III. Otras Resoluciones

Consejería de Hacienda y Relaciones con la Unión Europea

2151 *Instituto Canario de Estadística.- Resolución de 29 de mayo de 2025, del Director, por la que se aprueba la política de protección de datos y cesión altruista de datos.*

Vista la política de protección de datos y cesión altruista de datos elaborada por el Instituto Canario de Estadística.

Visto el informe de la Comisión Ejecutiva del Instituto Canario de Estadística, de fecha 7 de mayo de 2025.

Visto el ámbito de aplicación del Decreto 89/2023, de 25 de mayo, de régimen de gobierno y análisis de datos del Sistema Estadístico de Canarias, establecido en su artículo 2.

Considerando lo dispuesto en el artículo 12.c) del Decreto 89/2023, de 25 de mayo, de régimen de gobierno y análisis de datos del Sistema Estadístico de Canarias: "El tercer nivel lo constituyen los protocolos de federación aprobados por la Comisión Superior de Administración Pública de la Comunidad Autónoma de Canarias, y las políticas de activos de datos aprobadas por Resolución de la persona titular de la Dirección del Instituto Canario de Estadística, que deben ser comunicadas a la Comisión Ejecutiva".

Considerando que las políticas de activos de datos se definen en el artículo 14 del citado Decreto: "Las políticas de activos de datos son un conjunto de principios amplios y de alto nivel que forman el marco rector en el que se gestionan los activos de datos". Entre ellas, se encuentra la política de protección de datos y cesión altruista de datos.

Considerando que el artículo 15 del Decreto 89/2023, de 25 de mayo, establece la aprobación de las políticas de activos: "Las políticas de activos de datos son aprobadas por Resolución de la persona titular de la Dirección del Instituto Canario de Estadística y comunicadas a la Comisión Ejecutiva". Igualmente, establece el contenido mínimo de las políticas.

En virtud de lo anteriormente expuesto, y al amparo de las facultades que me confieren el artículo 15 del Decreto 89/2023, de 25 de mayo, de régimen de gobierno y análisis de datos del Sistema Estadístico de Canarias, así como en los artículos 13.2.b) y 13.2.a) del Decreto 11/2017, de 16 de enero, por el que se aprueba el Reglamento de organización y funcionamiento del Instituto Canario de Estadística,

R E S U E L V O :

Primero.- Aprobar la política de protección de datos y cesión altruista de datos, que figura como anexo.

Segundo.- Publicar la presente política en el Boletín Oficial de Canarias.

Las Palmas de Gran Canaria, a 29 de mayo de 2025.- El Director, Sergio Fernando Alonso Rodríguez.

istac | INSTITUTO CANARIO DE ESTADÍSTICA

POLÍTICA | ISTAC-POL-PROTEGE-0001

PROTECCIÓN DE DATOS Y CESIÓN ALTRUISTA DE DATOS

CONTENIDO

1. Preámbulo

De conformidad con el artículo 14 apartado f) del Decreto 89/2023, de 25 de mayo, de régimen de gobierno y análisis de datos del Sistema Estadístico de Canarias (en adelante, el "Decreto 89/2023"), el Sistema Estadístico de Canarias (en adelante, el "SEC") debe contar con una Política de protección de datos y cesión altruista de datos.

Con carácter general, los datos estadísticos están sujetos a dos marcos esenciales de protección:

> **Marco general de protección de datos**: El marco general de protección de datos, se encarga de establecer el marco legal de referencia que desarrolla el derecho fundamental a la protección de datos personales, incluyendo, entre otras cuestiones, los principios relativos al tratamiento, los derechos de las personas interesadas, así como las obligaciones del responsable del tratamiento.

> **Marco específico de protección de datos recogidos con fines estadísticos:** La protección de los datos recopilados con fines estadísticos, conocido también como secreto estadístico, constituye un principio fundamental en la realización de estadísticas. Por tanto, el marco específico regula, principalmente, la obligación concreta de no divulgar ni comunicar aquel conocimiento que una persona posee como consecuencia de la actividad estadística, así como la obligación de no actuar sobre la base de dicho conocimiento.

En el ámbito del SEC, dependiendo del supuesto, podrá ser de aplicación un marco u otro, así como ambos a la vez, tal y como se muestra a continuación.

¿Se tiene previsto tratar datos de carácter personal?	¿Es de aplicación el secreto estadístico al tratamiento?	Marco aplicable
Sí	Sí	Se trataría de datos de carácter personal sujetos a secreto estadístico. Resultarían de aplicación los dos marcos: general y específico.
No	Sí	Se trataría de datos sujetos a secreto estadístico, pero no a la normativa en materia de protección de datos. Resultaría de aplicación el marco específico.
Sí	No	Se trataría de datos personales recopilados con fines distintos de los estadísticos. Resultaría de aplicación el marco general.

2. Ámbito de aplicación

La presente Política será de aplicación a la actividad de gobierno y análisis de datos de la estadística pública para fines de la Comunidad Autónoma de Canarias y, en particular, a la realizada por las siguientes entidades y organismos que forman parte de la misma:

> Sector público autonómico de la Comunidad Autónoma de Canarias.

> Sector público local de la Comunidad Autónoma de Canarias.

3. Glosario

Para facilitar la comprensión de esta Política, se ofrecen las siguientes definiciones clave, en función del marco general de protección de datos y el marco específico de protección de datos con fines estadísticos:

Marco general de protección de datos personales	Marco específico de protección de datos con fines estadísticos
Datos personales: Información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.	**Datos confidenciales**: datos que permiten identificar unidades de observación, ya sea directa o indirectamente, revelando información individual. Para determinar si una unidad de observación es identificable, deben considerarse todos los medios razonables que un tercero podría usar para identificar la unidad de observación.
Interesado: la persona cuyos datos personales son recopilados, almacenados o tratados por el responsable del tratamiento.	**Unidad de observación**: Persona física o jurídica, hogar u otro tipo de operador al que se refieren los datos.
Finalidad de la recogida de datos: los datos personales se recogen y tratan para diferentes finalidades específicos y legítimos, que deberán determinarse en cada caso.	**Finalidad de la recogida de datos**: los datos se recogen únicamente para fines estadísticos.
Alcance: datos de carácter personal relativos a personas físicas.	**Alcance**: datos recopilados para fines estadísticos en conformidad con la legislación aplicable; puede incluir datos sobre personas físicas, hogares y entidades empresariales.

Así mismo, a efectos de esta Política se consideran las siguientes definiciones:

Acceso. Tratamiento, por parte de un usuario de datos, de los datos facilitados por un titular de datos, de conformidad con unos requisitos técnicos, jurídicos u organizativos específicos, sin que ello implique necesariamente la transmisión o la descarga de los datos.

Actividad estadística pública. Conjunto de tareas constituidas por la recopilación u obtención, elaboración, ordenación, almacenamiento, difusión, publicación, análisis de datos, y otras de similar naturaleza, relativas a los aspectos demográficos, sociales, económicos, ambientales y territoriales para fines de la Comunidad Autónoma de Canarias.

Activos de datos. Cualquier representación de datos que aporta valor a la actividad estadística, que deben ser protegidos como activos de información del Sistema Estadístico de Canarias en la lógica del Esquema Nacional de Seguridad.

Análisis masivo de datos. Estudio exhaustivo de los mismos mediante técnicas estadísticas con el objeto de describir u obtener conclusiones a cuestiones planteadas en los ámbitos de la demografía, la economía, la sociedad, el medio ambiente, o la gestión pública y que solo se pueden responder de manera adecuada a partir de datos pertinentes y detallados que permitan un análisis en profundidad.

Anonimización. Proceso para eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de los mismos, es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleva una distorsión de los datos reales.

Cesión altruista de datos. Todo intercambio voluntario de datos basado en el consentimiento de los interesados para que se traten sus datos personales, o en el permiso de los titulares de datos para que se usen sus datos no personales, sin ánimo de obtener o recibir una gratificación que exceda de una compensación relativa a los costes en que incurran a la hora de facilitar sus datos, con objetivos de interés general tal como se disponga en el Derecho nacional, en su caso, como, por ejemplo, la asistencia sanitaria, la lucha contra el cambio climático, la mejora de la movilidad, la facilitación del desarrollo, elaboración y difusión de estadísticas oficiales, la mejora de la prestación de servicios públicos, la elaboración de políticas públicas o la investigación científica de interés general.

Confidencialidad. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Datos. Representación digital de actos, hechos o información, así como su recopilación, incluso, como grabación sonora, visual o audiovisual.

Datos no personales. Datos que no sean datos personales, tal como se definen en el artículo 4, punto 1, del Reglamento (UE) 2016/679.

Datos sensibles (o categorías especiales de datos). Datos de personas físicas que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento

de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física. Igualmente, los datos personales relativos a condenas e infracciones penales.

Esquema Nacional de Seguridad. Instrumento que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

Fichero. Conjunto estructurado de datos, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

Gobierno del dato. Disciplina que se encarga de establecer un marco de referencia en todo lo relacionado con los datos de una organización: personas, procedimientos, tecnologías, accesibilidad, integridad y usabilidad. Es, en definitiva, el ejercicio de autoridad y control sobre la gestión de los activos de datos.

