PERÚ | Ministerio de Justicia y Derechos Humanos

PREGUNTAS Y RESPUESTAS

En relación a la directiva que establece disposiciones para la designación, desempeño y funciones del Oficial de Datos Personales (ODP)

Autoridad Nacional de Protección de Datos Personales - ANPD

En relación a la directiva que establece disposiciones para la designación, desempeño y funciones del Oficial de Datos Personales (ODP)[1]

I. Designación del ODP

1 ¿Cuál es el procedimiento y el medio para comunicar o registrar la designación del ODP ante la Autoridad Nacional de Protección de Datos Personales (ANPD)?

La designación del ODP debe constar en un **acto formal** adoptado por el máximo órgano de administración de la entidad pública, organización o empresa, en el caso de estas dos últimas, **conforme a su régimen societario interno,** pudiendo emplearse la denominación documental que corresponda (acuerdo, acta, resolución u otro instrumento equivalente), de conformidad con el numeral 7.1.2 de la Directiva.

Para efectos de su **comunicación ante la ANPD**, dicho documento debe ser remitido a través de la mesa de partes virtual del Ministerio de Justicia y Derechos Humanos (https://sgd.minjus.gob.pe/sgd-virtual/public/ciudadano/ciudadanoMain.xhtml), debiendo contener como mínimo los siguientes datos:

- Nombres y apellidos completos.
- DNI o documento equivalente de identificación.
- Cargo o rol de la entidad, organización o empresa (si es en adición a sus funciones como es en el caso de las entidades públicas).
- Datos de contacto (correo electrónico institucional, teléfono, domicilio físico en Perú, de ser el caso).

2 ¿Es una obligación comunicar a terceros, distintos a la ANPD, la identidad del ODP?

Sí. De conformidad con el numeral 7.7.2 de la Directiva, la entidad pública, organización o empresa tiene la obligación de mantener actualizada y accesible, a nivel externo, la información de contacto del ODP.

Para cumplir con dicha obligación, el sujeto obligado debe **hacer público**, como mínimo, el **nombre completo del ODP** y una **dirección de correo electrónico**, empleando la **política de privacidad o un documento idóneo** para la difusión de dicha información, conforme a la normativa vigente.

La Directiva precisa que esta obligación no se encuentra condicionada ni supeditada a otros deberes de comunicación o registro ante la ANPD.

En consecuencia, la comunicación de la identidad del ODP a terceros distintos de la Autoridad, constituye una obligación específica de transparencia y accesibilidad, orientada a garantizar que los titulares de datos personales y terceros vinculados al tratamiento cuenten con un canal directo de contacto claramente identificable para fines relacionados con la protección de datos personales.

[1]Directiva con Código M6.DGTAIPD.DI.001, versión 01, aprobada por Resolución Directoral N° 100-2025-JUS/DGTAIPD publicada en el boletín de Normas Legales del diario oficial El Peruano en fecha 31 de diciembre de 2025.

3 ¿Las organizaciones que designan un ODP de manera voluntaria, están sujetas al mismo estándar de requisitos que las entidades públicas, organizaciones o empresas obligadas?

La designación voluntaria de un ODP **se rige por el mismo estándar de requisitos que la designación obligatoria.** Según el numeral 6.7 de la Directiva, las organizaciones que opten por esta figura de manera facultativa están sujetas a las mismas disposiciones que regulan su designación, desempeño y funciones, garantizando así la uniformidad en la protección de los datos personales.

Este criterio se sustenta en que la naturaleza del cargo y la responsabilidad técnica no varían según el origen de la designación. Al exigir el cumplimiento de los mismos requisitos, la Directiva asegura que cualquier profesional que actúe como ODP posea la idoneidad y los conocimientos especializados necesarios para proteger los derechos de los ciudadanos, evitando que existan distintos niveles de calidad en la tutela de la privacidad.

Finalmente, esta uniformidad garantiza la seguridad jurídica y la transparencia frente a los titulares de los datos. Independientemente de si la organización está obligada o no, minimizando así los riesgos derivados de un tratamiento inadecuado de la información personal.

