Naciones Unidas A/77/196

Asamblea General

Distr. general
20 de julio de 2022

Original: español

**Septuagésimo séptimo período de sesiones**
Tema 69 b) del programa provisional
**Promoción y protección de los derechos humanos: cuestiones de derechos humanos, incluidos otros medios de mejorar el goce efectivo de los derechos humanos y las libertades fundamentales**

# Derecho a la privacidad

## Nota del Secretario General

El Secretario General tiene el honor de transmitir a la Asamblea General el informe preparado por la Relatora Especial sobre el derecho a la privacidad, Ana Brian Nougrères, presentado de conformidad con la resolución 28/16 del Consejo.

22-11362 (S) 270722 180822

*Resumen*

Los principios que informan la privacidad y la protección de datos personales constituyen parte estructural de los sistemas jurídicos sobre la materia, en tanto cumplen con una doble función, de interpretación y de integración del ordenamiento normativo. Son el medio más valioso y útil, para los responsables y encargados del tratamiento que buscan realizar un adecuado procesamiento de la información personal, particularmente cuando tienen que hacer frente a los riesgos de un mal uso de las tecnologías de la información y de las comunicaciones.

Analizaremos en particular los siguientes principios: legalidad, licitud y legitimidad; consentimiento; transparencia; finalidad; lealtad; proporcionalidad; minimización; calidad; responsabilidad y seguridad, en tanto fundantes de todo el sistema jurídico de privacidad y protección de datos personales. Realizaremos un estudio comparativo, según la formulación de los principios contenida en siete documentos normativos internacionales, conforme se verá en el desarrollo que sigue. Destacaremos sus elementos comunes como una forma de trabajar en pos de un concepto de armonización en el contexto global, enfrentando los retos de la protección de la privacidad y de los datos personales, en tanto derechos humanos fundamentales que —en su transversalidad— son facilitadores de otros derechos humanos fundamentales, como el derecho a la libertad, a la igualdad, al honor y a la dignidad del ser humano en la era digital.

# Principios que informan la privacidad y la protección de datos personales

## I. Introducción

1. En materia de privacidad y protección de datos, existen principios rectores que se constituyen en pautas de interpretación y ayudan a completar vacíos en la legislación, que tienen un valor fundamental que se relaciona con la forma de encarar los problemas que se presentan a la hora de los tratamientos de datos personales, que utilizan las tecnologías de la información y de las comunicaciones.

2. Las normativas nacionales e internacionales en la materia se caracterizan por ser de carácter general. Por esa causa, es preciso que sean concretadas en las distintas actividades de tratamiento de datos personales, por los responsables y los encargados de los diferentes sectores en los que se encuentren, sean el público o el privado, sea en el ámbito nacional e internacional, cualquiera sea la tecnología[1] que se utilice. Un objetivo fundamental es el cumplimiento efectivo de las regulaciones sobre la materia, puesto que en un sistema democrático de Gobierno no basta con el mero reconocimiento y desarrollo legislativo de los derechos fundamentales. Estos derechos consagrados deben estar acompañados de garantías efectivas para su cumplimiento, cualquiera sea el contexto.

3. Ante esta situación, los principios rectores que vamos a analizar constituyen el medio más valioso y útil, al que recurrir para realizar un adecuado procesamiento de la información personal.

4. Los principios que informan la privacidad y la protección de los datos personales no deben ser considerados meras recomendaciones, pues tienen una jerarquía mayor que la de una recomendación. Dicha jerarquía les permite constituir una parte estructural de los sistemas jurídicos sobre la materia. Dichos principios comprometen a los responsables y a los encargados a actuar de manera adecuada en el tratamiento de los datos personales; así como a hacer frente a los riesgos de un mal uso de las tecnologías de la información y de las comunicaciones, de la inteligencia artificial y de otros desarrollos tecnológicos, lo que, a su vez, permitirá a los titulares de los datos, no perder el control que les corresponde con relación a su información personal.

5. Estos principios se encuentran estrechamente relacionados entre sí. Por esa causa, deben ser observados no solo de manera individual, sino como parte de un conjunto al que pertenecen, en la medida que lo que se busca es que se lleve a cabo una gestión adecuada de la información personal y respetuosa de los derechos y libertades fundamentales involucrados.

6. Resulta pertinente tener en cuenta las categorías especiales de datos personales, en particular los datos sensibles. Hoy en día, existe consenso en cuanto a las restricciones al tratamiento a las que deben estar sujetos dichos datos, requiriendo una mayor protección, en la medida que involucran la esfera más íntima de la persona; por lo que su tratamiento puede generar un riesgo mayor en cuanto a los derechos y a las libertades fundamentales.

[1] “La neutralidad tecnológica reviste particular importancia habida cuenta de la rapidez de la innovación tecnológica y contribuye a garantizar que la legislación siga pudiendo dar cabida a las novedades futuras y no resulte anticuada muy pronto.” Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, *Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas* (Viena, 2009).

7. De acuerdo con los documentos normativos internacionales, en la mayoría de los países, los datos sensibles, como regla general, no deberían ser tratados, a excepción de los casos establecidos explícitamente en las normas. Esta regla tiene su razón de ser en la necesidad de eliminar riesgos de discriminación para sus titulares.

8. Se entiende conveniente que las legislaciones indiquen las categorías de datos personales sensibles, estableciendo el alcance y las excepciones de su protección; siendo legítimo que los Estados tengan en cuenta su contexto (cultural, social o político) y las realidades locales, para considerar los datos pertenecientes a esta categoría.

9. El tratamiento de los datos personales sensibles debería permitirse cuando las legislaciones consagren garantías adecuadas para su protección. Dichas garantías habrán de comprender específicamente la necesidad de la aplicación de los principios rectores sobre la privacidad y la protección de datos.

10. Como punto de base para lograr el objetivo de desarrollar los principios de la privacidad y de la protección de datos personales en el contexto global, en el presente informe se han analizado los principios rectores contenidos en siete documentos normativos internacionales sobre la materia.

11. En estos documentos, se han resaltado fundamentalmente los aspectos básicos comunes y se han puesto en evidencia algunas particularidades, con el fin de buscar consensos que permitan la armonización de los esfuerzos para un tratamiento adecuado de los datos personales que responda a las exigencias de la defensa de este derecho, así como de la privacidad y de la dignidad de la persona en la era digital.

