar un análisis de necesidad de EIPD, basado en las características y operativas más comunes de los RT. En función de los resultados de ese análisis, se podría estandarizar la parte análisis de factores intrínsecos del AARR y EIPD, obteniendo como resultado los niveles de riesgo asociado a cada tratamiento, y por tanto el marco de control de medidas aplicable a cada nivel de riesgo. De esta forma, los RT tendrían conocimiento de qué medidas de seguridad y privacidad implantar en función del nivel de riesgo de los tratamientos, siempre y cuando las características de sus tratamientos se ajusten a los parámetros comunes. En caso de que no se ajustaran a dichos parámetros, el RT podría personalizarlos a través de la Herramienta de Cumplimiento , desde la que se le informaría de los nuevos niveles de riesgo y EIPD.
- **Privacidad desde el diseño (PdD)**: Desde el Servicio centralizado se podrían evaluar los escenarios más comunes en los RT que activan el proceso de PdD (ej: Desarrollo de software, adquisición de productos, contratación de terceros, cambio de locales, etc.), de tal forma que se vinculen a cada escenario las plantillas

de planes de acción, cláusulas, modelos, etc. que se deben tener en cuenta ante cada situación. Para los escenarios no tipificados, se podría indicar a nivel procedimental como actuar, con el soporte de los marcos de control ya desarrollados.

Guías, herramientas, enlaces, documentación

Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento (AEPD)

https://www.aepd.es/es/documento/guia-rgpd-para-responsables-de-tratamiento.pdf-0

Guía de privacidad desde el diseño (AEPD)

https://www.aepd.es/es/documento/guia-privacidad-desde-diseno.pdf

Guía de protección de datos por defecto (AEPD)

https://www.aepd.es/es/documento/guia-proteccion-datos-por-defecto.pdf

Guidelines 4/2019 on Article 25 Data Protection by Design and by Defaul (CEPD)

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2019/guidelines-42019-article-25-data-protection_en

Guía tecnologías y protección de datos en Administraciones Públicas (AEPD)

https://www.aepd.es/sites/default/files/2020-11/guia-tecnologias-admin-digital.pdf

Guía práctica de análisis de riesgos para el tratamiento de datos personales (AEPD)

https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

Herramienta Evalúa – Riesgo RGPD (AEPD)

https://www.aepd.es/es/guias-y-herramientas/herramientas/evalua-riesgo-rgpd

Modelo de informe de EIPD para las Administraciones Públicas y sector privado (AEPD)

https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-un-modelo-de-informe-para-ayudar-las-empresas

Listas de tipos de tratamientos de datos que requieren y que no requieren EIPD (AEPD)

https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-el-listado-de-tratamientos-en-los-que-no-es

Recomendación 01/2019 sobre el proyecto de lista del Supervisor Europeo de Protección de Datos en relación con las operaciones de tratamiento supeditadas al requisito de una EIPD (CEPD)

https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendation_201901_edps_39.4_dpia_list_es.pdf

Gestiona EIPD (AEPD)

https://www.aepd.es/es/guias-y-herramientas/herramientas/gestiona-eipd

ISO/IEC 29134:2017 – Guía de asesoramiento sobre el análisis de impacto a la privacidad

https://www.iso.org/standard/62289.html

ISO/IEC 31000:2018 - Gestión del Riesgo

https://www.iso.org/standard/65694.html

Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario (INCIBE)

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-ganar-competitividad-cumpliendo-rgpd-metad.pdf

Modelo de Registro de Actividades del Tratamiento (APDCAT)

https://apdcat.gencat.cat/es/documentacio/programari/aplicacio-per-gestionar-el-registre-de-les-activitats-de-tractament/

Modelo de Registro de Actividades del Tratamiento (CNIL – Francia)

https://www.cnil.fr/en/record-processing-activities

Cumplimiento de procesos de respuesta a terceros

Descripción y objetivo

Al igual que con los procesos clave mencionados anteriormente, la normativa de protección de datos obliga a dar una **adecuada cobertura a ciertos procesos iniciados por terceros que conllevan la resolución en plazos**, como son el de ejercicio de derechos, gestión de violaciones de seguridad o el proceso de reclamaciones recibidas por la autoridad de control. El objetivo es estandarizar estos procesos tanto en la parte del Responsable del Tratamiento (RT) como en el soporte prestado desde el Servicio centralizado, de cara a **garantizar los derechos y libertades de los ciudadanos**.