4 ¿La designación de un ODP que no cumple con el perfil previsto en la Directiva, constituye una infracción administrativa?

El análisis sobre la eventual configuración de una infracción administrativa debe partir del **principio de seguridad** que rige el tratamiento de datos personales. Conforme a los artículos 9 y 16 de la Ley N.° 29733, el titular del banco de datos personales tiene la obligación de adoptar medidas técnicas, organizativas y legales que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

En desarrollo de dicho mandato, el Reglamento de la Ley de Protección de Datos Personales (RLPDP) aprobado por el (Decreto Supremo N.º 016-2024-JUS) tipifica como infracción la realización de tratamientos de datos personales incumpliendo las medidas de seguridad, clasificándolas como leves, graves o muy graves, según la existencia de perjuicio, exposición no autorizada o el carácter sensible de los datos (artículos 132, 133 y 134 del RLPDP).

En este marco, la designación del Oficial de Datos Personales constituye una medida organizativa orientada a garantizar el cumplimiento del principio de seguridad. Por ello, la falta de adecuación del perfil del ODP no configura por sí sola una infracción administrativa, sino que debe evaluarse en función de su impacto real en la implementación de las medidas de seguridad exigidas por la Ley y su Reglamento. Solo cuando dicha situación evidencie la ausencia o ineficacia de medidas organizativas que afecten la seguridad del tratamiento, podría ser valorada en un procedimiento sancionador.

II. Perfil e Idoneidad del ODP

5 ¿Cómo debe interpretarse el numeral 7.3 de la Directiva referido al perfil e idoneidad de la persona a designar como ODP? ¿Se trata de requisitos concurrentes o alternativos?

El numeral 7.3 de la Directiva debe interpretarse de manera sistemática y conforme al artículo 38 del Reglamento de la Ley de Protección de Datos Personales, aprobado por el Decreto Supremo N.° 016-2024-JUS, el cual establece que el ODP es designado atendiendo a sus **cualidades profesionales y, en particular, a sus conocimientos y práctica en materia de protección de datos personales, debidamente acreditados**, a fin de garantizar el adecuado desempeño de las funciones previstas en el artículo 39 del citado Reglamento.

Bajo este enfoque, los **conocimientos especializados y la experiencia práctica en materia de protección de datos personales constituyen requisitos concurrentes,** en tanto ambos resultan necesarios para asegurar que el ODP cuente con la idoneidad técnica exigida por la normativa vigente. En efecto, no basta la sola formación teórica ni la experiencia desvinculada de la materia, sino que se requiere una combinación mínima de conocimientos específicos y práctica acreditada en protección de datos personales.

No obstante, en lo referido a la **formación académica,** la Directiva admite una interpretación flexible y razonable, conforme al principio de proporcionalidad y a la diversidad de trayectorias profesionales. En ese sentido, la acreditación de los conocimientos especializados puede realizarse a través de vías alternativas, tales como:

- Docencia en materias vinculadas a la protección de datos personales y/o;
- Investigación académica especializada y/o;
- Capacitación formal acreditada mediante cursos, programas o certificaciones, tales como cursos de especialización (por ejemplo, con una carga horaria mínima referencial de 90 horas) o diplomas de especialización (por ejemplo, con una carga horaria mínima referencial de 120 horas).

Esta interpretación permite garantizar un estándar técnico mínimo común, sin restringir indebidamente el acceso al cargo del ODP, y resulta coherente con la finalidad de la Directiva, orientada a fortalecer la función del ODP como asesor y supervisor técnico especializado.

6 ¿Qué ocurre si el ODP de una entidad pública no cumple con el perfil regulado en la Directiva? ¿Debe obligatoriamente designar a una persona con ese perfil? ¿Puede recaer esta designación en una persona distinta al Jefe (a) de la Oficina de Asesoría Jurídica y al Jefe (a) de la Oficina de Tecnologías de la Información?

Cuando el ODP de una entidad pública no cumple con el perfil regulado en la Directiva, ello **no genera automáticamente la invalidez de la designación ni exige su sustitución inmediata,** debiendo aplicarse un **enfoque de adecuación progresiva,** conforme a lo dispuesto en el numeral 6.8 de la Directiva.