# II. Análisis normativo

12. A continuación, analizaremos los principios de legalidad, licitud y legitimidad; consentimiento; transparencia; finalidad; lealtad; proporcionalidad; minimización; calidad; responsabilidad y seguridad. A los efectos del presente análisis, los documentos a continuación constituyen sus pilares basales:

- Reglamento General de Protección de Datos de la Unión Europea (Reglamento General)[2]
- Convenio modernizado del Consejo de Europa para la protección de las personas con respecto al tratamiento de datos personales (Convenio 108 modernizado)[3]
- Resolución 45/95 de la Asamblea General de las Naciones Unidas intitulada “Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales” (Principios rectores de las Naciones Unidas)
- Estándares de Protección de Datos Personales para los Estados Iberoamericanos, aprobados por la Red Iberoamericana de Protección de Datos (Estándares Iberoamericanos)[4]

[2] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.
[3] Disponible en: https://rm.coe.int/convenio-para-la-proteccion-de-las-personas-con-respecto-al-tratamient/1680968478.
[4] Red Iberoamericana de Protección de Datos, “Estándares de Protección de Datos de los Estados Iberoamericanos”. Disponible en: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf.

- Recomendaciones del Consejo sobre las Directrices para la Protección de la Privacidad y los Flujos Transfronterizos de Datos Personales de la Organización para la Cooperación Económica y el Desarrollo (OCDE) (Directrices OCDE)[5]
- Marco de privacidad (privacy framework) de la Cooperación Económica Asia-Pacífico (APEC) (Marco de privacidad APEC)[6]
- Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con anotaciones, aprobados por la Asamblea General de la Organización de Estados Americanos (OEA) (Principios de la OEA)[7]

## Principio de legalidad, licitud y legitimidad

13. Este principio alude a que el tratamiento de los datos personales, en todo el ciclo de vida de los mismos, debe ser realizado por el responsable o por el encargado, de manera respetuosa de las leyes sobre la materia, en tanto sean de conformidad con los derechos humanos internacionalmente reconocidos. Esto supondrá que, a través de un adecuado y, por lo tanto legal, tratamiento de los datos personales, se garantizará también el respeto de la privacidad, así como el de los otros derechos y de la dignidad de la persona humana como titular del dato.

14. El derecho a la protección de datos personales que es reconocido como un derecho que ofrece garantías para otros derechos[8], permitirá que un adecuado tratamiento de los datos que conciernen a una persona brinde, a su vez, la seguridad del respeto de otros derechos fundamentales que le correspondan.

15. Si bien es cierto que la legalidad debe ser el cauce por el que deben discurrir todas las actividades del tratamiento, durante todo el ciclo de vida de los datos personales, es decir desde su recopilación hasta la cancelación de los mismos, se suele poner énfasis en la primera actividad de tratamiento, que es la recopilación de los datos, en la medida que si esta es llevada a cabo de manera ilegal, afectará la legalidad de las otras actividades de tratamiento que se den a partir de ella[9].

16. En el caso del Convenio 108 modernizado, se menciona dentro de la legitimidad del tratamiento que este debe perseguir un fin legítimo en todas sus etapas, así como realizarse conforme a la ley (art. 5.1).

17. En el caso de los principios rectores de las Naciones Unidas, por el principio de licitud y lealtad la recolección y elaboración de la información personal deben realizarse por medio de procedimientos lícitos y leales.

18. Los distintos documentos normativos internacionales han ido diversificando o incorporando otros principios de la protección de datos que se relacionan y se complementan con el principio de legalidad.

[5] Disponible en: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#recommendation.

[6] Disponible en: https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015).

[7] Informe del Comité Jurídico Interamericano, “Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con anotaciones”. 9 de abril de 2021.

[8] Artículo 1 del Convenio 108 modernizado.

[9] Párrafo 7 de las Directrices OCDE; principio 1 de los Principios Actualizados del Comité Jurídico; artículo 1 de los Principios rectores.

19. En la línea señalada, el Reglamento General, en su artículo 6 y considerandos 39 y 40, considera que se cumple con el principio de licitud del tratamiento, cuando este se realice en virtud de una de las bases jurídicas establecidas por el derecho.

20. En el caso de los Estándares, es en cumplimiento del principio de legitimación que se podrá realizar el tratamiento de los datos personales, solo en la medida en que se esté en alguno de los supuestos establecidos por el derecho (art. 11).

21. En lo que concierne a la Recomendación del Consejo de la OCDE, se condiciona la recogida por medios legales y honestos y con el conocimiento o consentimiento del titular de los datos (art. 7).

22. La legalidad del procesamiento de datos personales tiene como requisito base la configuración de algunas de las causales legitimantes establecidas en la normativa que sea de aplicación. Del análisis de las disposiciones de los documentos normativos internacionales analizados, se desprende el cuadro 1, donde se muestran las bases legitimantes reconocidas internacionalmente.

Cuadro 1
**Causas legitimantes para el tratamiento**

| | *Convenio modernizado del Consejo de Europa para la protección de las personas con respecto al tratamiento de datos personales* | *Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales de las Naciones Unidas* | *Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos* | *Reglamento General de Protección de Datos de la Unión Europea* | *Directrices para la protección de la privacidad y los flujos transfronterizos de datos personales de la OCDE* | *Marco de privacidad de la APEC* | *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, con anotaciones, de la OEA* |
|---|---|---|---|---|---|---|---|
| | *Artículo* | *Artículo* | *Artículo* | *Artículo* | *Párrafo* | *Principio* | *Principio* |
| Consentimiento del titular | 5.2 | | 11.1.a) | 6.1.a) | 10.a) | III.24 | 1 |
| Consentimiento del titular para una finalidad incompatible con la que habilitó la recopilación | | 3 b) | | | | | |
| Ley | 5.3 | | 14.1 | | 10.b) | IV.25 c) | 1 |
| Obligación legal del responsable | | | 11.1.f) | 6.1.c) | | | 1 |
| Contrato o medidas precontractuales | | | 11.1.e) | 6.1.b) | | IV.25 b) | 1 |
| Interés público | | | 11.1.h) | 6.1.e) | | | 1 |
| Interés legítimo del responsable | | | 11.1.i) | 6.1.f) | | | 1 |
| Intereses vitales del titular o tercero | | | 11.1.g) | 6.1.d) | | | 1 |
| Reconocimiento o defensa de derechos del titular ante autoridad pública | | | 11.1.d) | | | | 1 |
| Orden judicial, resolución o mandato de autoridad pública | | | 11.1.b) | | | | 1 |

23. De los documentos normativos internacionales analizados, las causas habilitantes para el tratamiento de los datos personales, se dan en el siguiente orden de reiteración en su reconocimiento.

24. Seis documentos integran el consentimiento del titular como una de las bases legitimantes para el tratamiento de los datos personales, siendo la más constante dentro de las normativas analizadas.

