1. OBJETIVO

Establecer las disposiciones para la designación, desempeño y funciones del Oficial de Datos Personales, de conformidad con lo dispuesto en los artículos 37, 38 y 39 del Reglamento de la Ley de Protección de Datos Personales, Ley N° 29733, aprobado por el Decreto Supremo N° 016-2024-JUS.

2. BASE LEGAL

2.1. Constitución Política del Perú.
2.2. Ley N° 29733, Ley de Protección de Datos Personales.
2.3. Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
2.4. Decreto Supremo N° 29-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
2.5. Decreto Supremo N° 016-2024-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.

3. ALCANCE

Las disposiciones contenidas en la presente directiva son de cumplimiento obligatorio para:

3.1 Las entidades de la administración pública, señaladas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley de Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 004-2019-JUS.

3.2 Las personas jurídicas de derecho privado que se encuentren obligadas, de acuerdo a lo dispuesto por el Decreto Supremo N° 016-2024-JUS, que aprueba el Reglamento de la Ley de Protección de Datos Personales, Ley N° 29733, en lo que corresponda.

3.3 Las empresas bajo el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE), incluyendo al propio fondo, las cuales deberán designar a un Oficial de Datos Personales por cada empresa adscrita.

4. DEFINICIONES Y SIGLAS

Para efectos de la presente directiva se consideran las siguientes definiciones y siglas:

4.1. Definiciones

N°	Término	Definición
1	**Actividad principal**	Se dice de aquella desarrollada por una entidad pública, organización o empresa que se encuentra incorporada dentro de su objeto social, se caracteriza por ser aquella que genera su principal fuente de ingresos o que resulta esencial para el cumplimiento de su misión institucional.
2	**Autoridad Nacional de Protección de Datos Personales**	Es la autoridad ejercida por el Ministerio de Justicia y Derechos Humanos a través de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales en mérito a lo dispuesto por la Ley N° 29733, Ley de Protección de Datos Personales, la Ley N° 29809, Ley de Organización y Funciones del Ministerio de Justicia y Derechos Humanos y el Decreto Supremo N° 013-2017-JUS, que aprueba el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.
3	**Banco de datos personales**	Es el conjunto de datos de personas naturales computarizado o no, y estructurado conforme a criterios específicos, que permita acceder sin esfuerzos desproporcionados a los datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica.
4	**Datos biométricos**	Datos personales obtenidos mediante un tratamiento técnico específico relativo a propiedades biológicas, físicas, fisiológicas o conductuales de una persona natural, que permiten o confirman su identificación unívoca, como imágenes faciales o datos dactiloscópicos.
5	**Datos genéticos**	Datos personales obtenidos del análisis de muestras biológicas que revelan las características genéticas, heredadas o adquiridas de una persona y que permiten conocer información única sobre su identidad o salud.

N°	Término	Definición
6	**Datos sensibles**	Es aquella información relativa a datos genéticos o biométricos de la persona natural, datos neuronales, datos morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la afiliación sindical, salud física o mental u otras análogas que afecten su intimidad.
7	**Empresa**	Persona natural o jurídica que realiza actividades económicas con fines de lucro, incluyendo la producción, prestación o comercialización de bienes y servicios, incluyendo aquellas empresas en las que el Estado participa de forma directa o indirecta.
8	**Encargado de tratamiento de datos personales**	Es la persona natural, persona jurídica de derecho privado o entidad pública que realiza tratamiento de datos personales, por cuenta u orden del responsable de tratamiento o titular del banco de datos personales.
9	**Entidad pública**	Es toda entidad comprendida en el artículo I de Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley de Procedimiento Administrativo General, aprobado por Decreto Supremo N° 004-2019-JUS.
10	**Evaluación de impacto**	Es un mecanismo preventivo derivado del principio de responsabilidad proactiva que tiene por propósito examinar la conveniencia de adoptar determinadas medidas legales, técnicas y organizativas a partir de las operaciones de tratamiento de datos personales previstas de realizar por determinado titular de banco de datos personales, responsable o encargado de tratamiento de datos personales.
11	**Grupo empresarial**	Es el conjunto de personas jurídicas, nacionales o extranjeras conformado por al menos dos integrantes, donde alguno de ellos ejerce el control sobre el otro u otros, o cuando el control sobre las personas jurídicas corresponde a una o varias personas naturales que actúan de manera conjunta como una unidad de decisión.
12	**Incidente de seguridad de datos personales**	Es toda vulneración de la seguridad que ocasione o tenga la capacidad de ocasionar la destrucción, pérdida, alteración ilícita de los datos personales o la comunicación o exposición no autorizada a dichos datos.
13	**Mediana empresa**	Es la empresa con ventas anuales superiores a 1700 unidades impositivas tributarias (UIT) hasta 2300 unidades impositivas tributarias (UIT).

N°	Término	Definición
14	**Micro empresa**	Es la empresa con ventas anuales hasta 150 unidades impositivas tributarias (UIT).
15	**Obligado a la designación del Oficial de Datos Personales**	Es el titular del banco de datos personales, el responsable o el encargado del tratamiento de datos personales que, por mandato del artículo 37.1 del Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales, debe designar a un Oficial de Datos Personales. Esta obligación alcanza a toda entidad, organización o empresa, ya sea respecto de los datos que gestione internamente o de aquellos que trata por encargo de terceros, con independencia del servicio que brinde.
16	**Oficial de Datos Personales**	Es la persona designada por el titular de banco de datos personales, responsable o encargado del tratamiento, para la verificación, asesoramiento e implementación del cumplimiento del régimen jurídico sobre protección de datos personales.
17	**Organización**	Es la categoría empleada por la presente Directiva para denominar a los sujetos obligados a designar un Oficial de Datos Personales que no constituyen entidades públicas ni empresas. Entre ellas están, los organismos no gubernamentales sin fines de lucro que hacen tratamientos de datos personales.
18	**Pequeña empresa**	Es la empresa con ventas anuales superiores a 150 unidades impositivas tributarias (UIT) y hasta el monto máximo de 1700 unidades impositivas tributarias (UIT).
19	**Perjuicio evidente a derechos y libertades del titular del dato**	Menoscabo manifiesto y verificable al contenido de los derechos y libertades reconocidos en la Constitución, Ley o norma infra legal a una persona natural, titular del dato personal, ocasionado por el tratamiento no autorizado, ilegal o incorrecto de sus datos personales.
20	**Privacidad desde el diseño y por defecto**	Medidas proactivas de naturaleza tecnológica, organizacional, humana o procedimental que se adoptan desde la concepción, diseño y posterior tratamiento de datos personales con el fin de proteger la privacidad de la persona y asegurar el cumplimiento de la normativa de protección de datos personales en todas las fases del ciclo de vida del tratamiento, estableciendo que, por defecto, solo se traten datos estrictamente necesarios para cada finalidad.
21	**Registro Nacional de Protección de Datos Personales**	Es el registro administrativo, creado por el artículo 34 de la Ley N° 29733, Ley de Protección de Datos Personales, y que tiene por finalidad la inscripción de los bancos de datos personales de administración pública o privada, las