Gestión de datos. Desarrollo, ejecución y supervisión de planes, políticas, programas y prácticas que permiten gestionar, controlar, proteger, reutilizar e incrementar el valor de los datos y activos de información a lo largo de su ciclo de vida.

Inteligencia artificial. Software o sistema que se desarrolla empleando una o varias de las técnicas y estrategias estadísticas de aprendizaje y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa.

Intercambio de datos. Facilitación de datos, por parte de un titular de datos a un usuario de datos, directamente o a través de un intermediario y en virtud de un acuerdo voluntario, con el fin de hacer un uso conjunto o individual de los datos facilitados.

Interoperabilidad. Capacidad de los sistemas de información, y por ende de los procedimientos a los que dan soporte, de compartir datos y posibilitar de forma segura el intercambio de información entre ellos.

Personal estadístico. Es el personal al servicio de la Administración Pública, cualquiera que sea la naturaleza jurídica de su vínculo y el grupo, subgrupo o categoría profesional al que pertenezca, que intervenga en la actividad estadística pública o tenga acceso a los datos de la misma. Asimismo, tendrán la condición de personal estadístico quienes intervengan en cualquiera de las fases del proceso estadístico o tengan acceso a datos estadísticos, en virtud de acuerdo, convenio o contrato, los cuales incorporarán un compromiso de confidencialidad.

Responsable del tratamiento. Persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

Reutilización. Uso, por parte de personas físicas o jurídicas, de los datos conservados por órganos u organismos del sector público con fines comerciales o no comerciales distintos del propósito inicial de la

misión de servicio público para la que se hayan producido tales datos, excepto en el caso del intercambio de datos entre órganos u organismos del sector público con la única finalidad de cumplir su misión de servicio público.

Secreto estadístico. Obligación de no divulgar ni comunicar datos sobre una unidad de observación que una persona posee como consecuencia de la actividad estadística pública, así como la obligación de no actuar sobre la base de dicho conocimiento. Los datos amparados por el deber de secreto estadístico solamente podrán ser conocidos y utilizados por quienes deban emplearlos para la realización de las estadísticas y otras actuaciones de esta naturaleza, y exclusivamente para dicha finalidad.

Seudonimización. Tratamiento de datos de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Sistema de información. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

Titular de datos o cedente. Persona jurídica o física que, de conformidad con la legislación autonómica, nacional o de la Unión, tiene derecho a conceder acceso a determinados datos personales o no personales que estén bajo su control, o a compartir tales datos.

Tratamiento de datos. Operación o conjunto de operaciones realizadas sobre datos o conjuntos de datos, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Unidad informante. Persona física o jurídica que suministra datos sobre una unidad de observación.

Usuario/a de datos o requirente. Persona física o jurídica que tiene acceso legítimo a determinados datos personales o no personales y está autorizada a usarlos con fines comerciales o no comerciales.

4. Principios

Coordinación y cooperación

El gobierno del dato y el análisis masivo de datos se deberá llevar a cabo garantizando la coordinación de todas las actividades realizadas por los agentes del SEC para el desarrollo, elaboración y difusión de resultados estadísticos. Asimismo, deberán de cooperar activamente en el desarrollo de otros regímenes de gobierno de datos de la Comunidad Autónoma de Canarias.

Responsabilidad y responsabilidad proactiva

Se deberá asignar y aclarar al personal estadístico, así como demás partes implicadas, sus propias funciones y responsabilidades, fomentando comportamientos y acciones que sean coherentes con ellos.

Asimismo, los agentes del SEC deberán propiciar de forma activa una cultura de colaboración y responsabilidad compartida en todos los asuntos relacionados con los datos con fines estadísticos, desde su calidad, tratamiento y uso, hasta su debida protección, custodia y seguridad, yendo más allá del mero cumplimiento de las reglas y requisitos e impulsando la mayor concienciación posible acerca de su importancia y valor, tanto para el SEC, como para la sociedad en general.

Los agentes del SEC deberán aplicar medidas técnicas y organizativas adecuadas a fin de garantizar y poder demostrar que los tratamientos de datos que realizan se ajustan con la normativa aplicable en materia de protección de datos y secreto estadístico.

Gestión basada en riesgos

El análisis y la gestión de los riesgos son partes esenciales del gobierno de datos y el análisis masivo de datos, debiendo constituir una actividad continua y permanentemente actualizada dentro del marco de actuación del SEC.

Asimismo, cuando se trate de datos de carácter personal, los agentes del SEC, en calidad de responsables del tratamiento, deberán realizar una valoración del riesgo del tratamiento, así como en su caso, una evaluación del posible impacto del mismo, con el fin de determinar qué medidas y salvaguardas se deberán aplicar, todo ello de conformidad con la normativa aplicable.

Independencia profesional

La selección de técnicas, definiciones, metodologías y fuentes que deban utilizarse para el gobierno del dato y/o el análisis masivo de datos, deberá desarrollarse, elaborarse y difundirse de manera independiente por parte del personal estadístico.

Además, los agentes del SEC deben promover y salvaguardar la independencia profesional de su personal, dotándolo de las herramientas necesarias para la aplicación de las mejores prácticas en el ámbito de la protección de datos y ejercer sus funciones con total independencia.

Publicidad y transparencia

En el ámbito del SEC se deberá garantizar la publicación, de forma periódica y actualizada, de información cuyo conocimiento sea relevante para garantizar la transparencia de su actividad en materia de protección de datos.

Así mismo, los agentes del SEC establecerán mecanismos claros y accesibles para facilitar la consulta de la información relativa a los tratamientos de datos personales realizados, así como, su vinculación con las actividades estadísticas desarrolladas.

Fiabilidad y exactitud de los datos

En los casos en que se gestionen directorios de datos personales (listas de personas, empresas, entidades), ya sea con fines administrativos (como en procedimientos sancionadores) o estadísticos, los datos deberán ser exactos y, en su caso, actualizados.

Cuando los datos estadísticos pasan a ser anonimizados o agregados para fines estadísticos, se reconoce que pierden su naturaleza personal. En estos casos, al no estar vinculados directamente a personas identificables, no será aplicable el derecho de acceso o rectificación, ya que la exigencia de exactitud individual no resultará pertinente y, por tanto, los datos no tendrán que ser exactos.

Accesibilidad y claridad

Los resultados estadísticos se presentarán de forma clara y comprensible, difundiéndose de forma adecuada y conveniente. Asimismo, su disponibilidad y acceso tendrá carácter imparcial e irán acompañados de metadatos y orientación de apoyo que faciliten su interpretación y uso, de forma que puedan ser aprovechados por el mayor número de personas y fines posibles.

Se garantizará que la información estadística publicada sea accesible y se difunda en la mayor variedad de formatos y medios posibles, asegurando que se respeta plenamente la confidencialidad de los datos personales y que su publicación cumple con la normativa de protección de datos y secreto estadístico.

Confidencialidad estadística

Se deberá proteger los datos gobernados para fines estadísticos, impidiendo la revelación o utilización de los mismos con fines no estadísticos.

Además, de conformidad con el principio de integridad y confidencialidad, los datos deberán ser tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas por parte de los agentes del SEC.

Limitación de la finalidad

Los datos personales serán recogidos por los agentes del SEC, en calidad de responsables del tratamiento, con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

En ese sentido, el tratamiento ulterior de los datos personales con fines estadísticos no se considerará incompatible con los fines iniciales, de conformidad con la normativa aplicable.

Protección de datos personales desde el diseño y por defecto

Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, los agentes del SEC aplicarán, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos de la normativa aplicable.

Asimismo, se aplicarán las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos de cada tratamiento.

Minimización de datos

La recogida y almacenamiento de datos que se realice dentro del ámbito del SEC deberá ser adecuada, pertinente y limitada a lo necesario para el cumplimiento de los objetivos planificados.

Intercambio de datos seguro e interoperable

El intercambio de datos para fines estadísticos, por parte de los agentes del SEC, se realizará a través de medios electrónicos, permitiendo la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por las partes que intercambian datos, garantizado la protección de los datos de carácter personal, y facilitando la prestación conjunta de servicios a la población usuaria.

Reutilización y libre circulación

Los datos para fines estadísticos deberán gobernarse para facilitar su reutilización y libre circulación bajo los marcos jurídicos que regulan estos tratamientos.

5. Marco normativo y ético de referencia

A continuación, se detalla el marco normativo y ético de referencia que resulta de aplicación a la presente Política.

Normativa europea

> Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos).

> Reglamento no 557/2013 de la Comisión por el que se aplica el Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo, relativo a la estadística europea, en lo que respecta al acceso a datos confidenciales con fines científicos, y por el que se deroga el Reglamento (CE) no 831/2002. Directiva 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos.

> Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.° 45/2001 y la Decisión n.° 1247/2002/CE (RGPD).

> Directiva 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos.

> 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.

Normativa nacional

> Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

> Ley 12/1989, de 9 de mayo, reguladora de la Función Estadística Pública.

> Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

> Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Normativa autonómica

> Ley 1/1991, de 28 de enero, de estadística de la Comunidad Autónoma de Canarias.

> Decreto 89/2023, de 25 de mayo, de régimen de gobierno y análisis de datos del Sistema Estadístico de Canarias.

Marco ético

> Principios fundamentales de las estadísticas oficiales (Naciones Unidas)[1].