25. En el caso de Principios rectores de las Naciones Unidas, no se establece el consentimiento como una causa habilitante general, sino para realizar actividades de tratamiento con propósitos diferentes a los que habilitaron la recopilación. Teniendo en cuenta lo acabado de señalar, así como lo establecido en el artículo 1 de los principios, donde se regula el principio bajo análisis, lo que habilitaría el tratamiento de datos personales sería el observar procedimientos leales y lícitos, acordes con los propósitos de la Carta de las Naciones Unidas, lo que implicará que se cumpla con una medida de publicidad o se ponga en conocimiento del titular de la información.

26. Al consentimiento del titular, le sigue el imperio de la ley o disposiciones legales existentes en el derecho interno de cada país miembro, lo cual luce en cinco de los documentos.

27. Cuatro documentos incluyen a las relaciones contractuales y medidas precontractuales como base legitimante, cuyo reconocimiento, en el marco de las relaciones civiles y comerciales, sumado al comercio electrónico, resulta de particular relevancia en el contexto económico de la era digital.

28. Tres documentos reconocen las causas legitimantes referidas a: la obligación legal del responsable; el interés público; el interés legítimo del responsable y los intereses vitales del titular o de un tercero; y dos documentos incluyen al reconocimiento o defensa de derechos del titular ante autoridad pública y a la orden judicial, resolución o mandato de autoridad pública.

29. En respeto al derecho a la protección de datos personales, a la privacidad y a la dignidad de la persona, cualquiera sea el contexto normativo, para que un responsable del tratamiento, y un encargado, de ser el caso, puedan gestionar datos personales, deben encontrarse en una de las causas habilitantes para dicho fin.

## Principio de consentimiento

30. El consentimiento es una manifestación de voluntad, expresa o tácita, por la cual un sujeto se vincula jurídicamente. Cuando el titular de los datos da su consentimiento, se pone de manifiesto, de manera directa, el poder de control sobre sus datos personales, que le corresponde en su calidad de titular.

31. El principio de consentimiento está íntimamente unido al principio de legalidad, en la medida que es la causa habilitante para el tratamiento de los datos personales más común, internacionalmente reconocida.

32. El principio de consentimiento expresa la necesidad de que el sujeto titular de los datos manifieste su voluntad para que los mismos puedan ser recolectados, grabados, transformados, comunicados, transferidos y en general se pueda realizar cualquier actividad del tratamiento de sus datos hasta la eliminación de los mismos; habilitando y delimitando todo el ciclo de vida del dato en manos del responsable[10].

33. En los documentos normativos analizados, el consentimiento es una de las bases legitimantes más importantes para el tratamiento de datos personales, pues se

[10] Considerando 32 del Reglamento General.

encuentra específicamente previsto como tal, en seis de aquellos[11], con diversos elementos característicos.

34. Los elementos que a continuación se mencionan son una forma de definir los parámetros dentro de los cuales el consentimiento puede darse, como manera de reflejar la manifestación de voluntad del titular del dato, de la forma más fiel posible.

35. En el cuadro 2 a continuación se comparan las características encontradas en los siete documentos normativos internacionales analizados.

[11] Como ha quedado señalado en el acápite anterior, referido al principio de legalidad, licitud y legitimidad, en el caso de los Principios rectores de las Naciones Unidas, se establece el consentimiento solo como causa legitimante para realizar actividades de tratamiento con propósitos diferentes a los que habilitaron la recopilación.

Cuadro 2
**Características del consentimiento**

| | *Convenio modernizado del Consejo de Europa para la protección de las personas con respecto al tratamiento de datos personales* | *Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales de las Naciones Unidas* | *Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos* | *Reglamento General de Protección de Datos de la Unión Europea* | *Directrices parala protección de la privacidad y los flujos transfronterizos de datos personales de la OCDE* | *Marco de privacidad de la APEC* | *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, con anotaciones, de la OEA* |
|---|---|---|---|---|---|---|---|
| | *Artículo(s)* | *Artículo(s)* | *Artículo(s)* | *Artículo(s)* | *Párrafo* | *Principio* | *Principio* |
| Libre | 5.2 | | | 4.11 | | | 2 |
| Específico | 5.2 | | 12 | 4.11 | | | 2 |
| Informado | 5.2 | | | 7.3 y 4.11 | Punto 52 del memorándum | | 2 |
| Inequívoco | 5.2 | | 12 | 4.11 | | | 2 |
| Revocable | | | 12.2 | 7.3 | | | 2 |

36. Como bien puede verse, en el Convenio 108 modernizado (art 5.2), el Reglamento General[12] y los Principios Actualizados de la OEA (principio 2) son los textos que más características imprimen al tipo de consentimiento que requiere la protección de datos personales, como manifestación fiel de la voluntad del sujeto titular de los datos.

37. Este tipo de consentimiento, siguiendo el estudio de características encontradas en los textos, debe ser libre, específico, informado, inequívoco y revocable. Vemos que la revocabilidad es una característica *a priori* faltante en el Convenio 108 modernizado (al igual que en los Principios Rectores de las Naciones Unidas (art. 4), las Directrices OCDE y el Marco de Privacidad APEC (arts. 21 al 23 y 26)), aunque dicha acción puede encontrarse, en los distintos textos, prevista dentro de los derechos de los titulares de los datos[13]. La revocación, se presenta como un correlato de la facultad de consentir en sentido contrario y posterior en el tiempo, a la emisión del consentimiento.

38. En el caso de las Directrices OCDE, la característica del consentimiento informado no surge en principio de la redacción del articulado, el cual establece que la recolección de datos debe realizarse (en cuanto aplique) con el conocimiento o el consentimiento del titular. Sin embargo, el memorándum explicativo de los principios señala que, si bien puede establecerse o no el consentimiento del titular como requisito, el conocimiento debe ser el requisito mínimo[14]. Por lo tanto, cuando el consentimiento sea el requisito para la colecta de datos personales, debe ser informado, por cuanto el conocimiento del titular de los datos es el requisito mínimo que debe cumplirse.

39. La caracterización de la manifestación de voluntad, que autoriza el tratamiento de los datos, no siempre aparece dentro de los artículos que regulan el principio de consentimiento; pero ha de tenerse en cuenta que algunos de los documentos, como el artículo 4 del Reglamento General, establecen algunas de estas características dentro de las definiciones y en los considerandos.

40. En los Principios Rectores de las Naciones Unidas y el Marco de Privacidad de la APEC no se establecen características del consentimiento.

41. Debe quedar claro que, de ser el consentimiento la causa habilitante para el tratamiento de datos personales, el mismo debe ser otorgado de manera previa, al inicio de las actividades que le constituyan.