N°	Término	Definición
		comunicaciones de flujo transfronterizo de datos personales y las sanciones, medidas cautelares o correctivas impuestas por la Autoridad Nacional de Protección de Datos Personales.
22	**Responsable de tratamiento de datos personales**	Es la persona natural, persona jurídica de derecho privado o entidad pública que decide sobre la finalidad y medios del tratamiento de datos personales. Esta definición no se restringe al titular del banco de datos, sino que incluye a cualquier persona que decida sobre el tratamiento de datos personales, aun cuando no se encuentre en un banco de datos personales.
23	**Titular de banco de datos personales**	Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.
24	**Tratamiento de datos personales**	Es cualquier operación o conjunto de operaciones, automatizados o no, que se realicen sobre los datos personales o conjuntos de datos personales.

4.2. Siglas

N°	Término	Siglas
1	Autoridad Nacional de Protección de Datos Personales	ANPD
2	Banco de Datos Personales	BDP
3	Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales	DGTAIPD
4	Ley de Protección de Datos Personales	LPDP
5	Ministerio de Justicia y Derechos Humanos	MINJUSDH
6	Oficial de Datos Personales	ODP
7	Registro Nacional de Protección de Datos Personales	RNPDP
8	Reglamento de la Ley de Protección de Datos Personales	RLPDP
9	Titular de Banco de Datos Personales	TBDP
10	Titular del Dato Personal	TDP

5. RESPONSABILIDADES

5.1. La DGTAIPD, en ejercicio de las facultades conferidas por el inciso i) del artículo 33 de la LPDP, es responsable de emitir directivas, lineamientos y otros instrumentos normativos de carácter técnico y especializado, orientados a garantizar la adecuada implementación de la normativa sobre protección de datos personales en los sectores público y privado.

5.2. La DGTAIPD, en tanto ejerce la ANPD conforme a lo dispuesto en el artículo 32 de la LPDP, tiene la responsabilidad de implementar y actualizar, la presente Directiva; así como velar por el cumplimiento de las disposiciones establecidas.

5.3. Los ODP y los obligados a su designación, cumplen obligatoriamente las disposiciones de la Directiva.

6. DISPOSICIONES GENERALES

6.1. La Directiva contribuye con los sujetos obligados, en el entendimiento y cumplimiento de las obligaciones de la LPDP y el RLPDP relativas al ODP; garantiza la protección de los derechos fundamentales vinculados al tratamiento de datos personales, y promueve la correcta implementación y observancia de la normativa vigente.

6.2. La actuación de los ODP garantiza la observancia de los principios de legalidad, finalidad, proporcionalidad, seguridad, transparencia y responsabilidad proactiva, entre otros previstos en la LPDP y su Reglamento.

6.3. La función de los ODP tiene un carácter técnico especializado, orientada a la asesoría, supervisión y coordinación interna dentro de las entidades públicas, organizaciones o empresas en materia de protección de datos personales. Esta función se ejerce con autonomía técnica en el marco de sus responsabilidades.

6.4. Las funciones del ODP en su calidad de asesor y supervisor técnico, no deben confundirse con las ejercidas por el obligado a la designación del mismo; no es función ni responsabilidad del ODP determinar la finalidad, el contenido o los medios de tratamiento de los datos, ni tampoco ser el ejecutor de dicho tratamiento.

6.5. La designación del ODP no implica la transferencia o exoneración de las funciones y responsabilidades atribuidas por la LPDP y su Reglamento a los obligados.

6.6. El obligado, debe dotar al ODP de las herramientas, condiciones, facilidades y recursos suficientes que permitan el desempeño efectivo y óptimo de sus funciones.

6.7. Cualquier organización o empresa que no se encuentre obligada legalmente a designar un ODP pueda hacerlo como buena práctica. En tal supuesto, debe garantizarse que no exista confusión respecto a su cargo, puesto y funciones; asimismo, debe cumplir con lo dispuesto en el LPDP y la normatividad vigente en la materia.

6.8. La directiva rige desde el día siguiente de su publicación en el diario oficial El Peruano, salvo que la misma prevea un plazo de adecuación para el cumplimiento de alguna de sus disposiciones o no hayan transcurrido aún las fechas establecidas en el calendario previsto en la primera disposición complementaria final del RLPDP.

6.9. La ANPD establece el criterio interpretativo ante dudas sobre la procedencia o alcance de la obligación de designación de un ODP.

7. DISPOSICIONES ESPECÍFICAS

7.1. Designación del ODP

7.1.1. La designación del ODP debe realizarse mediante un acto formal adoptado por el máximo órgano de administración de la entidad pública, organización o empresa.

7.1.2. En el caso de organizaciones o empresas se puede emplear la denominación documental que corresponda a su régimen societario interno (acuerdo, resolución, acta o instrumento equivalente), siempre que asegure la validez formal del nombramiento y permita su verificación ante la ANPD.

7.1.3. Designación del ODP en entidades públicas

7.1.3.1. Cada entidad pública debe designar a un ODP, de conformidad con lo establecido en el numeral 1 del artículo 37.1 del RLPDP. Esta designación es indispensable para el cumplimiento de la normativa vigente.

7.1.3.2. La designación del ODP recae en la entidad principal o central cuando la entidad pública cuenta con dependencias o sedes descentralizadas que no posean autonomía técnica, administrativa o presupuesto propio. El ODP central es

responsable de supervisar y garantizar el cumplimiento de la normativa de protección de datos personales en todas sus dependencias.