En ese sentido, la entidad pública debe **evaluar el perfil del ODP designado** y adoptar las medidas necesarias para adecuar su designación y desempeño a los criterios de perfil e idoneidad desarrollados en la Directiva, lo que puede implicar:

- El fortalecimiento o complementación de su formación y experiencia,
- La reasignación de funciones internas,
- De resultar necesario, la designación de una nueva persona que cumpla con el perfil previsto.

La obligación de contar con un ODP con el perfil regulado **sí resulta exigible,** en tanto deriva del artículo 38 del Reglamento de la Ley de Protección de Datos Personales y es desarrollada por la Directiva; no obstante, su implementación debe realizarse dentro de los plazos de adecuación aplicables.

Ahora bien, en cuanto a la persona sobre la cual puede recaer la designación, el artículo 68.6 del Reglamento de la Ley de Gobierno Digital aprobado por D.S. Nº 029-2021-PCM establece que el rol de ODP es ejercido por un funcionario o servidor público designado por la máxima autoridad administrativa de la entidad, pudiendo recaer en el/la titular de la Oficina de Asesoría Jurídica o de la Oficina de Tecnologías de la Información, sin que ello implique una asignación exclusiva u obligatoria.

En consecuencia, la designación del ODP puede recaer válidamente en una **persona distinta** al/la Jefe/a de la Oficina de Asesoría Jurídica o al/la Jefe/a de la Oficina de Tecnologías de la Información, siempre que:

- Sea funcionario o servidor público de la entidad,
- Sea designado por la máxima autoridad administrativa,
- Cuente con el perfil e idoneidad técnica exigidos por la normativa sobre protección de datos personales y la directiva de la materia.

Esta interpretación resulta coherente con el carácter técnico especializado de la función del ODP, la autonomía organizativa de las entidades públicas y la finalidad de asegurar un ejercicio efectivo e independiente de las funciones de asesoría, supervisión y enlace con la ANPD.

En suma, la normativa vigente **no impone una designación rígida ni limitada a determinados cargos**, sino que habilita a las entidades públicas a designar como ODP a la persona que, dentro de su estructura organizativa, **garantice mejor el cumplimiento efectivo del régimen de protección de datos personales**, respetando los criterios de perfil e idoneidad previstos.

7 ¿Los criterios sobre el perfil e idoneidad del ODP, alcanzan también a las entidades públicas, organizaciones o empresas que ya designaron uno al tiempo de entrada en vigencia de la Directiva o cómo debe interpretarse el plazo de adecuación de ciento ochenta (180) días, previsto en el numeral 8.4 de la citada norma, respecto a los sujetos obligados?

Sí, los criterios sobre el perfil e idoneidad técnica del ODP son aplicables a todos los sujetos obligados, independientemente de si la designación se haya realizado con anterioridad a la entrada en vigencia de la Directiva. Esto se debe a que la norma no crea obligaciones nuevas, sino que desarrolla y precisa los estándares profesionales y de conocimiento ya exigidos por el artículo 38 del RLPDP, cumpliendo una función interpretativa y orientadora destinada a facilitar su correcta implementación.

No obstante, esta aplicación no es automática ni inmediata; conforme a lo dispuesto en el numeral 6.8 de la Directiva, rige un criterio de flexibilidad y de adecuación progresiva cuando la propia norma prevea plazos de adecuación. El plazo de ciento ochenta (180) días calendario previsto en el numeral 8.4, debe interpretarse como un plazo general de adecuación, aplicable tanto a las entidades públicas como a las organizaciones y empresas.

Por tal motivo, si bien el numeral 8.4 menciona expresamente a las **entidades públicas** que ya cuenten con un ODP designado, dicha referencia **no puede entenderse en un sentido que excluya** a las organizaciones y empresas comprendidas en el ámbito de aplicación de la Directiva, sino como una **precisión operativa** referida a uno de los grupos de sujetos obligados.