42. El principio de consentimiento está directamente vinculado al principio de transparencia, en la medida que un consentimiento válido por parte del titular de los datos, supone que este debe estar informado adecuadamente de las condiciones a las que será sometida su información personal.

43. Como aspecto destacable, cabe mencionar el consentimiento para el tratamiento de los datos personales de los menores de edad y cómo esto se ve reflejado en los distintos documentos. En lo que a la protección de datos personales respecta, los niños, niñas y adolescentes son considerados como un grupo vulnerable especialmente susceptible a las consecuencias del tratamiento de la información que les concierne, por lo que se requiere su protección integral y bienestar.

44. Tanto en los casos de los Estándares Iberoamericanos (art. 13), el Reglamento General (art. 8) como en los Principios de la OEA (principio 2, anotado), el consentimiento de menores es sometido a la autorización de los titulares de la patria potestad, o quienes ejerzan su representación legal, quienes serán los responsables

[12] Artículos 4.11; 6.3 a) y b); 6.1 a), b), c), d) y e); 7; y 8.
[13] Artículo 9 del Convenio 108 modernizado; artículo 4 de los Principios rectores.
[14] Memorándum explicativo (punto 52), pág. 19.

por las consecuencias del tratamiento. Sobre este punto, los citados documentos, establecen también que el derecho interno de cada Estado podrá establecer una edad mínima de los menores para que, por sí mismos, puedan dar el consentimiento, con las salvaguardias debidas.

## Principio de transparencia

45. Uno de los principios relativos al tratamiento de datos personales se refiere a que los datos deberán ser tratados por el responsable de manera transparente en relación con el titular de los datos. Este principio supone que el responsable deberá informar al titular de las condiciones de tratamiento a las que será sometida su información personal, desde el momento de la recogida, de tal forma que el titular de los datos esté en condiciones de poder materializar el control que le corresponde sobre los mismos.

46. En el cuadro 3 a continuación se aprecia cuál es la información que los documentos normativos internacionales analizados, consideran que los responsables deben proporcionar a los titulares de los datos.

Cuadro 3

**Información que se debe proporcionar a los titulares de los datos**

| | *Convenio modernizado del Consejo de Europa para la protección de las personas con respecto al tratamiento de datos personales* | *Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales de las Naciones Unidas* | *Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos* | *Reglamento General de Protección de Datos de la Unión Europea* | | *Directrices para la protección de la privacidad y los flujos transfronterizos de datos personales de la OCDE* | *Marco de privacidad de la APEC* | *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, con anotaciones, de la OEA* |
|---|---|---|---|---|---|---|---|---|
| | | | | *Cuando los datos se obtienen del titular* | *Cuando los datos no se obtienen del titular* | | | |
| | *Artículo(s)* | *Artículo(s)* | *Artículo(s)* | *Artículo(s)* | | *Párrafo* | *Principio* | *Principio* |
| Identidad y domicilio del responsable y/o representante | 8.1.a) | | 16.2a) | 13.1.a) | 14.1.a) | 12 | 21.d) | 2 |
| Existencia y/o características principales del tratamiento | | | 16.1 | | | 12 | 21.a) | |
| Fundamento o base jurídica | 8.1.b) | | | 13.1.c) | 14.1.c) y 14.2b) | | | 2 |
| Fines o propósito del tratamiento | 8.1.b) | | 16.2b) | 13.1.c) | 14.1.c) | 12 | 21.b) | 2 |
| Categorías de datos tratados | 8.1.c) | | | | 14.1.d) | | | |
| Origen de los datos cuando no se obtuvieron directamente del titular | | | 16.2.e) | | 14.2.f) | | | |
| Destinatarios o categoría de destinatarios | 8.1.d) | | 16.2.c) | 13.1.e) | 14.1.e) | | 21.c) | 2 |
| Información sobre los derechos y la forma de ejercerlos | 8.1.e) | | 16.2.d) | 13.2.b) y c) | 14.2.c) y d) | | 21.e) | 2 |
| Derecho a presentar una reclamación ante la autoridad de control | | | | 13.2.d) | 14.2. e) | | | |

| | *Convenio modernizado del Consejo de Europa para la protección de las personas con respecto al tratamiento de datos personales* | *Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales de las Naciones Unidas* | *Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos* | *Reglamento General de Protección de Datos de la Unión Europea* | | *Directrices para la protección de la privacidad y los flujos transfronterizos de datos personales de la OCDE* | *Marco de privacidad de la APEC* | *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, con anotaciones, de la OEA* |
|---|---|---|---|---|---|---|---|---|
| | | | | *Cuando los datos se obtienen del titular* | *Cuando los datos no se obtienen del titular* | | | |
| | *Artículo(s)* | *Artículo(s)* | *Artículo(s)* | *Artículo(s)* | | *Párrafo* | *Principio* | *Principio* |
| Si la comunicación es un requisito legal, contractual, o es necesaria para suscribir un contrato, y si el interesado está obligado a facilitar sus datos personales y las consecuencias de no facilitarlos | | | | 13.2.e) | | | | |
| Existencia de decisiones automatizadas, incluida la elaboración de perfiles, información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas de dicho tratamiento | | | | 13.2.f) | 14.2.g) | | | |
| Información sobre el fin cuando se proyecta un tratamiento ulterior para un fin que no sea aquel para el que se obtuvieron los datos | | | | 13.3 | 14.4 | | | |
| Datos de contacto del Delegado de Protección de Datos | | | | 13.1.b) | 14.1.b) | | | |

| | *Convenio modernizado del Consejo de Europa para la protección de las personas con respecto al tratamiento de datos personales* | *Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales de las Naciones Unidas* | *Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos* | *Reglamento General de Protección de Datos de la Unión Europea* | | *Directrices para la protección de la privacidad y los flujos transfronterizos de datos personales de la OCDE* | *Marco de privacidad de la APEC* | *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, con anotaciones, de la OEA* |
|---|---|---|---|---|---|---|---|---|
| | | | | *Cuando los datos se obtienen del titular* | *Cuando los datos no se obtienen del titular* | | | |
| | *Artículo(s)* | *Artículo(s)* | *Artículo(s)* | *Artículo(s)* | | *Párrafo* | *Principio* | *Principio* |
| Plazo de conservación o criterio para determinarlo | | | | 13.2.a) | 14.2.a) | | | |
| Si se prevé realizar comunicaciones o transferencias y la normativa que lo autoriza | | | | 13.1.f) | 14.1.f) | | | |
| Información a ser trasmitida | | | | | | | | 2 |
| Finalidades que motivan las transferencias | | | 16.2.c) | | | | | |

47. Como puede apreciarse, de los siete documentos normativos internacionales analizados, en los Principios rectores no se ha regulado el principio de transparencia; consecuentemente, en los seis documentos restantes analizaremos la recurrencia de la información que en ellos se señala debe proporcionarse a los titulares de los datos personales en cumplimiento del principio de transparencia.