[1] Disponible en: https://unstats.un.org/unsd/dnss/gp/FP-spanish.pdf

> Código de buenas prácticas de las estadísticas europeas (Eurostat)[2].

> Declaración sobre ética profesional (Instituto Internacional de Estadística)[3].

6. Alineamiento con estándares

El SEC, en aplicación de la presente Política, deberá alinearse con los siguientes estándares, guías y buenas prácticas recomendadas en materia de protección de datos personales y estadística pública.

Marco de protección de datos personales

> Comité Europeo de Protección de Datos [4]

El Comité Europeo de Protección de Datos (EDPB, por su denominación en inglés) es un órgano europeo independiente que contribuye a la aplicación coherente del RGPD y promueve la cooperación entre las autoridades de protección de datos de la Unión Europea. Para ello, publica directrices, recomendaciones y mejores prácticas para la correcta aplicación de la normativa en materia de protección de datos, del mismo modo que también asesora a la Comisión Europea sobre cualquier cuestión relacionada con la protección de datos en la UE y facilita la cooperación entre las autoridades de supervisión nacionales, como sería la AEPD en el caso de España.

> Agencia Española de Protección de Datos (AEPD)

- Orientaciones para tratamientos que implican comunicación de datos entre Administraciones Públicas ante el riesgo de brechas de datos personales[5].

  Orientaciones enfocadas en aquellos tratamientos de datos que, debido al gran volumen de información personal y la constante interconexión entre los sistemas de las Administraciones, son susceptibles de sufrir brechas masivas de datos personales de alto riesgo para los derechos fundamentales.

- Gestión del riesgo y evaluación de impacto en tratamientos de datos personales[6].

  Se trata de una guía para la gestión de riesgos para los derechos y libertades de las personas aplicable a cualquier tratamiento, independientemente de su nivel de riesgo. Además, y para los

[2] Disponible en: https://op.europa.eu/es/publication-detail/-/publication/661dd8ef-7439-11e8-9483-01aa75ed71a1/language-es
[3] Disponible en: https://isi-web.org/sites/default/files/2023-03/Spanish_Declaration-on-Professional-Ethics_2010.pdf
[4] Disponible en: https://www.edpb.europa.eu/
[5] Disponible en: https://www.aepd.es/guias/orientaciones-riesgo-brechas-masivas-aapp.pdf
[6] Disponible en: https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

casos de tratamientos de alto riesgo, incorpora las orientaciones necesarias para realizar la Evaluación de Impacto para la Protección de Datos (EIPD).

- Tecnologías y protección de datos en las Administraciones Públicas[7].

  Se trata de una guía que tiene como objeto principal llevar un análisis de algunas de las tecnologías que están aplicándose en el sector público con la finalidad de destacar sus aspectos más característicos desde el punto de vista de la protección de datos, así como poner de manifiesto sus posibles riesgos.

- Guía de protección de datos por defecto[8].

  Esta guía se centra en las medidas y salvaguardas adecuadas para garantizar la protección de datos por diseño y por defecto en los tratamientos que se lleven a cabo.

- Orientaciones y garantías en los procedimientos de anonimización de datos personales[9].

  Orientaciones elaboradas por la Autoridad Nacional de Protección de Datos de Singapur (PDPC) sobre cómo realizar adecuadamente la anonimización básica y la desidentificación de conjuntos de datos estructurados, textuales y no complejos.

> Comité Europeo de Innovación en materia de Datos[10]

El Comité Europeo de Innovación en materia de Datos (EDIB, por su denominación en inglés) es un organismo que se centra en la innovación y el uso ético de los datos en Europa. Trabaja en conjunto con diversas instituciones europeas para establecer directrices y marcos que promuevan la innovación en el manejo de datos, garantizando al mismo tiempo la protección y privacidad de los datos personales.

> Técnicas de seguridad. Extensión de las normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión de privacidad de la información. Requisitos y directrices. (ISO/IEC 27701:2019)

Esta norma en materia de seguridad de la información proporciona directrices específicas para la correcta gestión de la privacidad, ampliando las normas ISO/IEC 27001 e ISO/IEC 27002. Incluye requisitos para establecer, implementar, mantener y mejorar continuamente un correcto sistema de gestión de la información de privacidad (PIMS), enfocado al cumplimiento de la normativa aplicable en materia de protección de datos.

[7] Disponible en: https://www.aepd.es/guias/guia-tecnologias-admin-digital.pdf
[8] Disponible en: https://www.aepd.es/guias/guia-proteccion-datos-por-defecto.pdf
[9] Disponible en: https://www.aepd.es/documento/guia-basica-anonimizacion.pdf
[10] Disponible en: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupId=3903&fromMeetings=true&meetingId=56724

> Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para la protección de la información de identificación personal (ISO/IEC 29151:2017) *(Ratificada por la Asociación Española de Normalización en mayo de 2022)*

La norma ISO/IEC 29151:2017 tiene por objetivo proporcionar directrices y mejores prácticas para la privacidad y protección de datos personales en el entorno digital.

> Tecnología de la Información. Técnicas de seguridad. Código de práctica para la protección de identificación personal (PII) en nubes públicas que actúan como procesadores PII (ISO/IEC 27018:2019) *(Ratificada por la Asociación Española de Normalización en julio de 2020)*

La norma ISO/IEC 27018:2019 establece controles y directrices con el objetivo de implementar medidas para la protección de la información personal identificable (PII, por su denominación en inglés) en nubes públicas.

> UNE-EN 17799:2023 Requisitos de protección de datos personales para las operaciones de tratamiento *(Ratificada por la Asociación Española de Normalización en diciembre de 2023)*

Esta norma establece los requisitos específicos para la protección de datos personales en operaciones de tratamiento. Proporciona un marco detallado para asegurar que las operaciones de tratamiento de datos cumplan con los estándares de protección de datos más estrictos.

> UNE-EN 17740:2023 Requisitos de los perfiles profesionales relacionados con el tratamiento y la protección de datos personales *(Ratificada por la Asociación Española de Normalización en diciembre de 2023)*

Esta norma define los requisitos para los perfiles profesionales que trabajan en el ámbito del tratamiento y protección de datos personales, estableciendo las competencias y conocimientos necesarios para asegurar que los profesionales estén debidamente capacitados para gestionar y proteger los datos personales.

Marco estadístico

> Oficina de Estadística de la Unión Europea (Eurostat)

- Código de buenas prácticas de estadísticas europeas[11]

  El Código de buenas prácticas de estadísticas europeas proporciona un marco de referencia para asegurar la calidad de las estadísticas producidas por los sistemas estadísticos nacionales y

[11] Disponible en: https://ec.europa.eu/eurostat/documents/4031688/9394048/KS-02-18-142-ES-N.pdf/e792b761-6f09-42a9-a1e0-3a3356a0de1c

europeos. Promueve 16 principios que abarcan el entorno institucional y los procesos y la producción estadística.

- Manual de control de divulgación estadística (del inglés *Handbook on Statistical Disclosure Control*)[12]

  Este manual de control de divulgación estadística ofrece directrices para garantizar que los datos proporcionados por los países miembros cumplan con los principios de confidencialidad y protección de datos cuando se publican resultados estadísticos, evitando que se revele información personal o confidencial.

- Marco de garantía de calidad (del inglés *Quality Assurance Framework*)[13]

  Bajo este marco se definen los principios y directrices que garantizan la calidad de las estadísticas europeas, promoviendo buenas prácticas en todos los procesos estadísticos que abarcan desde la recopilación de los datos hasta la difusión de los resultados.

> Centro de excelencia en control de divulgación estadística[14]

El Centro de Excelencia sobre Control de la Divulgación Estadística (CoE on SDC, por su denominación en inglés) proporciona soporte y mantenimiento de las herramientas que facilitan a los productores de estadísticas europeas la aplicación del control de divulgación estadística (SDC). Además de prestar apoyo a los productores de estadísticas europeas y proporcionar orientaciones.

> Comisión Económica para Europa y División de Estadísticas de Naciones Unidas (UNECE y UNSD respectivamente, por sus denominaciones en inglés)

- Gestión de la confidencialidad estadística y acceso a microdatos. Principios y directrices de buenas prácticas (del inglés *Managing Statistical Confidentiality & Microdata Access. Principles and guidelines of good practice)*[15]

  En este documento se presentan principios y directrices que promueven y facilitan el acceso a microdatos por parte de investigadores, a la par que se busca la uniformidad entre países en el acceso a estos datos y mejorar la protección de la confidencialidad en su uso.

- Manual para la gestión y organización de los sistemas estadísticos nacionales (del inglés *Handbook on Management and Organization of National Statistical Systems*)[16]

[12] Disponible en: https://cros.ec.europa.eu/system/files/2023-12/SDC_Handbook.pdf
[13] Disponible en: https://ec.europa.eu/eurostat/web/quality/european-quality-standards/quality-assurance-framework
[14] Disponible en: https://cros.ec.europa.eu/coe-sdc
[15] Disponible en: https://unece.org/DAM/stats/publications/Managing.statistical.confidentiality.and.microdata.access.pdf
[16] Disponible en: https://unstats.un.org/capacity-development/handbook/index.cshtml

La división de estadísticas de las Naciones Unidas (UNSD, por su denominación en inglés) ha publicado este manual en el que se proporcionan directrices y buenas prácticas para la gestión y organización de los sistemas estadísticos nacionales. Se incluye información sobre los procesos de recopilación y difusión de los datos, la integración de fuentes de datos innovadoras y el uso de las nuevas tecnologías, destacando la importancia de la gestión ética y segura de los datos en la producción estadística.