En consecuencia, las entidades públicas, organizaciones y empresas que ya cuenten con un ODP designado disponen del citado plazo para evaluar el perfil actual del ODP y, de ser el caso, adecuar formalmente su designación y el ejercicio de sus funciones a los criterios técnicos desarrollados en la Directiva, bajo un enfoque de razonabilidad.

III. Formación Académica

8 ¿Los requisitos de formación académica y complementaria, previstos en el numeral 7.3.4. de la Directiva, deben cumplirse de manera concurrente o basta con acreditar uno de ellos?

Los requisitos vinculados a la formación académica y a los conocimientos en materia de protección de datos personales previstos en la Directiva, entiéndase, formación académica acreditada, experiencia probada y continua de docencia universitaria e investigación sobre protección de datos personales y/o materiales afines, **pueden no cumplirse de manera concurrente,** pues se trata de mecanismos alternativos de acreditación del perfil del ODP.

En ese sentido, no resulta exigible acreditar simultáneamente todas las modalidades previstas, bastando con que el ODP acredite razonablemente uno de los mecanismos establecidos en la Directiva, este permitirá verificar su formación para el adecuado desempeño de sus funciones.

9 ¿La formación académica a la que se alude en el numeral 7.3.4.2. de la Directiva, puede acreditarse alternativamente mediante estudios de posgrado concluidos o grado académico afín, o mediante certificados de especialización o diplomados?

El numeral 7.3.4.2. de la Directiva regula la formación académica estableciendo vías alternativas de acreditación para cada uno de estos componentes del perfil del ODP.

En primer lugar, esta formación puede acreditarse mediante:

a) Estudios de **posgrado concluidos** o un grado académico vinculado a la materia de protección de datos personales y/o a materias afines; o, a través de,

b) Programas de especialización acreditados mediante certificados y/o diplomados, con una duración mínima de noventa (90) horas lectivas para los certificados y ciento veinte (120) horas lectivas para los diplomados, en protección de datos personales o las materias afines.

Estas modalidades permiten acreditar la formación académica en materias vinculadas o afines a la protección de datos personales, tales 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.

10 El estándar de formación académica, previsto en el numeral 7.3.4.2 de la Directiva, es rígido? ¿Cómo se justifica la carga horaria mínima establecida?

El numeral 7.3.4.2 de la Directiva establece un **estándar técnico orientador** para determinar en general el perfil e idoneidad del ODP, vale decir, para la ANPD, ese **es el estándar que se requiere para acreditar iure et de iure (sin admitir prueba en contrario) una formación académica y conocimientos** suficientes para desempeñar labores de ODP. Sin embargo; el uso del verbo "puede" da pie a que la ANPD, evalúe en cada caso concreto si el estándar establecido **admite ajustes razonables** dada la naturaleza del sujeto obligado a designar el ODP, la formación académica y conocimientos acreditados y la oferta formativa o académica disponible.

Ahora bien, en relación a la carga horaria mínima de noventa (90) horas para programas de especialización y ciento veinte (120) para diplomados, establecidos en la Directiva, ello se sustenta en criterios objetivos del sistema educativo peruano. En particular, la Ley N.° 30220, Ley Universitaria, reconoce que los diplomados de posgrado constituyen programas formativos estructurados, con una carga mínima de (24) créditos, lo que evidencia que los umbrales horarios previstos por la Directiva responden a un criterio de proporcionalidad y razonabilidad, sin exigir la carga completa de un posgrado.

Asimismo, el estándar de **noventa (90) horas** para programas de especialización[2] se encuentra alineado con los criterios establecidos por la **Autoridad Nacional del Servicio Civil (SERVIR)[3],** que reconoce como programas de especialización aquellas capacitaciones estructuradas con una duración no menor a dicho umbral, reforzando la necesidad de una formación técnica efectiva para el desempeño de funciones especializadas como las del ODP.

11 ¿Existe un plazo de vigencia o antigüedad para los certificados que se pretenda acreditar?

La Directiva **no establece un plazo de vigencia ni una antigüedad máxima** para los certificados, diplomados o estudios que se presenten para acreditar la formación académica o los conocimientos del ODP.