48. Seis documentos señalan que se debe informar sobre la identidad y domicilio del responsable o de su representante, así como los fines o propósitos del tratamiento. Estos datos constituyen los básicos iniciales para la actuación transparente.

49. Cinco documentos señalan que se informe sobre los derechos que le corresponden al titular de los datos y la forma de ejercerlos, así como sobre los destinatarios o categoría de estos. Con respecto a que el titular tenga información sobre los derechos que, en su calidad de tal, le corresponden, expresa la importancia de que esté en condiciones apropiadas para ejercer su poder de control sobre la información personal que le concierne.

50. Tres documentos señalan que se informe sobre el fundamento o base jurídica que habilita el tratamiento, así como de la existencia y/o características principales del tratamiento.

51. El principio de transparencia debe observarse independientemente de cuál sea la base jurídica que legitima el tratamiento. Pueden encontrarse situaciones de excepción, relacionadas a la oportunidad en que se proporciona la información al titular del dato[15], o cuando este no es la fuente de la que se recopila su información personal[16], debiendo ser aplicadas de manera que se busque la mayor transparencia posible y se cumpla con la lealtad.

52. Dos documentos señalan que se informe sobre la categoría de los datos tratados y sobre el origen de ellos cuando no se obtuvieron directamente del titular.

53. Se ha considerado, también, incluir informaciones que solo en un documento normativo internacional se establece que deben ser materia de comunicación para el titular del dato personal, en la medida que buscan proporcionar mejores condiciones para que este ejerza su poder de control.

54. En esta situación tenemos el caso de los Estándares para los Estados Iberoamericanos en relación a las finalidades que motivan las transferencias, y el caso del Reglamento General, sobre los siguientes puntos: datos de contacto del delegado de protección de datos; plazo de conservación o criterio para determinarlo; si se prevé realizar comunicaciones o transferencias y la normativa que lo autoriza; el derecho a presentar una reclamación ante la autoridad de control; si la comunicación es un requisito legal, contractual, o es necesaria para suscribir un contrato, y si el interesado está obligado a facilitar sus datos personales y las consecuencias de no facilitarlos; la existencia de decisiones automatizadas, incluida la elaboración de perfiles, información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas de dicho tratamiento; y la información sobre el fin cuando se proyecta un tratamiento ulterior para un fin que no sea aquel para el que se obtuvieron los datos.

55. Dentro de las informaciones que, de manera exclusiva, se establecen en el Reglamento General, mencionaremos solo una, la que persigue que el titular del dato pueda entender el comportamiento del tratamiento al que será sometida la información que le concierne, por ejemplo, si se trata de un caso de inteligencia

[15] Artículo 22 del Marco de privacidad APEC.
[16] Artículo 8.3 del Convenio 108 modernizado.

artificial, y es la que señala que se le debe dar: “información significativa sobre la lógica aplicada” y “la importancia y las consecuencias previstas”[17].

56. La información que debe conocer el titular del dato, para cumplir con el principio de transparencia, debe ser proporcionada en lenguaje sencillo, claro, inteligible y de fácil acceso y comprensión[18], teniendo especial cuidado en estos aspectos si se trata de niños, niñas y adolescentes[19].

57. Es dable agregar el interés especial de una debida actuación del responsable al gestionar información personal, en tanto deberá contar con políticas transparentes del tratamiento de datos personales[20].

## Principio de finalidad

58. El principio de finalidad guía y delimita todas las actividades del tratamiento de los datos personales desde la recopilación hasta la cancelación. La finalidad será definida, como regla, por el responsable, pero no será considerada como tal si no se encuentra vinculada a alguna de las causas legitimantes que lo habiliten para el tratamiento.

59. Desde la recopilación, la finalidad debe cumplir determinadas características, las cuales son señaladas en los documentos normativos internacionales analizados. Así, la finalidad debe ser: explícita, específica, legítima y pertinente. Cumplidas las características que las normativas establecen para definir la finalidad o finalidades, estas funcionarán como delimitadoras de las actividades de tratamiento a las que serán sometidos los datos personales.

60. Conforme este principio, los datos recolectados pueden ser utilizados exclusivamente dentro de los límites de la finalidad para la cual fueron recabados. Se posiciona como una limitante para las distintas actividades de tratamiento, desde la recolección, pasando por el almacenamiento, modificación, comunicación y transferencia, así como para cualquier procesamiento de los datos, hasta la cancelación de los mismos.

61. Por lo señalado, cualquier actividad de tratamiento, no debe estar fuera de lo permitido por las finalidades inicialmente definidas, tal como lo señalan los distintos documentos normativos[21], salvo habilitación expresa de la normativa aplicable y con las salvaguardias del caso. Un ejemplo de lo acabado de señalar, lo encontramos en el Marco de privacidad[22], donde se menciona la posibilidad de que los datos sean utilizados con otros fines que sean compatibles con los fines inicialmente establecidos.

---

[17] Agencia Española de Protección de Datos. *Adecuación al Reglamento General de Protección de Datos de tratamientos que incorporan inteligencia artificial: una introducción*. Febrero 2020, pág. 24. Disponible en: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf.

[18] Artículo 16.3 de los Estándares Iberoamericanos; artículo 12.1 del Reglamento General; artículo 21 del Marco de privacidad APEC.

[19] Artículo 16.3 de los Estándares Iberoamericanos; artículo 12.1 del Reglamento General.

[20] Artículo 16.4 de los Estándares Iberoamericanos; párrafo 12 de las Directrices OCDE; artículo 21 del Marco de privacidad APEC.

[21] Artículo 5.4 b) del Convenio 108 modernizado; artículo 3 de los Principios rectores de las Naciones Unidas; artículo 17 de los Estándares Iberoamericanos; artículo 5.1 b) del Reglamento General;
párrafo 9 de las Directrices OCDE; artículos 24 y 25 del Marco de privacidad APEC; Principio 1 de los Principios Actualizados de la OEA.

[22] Artículo 25, Título IV del Marco de privacidad APEC.

62. El principio de finalidad se encuentra establecido en todos los textos analizados[23], explicitando sus características y la consecuencia de su aplicación en la práctica. Se relaciona estrechamente con el principio de legalidad o licitud, al establecer como característica necesaria que los fines deben ser legítimos.