- Principios y directrices sobre los aspectos de confidencialidad en la integración de datos para fines estadísticos o propósitos de investigación relacionados (del inglés *Principles and Guidelines on Confidentiality Aspects of Data Integration Undertaken for Statistical or Related Research Purposes*)[17]

  Este documento establece directrices sobre la confidencialidad en la integración de datos para fines estadísticos o de investigación.

> Guías de conservación y difusión de datos (del inglés Data archiving and dissemination)[18]

La Red Internacional de Encuestas y Hogares (IHSN, por su denominación en inglés) ofrece guías y buenas prácticas relacionadas con la adquisición, documentación, difusión y conservación de los microdatos de encuestas. También ofrece buenas prácticas para garantizar que los microdatos sean utilizados cumpliendo con las recomendaciones internacionales sobre confidencialidad y protección de datos personales.

> Manual de control de divulgación estadística de resultados (del inglés *Handbook on Statistical Disclosure Control for Outputs*)[19]

Este manual, realizado por el grupo de trabajo de profesionales de servicios de acceso seguro de datos (del inglés *Safe Data Access Professionals Working Group*), describe un marco de referencia para garantizar que se aplican técnicas de control de divulgación estadística (SDC, por su denominación en inglés) a los resultados estadísticos. De esta manera, se asegura que no se difunda información que permita identificar a las personas o unidades de observación, ni se libere ninguna información confidencial.

7. Roles y asignación de responsabilidades

Cada agente del SEC debe definir los roles, establecer las funciones y asignar las responsabilidades, en materia de protección y cesión altruista de datos, a su personal y colaboradores, de acuerdo con su estructura y organización. Asegurando que todas las personas involucradas comprendan claramente sus responsabilidades en relación con esta Política.

[17] Disponible en: https://unece.org/DAM/stats/publications/Confidentiality_aspects_data_integration.pdf
[18] Disponible en : https://www.ihsn.org/archiving
[19] Disponible en: https://securedatagroup.org/guides-and-resources/sdc-handbook/

A continuación, se especifican los roles y responsabilidades del personal y colaboradores del ISTAC en relación con la protección y la cesión altruista de datos.

Responsable de la información y del servicio

De conformidad con la Política de Seguridad del ISTAC, el responsable de la información y del servicio son desempeñadas por la persona titular de la Dirección del ISTAC y tendrá las siguientes funciones:

> Establecer las necesidades de seguridad de la información y efectuar las valoraciones del impacto que tendría un incidente que afectara a su seguridad, así como modificar el nivel de seguridad requerido para la misma.

> Determinar los requisitos de seguridad de los servicios prestados.

Para desarrollar estas funciones, la persona responsable de la información y del servicio contará con la colaboración de las personas gestoras, que se corresponderán con las personas titulares de aquellas unidades a su cargo con rango de Servicio o equivalentes.

Comité para la Gestión y Coordinación de la Seguridad de la Información

De conformidad con el artículo 8 de la Política de Seguridad del ISTAC, el Comité para la Gestión y Coordinación de la Seguridad de la Información tendrá las siguientes funciones:

> Elaborar los borradores de modificación y actualización de la PSI.

> Analizar los riesgos e impulsar su evaluación.

> Revisar el informe de Análisis de Riesgos realizado por la persona Responsable de Seguridad.

> Impulsar la actualización de los criterios y directrices sobre seguridad de la información.

> Impulsar medidas para mejorar y reforzar los sistemas de seguridad y control.

> Impulsar el cumplimiento y difusión de la PSI, promoviendo las actividades de concienciación y formación en materia de seguridad para el personal del ISTAC.

> Elaborar los borradores de directrices y normas de seguridad generales del ISTAC, que deberán cumplir el marco normativo de la presente Orden.

> Elaborar la normativa de seguridad de segundo nivel, que se corresponde con las políticas específicas de seguridad y con las Normas de Seguridad TIC (en adelante, Normas STIC), de obligado cumplimiento.

> Coordinar las decisiones y actuaciones de la persona Responsable de Seguridad, asesorando la resolución de los posibles conflictos entre los mismos bajo el criterio de garantizar la seguridad de las infraestructuras tecnológicas compartidas.

> Impulsar los proyectos para la adecuación al cumplimiento del Esquema Nacional de Seguridad.

> Compartir experiencias de éxito en materia de seguridad entre sus miembros para velar por el cumplimiento de la PSI y su normativa de desarrollo.

> Coordinar todas las actividades relacionadas con la seguridad de los sistemas de información.

> Velar porque la seguridad de la información sea parte del proceso de planificación del ISTAC.

> Cualquier otra actuación en materia de seguridad de la información que no corresponda específicamente a otro agente.

Delegado de Protección de Datos (DPD)

El ISTAC ha designado a su Servicio de Secretaría General como Delegado de Protección de Datos (DPD).

Las funciones principales del DPD (especificadas en el art. 39 RGPD) son las siguientes:

> Informar y asesorar al responsable (ISTAC) o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, de las obligaciones en materia de protección de datos.

> Supervisar el cumplimiento de la normativa aplicable en materia de protección de datos, y de las políticas del responsable del tratamiento (ISTAC) en dicha materia, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.

> Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación conforme al artículo 35 del RGPD.

> Cooperar con la autoridad de control, actuando como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa del artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

Unidad de Gestión de Datos

De conformidad con el art. 7.4 a) del Decreto 89/2023, de 25 de mayo, de régimen de gobierno y análisis de datos del Sistema Estadístico de Canarias, la Unidad de Gestión de Datos se constituye como un equipo de área responsable de la coordinación del nivel operativo. En ese sentido, el Decreto 65/2019, de 6 de mayo, por el que se establece el modelo de referencia para la coordinación, asistencia y transmisión del conocimiento de la actividad administrativa de la Administración Pública de la Comunidad Autónoma de Canarias y sus organismos públicos vinculados o dependientes establece la posibilidad de crear los Equipos

de Proyecto como grupos de trabajo constituidos por las personas adscritas a la ejecución de un proyecto. A efectos de la presente Política, cabe destacar los siguientes equipos que forman parte de dicha Unidad de Gestión de Datos, así como sus principales funciones.

> Equipo de proyecto de protección y seguridad de la información

- Coordinación en protección de datos personales: acciones vinculadas al gobierno de la protección de datos personales, asesorar a las personas responsables, encargadas o implicadas en tratamiento de datos personales).
- Coordinación en infraestructura TIC. Restaurar datos a partir de copias de seguridad y atención a incidencias de seguridad.
- Coordinación en secreto estadístico: acciones vinculadas al secreto estadístico y a la gestión de su protección.
- Coordinación en seguridad de la Información: gestionar y coordinar las actividades vinculadas al Esquema Nacional de Seguridad y establecer los niveles de seguridad de activos de datos estadísticos.

> Equipo de proyecto de acceso a datos

- Solicitar y recepcionar los ficheros de datos para fines estadísticos, así como de los documentos y metadatos necesarios para su interpretación y uso, que se soliciten para el desarrollo de la actividad estadística de interés de la Comunidad Autónoma de Canarias.
- Recepcionar los ficheros de datos para fines estadísticos que, desde cualquier consejería de la Administración Pública de la Comunidad Autónoma de Canarias, y organismos, entes o empresas dependientes de la misma, se deban remitir a otras administraciones y organismos del sector público.
- Elaborar y hacer cumplir los requisitos técnicos para la formación, conservación y actualización de ficheros administrativos que puedan ser utilizados con finalidad estadística.
- Conservar y custodiar la información obtenida como consecuencia de la actividad estadística, aunque se hayan difundido las estadísticas correspondientes.

> Equipo de proyecto de marco de calidad

- Coordinación las actuaciones necesarias para establecer un sistema de calidad de la actividad estadística.

Agentes sujetos a secreto estadístico

De conformidad con el artículo 66 del Decreto 89/2023, de 25 de mayo, de régimen de gobierno y análisis de datos del Sistema Estadístico de Canarias, se deberá crear un Registro de agentes sujetos al secreto estadístico, cuya finalidad es:

> La identificación de todas las personas físicas o jurídicas que por razón de su actividad tengan acceso a información protegida por el deber del secreto estadístico.

> La identificación del personal estadístico y la acreditación del personal estadístico funcionario con carácter de agente de la autoridad a los efectos procedentes.

> La acreditación e información pública del personal estadístico autorizado para solicitar información a las personas físicas y jurídicas obligadas a suministrar información para fines estadísticos.

Corresponde a los agentes sujetos a secreto estadístico las siguientes responsabilidades:

> Comunicar a las unidades informantes las normas que han de observar en la cumplimentación de los cuestionados, o de los documentos de similar naturaleza, y de las sanciones que podrán imponerse por su incumplimiento.

> Cumplir las normas técnicas aprobadas en materia de secreto estadístico.