Buena práctica

Como parte de este trabajo de estandarización y cumplimiento de los **procesos de respuesta a terceros, debemos tener en cuenta que dichos procesos deben encontrarse formalizados y bien gestionados**, de cara a que la respuesta se proporcione en **plazos y sea adecuada y pertinente** a la comunicación recibida. Para ello, se deberían tener en cuenta los siguientes requisitos:

- Formalizar el procedimiento de ejercicio de derechos, donde figuren las diferentes partes del proceso (recepción, registro, validación, gestión y respuesta) así como las responsabilidades del RT y la posible intervención del Servicio centralizado.
- Formalizar el procedimiento de violaciones de seguridad, donde figuren las diferentes partes del proceso (identificación, detección, notificación, valoración, registro, seguimiento, contención, resolución y notificación a la autoridad de control e interesados) así como las responsabilidades del RT y la posible intervención del Servicio centralizado.
- Formalizar el procedimiento de reclamaciones recibidas de la autoridad de control o el interesado, donde figuren las diferentes partes del proceso (recepción, registro, validación, gestión y respuesta) así como las responsabilidades del RT, y la posible intervención del Servicio centralizado.
- Disponer de herramientas automáticas que permitan registrar y gestionar los plazos de cada uno de estos procedimientos.

Ejemplos de implantación

Como ejemplo de esta buena práctica, los procedimientos podrían implantarse con la siguiente organización:

- **Ejercicio de derechos**: Estandarizar el proceso de recepción, ya sea a través del RT o través de la Ventanilla Única, trasladando la petición a Soporte Especializado del Servicio. Soporte procederá a la validación de la petición y a su redirección hacia los destinos más adecuados para resolver la petición, en función del derecho ejercido, realizando el seguimiento según los plazos asociados y respondiendo a través del mismo medio utilizado por el interesado.
- **Violaciones de seguridad**: Debido a la criticidad y los plazos ajustados de este proceso, se podría realizar en dos etapas: la primera, de recepción y canalización hacia Soporte Especializado del Servicio, una vez se ha detectado o notificado el incidente. En paralelo a los procesos de contención del incidente, Soporte procederá al registro y recopilación de la mínima información necesaria para valorar en primera instancia la necesidad de notificar o no a la autoridad de control e interesados (en cuyo caso, se recopilaría adicionalmente el resto de información necesaria para abrir la notificación en los plazos establecidos). Posteriormente, se iniciarían los procesos de gestión, seguimiento, resolución y notificación del incidente.
- **Reclamaciones**: Estandarizar el proceso de recepción, ya sea a través del RT o través de la Ventanilla Única , trasladando la petición a Soporte Especializado del Servicio. Soporte procedería a la validación de la petición y a su redirección interna, realizando el seguimiento según los plazos asociados y respondiendo a través de los medios establecidos.

Guías, herramientas, enlaces, documentación

Guía para la gestión de brechas de seguridad (AEPD)

https://www.aepd.es/es/documento/guia-brechas-seguridad.pdf

Guidelines 01/2021 on Examples regarding Data Breach Notification (CEPD)

https://cutt.ly/fRefN51

Directrices sobre notificación de brechas de datos personales (AEPD)

https://www.aepd.es/sites/default/files/2019-09/wp250rev01-es.pdf

Herramienta Comunica - Brecha RGPD (AEPD)

https://www.aepd.es/es/guias-y-herramientas/herramientas/comunica-brecha-rgpd

Guía para el ciudadano

https://www.aepd.es/sites/default/files/2020-05/guia-ciudadano.pdf

Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento (AEPD)

https://www.aepd.es/es/documento/guia-rgpd-para-responsables-de-tratamiento.pdf-0

Sección de ejercicio de derechos (AEPD)

https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos

Supervisión de cumplimiento

Descripción y objetivo

El objetivo de este elemento es el de establecer los mecanismos de evaluación por parte de los Responsables de Tratamiento (RT), para dar **cumplimiento a los procesos de verificación** establecidos en la normativa de protección de datos, y **demostrar su responsabilidad proactiva** en la protección de los tratamientos.