63. Los documentos normativos internacionales señalan las características que debe cumplir la finalidad para habilitar el tratamiento de los datos personales; tal y como se muestra en el siguiente cuadro, los fines deben ser explícitos, específicos, legítimos y pertinentes:

[23] Artículo 5.4 b) del Convenio 108 modernizado; artículo 3 de los Principios rectores de las Naciones Unidas; artículo 17 de los Estándares; artículo 5.1 b) del Reglamento General; artículo 9 de las Directrices OCDE; artículos 24 y 25 del Marco de privacidad APEC; Principio 1 de los Principios OEA.

Cuadro 4
**Características de la finalidad**

| | *Convenio modernizado del Consejo de Europa para la protección de las personas con respecto al tratamiento de datos personales* | *Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales de las Naciones Unidas* | *Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos* | *Reglamento General de Protección de Datos de la Unión Europea* | *Directrices parala protección de la privacidad y los flujos transfronterizos de datos personales de la OCDE* | *Marco de privacidad de la APEC* | *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, con anotaciones, de la OEA* |
|---|---|---|---|---|---|---|---|
| | *Artículo(s)* | *Artículo(s)* | *Artículo(s)* | *Artículo(s)* | *Párrafo* | *Principio* | *Principio* |
| Explícita | 5.4 b) | 3 | 17 | 5.1 b) | 9 | 24 y 25 | 1 |
| Específica | 5.4 b) | 3 | 17 | 5.1 b) | 9 | 24 y 25 | |
| Legítima | 5.4 b | 3 | 17 | 5.1 b) | | 24 y 25 | 1 |
| Pertinente | 5.4 b | 3 | 17 | 5.1 b) | 9 | 24 y 25 | |

64. En lo que concierne a la legitimidad, únicamente el párrafo 9 de las Directrices OCDE no la introdujo como característica de los fines para el tratamiento de los datos. Esto puede deberse tanto a un simple tema de redacción, como al hecho de obviar algo que en principio parecía estar implícito en el análisis de todo el documento normativo.

65. En el caso de los Principios de la OEA, todas las características de las finalidades, aunque no se desprendan expresamente del texto del principio 1, sí se entiende que están comprendidas en la anotación de dicho principio.

66. En cuanto a la especificidad del tratamiento con respecto a un fin, cabe decir que tanto el Reglamento General (art. 5.1), los Estándares Iberoamericanos (art. 17.3), el Convenio 108 modernizado (art. 5.4 b)) y los Principios de la OEA (principio 4) plantean la posibilidad de utilizar los datos con fines distintos para los cuales fueron recolectados, siempre y cuando estos tengan una finalidad estadística, histórica o científica.

67. Como ha quedado señalado, el fin o las finalidades legítimas que autorizaron el tratamiento, delimitan la actuación del responsable y del encargado, en su caso, por lo que, agotado o cumplido el fin, se perderá la legitimidad para seguir con el mismo, salvo disposición expresa de la normativa aplicable, que funja como nueva causa habilitante.

## Principio de lealtad

68. Este principio refiere a que la información personal debe ser tratada, respetando de manera fiel todos los términos y condiciones que habilitaron su recopilación y a la vez utilizando medios para el tratamiento que faciliten dicho objetivo.

69. Analizaremos, a continuación, los documentos normativos internacionales en los que se encuentra regulado el presente principio.

70. En el artículo 1 de los Principios rectores de las Naciones Unidas, se encuentra previsto como principio de licitud y lealtad. Se busca que los datos no sean tratados de manera ilícita o desleal y que tampoco vayan en contra de los principios de la Carta de las Naciones Unidas. En términos generales se refiere a que no se produzcan discriminaciones arbitrarias para el titular de los datos, desarrollándose el tratamiento de datos con sujeción a los principios, normas nacionales e internacionales, además de respetarse fielmente los derechos de las personas.

71. En el caso de los Estándares Iberoamericanos, se regula como principio de lealtad (art. 15). Conforme al mismo, el responsable tiene la obligación de privilegiar la protección de los intereses del titular y abstenerse de tratarlos a través de medios engañosos o fraudulentos. Considera desleales aquellos tratamientos que den lugar a una discriminación injusta o arbitraria contra sus titulares.

72. Asimismo, el Reglamento General en su artículo 5.1 a) establece que uno de los principios que debe ser observado en el tratamiento de los datos personales será el de lealtad, junto a la licitud y transparencia en relación con el interesado.

73. En las Directrices OCDE se alude a la honestidad dentro del principio de limitación de colecta (párr. 7). Este artículo se ocupa de dos temas: a) los límites a la recolección de datos; y b) los requisitos relativos a los métodos de recolección de datos, siendo justamente en este segundo aspecto donde se especifica que los datos deben obtenerse por medios legales y honestos.

74. Por su parte, el Marco de privacidad APEC en su artículo 24 alude de alguna manera al principio de lealtad estableciendo que los métodos de recopilación deben ser legales y justos.

75. Al igual que en el caso anterior, el Convenio 108 modernizado no hace expresa mención a este principio, pero se puede inferir que se encuentra regulado cuando establece en su artículo 5.4 a) que durante su tratamiento los datos deberán ser utilizados de forma justa, sin limitar esta condición no solo a la primera actividad del tratamiento, como es la recopilación, sino a cualquier actividad que suponga tratamiento de los mismos.

76. Finalmente, los Principios de la OEA lo establece integrando el primer principio "Finalidades legítimas y lealtad", señalando que "Los datos personales deberían ser recopilados solamente para finalidades legítimas y por medios leales y legítimos". En este caso se regula de manera expresa la lealtad con relación a los medios que se utilicen para la recopilación de los datos personales.

77. En los Principios de la OEA se explica que "la lealtad es contextual y depende de las circunstancias", y advierte que se requiere que se ofrezcan opciones apropiadas a las personas respecto a la forma y el momento en que vayan a proporcionar sus datos, excluyendo la obtención de los mismos por medio del fraude, del engaño y de pretextos falsos.

78. La lealtad debe observarse en todas las actividades de tratamiento de los datos personales; los documentos normativos internacionales que ponen énfasis en la actividad de la recopilación persiguen poner de relieve que una incorrecta o ilegal forma de proceder al inicio puede marcar y definir las posteriores actividades subsecuentes de tratamiento.

79. No debe quedar duda que el tratamiento leal debe caracterizar el proceder del responsable y del encargado durante todo el ciclo de vida del dato personal independientemente del contexto y de la tecnología que se utilice. Actuar lealmente supone responsabilidad, ética y observación de la normativa aplicable a la luz de los principios.