> No difundir ni comunicar a personas no autorizadas datos individualizados amparados por el secreto estadístico.

> No comunicar datos a personas no obligadas a mantener el secreto estadístico, de forma que con ello se pueda deducir información confidencial sobre datos personales.

> No exigir información para la elaboración de estadísticas sin la existencia de las correspondientes normas reguladoras.

> No usar, para finalidades distintas de las propiamente estadísticas, datos personales obtenidos directamente de las unidades informantes.

8. Directrices de aplicación

Marco general de directrices

A continuación, se destacan las principales medidas en materia de protección de datos que los agentes del SEC deberán cumplir, en calidad de responsables del tratamiento.

> Legitimación de los tratamientos

Para tener la certeza de que el tratamiento que se vaya a realizar sobre los datos de carácter personal sea lícito, los agentes del SEC, en calidad de responsables del tratamiento, deberán, con carácter previo al tratamiento de datos que pretendan realizar, identificar la base jurídica que permita legitimar el citado tratamiento.

En el ámbito concreto del SEC, las principales bases de legitimación aplicables serán las siguientes:

- Consentimiento y consentimiento explícito

  En los casos en que la base jurídica de los tratamientos sea el consentimiento, éste deberá tener las características previstas por el RGPD, que exige que sea informado, libre, específico y otorgado por los afectados mediante una manifestación que muestre su voluntad de consentir o mediante una clara acción afirmativa.

  Asimismo, en el caso de los menores de 14 años (art. 7 LOPDGDD), se asegurará que se cuenta con el consentimiento de los padres o tutores legales del menor.

- Interés público y/u obligación legal

  En el ámbito del SEC la base jurídica que legitima la mayoría de los tratamientos será el cumplimiento de una tarea en interés público o el ejercicio de poderes públicos, así como el cumplimiento de una obligación legal. En ambos casos, debe existir una previsión normativa con rango de ley, además de estar, en el caso de los tratamientos estadísticos, asociados a actividades estadísticas previstas en los instrumentos de planificación estadística.

> Categorías especiales de datos

El RGPD incluye en el concepto de categorías especiales de datos los denominados datos especialmente protegidos como son las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, los que revelen el origen racial o étnico, y los relativos a la salud o a la vida u orientación sexual de una persona, así como los datos genéticos y los datos biométricos.

La regla general contemplada en el RGPD es la prohibición del tratamiento de categorías especiales de datos, salvo que concurra alguna de las excepciones a esta regla general previstas en el art. 9.2 RGPD. Dentro de dichas excepciones, cabe destacar el apartado j):

[...] el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

> Análisis de riesgos y evaluaciones de impacto

La gestión de riesgos, según la AEPD, se puede dividir en tres etapas diferenciadas[20]:

- La identificación de las amenazas (factores de riesgo concurrentes que, en caso de materializarse, puede provocar daños a los derechos de las personas interesadas) y de los riesgos (la combinación de la posibilidad de que se materialicen las amenazas previamente identificadas y sus consecuencias negativas). En la identificación y descripción de las amenazas y riesgos hay que considerar todo el ciclo de vida de los datos.

- La evaluación de los riesgos, que consiste en valorar el impacto (significativo o no) de la exposición a la amenaza, entendido como los posibles daños que se pueden producir si la amenaza se materializa, junto a la probabilidad de que esta se materialice).

- El tratamiento de los riesgos detectados.

El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto. El objetivo de tratar los riesgos es disminuir su nivel de exposición con medidas de control que permitan reducir la probabilidad y/o impacto de que estos se materialicen. El riesgo inherente se puede tratar con el objetivo de reducir o mitigar el mismo, en función de la medida que se adopte, hasta situar el riesgo residual en un nivel que se considere razonable.

Por otra parte, la EIPD es una herramienta con carácter preventivo que deberán realizar los agentes del SEC para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas.

[20] Se recomienda la lectura de la Guía de Análisis de Riesgos de la AEPD. Disponible en: https://www.aepd.es/documento/guia-analisis-de-riesgos-rgpd.pdf

> Protección de datos desde el diseño y por defecto

Dentro del ámbito del SEC se deberán tener en cuenta las siguientes medidas para garantizar la protección de datos desde el diseño y por defecto.

- Protección de datos desde el diseño

  Teniendo en cuenta que la fase del diseño del tratamiento es la que define el flujo de los datos personales, así como todos los elementos que intervendrán a lo largo del mismo, será en dicha fase en la que se deberán definir las medidas de control, de seguridad, técnicas y organizativas que resulten apropiadas para el tratamiento, a fin de cumplir los requisitos de la normativa aplicable.

  Dentro de las medidas recomendadas por la normativa aplicable, se encuentra la seudonimización, siendo este el tratamiento de datos de carácter personal, de manera que ya no puedan atribuirse a una persona sin utilizar información adicional. A colación de lo anterior, resulta muy importante destacar la diferencia que existe entre anonimización y seudonimizacion:

  - La información anónima es un conjunto de datos que no guarda relación con una persona física identificada o identificable y, por tanto, queda excluida del ámbito de aplicación del RGPD. Para ello, deberá poder demostrarse objetivamente que no existe capacidad material para asociar los datos anonimizados a una persona física determinada, directa o indirectamente, ya sea mediante el uso de otros conjuntos de datos, informaciones o medidas técnicas y materiales que pudieran existir a disposición de terceros.

  - Por el contrario, la información seudonimizada es un conjunto de datos que no puede atribuirse a una persona sin utilizar información adicional, requiere que dicha información adicional figure por separado y, además, esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable. Dado que, en este caso, con información adicional, sí sería posible identificar a las personas, este tratamiento de datos se produce bajo el ámbito del RGPD.

- Protección de datos por defecto

  Cada agente del SEC, en calidad de responsable del tratamiento, deberá implementar las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

  Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

> Comunicaciones de datos y transferencias internacionales de datos

En primer lugar, a priori existe un deber de colaboración entre las Administraciones públicas, por lo que la comunicación de datos entre los agentes del SEC y otras Administraciones Públicas sería lícita aun y cuando la finalidad ulterior pretendida sea diferente a la finalidad inicial por la que se recabaron los datos por la Administración cedente, siempre que exista una base de legitimación suficiente (obligación legal y/o interés público).

No obstante lo anterior, se habrá de estar a lo recogido en las normas especiales con respecto a la comunicación de datos. Si a la Administración cedente le fuese de aplicación una norma especial, se debería estar a lo recogido en esta.

En concreto, en el ámbito estadístico, de conformidad con lo dispuesto en el art. 25 LOPDGDD, la comunicación de los datos a los órganos competentes en materia estadística solo se entendería amparada en el cumplimiento de una misión realizada en interés público (art. 6.1 e) RGPD) cuando la estadística para la que se requiera la información venga exigida por una norma de Derecho de la Unión Europea o se encuentre incluida en los instrumentos de programación estadística legalmente previstos.

Asimismo, de conformidad con el principio de minimización de datos (art. 5.1 b) RGPD), la solicitud no podrá responder a un acceso masivo e indiscriminado a datos personales, debiendo ser siempre específico en cada caso ajustado a los datos que resulten precisos para la consecución de la finalidad. En el ámbito del SEC, la información que venga exigida por los instrumentos de planificación estadística, se entenderá legitimada en el ejercicio de una misión realizada en interés público.

En cualquier caso, resultará necesario analizar cada supuesto normativo concreto, en aras a verificar que los procedimientos seguidos no contravengan la normativa en materia de protección de datos de carácter personal.

Por otra parte, cuando los datos personales se envían fuera del ámbito del Espacio Económico Europeo, se produce una transferencia internacional de datos, en cuyo caso los agentes del SEC deberán cumplir con los requisitos del RGPD para poder ser legítima.

Si bien, con carácter general, en el ámbito del SEC no se producen transferencias internacionales de datos, en caso de producirse, se deberán tener en cuenta las posibles implicaciones internacionales, debiendo las transferencias internacionales llevarse a cabo sobre la base de los adecuados instrumentos previstos por la normativa aplicable[21].

[21] Para mayor información al respecto, consultar el siguiente enlace: https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/garantias-transferencias-datos-personales

> Cumplimiento del deber de información (arts. 13 y 14 RGPD)

Cada agente del SEC, como responsable del tratamiento, cuando vaya a tratar datos de carácter personal, deberá cumplir con la obligación de transparencia e información que exige la normativa aplicable en materia de protección de datos, así como en materia estadística.

Para ello, se empleará el sistema de información por capas, el cual está compuesto por una información más sencilla o básica en un primer nivel (primera capa), de forma resumida, en el mismo momento y en el mismo medio en que se recojan los datos, y una información adicional en un segundo nivel (segunda capa), donde se presentará detalladamente el resto de la información, en un medio más adecuado para su presentación, comprensión y, si así se estima, archivo.

> Atención de los derechos de las personas interesadas (arts. 15 a 22 RGPD)

Las personas interesadas, como titulares de sus datos, podrán ejercitar ante el agente del SEC correspondiente, los derechos de acceso, rectificación, supresión ("derecho al olvido"), oposición y limitación al tratamiento de los mismos, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos.