Buena práctica

Las buenas prácticas en este elemento deberían ir claramente orientadas a diseñar e implantar un **proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas**, así como a demostrar los principios de responsabilidad proactiva del RT en sus funciones de velar por el cumplimiento de la normativa de protección de datos. Para ello, se debería tener en cuenta los siguientes requisitos:

- Definir los mecanismos válidos para realizar los procesos de verificación y cumplimiento.
- Documentar los procesos y recursos asociados a dichos mecanismos, y que se pongan a disposición de los RT a través de la normativa interna y las herramientas de cumplimiento.
- Definir las periodicidades de los procesos de verificación y cumplimiento, atendiendo a criterios validados por el RT y los órganos de gobierno.
- Definir los criterios de revisión y almacenamiento de evidencias, para aquellos mecanismos que lo requieran.

Ejemplos de implantación

Como ejemplo de implementación de esta buena práctica, se podrían definir los siguientes procesos de supervisión del cumplimiento:

- **Autoevaluación**: Proceso rápido e informal, a través del cual desde el Servicio centralizado se elaboraría un cuestionario de diagnóstico compuesto por preguntas relacionadas con el cumplimiento de las medidas establecidas en la Normativa Interna, junto con la ayuda y referencias necesarias para completarlo. Este cuestionario se enviaría a los RT a través de la Herramienta de Cumplimiento, los cuales se encargarían de responder a cada pregunta. En función de las respuestas, se les mostraría su estado de cumplimiento y las principales carencias que deberían solucionar. Desde el Servicio centralizado se fijarían unos umbrales de cumplimiento mínimo y, en caso de no superarse, se realizaría un seguimiento posterior para proporcionar soporte a la implantación de las medidas necesarias para alcanzar esos mínimos.
- **Verificación con evidencias**: Proceso rápido y semiformal, a través del cual desde el Servicio centralizado se lanzaría un proceso similar al de Autoevaluación pero, a diferencia de este, para un conjunto determinado de preguntas se requeriría la aportación de evidencias por parte del RT que avalen su respuesta. En este caso, una vez completado el cuestionario, desde Soporte Especializado del Servicio centralizado se analizarían las evidencias aportadas, dictaminando sobre su conformidad o no, en base a criterios preestablecidos.
- **Auditoría externa**: Proceso lento y formal, a través del cual un auditor externo al RT evaluaría el cumplimiento de la normativa de protección de datos, a través de procesos reglados y la aportación de evidencias. Desde el Servicio centralizado se podría llevar a cabo un proceso de negociación y homologación de proveedores de auditoría, para homogeneizar el proceso y estandarizar el catálogo tasado de servicios de auditoría.

Guías, herramientas, enlaces, documentación

ISO/IEC 19011: 2018 - Directrices para la auditoría de los sistemas de gestión

https://www.iso.org/standard/70017.html

Verificación cumplimiento medidas del ENS (CCN)

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/518-ccn-stic-808-verificacion-del-cumplimiento-de-las-medidas-en-el-ens-borrador/file.html

Guía de Requisitos de Auditoría de Tratamientos que incluyan Inteligencia Artificial (AEPD)

https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-guia-requisitos-auditorias-tratamiento-ia

COBIT (ISACA)

https://www.isaca.org/resources/cobit

Seguro de protección de datos

Descripción y objetivo

El objetivo de este elemento es el de poner a disposición de los Responsables de Tratamiento (RT) un seguro específico para la **gestión de riesgos de privacidad y seguridad** existentes. El seguro dispondría de las coberturas necesarias en caso de contingencia respecto del tratamiento de los datos personales de los interesados afectados, a efectos de **mitigar las posibles consecuencias derivadas de sanciones o incidentes** cuya responsabilidad recaiga sobre los Responsables de Tratamiento.

Buena práctica

Pese a que se realice un cumplimiento completo y exhaustivo de la normativa de protección de datos, siempre existe el **riesgo de que ocurra algún error o violación que pueda comprometer datos de carácter personal**. Por ello, de manera complementaria al cumplimiento riguroso, es recomendable establecer estrategias de **transferencia del riesgo mediante la contratación de un seguro especializado** que cubra este tipo de contingencias. No obstante, a la hora del análisis y contratación de un seguro de protección de datos (también conocido como seguro de ciberriesgos), sería necesario tener en cuenta los siguientes requisitos:

- Definir adecuadamente el alcance, fijando claramente quienes serán los asegurados cubiertos por el seguro, el ámbito territorial del mismo y los límites temporales del seguro (desde y hasta cuando es de aplicación, y si cubre la retroactividad de eventos ocurridos antes de contratar la póliza que pudieran desembocar en un siniestro futuro).
- Definir adecuadamente las coberturas en caso de siniestro, teniendo en cuenta, como mínimo, las siguientes: daños propios o pérdidas (gastos incurridos en recuperación / restitución, errores humanos, incidentes, extorsión cibérnetica, indisponibilidad...), reclamaciones de terceros (RC, indemnizaciones, sanciones de protección de datos, fianzas), asistencia jurídica y técnica (contención de la crisis, análisis forense, gastos legales, restitución de imagen).
- Definir y analizar las exclusiones, ya que como mínimo se deberán valorar los esfuerzos en base al riesgo para implementar las medidas que ayuden a prevenir la ocurrencia de los eventos excluidos.
- Asegurar que los límites económicos cubiertos y las franquicias establecidas, cubran adecuadamente los impactos organizativos y sanciones más probables.
- Analizar que la prima anual del seguro se encuentre equilibrada en relación al coste de las medidas implantadas y al límite cubierto en caso de siniestro.
- Revisar todos los criterios anteriores de forma anual, para alinearlos con la realidad de los RT.
- Cubrir el Servicio centralizado por el seguro, siempre y cuando su relación con los RT conlleve el tratamiento de sus datos.

Ejemplos de implantación

Como ejemplo de implementación de esta buena práctica, desde el Servicio centralizado se podría negociar un contrato con aseguradoras en base a los criterios anteriores, partiendo de la base de que todos los tratamientos que se realizan por los RT son homogéneos y con los límites y coberturas aprobadas por los Órganos de Gobierno. Una vez negociado, se podría contratar el seguro en base a dos modelos diferentes: un modelo de contrato de seguro marco donde cada RT que esté interesado contactara con la aseguradora para adherirse individualmente, o bien un modelo por el cual desde el Servicio centralizado se contratara la póliza y se cubriera a todos los RT adheridos.

Guías, herramientas, enlaces, documentación

ISO/IEC 27102:2019 - Guías y Directrices para Ciber Seguros

https://www.iso.org/standard/72436.html

Código de conducta

Descripción y objetivo

El objetivo de este elemento es el disponer de un **código de conducta** en Responsables de Tratamiento (RT) en los términos reconocidos por la Autoridad de Control para este tipo de documentos, como mecanismo de autorregulación para los RT, **impulsar la cultura de privacidad** en los mismos, **fortalecer los procesos** que ayuden a garantizar los derechos y libertades de los interesados y **reducir los riesgos** e impactos de una posible sanción.

Buena práctica

La formalización del código de conducta es un proceso **voluntario, aunque altamente recomendable** cuando nos encontramos frente al cumplimiento de protección de datos en un sector específico y delimitado. Esto es debido a que la aprobación del código de conducta por parte de la autoridad de control puede **proporcionar una seguridad adicional** en cuanto a que las directrices de cumplimiento establecidas en dicho código son válidas, y por tanto la adhesión al mismo es un claro valor añadido para los RT. A la hora de plantear la elaboración y aprobación de un código de conducta, se debe observar cuidadosamente el cumplimiento de los artículos 40 y 41 del RGPD y el artículo 38 y título IX de la LOPDGDD, junto con los criterios de acreditación del organismo de supervisión de códigos de conducta emitidos por la AEPD, prestando especial atención a los siguientes requisitos:

- Analizar y establecer claramente los roles de promotor del código y organismo supervisor del código de conducta, atendiendo especialmente a las limitaciones y condicionantes prefijados en caso de que ambos roles los asuma una misma organización.
- Fijar claramente el ámbito del código, con la naturaleza y tratamientos cubiertos por el mismo.
- Asegurar que el contenido del código de conducta no sea una mera reproducción de la normativa de protección de datos, ya que debe especificar la necesidad y utilidad del código tanto para los RT como para los ciudadanos.
- Contar con procesos de gestión y respuesta de las reclamaciones extrajudiciales que los ciudadanos pueden interponer en relación al incumplimiento del código o al propio contenido del código, garantizando unas medidas mínimas de independencia y conflicto de intereses.
- Asegurar que, una vez aprobado el código por la Autoridad de Control, se proporcionen mecanismos sencillos y robustos para que los RT se adhieran al mismo.
- Realizar procesos periódicos de supervisión del cumplimiento del código en los RT adheridos, y que se gestionen los incumplimientos conforme a lo especificado en la normativa.