## Principio de proporcionalidad

80. El principio de proporcionalidad impone limitaciones al tratamiento de los datos personales. En virtud del mismo, los datos personales, así como las actividades de tratamiento a los que aquellos sean sometidos, deben limitarse únicamente al cumplimiento de los fines para los cuales fueron recopilados[24].

81. Debemos tener en cuenta que este principio debe respetarse en todas las etapas del tratamiento, desde el momento en que se esté decidiendo si llevar a cabo el tratamiento o no, con el objetivo de iniciar la primera etapa de la recopilación de manera adecuada y legal.

82. Estrechamente vinculado a este principio se encuentran el principio de finalidad, conforme el cual los datos deberían tratarse de forma compatible con la finalidad para la cual se recopilaron, y el principio de minimización, según el cual los datos deben ser los mínimos indispensables para llevar a cabo la finalidad establecida.

[24] Artículos 5.1 y 5.4 c) del Convenio 108 modernizado; artículo 18.1 de los Estándares Iberoamericanos; artículo 24 del Marco de privacidad APEC; artículo 5.1.c) del Reglamento General; artículo 3 a) de los Principios rectores de las Naciones Unidas; párrafo 9 de las Directrices OCDE; principios 3 y 4 de Principios de la OEA.

83. Dentro de las exigencias del principio de proporcionalidad, se encuentra la evaluación que el responsable debe realizar para elegir, entre los diversos tratamientos que le permitan cumplir la finalidad autorizada, el menos invasivo para la privacidad e intimidad. Esta evaluación se torna particularmente necesaria cuando se recurre al uso de determinadas tecnologías de la información y las comunicaciones que puedan poner en riesgo los derechos fundamentales.

84. Este principio se encuentra regulado en todos los documentos normativos internacionales analizados, ya sea de forma específica, como en el caso de los Estándares Iberoamericanos en su artículo 18, como dentro de otros principios. En los Principios rectores de las Naciones Unidas lo encontramos dentro del principio de finalidad (art. 3 a)); en el Convenio 108 modernizado en el principio de legitimidad del tratamiento y calidad de los datos (arts. 5.1 y 5.4 c)); en el caso del Reglamento General como contenido del principio de minimización de datos (art .5.1 c)); el Marco de privacidad APEC lo regula dentro del principio de limitación de la colecta (art. 24); en las Directrices OCDE dentro del principio de especificación del propósito (párr. 9); y finalmente, en la Principios de la OEA dentro del principio de pertinencia y necesidad (principio 3) y el principio de tratamiento y conservación limitados (principio 4).

85. De acuerdo con el cuadro 5, podemos apreciar que los Estándares Iberoamericanos, el Reglamento General, los Principios rectores de las Naciones Unidas y los Principios de la OEA, refieren a la pertinencia de los datos con relación al fin. Por otro lado, el Convenio 108 modernizado, los Estándares Iberoamericanos, el Reglamento General y los Principios de la OEA refieren a que los datos deben ser adecuados al fin.

86. Todos los documentos normativos internacionales analizados, a excepción de los Principios rectores de las Naciones Unidas, establecen, de alguna forma u otra, que los datos deben ser limitados y no deben ser excesivos con relación a la finalidad para la cual fueron recolectados. Los Estándares Iberoamericanos, el Reglamento General, el Marco de privacidad APEC y los Principios de la OEA establecen que los datos deben ser limitados a lo necesario en relación con la finalidad.

87. Por su parte, el Convenio 108 modernizado hace referencia a que los datos no deben ser excesivos en relación con el propósito en función del cual están siendo tratados; también se refiere a que los datos deben ser relevantes en relación al propósito y que el tratamiento de datos deberá ser proporcional al fin legítimo perseguido. En las Directrices OCDE se menciona que el uso de los datos estaría limitado al cumplimiento de los fines establecidos en el momento en que se recolectan los datos, o de otros que no sean incompatibles con esos fines.

Cuadro 5

**Limitaciones que configuran el principio de proporcionalidad**

| | *Convenio modernizado del Consejo de Europa para la protección de las personas con respecto al tratamiento de datos personales* | *Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales de las Naciones Unidas* | *Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos* | *Reglamento General de Protección de Datos de la Unión Europea* | *Directrices para la protección de la privacidad y los flujos transfronterizos de datos personales de la OCDE* | *Marco de privacidad de la APEC* | *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, con anotaciones, de la OEA* |
|---|---|---|---|---|---|---|---|
| | *Artículo* | *Artículo* | *Artículo* | *Artículo* | *Párrafo* | *Principio* | *Principio* |
| Adecuado al fin | 5.4.c) | | 18.1 | 5.1 c) | | | 3 |
| Relevante al fin | 5.4.c) | | | | | | |
| Pertinente al fin | | 3.a) | 18.1 | 5.1 c) | | | 3 |
| Limitado y no excesivo con relación al fin | 5.4.c.) | | 18.1 | 5.1 c) | 9 | 24 | 3 |

88. Con relación al principio bajo análisis, se puede encontrar que textualmente hay algunos documentos normativos internacionales que se refieren expresamente a los "datos personales", por ejemplo los Estándares Iberoamericanos, el Marco de privacidad APEC, el Reglamento General y los Principios rectores de las Naciones Unidas; otros al "tratamiento" de dichos datos, como las Directrices OCDE; y otros, tanto a los datos personales como al tratamiento que se vaya a realizar de los mismos, como el Convenio 108 modernizado y los Principios de la OEA.

89. No obstante lo señalado, y teniendo en cuenta los textos integrales de los documentos normativos internacionales, en general, el principio de proporcionalidad debe ser observado tanto con relación a los datos personales que se recopilan como a las actividades de tratamiento a los que serán sometidos dichos datos, siendo que —en ambos casos— deben ser los adecuados, relevantes, pertinentes y limitados a los fines legítimos para los que fueron recogidos.

## Principio de minimización

90. La minimización es el principio por el cual los datos deben ser en cada momento limitados a lo indispensable para llevar a cabo la finalidad establecida.

91. Es en este sentido que este principio se encuentra estrechamente vinculado con el de finalidad, el cual sirve como parámetro para limitar la cantidad de los datos a tratar.

92. El Reglamento General es el único instrumento que regula el principio de minimización de forma específica, en su artículo 5.1 c) estableciendo que: los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. El contenido de este principio se encuentra comprendido, en los otros documentos analizados[25], dentro del principio de proporcionalidad o de otro principio.

93. El principio de minimización, se encuentra también relacionado con determinadas obligaciones que el Reglamento General establece para el responsable y el encargado del tratamiento, como la privacidad por diseño y por defecto. La minimización como medida de prevención ayuda a disminuir el riesgo a las vulneraciones de seguridad y su impacto en las bases de datos.