Por otra parte, se podrán denegar las solicitudes de ejercicio de los derechos establecidos en los artículos 15 a 22 del RGPD cuando los datos se encuentren amparados por las garantías del secreto estadístico previstas en la legislación estatal o autonómica.

En caso de recibir una solicitud de ejercicio de derechos en materia de protección de datos, se deberá responder en el plazo máximo de un mes, pudiendo prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes, si bien se deberá informar a la persona interesada de la citada prórroga en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación.

Si la persona interesada presentase la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que dicha persone solicite que se facilite de otro modo.

> Medidas de seguridad (art. 32 RGPD)

Cada agente del SEC debe dispone de un listado de medidas de seguridad técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo en función del estado de la técnica, los costes de aplicación y, la naturaleza, el alcance, el contexto y los fines de los tratamientos realizados, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas.

Asimismo, se deberá emplear el Esquema Nacional de Seguridad (ENS) para seleccionar las medidas que deban implantarse para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos.

> Encargos de tratamiento (art. 28 RGPD)

Cada agente del SEC, en su calidad de responsable del tratamiento, podrá designar a terceros como encargados del tratamiento. Todo encargo de tratamiento de datos personales deberá formalizarse mediante un contrato o acto jurídico equivalente conforme al artículo 28 del RGPD. Este contrato establecerá las obligaciones específicas y responsabilidades del encargado en relación con el tratamiento de datos personales, el cual estará estrictamente limitado a las instrucciones proporcionadas por el responsable del tratamiento.

Las obligaciones contractuales incluirán, entre otras, las siguientes:

- Tratar los datos personales únicamente según las instrucciones indicadas y para los fines específicos establecidos en el contrato.
- Implementar medidas de seguridad adecuadas en función de los riesgos asociados al tratamiento y el tipo de datos, de acuerdo con el artículo 32 del RGPD y el ENS.
- Asegurar la confidencialidad de los datos personales y prohibir su divulgación a terceros sin la autorización expresa del responsable del tratamiento.

> Medidas orientadas a la protección de la privacidad por uso de Inteligencia Artificial (IA)

Si los agentes del SEC empleasen sistemas de Inteligencia artificial (IA) y/o modelos de datos sintéticos, deberán cumplir con la normativa aplicable para garantizar que el desarrollo y uso de estas tecnologías respeten los derechos de las personas interesadas. En ningún caso se podrán desarrollar o utilizar sistemas que estén prohibidos normativamente, o estén clasificados como de alto riesgo.

Para ello, cada sistema de IA será sometido, con carácter previo a su implementación, a un sistema de gestión de riesgos, que deberá ser documentado.

Asimismo, el agente del SEC deberá garantizar que los conjuntos de datos utilizados en el desarrollo del sistema de IA, incluidos el entrenamiento, la validación y la prueba, han sido y serán sometidos a una gestión de datos adecuada al contexto de uso, así como a la finalidad prevista del sistema de IA. Del mismo modo, el agente del SEC adoptará procedimientos para detectar y corregir sesgos durante el entrenamiento y la implementación de modelos.

Cuando sea viable, se priorizará el uso de datos sintéticos para entrenamiento y pruebas de los sistemas de IA, especialmente cuando los datos reales puedan comprometer la privacidad de las personas. Los datos sintéticos corresponden a aquellos datos que, en lugar de ser reales, corresponden a datos generados artificialmente, si bien deberán preservar las características y propiedades de los datos reales para un caso de uso específico. Por tanto, los datos sintéticos deben generarse de manera que imiten las características estadísticas de los datos reales, sin permitir la identificación directa o indirecta de las personas. Los datos sintéticos empleados en los sistemas de IA deberán cumplir con requisitos de integridad y representatividad para que los resultados obtenidos sean fiables y consistentes con el contexto real en el que se implementarán.

Toda documentación relacionada con el sistema de IA, incluidos los riesgos detectados, las medidas de mitigación adoptadas y los resultados de auditorías previas, será mantenida y actualizada para asegurar un registro completo del ciclo de vida del sistema de IA.

> Cumplimiento del secreto estadístico

Los agentes del SEC deberán velar por el cumplimiento de los principios de confidencialidad y secreto estadístico. Para ello, dispondrán de las medidas organizativas y técnicas necesarias que garanticen la protección de la información en todos los procesos estadísticos, tales como el uso de tecnologías avanzadas, técnicas de anonimización, formación, protocolos que limiten el acceso y manipulación de los datos o el Registro de agentes sujetos a secreto estadístico, entre otras.

La difusión de los resultados estadísticos y la transparencia de la actividad estadística pública son principios fundamentales en el ámbito del SEC. En este sentido, es imprescindible garantizar la implementación de técnicas de control de divulgación estadística adecuadas que protejan la privacidad y seguridad de los datos en todas las fases del proceso de divulgación y, con ello, el secreto estadístico.

El deber de colaboración, según lo dispuesto en la Ley 1/1991, de 28 de enero, de estadística de la Comunidad Autónoma de Canarias, obliga a las unidades estadísticas a proporcionar datos veraces y completos cuando se soliciten para actividades estadísticas que figuren en los instrumentos de planificación estadística. En estos casos, los agentes del SEC deben garantizar la protección de la información suministrada mediante la aplicación del deber de secreto estadístico.

> Garantías necesarias para la comunicación y la cesión altruista de datos

En el ámbito del SEC se deben articular los protocolos necesarios que permitan ejercer el derecho de renuncia a la protección del secreto estadístico y el cumplimiento en lo relativo a la cesión altruista de datos dispuesto en el Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos, o normativa que lo sustituya.

> Reutilización de datos estadísticos protegidos

En el ámbito del SEC se deben establecer procedimientos que faciliten la reutilización de datos estadísticos protegidos con el fin de apoyar proyectos públicos de ciencias de datos siempre que se respete la confidencialidad, el secreto estadístico y la protección de los datos. Todo ello, con el objetivo de promover iniciativas que contribuyan al bien público o mejora del gobierno público.

Directrices específicas aplicables

> **Directriz 0:** La protección del secreto estadístico se debe contemplar desde el diseño de las actividades estadísticas y en todos sus procesos asociados.

> **Directriz 1:** Cada actividad estadística incluida en los instrumentos de planificación estadística deben disponer, si procediera, de su correspondiente registro como actividad de tratamiento de datos personales para fines estadísticos.

> **Directriz 2:** Cada tratamiento de datos personales para fines estadísticos debe disponer de su correspondiente análisis de riesgos y, si procede, su evaluación de impacto sobre derechos y libertades.

> **Directriz 3:** En las entrevistas directas de encuestas y censos se debe informar sobre, al menos, sobre los siguientes preceptos:

- Información obligatoria de acuerdo con la normativa estadística
    - La naturaleza, características y finalidad de la actividad estadística pública que se realiza.
    - La obligatoriedad, en su caso, de colaborar.
    - Las sanciones que pudieran imponérsele por el incumplimiento de las obligaciones recogidas en la normativa estadística.
    - La protección que le dispensa el secreto estadístico.
- Identificación e información sobre el registro de la actividad de tratamientos de datos personales de la actividad estadística pública que ampara la recogida de datos.

> **Directriz 4:** Cuando los datos requieran del consentimiento de las unidades de observación para su tratamiento ulterior con fines estadísticos, el órgano responsable del tratamiento de los datos o titular de los mismos informará y recabará el consentimiento libre, expreso e inequívoco de las unidades de observación para la comunicación de sus datos al correspondiente agente del SEC con fines estadísticos.

> **Directriz 5:** Los agentes competentes para el ejercicio de la función estadística pública del SEC podrán denegar las solicitudes de ejercicio por los afectados de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 cuando los datos se encuentren amparados por las garantías del secreto estadístico previstas en la legislación estatal o autonómica.

> **Directriz 6:** En las actividades estadísticas de directorios para fines estadísticos las unidades de observación tienen el derecho de acceso y de rectificación.

> **Directriz 7:** En el caso de tratamientos de datos de menores y personas con discapacidad, se precisará de la adopción de las medidas y salvaguardas adicionales adecuadas. Además, si el consentimiento fuese la base de legitimación del tratamiento en el caso de los menores de 14 años (art. 7 LOPDGDD), se asegurará que se cuenta con el consentimiento de los padres o tutores legales del menor.

> **Directriz 8:** En las actividades estadísticas se deben recoger únicamente los datos que sean necesarios para su realización, en aplicación del principio de minimización de datos personales.

> **Directriz 9:** El acceso a datos de titularidad pública para fines estadísticos se realizará por medios electrónicos, de forma segura e interoperable y utilizando entornos cerrados de comunicación. Se

facilitará el acceso especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad.

> **Directriz 10:** En el banco de datos internos de la Infraestructura de Datos y Metadatos Estadísticos de Canarias (eDatos) deben aplicarse medidas de seudonimización de datos, encriptado y control de acceso.

> **Directriz 11:** En la difusión de resultados estadísticos se debe asegurar la anominización de datos de las unidades de observación en aplicación del secreto estadístico.

> **Directriz 12:** Las unidades de observación tienen el derecho a renunciar a la anonimización de datos protegidos por el secreto estadístico.

> **Directriz 13:** La protección del secreto estadístico expira cuando hayan transcurrido al menos veinticinco años desde la muerte de la unidad de observación o cincuenta años desde el suministro de la información.