7.1.3.3. El ODP designa, de ser necesario, un punto de contacto en las dependencias o sedes descentralizadas, para trasladar consultas, coordinar la implementación de directivas o políticas de protección de datos y garantizar la correcta aplicación de la normativa a nivel institucional.

7.1.3.4. El punto de contacto, no sustituye la función del ODP, en todos los casos actúa bajo su coordinación.

7.1.4. Evaluación para designación del OPD por tratamientos de grandes volúmenes de datos personales

7.1.4.1. Los criterios desarrollados en la Directiva identifican la designación de un ODP por tratamientos de grandes volúmenes de datos[1].

7.1.4.2. La ANPD aplica una evaluación conforme a los criterios establecidos en el **Anexo 1 "Criterios de Evaluación para la Designación del ODP por Grandes Volúmenes de Datos**", que considera:

a) El número de titulares comprendidos en el tratamiento (criterio determinante)
b) Sensibilidad y tipología de los datos personales (criterio determinante)
c) Finalidad del tratamiento o riesgo asociado a derechos o libertades (criterio determinante)
d) Frecuencia, duración o continuidad del tratamiento (criterio modulador)
e) Demarcación territorial del tratamiento (criterio modulador)

7.1.4.3. El resultado de la evaluación determina si el tratamiento califica como uno de grandes volúmenes de datos y, si corresponde la designación del ODP mediante reglas de decisión.

7.1.4.4. Las reglas de decisión para determinar si un tratamiento configura o no como uno de gran volumen de datos se

[1] Numeral 2 del artículo 37.1 del RLPDP.

encuentran detalladas en el **Anexo 1 "Criterios de Evaluación para la Designación del ODP por Grandes Volúmenes de Datos"**, el cual es parte integrante de la presente Directiva.

7.1.4.5. Los criterios para identificar un tratamiento de grandes volúmenes de datos son los siguientes:

A) **Número de titulares:** El criterio de número de titulares incorpora lo previsto en la normativa vigente[2] considerando la magnitud del tratamiento, entendida como la evaluación conjunta del número de titulares involucrados y la cantidad de datos personales tratados respecto de cada uno de ellos.

El Criterio A, se evalúa según los niveles detallados en el **Anexo 1** de la presente Directiva

B) **Sensibilidad y tipología del dato:** Este criterio desarrolla lo referido al tipo de datos personales señalado en la normativa de protección de datos personales[3],que comprende tanto las categorías generales de datos personales como aquellas especialmente protegidas como los datos sensibles, cuya exposición incrementa la magnitud y riesgo del tratamiento.

Este criterio evalúa la intensidad del tratamiento considerando la sensibilidad del dato y el número de titulares respecto de los cuales se tratan dichos datos sensibles, de acuerdo con los niveles definidos en la matriz de evaluación del **Anexo 1**.

La sensibilidad y tipología se identifican considerando además de lo señalado en el **Anexo 1**, las siguientes categorías de datos personales, cuya presencia en el tratamiento constituye un factor cualitativo que se integra a la evaluación cuantitativa prevista en el citado Anexo:

- Datos relativos a salud, origen étnico, racial, convicciones religiosas, filosóficas o morales,

[2] Numeral 2, del artículo 37.1 del RLPDP.
[3] Numeral 2 del artículo 37.1 del RLPDP

orientación sexual, afiliación sindical y datos biométricos que permitan identificar de manera unívoca a la persona.
- Datos financieros, patrimoniales o de solvencia económica.
- Datos de geolocalización, telecomunicaciones o seguimiento de actividades en línea.
- Datos relativos a menores de edad u otros grupos en situación de especial vulnerabilidad.

Constituyen datos sensibles, por el impacto en la esfera más íntima de la persona, también los datos genéticos o biométricos, datos neuronales o los derivados del sistema nervioso periférico, datos morales o emocionales, hechos o circunstancias de la vida afectiva o familiar, información relativa a la afiliación sindical, salud física o mental u otras análogas que afecten su intimidad, los cuales deben ser evaluados como factores cualitativos conjuntamente con los niveles establecidos en la matriz del **Anexo 1.**

C) Finalidad y riesgo asociado

Este criterio evalúa la finalidad del tratamiento y el nivel de riesgo que la misma genera sobre los derechos y libertades de los titulares, atendiendo al impacto de sus decisiones, inferencias, evaluaciones o usos derivados del tratamiento de datos personales.

El Criterio C, determina y evalúa conforme a los niveles detallados en el **Anexo 1** de la presente Directiva.

Cuando la finalidad del tratamiento tenga la capacidad de producir un perjuicio evidente, es decir, una amenaza cierta o reconocible a los derechos o libertades del titular, dicho tratamiento se considera de nivel alto, conforme a la normativa de la materia[4].

D) Frecuencia, duración y continuidad del tratamiento

Este criterio evalúa la regularidad, persistencia y continuidad del tratamiento de datos personales,

[4] Numeral 2 del artículo 37.1 del RLPDP.

considerando el tiempo durante el cual se realiza, la periodicidad de las operaciones y la intensidad temporal del tratamiento del procesamiento. El Criterio D, se determina y evalúa conforme a los niveles detallados en el **Anexo 1** de la presente Directiva.

E) Demarcación territorial del tratamiento

Este criterio evalúa la ubicación donde los datos personales son tratados, sea en bancos de datos personales contenidos total o parcialmente en servidores ubicados fuera del territorio nacional, dentro del territorio o de forma local.

El Criterio E, se determina y evalúa conforme a los niveles detallados en el **Anexo 1** de la presente Directiva.

7.1.5. Designación del ODP en actividades principales o de giro de negocio que comprendan tratamiento de datos sensibles

7.1.5.1 Este supuesto se configura cuando la actividad principal o de giro de negocio del responsable o encargado, requiere el tratamiento de datos sensibles para la consecución de sus fines.

7.1.5.2 La obligación también se configura cuando, aun no estando el tratamiento de datos sensibles asociado a la actividad principal o de giro de negocio, este resulta inescindible para el diseño, planificación, sustento, evaluación, monitoreo, proyección o realización de dicha actividad o negocio.

7.1.5.3 El tratamiento inescindible que involucra una cantidad significativa de titulares o datos sensibles, se evalúa conforme a los criterios previstos en el **Anexo 1**, integrando dicha valoración al análisis propuesto por la ANPD.