Ejemplos de implantación

La implementación de esta buena práctica varía sustancialmente en función de si los dos roles principales (promotor y organismo supervisor) los desempeña la misma organización u organizaciones diferentes. El primer caso, si bien es posible, entraña complicaciones que deben ser valoradas por las organizaciones, y que quedan bien definidas en la guía de la AEPD "Criterios de acreditación para los organismos de supervisión de códigos de conducta". Estas limitaciones van principalmente encaminadas a garantizar la independencia necesaria entre ambos roles, que debe quedar patente en todos los niveles y estructuras de la organización.

Guías, herramientas, enlaces, documentación

Directrices 1/2019 sobre códigos de conducta y organismos de supervisión con arreglo al Reglamento (UE) 2016/679 (CEPD)

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_es.pdf

Criterios de acreditación para los organismos de supervisión de códigos de conducta (AEPD)

https://www.aepd.es/es/documento/acreditacion-organismos-supervision-cc.pdf

Directrices 04/2021 sobre códigos de conducta como herramienta para transferencias (CEPD)

https://edpb.europa.eu/system/files/2021-07/edpb_guidelinescodesconducttransfers_publicconsultation_en.pdf

Certificación de privacidad

Descripción y objetivo

El objetivo de este elemento es establecer los requerimientos mínimos necesarios para acometer, individual y voluntariamente, en cada Responsable del Tratamiento (RT) un **proceso de certificación en privacidad que atienda a los estándares internacionales** reconocidos, como medida adicional para acreditar el cumplimiento normativo. Todo ello, alineado al soporte prestado desde el Servicio centralizado.

Buena práctica

Al igual que los códigos de conducta, la certificación en privacidad es un **proceso voluntario, aunque altamente recomendable para demostrar el compromiso** y cumplimiento de las medidas de seguridad y privacidad en los tratamientos de datos de carácter personal. Para acometer un proceso de certificación de privacidad, sería necesario tener en cuenta los siguientes requisitos:

- Definir adecuadamente el alcance de certificación, y asegurar que es relevante acorde a los tratamientos que se desean cubrir, los sistemas técnicos implicados y los procesos y procedimientos relacionados con la operativa.
- Seleccionar un mecanismo de certificación acorde a estándares internacionalmente reconocidos y avalados por las autoridades de control.
- Definir un conjunto de recursos estandarizados y disponibles para que el RT pueda acometer con garantías el proceso de certificación.
- Asegurar que el soporte prestado por el Servicio centralizado se encuentre alineado con los recursos puestos a disposición del RT y los objetivos de la certificación.
- Asegurar que los procedimientos, normativa interna y procesos de supervisión estén alineados con los requisitos de la certificación.

Ejemplos de implantación

La implementación de esta buena práctica varía en función de los alcances y objetivos de la certificación, si bien se podría plantear de la siguiente forma:

- Desde el Servicio centralizado: Realizar propuestas de objetivos y alcances de certificación. Analizar los mecanismos de certificación que mejor se ajusten a los requisitos normativos y a las capacidades de los RT. Elaborar un catálogo de entidades de certificación acreditadas y, en lo posible, tasar con ellas el servicio de certificación en base a los objetivos y alcances propuestos. Elaborar hojas de ruta para los RT que deseen certificarse, con las tareas a realizar antes y después de la certificación. Elaborar materiales adicionales para los RT que deseen certificarse, o bien alinear la Normativa Interna, recursos y Herramientas para que estén preparados para las tareas derivadas de la certificación. Establecer los servicios de soporte necesarios para el proceso de implantación previo a la certificación, y su posterior mantenimiento.
- Desde los Responsables de Tratamiento: Que se implanten los requisitos establecidos en la hoja de ruta para optar a la certificación. Contratar la entidad de certificación deseada. Obtener el certificado y realizar los procesos necesarios posteriores que permitan mantener la certificación.