> **Directriz 14:** La reutilización de datos protegidos por secreto estadístico para fines científicos se debe fundamentar en los principios de datos seguros, proyectos seguros, personas seguras, entornos seguros y resultados seguros (*Five Safes model*).

> **Directriz 15:** El personal estadístico debe estar inscrito en el Registro de agentes sujetos a secreto estadístico.

> **Directriz 16:** El Instituto Canario de Estadística establecerá para cada operación estadística las integraciones permitidas de datos procedentes de diferentes fuentes.

> **Directriz 17:** El Instituto Canario de Estadística actuará como un tercero de confianza en la integración de datos para fines estadísticos o de investigación estadística de la Comunidad Autónoma de Canarias. En el ejercicio de integrador de confianza se aplicarán métodos de vinculación de registros con preservación de la privacidad y protección de datos de carácter personal.

> **Directriz 18:** Los agentes del SEC deben asegurarse de regular la relación con los proveedores y/o entidades que vayan a tratar y/o acceder a datos de carácter personal por cuenta del agente (en calidad de encargados del tratamiento), mediante la suscripción de Acuerdos de Encargo de Tratamiento, todo ello de conformidad con lo dispuesto en la normativa aplicable en materia de protección de datos.

> **Directriz 19:** Los agentes del SEC establecerán y aplicarán condiciones específicas para responder a solicitudes de cesión de datos por parte de terceros de información estadística, en cumplimiento con la normativa aplicable.

> **Directriz 20:** Los datos sintéticos deben generarse de manera que imiten las características estadísticas de los datos reales, sin permitir la identificación directa o indirecta de las personas.

> **Directriz 21:** Los contratos que impliquen el uso de sistemas y/o modelos de IA, deberán incluir clausulado específico que garantice el cumplimiento de la normativa aplicable.

Cuadro resumen de directrices generales y específicas

Cada agente del SEC debe establecer los roles y responsabilidades sobre las directrices generales y específicas, de acuerdo con su estructura y organización, en relación con esta Política.

A continuación, se especifican los roles y responsabilidades del ISTAC en relación con las directrices generales y específicas relacionadas con la protección de datos y la cesión altruista de datos.

Directriz general	Directrices específicas relacionadas	Roles y responsabilidades
Legitimación de los tratamientos	Directrices 1, 4 y 7	**DPD:** asesorar sobre el cumplimiento de la normativa en relación con la protección de datos personales y verificar la base legal de los tratamientos. **Equipo de proyecto de protección y seguridad de la información:** gestionar la coordinación en materia de protección de datos personales.
Categorías especiales de datos	Directrices 1, 7 y 8	**Responsable de la información y del servicio:** determinar la seguridad necesaria para el tratamiento de los datos sensibles. **DPD**: supervisar el cumplimiento normativo en el tratamiento de categorías especiales de datos. **Equipo de proyecto de protección y seguridad de la información:** gestionar la coordinación en seguridad y protección de datos sensibles. **Agentes sujetos a secreto estadístico**: implantar la adopción de medidas y salvaguardas en las actividades estadísticas con categorías especiales de datos.
Análisis de riesgos y evaluaciones de impacto (EIPD)	Directriz 2	**Comité para la Gestión y Coordinación de la Seguridad de la Información:** revisar y aprobar los análisis de riesgos y EIPD. **DPD:** asesorar en la realización de los análisis de riesgos y las evaluaciones de impacto de protección de datos. **Equipo de proyecto de protección y seguridad de la información:** coordinar los análisis de riesgos y EIPD.

Protección de datos desde el diseño y por defecto	Directrices 0, 8 y 10	**Responsable de la información y del servicio:** implementar medidas de seguridad en la fase de diseño de los sistemas. **DPD:** revisar y asesorar sobre la aplicación de la privacidad desde el diseño y por defecto. **Equipo de proyecto de protección y seguridad de la información:** coordinar la formación a las personas responsables, encargadas o implicadas en la protección de datos desde el diseño y por defecto. **Agentes sujetos a secreto estadístico**: implantar en las actividades estadística la protección de datos desde el diseño y por defecto.
Comunicaciones de datos y transferencias internacionales de datos	Directrices 9 y 17	**DPD:** asesorar y verificar el cumplimiento normativo sobre las comunicaciones y transferencias de datos. **Equipo de proyecto de acceso a datos:** coordinar las solicitudes, aprovisionamiento y gestión de los datos para fines estadísticos, asegurando que se cumpla la normativa aplicable.
Cumplimiento del deber de información	Directriz 3	**DPD**: asegurar que las personas están informadas sobre el tratamiento de sus datos. **Equipo de proyecto de protección y seguridad de la información:** coordinar acciones de comunicación y transparencia en protección de datos. **Agentes sujetos a secreto estadístico**: cumplir en las actividades estadísticas con el deber de información.
Atención a los derechos de las personas interesadas	Directrices 5 y 6	**DPD:** gestionar los derechos de las personas interesadas (acceso, rectificación, supresión, etc.). **Agentes sujetos a secreto estadístico**: atender a las unidades de observación en su derecho de acceso y rectificación en las actividades de directorios para fines estadísticos.
Medidas de seguridad	Directrices 10, 11, 14, 15, 16, 17 y 20	**Comité para la Gestión y Coordinación de la Seguridad de la Información:** impulsar medidas para mejorar y reforzar los sistemas de seguridad y control, coordinar las decisiones y actuaciones de la persona responsable de seguridad, etc. **Responsable de la información y del servicio:** establecer las necesidades de seguridad de la información y determinar los requisitos de seguridad. **Equipo de protección de datos y seguridad de la información:** coordinar la organización de actividades relacionadas con la seguridad de la información, gestionando y coordinado tareas

		vinculadas al Esquema Nacional de Seguridad y estableciendo niveles de seguridad para los activos de datos estadísticos. Agentes sujetos a secreto estadístico: implantar en la difusión de resultados estadísticos la anonimización de datos de las unidades de observación en aplicación del secreto estadístico.
Encargos de tratamiento	Directriz 18	DPD: asesorar y supervisar el cumplimiento de la normativa en materia de protección de datos en relación con los encargados de los tratamientos (proveedores y/o entidades). Equipo de proyecto de protección y seguridad de la información: coordinar las actividades de los encargados externos que acceden y/o tratan datos personales o en custodia bajo el secreto estadístico.
Medidas orientadas a la protección de la privacidad por uso de IA	Directriz 20 y 21	DPD: asesorar en la realización de los contratos que implique el uso de sistemas y/o modelos de IA. Equipo de proyecto de protección y seguridad de la información: coordinar la elaboración del clausulado específico que debe ser incluido en los contratos que impliquen el uso de sistemas y/o modelos de IA. Agentes sujetos a secreto estadístico: implantar medidas orientadas a la protección de la privacidad por uso de IA.
Cumplimiento del secreto estadístico	Directrices 0, 3, 10, 11, 13, 15 y 16	Equipo de proyecto de marco de calidad: coordinación de las actuaciones necesarias para establecer un sistema de calidad de la actividad estadística. Equipo de proyecto de protección y seguridad de la información: coordinar acciones vinculadas al secreto estadístico y a la gestión de su protección. Registro de agentes sujetos a secreto estadístico: identificar a las personas autorizadas para acceder y tratar la información protegida con finalidad estadística.
Garantías necesarias para la comunicación y la cesión altruista de datos	Directriz 12 y 19	Responsable de la información y del servicio: establecer las necesidades de seguridad de la información y determinar los requisitos de seguridad. DPD: supervisar y verificar que las renuncias al secreto estadístico y las cesiones de datos cumplen con la normativa de secreto estadístico y de protección de datos.

		Equipo de proyecto de acceso a datos: coordinar el aprovisionamiento y gestión del acceso a los datos cedidos para fines estadísticos. **Agentes sujetos a secreto estadístico**: implantar en las actividades estadísticas las garantías necesarias para la comunicación y la cesión altruista de datos.
Reutilización de datos	Directriz 14	**DPD:** supervisar el cumplimiento de la normativa en materia de reutilización y protección de datos. **Equipo de proyecto de acceso a datos:** coordinar el actuaciones necesarias para el cumplimiento de los requisitos para la cooperación en ciencia de datos dentro de entornos de tratamiento seguros.

9. Concienciación y formación

Los agentes del SEC implementarán un programa de concienciación y formación integral que debe contemplar la comunicación y difusión de la propia Política. Este programa debe entenderse como una actividad continua, que ha de repetirse y revisarse periódicamente, de forma que se adapte a los cambios que puedan surgir en materia de protección de datos y cesión altruista de datos dentro del ámbito de la estadística pública.

Así, las actividades de concienciación y formación se ajustarán a las necesidades de los distintos perfiles de usuarios y se actualizarán de forma continua para reflejar los cambios normativos, técnicos y/o procedimentales.

Públicos objetivos y perfiles de formación

El plan de formación diferenciará, al menos, entre los siguientes perfiles de destinatarios, adaptando los contenidos y los medios a cada uno de ellos.

> Personal interno: plantilla de la entidad u organismo, con énfasis en aquellas que gestionan o acceden regularmente a datos personales o estadísticos sensibles.