7.1.5.4 Este supuesto constituye un criterio autónomo de designación del ODP[5], no estando sujeto a la evaluación cuantitativa del **Anexo 1**.

7.1.5.5 El tratamiento de datos sensibles es entendido en este acápite como parte de la actividad principal o inescindible cuando

[5] Numeral 3 del artículo 37.1 del RLPDP.

resulte indispensable para la prestación, ejecución u operación del servicio o actividad del obligado, no siendo aplicable a tratamientos de datos sensibles que sean incidentales, accesorios u ocasionales.

7.2. Excepciones del ámbito de aplicación

7.2.1. Se aplican las excepciones que la LPDP y el RLPDP establezcan. Para las organizaciones o empresas, se debe considerar que la directiva aplica en todos sus extremos, conforme al artículo 37 del RLPDP.

7.2.2. Las excepciones previstas en la LPDP y su Reglamento alcanzan únicamente a los contenidos o destinados a ser contenidos en bancos de datos personales de las entidades públicas, siempre que su tratamiento sea estrictamente necesario para el cumplimiento de las competencias y funciones asignadas por ley en materia de defensa nacional, seguridad pública o para actividades en materia penal orientadas a la investigación y represión del delito.

7.2.3. Para los tratamientos de datos personales con finalidades distintas a las materias señaladas en el numeral anterior, la excepción no es aplicable. En ese supuesto, la entidad pública, organización o empresa, debe designar a un ODP para coadyuvar al cumplimiento de las obligaciones que se deriven de dicho tratamiento.

7.2.4. La obligación de designar un ODP, no aplica a personas naturales que realicen el tratamiento de datos personales de manera personal, directa o aislada, en el marco de su oficio, ocupación o profesión, aun cuando involucren datos sensibles o un número importante de TDP.

7.2.5. Lo dispuesto no exime a las entidades públicas, organizaciones o empresas de cumplir con las obligaciones establecidas en la LPDP y su Reglamento, incluyendo la adopción de medidas de seguridad apropiadas para prevenir, mitigar o impedir situaciones que comprometan o pongan en riesgo el adecuado tratamiento de los datos personales.

7.3. Perfil e idoneidad del ODP

7.3.1. El ODP se designa considerando sus cualidades profesionales y, en particular, sus conocimientos especializados y experiencia práctica en materia de protección de datos personales, debidamente acreditados[6].

[6] Artículo 38 del RLPDP.

7.3.2. La designación siempre recae en una persona natural, lo que no impide que esta se vincule a una persona jurídica a la que pertenece o represente para el cumplimiento de sus funciones y siempre que no se encuentre impedida de hacerlo por configurarse el supuesto previsto en el numeral 7.3.6.2 de la presente directiva.

7.3.3. Experiencia profesional

7.3.3.1. Experiencia general: No inferior de dos (2) años, desempeñando labores afines a la materia de protección de datos personales de manera continua o acumulada y/o en materias como seguridad y gestión de la información, ciberseguridad, gobierno digital, inteligencia artificial o cualquier otra materia vinculada al tratamiento de datos personales en entidades públicas y/o privadas.

7.3.3.2. Experiencia específica: No inferior a un (1) año desempeñando labores en materia de protección de datos personales de manera continua o acumulada; la cual se puede acreditar a través de la experiencia profesional pública o privada, puede ser a nivel nacional o internacional.

7.3.4. Formación académica y complementaria

7.3.4.1. La formación y conocimientos en protección de datos personales se pueden acreditar mediante la experiencia probada y continua en la docencia universitaria o en la investigación sobre temas de protección de datos personales y/o afines.

7.3.4.2. La formación académica puede ser acreditada de acuerdo a los siguientes requisitos:

a) Contar con estudios de posgrado concluidos o grado académico afines a la materia de protección de datos personales y/o en materias como seguridad y gestión la información, ciberseguridad, gobierno digital, inteligencia artificial o cualquier otra materia vinculada al tratamiento de datos personales en entidades públicas y/o privadas.

b) Contar con certificado de especialización y/o diplomado en protección de datos personales o las materias afines señaladas en el literal precedente, con una duración

mínima de noventa (90) horas lectivas para los certificados y ciento veinte (120) horas lectivas para los diplomados.

7.3.4.3. Para garantizar la formación académica las capacitaciones, certificaciones o diplomados (nacionales o extranjeros), deben ser impartidos por entidades o instituciones formativas que cuenten con reconocido prestigio y trayectoria en protección de datos personales, seguridad de la información, ciberseguridad, gobierno digital, inteligencia artificial o cualquier otra materia afín al tratamiento de datos personales.

7.3.5. Conocimientos e independencia

7.3.5.1. Constituye un criterio orientativo, el conocimiento del sector en el que se inserta la entidad pública, organización o empresa, las regulaciones aplicables al mismo y las obligaciones derivadas de ellas que incidan, directa o indirectamente, en las operaciones de tratamiento de datos personales.

7.3.5.2. Es indispensable que el ODP conozca las normas internas, directivas, lineamientos, y procedimientos que regulan la gestión institucional de la entidad pública, organización o empresa, en materia de protección de datos personales.

7.3.5.3. El ODP ejerce sus funciones con independencia funcional, lo que implica que la entidad pública, organización o empresa, no puede instruirlo o direccionarlo sobre el contenido de sus opiniones, recomendaciones o decisiones técnicas en materia de protección de datos personales.

7.3.5.4. La independencia funcional no modifica la dependencia jerárquica ni la estructura organizacional.

7.3.5.5. El ODP, sea un servidor de la entidad pública, organización o empresa o un tercero, no puede ser sancionado, removido o sufrir cualquier forma de represalia por el contenido de sus informes, opiniones o recomendaciones en materia de protección de datos personales.

7.3.5.6. El ODP reporta funcionalmente a la máxima autoridad de administración de la entidad pública, organización o empresa, garantizando en todo momento su independencia funcional.

7.3.5.7. La independencia funcional no excluye la responsabilidad del ODP en casos de dolo, negligencia o incumplimiento de las obligaciones o funciones establecidas en la LPDP, el RLPDP, el Código de Ética de la Función Pública, o contrato de prestación de servicios según corresponda.