En ese sentido, **no corresponde descartar automáticamente** certificados por el solo transcurso del tiempo desde su emisión. Lo relevante, conforme al enfoque de la Directiva, es que la formación acreditada:

a) Guarde relación con la materia de protección de datos personales o materias afines; y,
b) Resulte pertinente, razonable y suficiente para el adecuado desempeño de las funciones del ODP.

Sin perjuicio de ello, la evaluación del perfil del ODP debe realizarse bajo un **enfoque integral**, considerando no solo la antigüedad de los certificados, sino también, la trayectoria profesional del ODP, la **experiencia práctica** en la materia, y, de ser el caso, la actualización continua de conocimientos, en atención al carácter dinámico de la protección de datos personales y los entornos tecnológicos asociados.

12 ¿Existe un plazo de vigencia o antigüedad para los certificados que se pretenda acreditar?

Las certificaciones internacionales que utilizan créditos (como los **ECTS** europeos) **son válidas** para acreditar la formación exigida. Para su validación, **se aplica el estándar oficial de conversión** del sistema educativo peruano, donde cada crédito académico equivale a un mínimo de 16 horas lectivas. Esto permite que cualquier programa internacional que alcance el total de horas requerido sea reconocido como equivalente.

[2] La Resolución de Presidencia Ejecutiva N.º 141-2016-SERVIR-PE modificada con Resolución de Presidencia Ejecutiva N.° 000214-2025-SERVIR-PE de fecha 31 de diciembre de 2025, en la cual se aprueba la Directiva "Normas para la gestión del proceso de capacitación en las entidades públicas", reconoce como Programas de Especialización a un conjunto de módulos organizados para profundizar en una temática específica; los cuales tienen como propósito el perfeccionamiento profesional y laboral en áreas específicas, teniendo una duración mínima de noventa (90) horas o de ochenta (80) si son organizados por disposición del ente rector en la materia en el marco de sus atribuciones normativas.

[3] Literal h, numeral 7.1.1, Tipo de Acciones de Formación Laboral, Directiva "Normas para la Gestión del Proceso de Capacitación en las entidades públicas", aprobado por Resolución de Presidencia Ejecutiva N.° 000214-2025-SERVIR-PE y modificada por la Resolución de Presidencia Ejecutiva N.° 000005-2026-SERVIR-PE de fecha 09 de enero de 2026.

13 ¿La formación académica y complementaria puede ser impartida por entidades privadas o empresas que actúan como representantes o partners autorizados de instituciones internacionales?

La formación académica y complementaria **puede ser impartida** por entidades privadas, empresas o partners autorizados que actúen en representación de instituciones internacionales. La validez de estas capacitaciones **se sustenta** en el respaldo técnico de la institución matriz, siempre que el certificado emitido **acredite** fehacientemente el cumplimiento de las 90 o 120 horas lectivas exigidas y cuente con el aval de la entidad responsable del programa.

14 ¿La exigencia de que la formación sea impartida por entidades de reconocido prestigio se limita a universidades e institutos o incluye también a organizaciones especializadas y empresas certificadoras?

La condición de entidad de "reconocido prestigio" **no se limita** exclusivamente a universidades e institutos del Perú o del extranjero, sino que **incluye** a organizaciones internacionales especializadas y empresas certificadoras de trayectoria comprobada en la materia o afines sea en Perú o también en el extranjero. Este reconocimiento **se sustenta** no solo en la especialización temática, sino en la solidez de la metodología de estudio, la calidad de la plana docente y el rigor de los procesos de evaluación.

Una institución con una infraestructura académica robusta, garantiza que el proceso de aprendizaje del ODP sea efectivo, estructurado y orientado al desarrollo de competencias reales.

Esta visión integral se alinea con el artículo 47.5 de la Ley Universitaria, que exige condiciones básicas de calidad y procesos de interacción que aseguren un servicio educativo óptimo. Al valorar la capacidad metodológica de la institución, la Directiva evita la creación de barreras injustificadas y permite que el ODP elija centros de estudios que, por su prestigio académico general, aseguren un alto estándar en la impartición de conocimientos técnicos y prácticos.