> Personal técnico: personal interno o personal colaborador externo cuya función está directamente relacionada con el tratamiento, análisis o manejo de datos y que necesiten conocimientos específicos sobre protección de datos, privacidad y secreto estadístico.

> Personal colaborador: personal colaborador externo que deba conocer los aspectos básicos de la normativa y los riesgos asociados al uso y cesión de los datos dentro del ámbito de la estadística pública.

Programa de formación

El programa de formación, para asegurar que todo el personal (interno y externo) mantenga un conocimiento adecuado de las normas y buenas prácticas incluirá, como mínimo, los siguientes elementos:

> Formación para personas recién incorporadas.

> Formación continua y de actualización.

> Videos explicativos (píldoras formativas).

> Materiales de referencia y concienciación (procedimientos, guías, manuales, cursos, bibliografía, etc.).

Por otro lado, el programa de formación deberá adaptarse al público objetivo, pero sin perder de vista que los contenidos deben cubrir aspectos que pueden ayudar al cumplimiento de las directrices establecidas en la Política.

Canales de comunicación y sensibilización

Para promover una cultura de protección de datos y cesión altruista de datos, los agentes del SEC desarrollarán campañas de sensibilización utilizando diversos medios, de acuerdo con su estructura, organización y recursos, tales como:

- Avisos, correos electrónicos y boletines informativos.
- Buzón de sugerencias.
- Encuestas al personal.

Evaluación y seguimiento

Los agentes del SEC llevarán a cabo evaluaciones periódicas de su programa de formación y sensibilización, adaptándolo continuamente a los cambios normativos y tecnológicos. Para ello, se realizarán:

> Reuniones valorativas periódicas: encuentros regulares con cada área para evaluar el impacto del programa y recoger los comentarios del personal.

> Revisión y mejora continua: análisis de los resultados de las encuestas y comentarios del buzón de sugerencias, con el fin de optimizar los materiales y las metodologías de capacitación.

Con estas acciones, se busca consolidar el cumplimiento de la normativa, así como promover el compromiso ético entre las personas vinculadas a la actividad estadística dentro del SEC, asegurando un uso responsable, seguro y respetuoso de los datos personales y estadísticos.

10. Indicadores de seguimiento

Para garantizar que la Política se mantiene actualizada y está alineada, en todo momento, con los objetivos del SEC, cada agente debe establecer los procedimientos de seguimiento y revisión periódica que mejor se ajusten a su entidad u organismo, en función de su estructura y recursos.

Con el fin de que todos los agentes del SEC estén alineados se definirán indicadores de seguimiento dentro de las siguientes categorías:

> Implantación de la Política.

> Cumplimiento de las directrices.

> Concienciación y formación.

> Medidas técnicas, administrativas y organizativas.

11. Normativa y referencias bibliográficas

Normativa europea

> Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos).

> Reglamento no 557/2013 de la Comisión por el que se aplica el Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo, relativo a la estadística europea, en lo que respecta al acceso a datos confidenciales con fines científicos, y por el que se deroga el Reglamento (CE) no 831/2002. Directiva 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos.

> Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (RGPD).

> Directiva 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos.

> 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.

Normativa nacional

> Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

> Ley 12/1989, de 9 de mayo, reguladora de la Función Estadística Pública.

> Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

> Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Normativa autonómica

> Ley 1/1991, de 28 de enero, de estadística de la Comunidad Autónoma de Canarias.

> Decreto 89/2023, de 25 de mayo, de régimen de gobierno y análisis de datos del Sistema Estadístico de Canarias.

Marco ético

> Principios fundamentales de las estadísticas oficiales (Naciones Unidas).

> Código de buenas prácticas de las estadísticas europeas (Eurostat).

> Declaración sobre ética profesional (Instituto Internacional de Estadística).

Marco general de protección de datos

> Comité Europeo de Protección de Datos

> Agencia Española de Protección de Datos (AEPD)

- Orientaciones para tratamientos que implican comunicación de datos entre Administraciones Públicas ante el riesgo de brechas de datos personales.

- Garantías para las transferencias de datos personales a terceros países u organizaciones internacionales
- Gestión del riesgo y evaluación de impacto en tratamientos de datos personales.
- Guía de protección de datos por defecto.
- Herramienta EVALÚA RIESGO
- Lista de tratamientos que no requieren EIPD
- Lista de tratamientos que sí requieren EIPD
- Orientaciones y garantías en los procedimientos de anonimización de datos personales
- Tecnologías y protección de datos en las Administraciones Públicas.

> Comité Europeo de Innovación en materia de Datos

Marco específico de protección de datos recogidos con fines estadísticos

> Oficina de Estadística de la Unión Europea (Eurostat)

- Código de buenas prácticas de estadísticas europeas
- Manual de control de divulgación estadística
- Marco de garantía de calidad

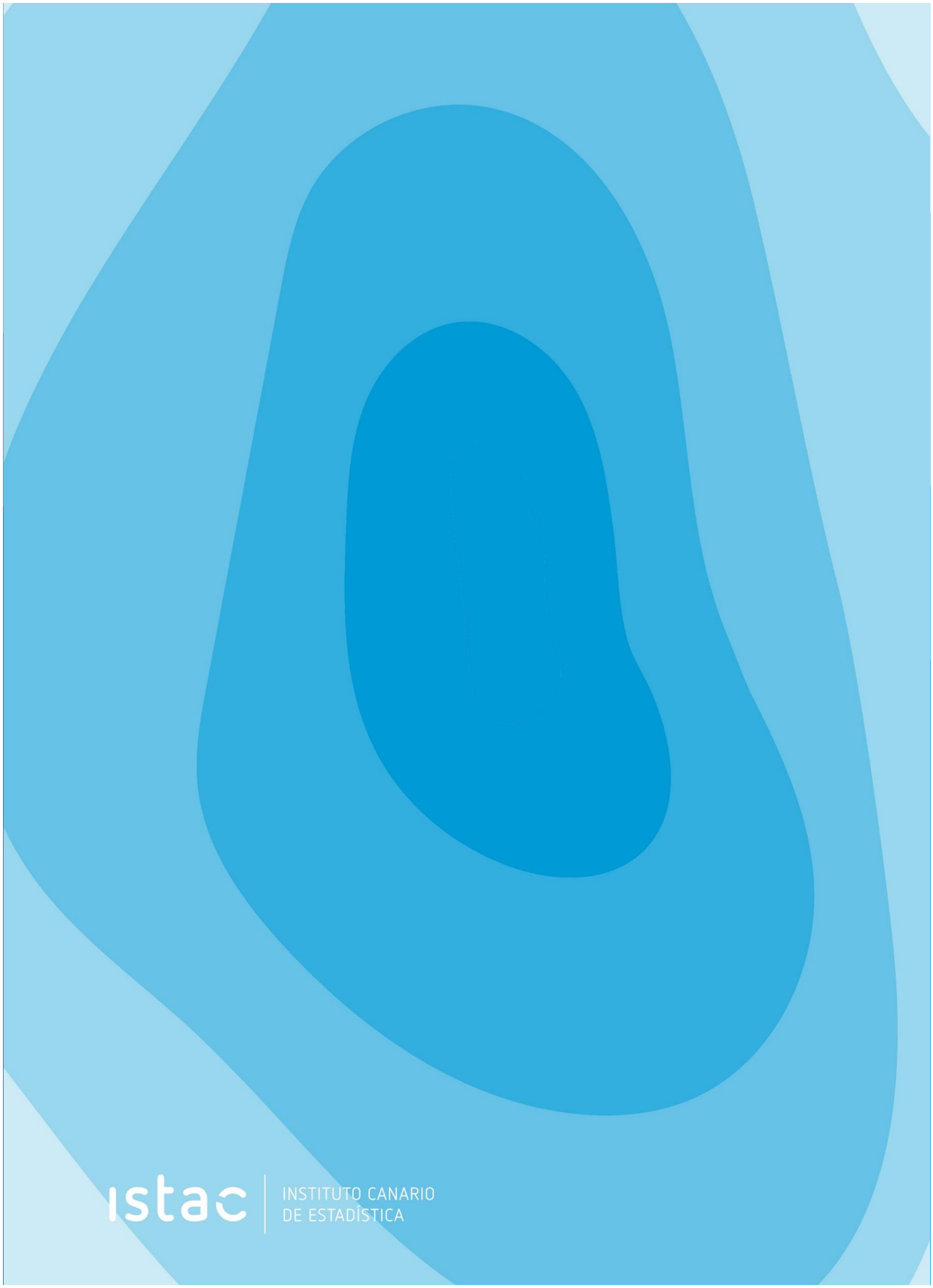
> Centro de excelencia en control de divulgación estadística

> Comisión Económica para Europa y División de Estadísticas de Naciones Unidas (UNECE y UNSD)

- Gestión de la confidencialidad estadística y acceso a microdatos. Principios y directrices de buenas prácticas
- Manual para la gestión y organización de los sistemas estadísticos nacionales
- Principios y directrices sobre los aspectos de confidencialidad en la integración de datos para fines estadísticos o propósitos de investigación relacionados

> Guías de conservación y difusión de datos (International Household Survey Network, IHSN)

> Manual de control de divulgación estadística de resultados (Safe Data Access Professionals, SDAP)


istac
INSTITUTO CANARIO
DE ESTADÍSTICA