7.3.6. Idoneidad moral y ética

7.3.6.1 Para personas naturales:

- No debe tener sentencia condenatoria firme por delito doloso.
- No contar con sanción y/o inhabilitación vigente a consecuencia de un procedimiento disciplinario u otro análogo.
- No es idónea la persona que tenga una investigación penal formal o condena por delitos informáticos.
- No es idónea la persona que haya sido sancionada por faltas éticas vinculadas al tratamiento de información, protección de datos personales, transparencia, confidencialidad o integridad en el ejercicio de la función pública o profesional.

7.3.6.2 Si el ODP es asumido por una persona natural contratada a través de una persona jurídica, se debe verificar que dicha persona jurídica no haya sido responsable administrativamente por los delitos señalados en el artículo 1 de la Ley N° 30424, ni haber sido inhabilitada o suspendida para contratar con el estado.

7.4. Funciones del ODP

7.4.1. El ODP desempeña las funciones previstas en la normativa vigente[7]. Las entidades públicas y los actores privados elaboran guías, lineamientos, directrices y/o protocolos internos que expliciten los supuestos bajo los cuales se podrá requerir o solicitar la asistencia del ODP, los cuales también deben servir para regular más exhaustivamente el marco de su actuación en el desempeño de sus funciones.

7.4.2. El OPD presta especial atención a los riesgos asociados a las operaciones de tratamiento de datos personales, considerando su

[7] Artículo 39 del RLPDP.

naturaleza, alcance, contexto y fines. Esta labor coadyuva a la entidad pública, organización o empresa en el asesoramiento para la realización de evaluación de impacto en protección de datos personales, de corresponder.[8]

7.4.3. El ODP orienta y/o propone en lo siguiente:

- Definición de la metodología a utilizar.
- Identificación de los ámbitos sujetos a auditoría y revisión.
- Programación de actividades de formación y capacitación.
- Identificación de las operaciones de tratamiento de datos que se lleven a cabo por la entidad pública, empresa u organización.

7.4.4. El ODP, en el desarrollo de sus funciones, según sea el caso, debe:

a) Coordinar según corresponda, la realización de programas de capacitación y sensibilización dirigidas al personal de la entidad pública, organización o empresa, en materia de protección de datos personales.

b) Gestionar, según corresponda, con la entidad pública, organización o empresa, la conformación de un equipo de apoyo en materia de protección de datos personales, cuando la magnitud de las funciones de supervisión o asesoramiento así lo requieran, a fin de facilitar el cumplimiento eficaz de sus responsabilidades.

c) Elaborar informes, opiniones o recomendaciones técnicas o de supervisión, sobre el cumplimiento de la normativa en materia de protección de datos personales dentro de la entidad pública, organización o empresa, cuando se solicite o corresponda, los cuales deben ser puestos en conocimiento de la alta dirección de la entidad pública, directorio o análogo de la organización o empresa.

d) Recabar, según corresponda, información de las unidades, oficinas o departamentos pertinentes de la entidad pública, organización o empresa, a fin de verificar el cumplimiento de la normativa aplicable en las actividades de tratamiento de datos personales.

e) Revisar la información pertinente y realizar un examen de correspondencia de la información obtenida con los contenidos comprendidos en la LPDP y su Reglamento, o normas y documentos afines.

[8] Conforme a lo dispuesto por el artículo 40 del RLPDP.

f) Revisar periódicamente las resoluciones, opiniones, guías y demás documentos emitidos por la ANPD, en cuanto resulten relevantes para el cumplimiento eficiente de sus funciones.

g) Promover una cultura de protección de datos personales dentro de la entidad pública, organización o empresa.

7.4.5. Lo dispuesto en este apartado se aplican en concordancia con lo establecido en los numerales 6.5 y 6.6 de la presente directiva, respecto a la no transferencia de responsabilidades del ODP.

7.4.6. El ODP guarda estricta confidencialidad respecto de la información que conozca en el ejercicio de sus funciones; particularmente aquella que, de develarse, pudiera poner en riesgo o afectar la eficacia de las mismas, bajo responsabilidad administrativa, civil y/o penal, según corresponda.

7.4.7. En lo que respecta a aquellas solicitudes de información que reciba el ODP en el marco de sus funciones, debe deliberar sobre la atención correspondiente teniendo en cuenta, adicionalmente, las consideraciones previstas en la Ley N° 27806, Ley de Transparencia, y Acceso a la Información Pública, el Texto Único Ordenado aprobado por Decreto Supremo N° 21-2019-JUS y su Reglamento, aprobado por el Decreto Supremo N° 007-2024-JUS o el que lo sustituya.

7.4.8. El ODP informa periódicamente al obligado sobre las acciones realizadas en el ejercicio de sus funciones.

7.4.9. La confidencialidad no aplica a la rendición de cuentas que deba realizar al obligado que lo designa. Sin embargo, cuando dicha rendición comprometa la identidad de personas que informan hechos relacionados con el tratamiento de datos personales de la entidad pública, organización o empresa, el ODP se encuentra excusado de revelar tal información, salvo frente a las autoridades competentes.

7.4.10. Respecto a las solicitudes y consultas relacionadas con la protección de datos personales, estas son supervisadas por el ODP, en tanto es el responsable de velar por el cumplimiento de la normativa y de canalizar adecuadamente las comunicaciones vinculadas a la materia. Cuando dichas solicitudes o consultas requieran un análisis técnico o una recomendación del ODP, este elabora un informe técnico correspondiente.

7.4.11. El ODP orienta o asesora de manera especializada a la unidad o gerencia responsable sobre la correcta tramitación, interpretación legal y cumplimiento de los plazos en la normativa vigente para la atención de las solicitudes de derechos ARCO (acceso, rectificación, cancelación y oposición), asegurando así la respuesta oportuna conforme a Ley.

7.5. Capacidad para el cumplimiento de sus funciones

7.5.1. El ODP debe tener la capacidad de cumplir las funciones derivadas de su designación, lo que supone contar con conocimientos teóricos y prácticos en materia de protección de datos personales, así como con competencias que le permitan desempeñar su rol dentro de la entidad pública, organización o empresa.

7.5.2. La participación oportuna del ODP garantiza la aplicación práctica de los principios previstos en la Ley y su Reglamento, así como la efectividad para la atención de los derechos de los titulares.