Finalmente, la combinación de experiencia temática y calidad metodológica garantiza la idoneidad técnica del ODP. El prestigio de la institución educativa respalda que el profesional ha superado un programa de formación serio y de alta exigencia, lo cual protege directamente a los ciudadanos. Un ODP formado bajo metodologías educativas de calidad está mejor preparado para aplicar la normativa de manera coherente y gestionar con ética y precisión los datos personales de la población.

IV. Criterios de Evaluación (Anexo 1)

15 ¿Cómo se identifican en la práctica los tratamientos individuales sobre datos personales que deben considerarse para la aplicación de los criterios B, C y D del Anexo 1, utilizados para determinar la obligación de designar un ODP por gran volumen de datos?

A efectos de la presente Directiva, el conteo de tratamientos individuales sobre datos personales parte de un criterio sencillo: se considera tratamiento individual a cada operación específica que persigue una finalidad determinada respecto de los datos de un titular.

Por ejemplo, un formulario para la creación de una cuenta de usuario en un determinado sistema de información (como una mesa de partes virtual), requiere que la persona que se registra ingrese como mínimo cinco (5) datos personales. De manera simultánea, a nivel interno, el sistema puede realizar comparaciones de los datos ingresados contra la base de datos institucional (para evitar la duplicidad de registros) y ejecutar finalmente una copia de seguridad de los datos recibidos. En ese escenario, todo el conjunto de operaciones descrito se considera un único tratamiento individual, en tanto la **finalidad es el registro del usuario,** siendo que el ingreso de cada dato, la comparación interna con la base de datos y la generación de respaldos técnicos, se consideren como operaciones de soporte indispensables para materializar dicha finalidad.

En ese sentido, no debe interpretarse que todas las acciones o procesos que los sistemas de información ejecutan sobre datos personales constituyen, por sí mismos, tratamientos individuales, siempre que dichas acciones o procesos formen parte del soporte técnico necesario para la ejecución de un mismo tratamiento con una finalidad única.

16 ¿Cómo identificamos los tratamientos individuales efectuados sobre datos personales sensibles (Criterio B), a partir del ejemplo anterior?

La entidad pública, organización o empresa solo aplicará a esta categoría **cuando alcance la cantidad de 1000 titulares únicos registrados en sus bancos** de datos para los que almacene, por lo menos, un dato personal sensible.

Tomando el ejemplo anterior, si el formulario para la creación de cuenta requiere el ingreso de, por lo menos, un dato sensible, este registro de usuario se tomará como un tratamiento individual de datos sensibles, sin importar la cantidad de datos ingresados.

En otro ejemplo, una entidad determinada mantiene registro de sus pacientes (3000 personas), donde se incluyen cinco (5) datos sensibles de salud por titular. Dentro de los tratamientos identificados, la entidad encontró que aplica algoritmos o filtros automatizados para realizar dos scoring o perfilamiento de los usuarios con finalidades distintas: el algoritmo **A** trata los cinco (5) datos sensibles registrados y tiene como objetivo categorizar al titular de acuerdo a sus necesidades clínicas, a fin de efectuar prospección comercial de servicios médicos especializados; el algoritmo **B,** por otro lado, solo emplea tres (3) datos sensibles y su finalidad es categorizar al titular de acuerdo a su perfil económico/social, a fin de ofrecerle descuentos sobre productos ya contratados. En este escenario, debido a su finalidad individual, la aplicación de cada algoritmo representa un tratamiento individual, a pesar que el banco de datos personales sobre los que se aplican los algoritmos A y B es el mismo.

ANPD | **Autoridad Nacional de Protección de Datos Personales**

Consultas telefónicas:
(01) 204 8020 anexo: 2410
De lunes a viernes
de 8:00 a. m. a 4:30 p. m.

Correo electrónico:
oficialdedatospersonales@minjus.gob.pe

Mesa de partes presencial:
Calle Scipión Llona n.º 350, Miraflores, Lima

Mesa de partes virtual

Página web:
www.gob.pe/anpd

PERÚ | Ministerio de Justicia y Derechos Humanos