Guías, herramientas, enlaces, documentación

Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento (CEPD)

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_es.pdf

Directrices 4/2018 relativas a la acreditación de los organismos de certificación conforme a lo dispuesto en el artículo 43 del RGPD (CEPD)

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_es.pdf

Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento (CEPD)

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_es

Madurez adaptativa

Descripción y objetivo

Cuando se dispone de un **conjunto heterogéneo** de Responsables de Tratamiento (RT), debería tenerse en cuenta que el nivel de madurez (en términos de cumplimiento de privacidad y seguridad) de cada uno de ellos puede variar sustancialmente, partiendo desde el nivel de madurez más bajo (aquellos que no tienen nada implantado) hasta el más avanzado (aquellos que tienen todo implantado, están certificados, etc.). **El Servicio centralizado debería ser capaz de dar un soporte adaptado a cada nivel de madurez**, de tal forma que se acompañe a cada RT de la forma más adecuada en cada etapa.

Buena práctica

Como buena práctica, el Servicio centralizado debería organizarse internamente para prestar el soporte adecuado en función del nivel de madurez del RT, teniendo en cuenta los siguientes requisitos:

- Definir y tipificar los diferentes niveles de madurez en los que pueden encajarse cada RT.
- Definir los itinerarios de actividades a realizar para pasar de un nivel de madurez a otro, y se pongan a disposición de los RT.
- Controlar desde el Servicio centralizado en qué nivel de madurez se encuentra cada RT.
- Estratificar, en la medida de lo posible, cada elemento del servicio en función del nivel de madurez del RT que lo está consumiendo.

Ejemplos de implantación

Como ejemplo de implementación de esta buena práctica, en relación a los elementos descritos en esta guía, se podrían definir los siguientes niveles de madurez en los RT (son acumulativos):

- **Nivel 0**: Adhesión al Servicio centralizado + notificación del DPD a la Autoridad de Control + Ventanilla Única + Soporte Especializado.
- **Nivel 1**: Responsabilidades internas designadas + distribución de Normativa Interna + Herramienta de Cumplimiento instalada + cláusulas firmadas con empleados y proveedores.
- **Nivel 2**: Cursos formativos realizados por el personal clave + implantación de Procesos Clave y Procesos de Respuesta + Implantación de medidas de seguridad y privacidad.
- **Nivel 3**: Herramienta de Cumplimiento completada + personalización de los procesos y procedimientos en función de las características del RT + Supervisión del Cumplimiento en modo autoevaluación.
- **Nivel 4**: Supervisión del Cumplimiento en modo verificación interna o auditoría anuales, superando el umbral mínimo de cumplimiento en todos los ámbitos + cursos de formación periódicos.
- **Nivel 5**: Adhesión al Código de Conducta y/o Certificación de Privacidad obtenida.

En base a estos niveles de madurez, el Servicio centralizado podría adaptar sus elementos acordes al nivel de madurez, por ejemplo: obligando a alcanzar el nivel 3 para poder optar al Seguro de Protección de Datos en las condiciones pactadas o reduciendo la cuota del seguro cuando están en nivel 5 (previo pacto con la entidad de seguros), lanzando procesos de supervisión acordes al nivel, lanzando cursos de formación más avanzados, asignando personal más especializado de Soporte, etc.

Guías, herramientas, enlaces, documentación

Metodología Ágil de Adaptación Continua (MADAC)

https://madac.es/

COBIT (ISACA)

https://www.isaca.org/resources/cobit

Capability Maturity Model Integration (CMMI)

https://cmmiinstitute.com/

Análisis global de riesgos en las organizaciones colegiales. Marco para realizar un modelo de prevención de riesgos y cumplimiento normativo, incluida la protección de datos (Unión Profesional - 2018)

http://www.unionprofesional.com/prevencion-de-riesgos-y-cumplimiento-normativo-en-las-corporaciones-colegiales/

ISO 37301:2021 - Compliance management systems - Requirements with guidance for use

https://www.iso.org/standard/75080.html

UNE 19601:2017 - Sistemas de gestión de compliance penal. Requisitos con orientación para su uso

https://tienda.aenor.com/norma-une-19601-2017-n0058338

Guía de buenas prácticas

para el cumplimiento del RGPD en organismos descentralizados

Colegio de Registradores de la propiedad mercantil y de bienes muebles
Octubre de 2021

En colaboración con Unión Profesional

Aplicación Web de Autoevaluación para Servicios Centralizados de Privacidad:

www.registradores.org/es/documentacion-y-descargas/cuestionario-de-autoevaluacion

Guía de buenas prácticas en formato web:

guiapd.registradores.org

Registradores DE ESPAÑA