7.5.3. El ODP tiene la capacidad de articular, cuando corresponda, con la ANPD y con los distintos actores relacionados a la materia, como aquellos vinculados al marco de confianza digital, gobernanza de datos, interoperabilidad, identidad, servicios, seguridad y arquitectura digitales del Estado, así como al Sistema Nacional de Transformación Digital.

7.5.4. Si el ODP es externo, el contrato que lo vincule debe garantizar, en lo aplicable, las condiciones necesarias para el cumplimiento de sus funciones.

7.6. Accesibilidad y ubicación

7.6.1. La entidad pública, organización o empresa que designe al ODP debe comunicar dicha designación a la ANPD. La comunicación se realiza a través de la mesa de partes virtual del MINJUSDH, dirigida a la DGTAIPD.

7.6.2. La comunicación con la ANPD debe incluir como mínimo los siguientes datos:

a) Nombres y apellidos completos del ODP.
b) DNI o documento equivalente de identificación.
c) Cargo o rol dentro de la entidad, organización o empresa.
d) Datos de contacto (correo electrónico institucional, teléfono, domicilio físico en Perú, si corresponde).

7.6.3. El ODP debe ser accesible, para la entidad pública, organización o empresa que lo designa y para la ANPD. La accesibilidad implica disponibilidad para el contacto e interacción que demande el adecuado ejercicio de sus funciones.

7.6.4. La disponibilidad del ODP no requiere necesariamente su presencia física en territorio nacional, pero sí la posibilidad de contacto e interacción (física y/o digital) dentro del ámbito de aplicación de la Ley y su Reglamento en el territorio peruano, como medio seguro de comunicación.

7.6.5. El ODP, con ayuda de un equipo de trabajo cuando sea necesario, debe garantizar una comunicación eficaz y comprensible con los titulares de datos personales, asegurando que dicha comunicación se realice, cuando corresponda, en el idioma utilizado por los titulares de datos afectados.

7.6.6. Para los casos de grupos empresariales, se permite la designación de un único ODP común para todos o algunas de las empresas que los integran, independientemente de si el grupo desarrolla sus actividades únicamente en Perú o también en el extranjero, en estos supuestos, el ODP designado (donde se encuentre ubicado) debe ser accesible para atender los requerimientos de la ANPD y de cada integrante del grupo.

7.6.7. Si el ODP es una persona externa a la organización o empresa, estas últimas deben establecer los parámetros de accesibilidad, los cuales no pueden comprometer el principio de eficacia. En todo caso, la accesibilidad para la ANPD, debe ser siempre inmediata, oportuna y pertinente respecto de las cuestiones vinculadas al tratamiento de datos personales que legitiman su intervención.

7.6.8. Cuando la función del ODP sea externalizada y/o se valga de una persona jurídica para el cumplimiento de sus funciones, conforme lo establece en el numeral 7.3.2 de la presente Directiva, la persona natural designada siempre será el punto de contacto ante la ANPD.

7.7. Obligaciones derivadas de su designación

7.7.1. La entidad pública, organización o empresa comunica internamente la designación del ODP y la hace pública externamente conforme a sus obligaciones o deberes de transparencia.

7.7.2. La información de contacto del ODP se mantiene actualizada y accesible. A nivel externo, la entidad pública, organización o empresa

hace público, como mínimo, el nombre completo del ODP y una dirección de correo electrónico. Esta obligación se realiza conforme a la normativa vigente[9] empleando la política de privacidad o documento idóneo para la difusión de dicha información y con prescindencia de la obligación descrita en el numeral 7.6.1.

7.7.3. El ODP recibe consultas oportunamente en toda decisión que tenga incidencia con el tratamiento de datos personales o en el cumplimiento de la normativa aplicable, debiendo transmitirle la información pertinente con la debida anticipación para que pueda brindar un asesoramiento adecuado.

7.7.4. En caso que sus recomendaciones no sean seguidas, se deja constancia expresa de ello, a fin de acreditar que su rol técnico ha sido ejercido y que la decisión final corresponde a la entidad pública, organización o empresa.

7.7.5. El ODP mantiene debe mantener un nivel de competencia actualizado, participando regularmente en procesos de capacitación, actualización o especialización en materia de protección de datos personales y disciplinas afines, conforme a la evolución normativa, tecnológica y de riesgos.

7.8. Garantías para el desempeño funcional

7.8.1. Para asegurar el adecuado desempeño funcional del ODP, se deben implementar, como mínimo, las siguientes garantías:

- Proveer la infraestructura, financiamiento y acceso a formación continua necesarios para el adecuado ejercicio de sus funciones.
- Evitar que se impartan instrucciones al ODP respecto al criterio técnico o jurídico que deba adoptar.
- Facilitar el acceso del ODP a la información y documentación necesaria para el ejercicio de sus funciones.
- Asegurar su participación o consulta oportuna en decisiones que incidan en el tratamiento de datos personales.

7.9. Conflicto de intereses

7.9.1. El ODP desempeña funciones en pro de la protección de los datos personales que son tratados por su entidad, organización o empresa;

[9] Conforme al numeral 37.4 del artículo 37 del RLPDP.

por lo tanto, no debe incurrir en situaciones que hagan inviable dicho desempeño por un conflicto de intereses.

7.9.2. Se entiende por conflicto de intereses cualquier situación en la que los intereses personales, profesionales o económicos del ODP interfieren en el cumplimiento objetivo e independiente de sus funciones.

7.9.3. Si un conflicto de intereses surge después de la designación, la entidad pública, organización o empresa lo gestiona oportunamente mediante las medidas internas que resulten aplicables, lo que podría implicar la adopción de acciones correctivas o preventivas conforme a su propio marco normativo y contractual, hasta que cese la situación generadora.

7.9.4. Cuando el conflicto de intereses no se gestione en el corto plazo, la entidad pública, organización o empresa procede a la sustitución del ODP.

7.9.5. La entidad pública, organización o empresa, establece directrices o protocolos que identifiquen puestos sensibles o incompatibles con la función de ODP, tomando como referencia la Ley Nº 31564 - "Ley de Prevención y Mitigación del Conflicto de Intereses en el Acceso y Salida de Personal del Servicio Público" y su Reglamento.

8. DISPOSICIONES COMPLEMENTARIAS

8.1 La DGTAIPD, es el órgano competente para interpretar los alcances de la presente directiva, así como para emitir lineamientos y precisiones adicionales en el marco de sus competencias.

8.2 La directiva se aplica de manera supletoria a aquellas situaciones relacionadas con la designación, funciones y responsabilidades del ODP que no se encuentren previstas en normas de mayor jerarquía.

8.3 Cuando se trate de organizaciones sin fines de lucro, el criterio de ventas anuales[10] se entenderá referido a sus ingresos anuales en base a donaciones, subvenciones, presupuesto ejecutado o financiamiento recibido, según corresponda, en concordancia con lo establecido en el artículo 37 del RLPDP, a fin de determinar la fecha de entrada en vigencia de la obligación de designar a un ODP, según sea el caso.

[10] De conformidad con lo dispuesto en la Primera Disposición Complementaria Final del RLPDP.

8.4 Las entidades públicas que ya cuenten con un ODP designado deben adecuar su designación y funciones a lo dispuesto en la presente directiva, en un plazo no mayor de ciento ochenta (180) días calendario.

8.5 Cuando por cese de operaciones o modificación en las actividades de tratamiento, deje de resultar exigible la designación y/o actuación de un ODP ya designado, dicha situación debe ser comunicada a la ANPD, dentro del plazo de diez (10) días hábiles, contados a partir de la emisión del acto o documento que dispone el cese o la modificación correspondiente, indicando las razones que sustentan la variación y las medidas adoptadas respecto al tratamiento de datos personales involucrados.

8.6 Las entidades públicas, organizaciones o empresas establecen mecanismos de suplencia temporal para garantizar la continuidad de las funciones del ODP en casos de vacancia, renuncia, licencia, enfermedad u otros impedimentos. La suplencia solo opera de manera temporal hasta que se designe o reincorpore el ODP titular.

9. ANEXO

Anexo N° 01: Criterios de evaluación para la designación del ODP por grandes volúmenes de datos.

PERÚ
MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

Firmado digitalmente por LUNA CERVANTES Eduardo Javier FAU 20131371617 soft

ANEXO N° 01

CRITERIOS DE EVALUACIÓN PARA LA DESIGNACIÓN DEL ODP POR GRANDES VOLÚMENES DE DATOS

9.1. Criterios de Evaluación

La evaluación se realiza considerando **5** criterios.

a) Los tres primeros **(A, B y C)** constituyen criterios determinantes, pues representan la magnitud del riesgo de tratamiento.
b) Los criterios **(D y E) son criterios moduladores**, que complementan la evaluación, pero **no determinan por sí solos la existencia de Gran volumen.**
c) Siempre que se realice el tratamiento de datos aplicado a un criterio, se tomará como nivel de referencia el tratamiento más alto.
d) La aplicación de los criterios de evaluación para los encargados del tratamiento de datos personales, se realiza con respecto a sus características como entidad pública, organización o empresa obligada y no respecto al tratamiento de datos que ejecuta, como encargado, a nombre del titular del banco de datos o responsable de tratamiento.

9.2. Asignación relativa a cada criterio:

Criterio	Descripción
A (Determinante)	Número de titulares.
B (Determinante)	Tipología / sensibilidad del dato.
C (Determinante)	Finalidad del tratamiento y riesgo asociado.
D (Modulador)	Frecuencia, duración y continuidad del tratamiento.
E (Modulador)	Demarcación territorial del tratamiento.

A. Número de Titulares de Datos Personales

En esta categoría, se considera el número de titulares únicos contenidos en todas las bases de datos de entidades públicas, organizaciones o empresas (esto debe considerar bancos de datos de clientes, trabajadores, prospectos u otros).

No se consideran aquellos registros duplicados producto del perfilamiento, segmentación o tratamiento automatizado, sino la cantidad de titulares. En ese sentido, a efectos de determinar el número titulares se establecen los siguientes niveles:

- **NIVEL ALTO:** ≥ 50 000 de titulares.
- **NIVEL MEDIO:** 10 000 – 49 999 de titulares
- **NIVEL BAJO:** < 10 000 titulares

B. Sensibilidad y Tipología del Dato

En esta categoría, se evalúa todo tratamiento individual realizado sobre datos sensibles, siempre que el número total de tratamientos corresponda a más de 1000 titulares.

Se entiende por tratamiento individual a cada operación específica sobre los datos sensibles de un titular. En este sentido, no debe interpretarse que cada operación ejecutada por los sistemas de información[11] constituye por sí misma un tratamiento individual, siempre que dicha operación forme parte del soporte necesario para la ejecución de dicho tratamiento[12].

Las operaciones de tratamiento comprenden, entre otras, la recolección, registro, organización, almacenamiento, conservación, consulta de datos,

[11] Parte del funcionamiento de un sistema de información al momento de realizar un tratamiento individual, como la búsqueda de un dato sensible mediante un formulario de consulta, puede implicar que se realicen indexaciones o listados a nivel interno con la finalidad de lograr la búsqueda. Estas acciones no serán consideradas tratamientos individuales, y pueden incluir lecturas automatizadas de la base de datos, procesos internos de indexación, consultas de rutina propias del funcionamiento de la aplicación, entre otros.

[12] Considerar estas acciones de soporte como tratamientos individuales conduciría a una sobreestimación del número de tratamientos individuales, ya que los sistemas de información pueden ejecutar operaciones de indexación o búsqueda a nivel interno que no representan el tratamiento individual. Por ejemplo, en una entidad especializada que realiza un proceso interno de segmentación de personas en función de datos sensibles relacionados con su historial clínico, el tratamiento principal consiste en clasificar a los titulares en grupos con la finalidad de proporcionar un servicio. Para materializar dicho tratamiento, los sistemas de información pueden ejecutar diversas operaciones técnicas de soporte, tales como la normalización y depuración de datos, la generación de índices sobre datos clínicos para optimizar las consultas, la creación de tablas intermedias para consolidar información, la detección y fusión de registros duplicados de una misma persona, la ejecución de procesos de agregación y anonimización parcial para elaborar reportes internos, así como la generación de copias de respaldo. Ninguna de estas operaciones constituye, por sí misma, un tratamiento individual adicional, en la medida en que se limitan a ser operaciones técnicas necesarias para soportar y hacer operativo el tratamiento de segmentación de personas.

utilización para una finalidad determinada, interconexión, comunicación, prospección, evaluación, bloqueo o supresión de los datos, sin incluir la mera generación de copias, respaldos técnicos o réplicas que no impliquen uno de los tratamientos ya mencionados.

- **NIVEL ALTO:** más de 5000 tratamientos individuales
- **NIVEL MEDIO:** entre mil y menos de 5000 tratamientos individuales
- **NIVEL BAJO:** más de 100 y menos de 1000 tratamientos individuales

C. Finalidad del Tratamiento o Riesgo Asociado

En esta categoría se identifica el tratamiento de datos personales de nivel más alto realizado, siempre que este supere los 20 tratamientos individuales, sin importar la cantidad de titulares implicados. En este apartado se considera la finalidad del tratamiento de los datos independientemente de si este se realiza bajo medios tradicionales o mediante herramientas y/o algoritmos potenciados por inteligencia artificial, aprendizaje automático, entre otros relacionados.

- **NIVEL ALTO**
  Finalidades orientadas a evaluaciones o decisiones que pueden generar un riesgo para la vida humana, la dignidad, la libertad, la seguridad física y los demás derechos fundamentales de las personas, tales como perfilamiento o scoring detallado de personas, telemarketing o televentas, decisiones automatizadas con efectos legales, segmentación conductual, geolocalización constante, vigilancia o monitoreo intensivo y análisis masivo con cruces de bases de datos que permitan inferencias sensibles, entre otros.

- **NIVEL MEDIO**
  Finalidades vinculadas principalmente a la gestión administrativa continua o de soporte, tratamiento con fines estadísticos o de investigación con datos seudonimizados, procesos rutinarios de pruebas y desarrollo, respaldo de base de datos o trámites masivos de back-office que implican tratamiento estable.

- **NIVEL BAJO**
  Finalidades básicas y acotadas, centradas el mero almacenamiento, por ejemplo, nóminas pequeñas, directorios y listados simples, así como registros puntuales de actividades o eventos y atenciones individuales o expedientes aislados, en los que no se realizan evaluaciones complejas, ni decisiones automatizadas relevantes, ni análisis intensivo de la información personal. También se considerará en este nivel los contactos digitales o llamadas vinculados a las labores internas de la

organización (control de personal, comunicaciones, correos electrónicos, entre otros).

D. Frecuencia, Duración y Continuidad del Tratamiento

En esta categoría se identifica la frecuencia de nivel más alto realizado sobre datos personales, siempre que este supere los 20 tratamientos individuales, sin importar el número de titulares implicados.

En relación a la frecuencia del tratamiento de los datos, esta se considera independientemente de si este se realiza bajo medios tradicionales o mediante herramientas y/o algoritmos potenciados por inteligencia artificial, como llamadas o mensajes automatizados, entre otros relacionados.

- **NIVEL ALTO**
  Tratamientos continuos, permanentes o de ejecución diaria, con monitoreo intensivo o sistemático y procesamiento automatizado constante (por ejemplo, sistemas en producción 24/7 o registros en tiempo real), así como conservaciones prolongadas sin depuración suficiente, que generan una exposición temporal elevada y sostenida de los datos personales.

- **NIVEL MEDIO**
  Tratamientos recurrentes con una periodicidad definida (semanal, mensual, trimestral u otra similar), campañas o procesos que se repiten a lo largo del tiempo, operaciones programadas de respaldo y mantenimiento, o proyectos de duración extendida pero no permanente, en los que el uso de los datos es regular y estable, aunque no continuo.

- **NIVEL BAJO**
  Tratamientos puntuales, ocasionales o excepcionales, tales como campañas únicas, encuestas o proyectos específicos, pilotos o pruebas de concepto de corta duración, verificaciones esporádicas y tratamientos ligados a eventos concretos, en los que el uso de los datos se limita a una ventana temporal reducida y, en principio, se prevé la supresión o anonimización posterior.

E. Demarcación Territorial del Tratamiento

En esta categoría se establece que la ubicación de los datos personales y donde estos son tratados, constituye un elemento modulador para determinar a designación del ODP por grandes volúmenes de datos.

- **NIVEL ALTO:**

Bancos de datos personales contenidos total o parcialmente en servidores ubicados fuera del territorio nacional, o gestionados (accesados) mediante servicios en la nube o macro servicios cuya infraestructura principal o de respaldo se encuentra fuera de territorio nacional. Se incluye también el uso habitual de conexiones remotas (VPN, SSH, FTP/SFTP u otros protocolos) por parte de usuarios o administradores localizados fuera del país, cuando acceden a datos personales alojados en bancos de datos nacionales.

Implica una alta complejidad técnica y de coordinación, al activar marcos regulatorios y exigencias de cumplimiento adicionales.

- **NIVEL MEDIO:**
  Bancos de datos personales contenidos en servidores o infraestructuras localizadas en territorio nacional, gestionados dentro del país, aunque puedan emplearse conexiones virtuales internas (VPN, redes privadas, accesos remotos desde distintas sedes nacionales).

- **NIVEL BAJO:**
  Bancos de datos personales gestionados de forma local, ya sea en soportes físicos (expedientes, formularios, legajos) o en servidores y equipos ubicados territorio nacional, sin exposición directa a internet ni accesos remotos. El tratamiento se circunscribe a intranets o redes locales cerradas, sin participación de proveedores extranjeros ni transferencias internacionales de datos.

9.3. Reglas de Decisión:

Condición	**Clasificación del tratamiento**
Si por lo menos **uno** de los criterios determinantes (A, B o C) se encuentra en **nivel alto**, con independencia de los niveles de D y E.	Gran volumen de datos personales.
Si por lo menos **dos** de los criterios determinantes (A, B o C) se encuentran en **nivel medio** (incluye el caso en que los **tres** estén en nivel medio), con independencia de D y E.	Gran volumen de datos personales.
Si por lo menos **uno** de los criterios determinantes (A, B o C) se encuentra en **nivel medio** y, además, por lo menos **uno** de los criterios complementarios (D o E) se encuentra en **nivel medio o alto**.	Gran volumen de datos personales.
Si los tres criterios determinantes (A, B y C) se encuentran **simultáneamente en nivel bajo**, con independencia de los niveles asignados a D y E.	No es gran volumen de datos personales.