94. Tal y como dice el artículo 25.2 del Reglamento General: "El responsable del tratamiento aplicará 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".

95. La minimización, debe observarse con mayor celo, teniendo en cuenta el uso cada vez más frecuente de las tecnologías de la información y comunicación, para el tratamiento de los datos personales.

## Principio de calidad

96. El principio de calidad implica que los datos sean precisos, exactos, completos y estén actualizados, lo que obliga a los responsables a disponer de medidas para

[25] Artículo 18 de los Estándares Iberoamericanos; artículo 3 de los Principios Rectores de las Naciones Unidas; artículos 5.1 y 5.4 c) del Convenio 108 modernizado; artículo 24 del Marco de Privacidad APEC; párrafo 9 de las Directrices OCDE; artículos 3 y 4 de los Principios de la OEA.

cumplir con ello. También se lo conoce en algunos documentos normativos internacionales como el principio de exactitud[26] o de integridad[27].

97. Tal como surge del cuadro 6 a continuación, los datos personales deben ser precisos, completos y exactos durante todo el proceso de tratamiento, y deben actualizarse siempre que sea necesario, ya sea de oficio, por parte del responsable, encargado, o a petición del interesado.

[26] Artículo 2 de los Principios rectores de las Naciones Unidas y artículo 7 de los Principios de la OEA.

[27] Artículo 27 del Marco de privacidad APEC.

Cuadro 6
**Características de la calidad del dato**

| | *Convenio modernizado del Consejo de Europa para la protección de las personas con respecto al tratamiento de datos personales* | *Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales de las Naciones Unidas* | *Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos* | *Reglamento General de Protección de Datos de la Unión Europea* | *Directrices para la protección de la privacidad y los flujos transfronterizos de datos personales de la OCDE* | *Marco de privacidad de la APEC* | *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, con anotaciones, de la OEA* |
|---|---|---|---|---|---|---|---|
| | *Artículo(s)* | *Artículo(s)* | *Artículo(s)* | *Artículo(s)* | *Párrafo* | *Principio* | *Principio* |
| Preciso/exacto | 5. 4.d) | 2 | 19.1 | 5.1.d) | 8 | 27 | 7 |
| Actualizado | 5. 4.d) | 2 | 19.1 | 5.1.d) | 8 | 27 | 7 |
| Completo | | 2 | 19.1) | | 8 | 27 | 7 |

98. En el artículo 5.4 d) del Convenio 108 modernizado se refiere a que los datos deben ser precisos y mantenerse actualizados. El artículo 2 de los Principios rectores de las Naciones Unidas refiere a la obligación de verificar la exactitud y pertinencia de los datos, a que continúen siendo lo más completos posibles a fin de evitar errores por omisión, y que se actualicen periódicamente.

99. En cinco documentos normativos internacionales, referidos a continuación, se vincula expresamente el principio que analizamos con el de finalidad del tratamiento.

100. Los Estándares Iberoamericanos en su artículo 19 establece como una obligación del responsable adoptar "medidas necesarias para mantener exactos, completos y actualizados los datos personales, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento".

101. El Reglamento General refiere a que los datos personales serán exactos y si fuera necesario actualizados, adoptando todas las medidas razonables para que se supriman o rectifiquen los que sean inexactos con relación a los fines del tratamiento (art. 5.1 d)).

102. Tanto las Directrices OCDE (párr. 8) como el Marco de privacidad APEC (art. 27), refieren a que los datos deberían ser exactos, completos y estar actualizados. Mientras, los Principios de la OEA , al referirse al principio de exactitud de los datos, establece que "deberían mantenerse exactos, completos y actualizados hasta donde sea necesario para las finalidades de su tratamiento, de tal manera que no se altere su veracidad" (principio 7).

103. La calidad de la información personal que esté siendo objeto de tratamiento, resulta vital para el buen logro de las finalidades que autorizaron su recopilación, así como su posterior tratamiento. Velar por la calidad del dato es signo de responsabilidad en la consecución de los fines autorizados.

104. Para el debido cumplimiento del principio de calidad, los responsables y encargados del tratamiento deben implementar medidas, al interior de sus organizaciones, orientadas a conseguir que los datos personales que recopilen y gestionen sean precisos, exactos, completos o íntegros y actualizados; el fin será el de cumplir las finalidades autorizadas con el debido respeto a los derechos de los titulares de la información personal, lo que redundará en beneficio de ellos mismos. Lo señalado es independientemente de las acciones que el titular del dato decida realizar; y, que estén orientadas a velar por la calidad de su información, cuando está siendo objeto de tratamiento por otra persona.

## Principio de responsabilidad

105. El principio de responsabilidad se puede analizar desde dos puntos de vista: por un lado, los responsables y encargados deben implementar mecanismos para cumplir con los principios relativos a la protección de datos y privacidad, resguardando y garantizando los derechos y libertades de los titulares; y, por otro lado, los responsables y encargados deben ser capaces de garantizar y demostrar el cumplimiento de dichos principios.

106. Dentro de los documentos normativos internacionales analizados encontramos que este principio se encuentra establecido en el artículo 20 de los Estándares Iberoamericanos; por el cual, el responsable debe implementar todos los mecanismos necesarios para el cumplimiento de los principios y obligaciones establecidas en dichos Estándares; así como, deberá rendir cuentas sobre el tratamiento de los datos personales al titular y a la autoridad de control. Para el fin señalado, podrá valerse de

estándares; mejores prácticas nacionales o internacionales; esquemas de autorregulación; sistemas de certificación, o cualquier otro mecanismo que determine adecuado para tales fines. Esto será aplicable también cuando los datos sean tratados por un encargado, así como al momento de realizar transferencias de datos.

107. Los Estándares Iberoamericanos detallan, de manera enunciativa, en su artículo 20.3 una serie de mecanismos que el responsable podrá adoptar para cumplir con el principio de responsabilidad; los mismos que revisará y evaluará permanentemente a fin de medir su eficacia en cuanto al cumplimiento de la legislación nacional aplicable.

108. En el Reglamento General se regula este principio, bajo el término responsabilidad proactiva (art. 5.2). Se lo puede definir como la necesidad u obligatoriedad de que el responsable aplique medidas técnicas y organizativas apropiadas a fin de garantizar y demostrar que el tratamiento de datos personales es conforme con el Reglamento (art. 24), especialmente los principios de: licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; e integridad y confidencialidad (art. 5.1). Para ello, el responsable deberá establecer procedimientos a través de los cuales se pueda garantizar la aplicación de la normativa y pueda demostrar frente a terceros la efectiva aplicación y su cumplimiento (art. 5.2).

109. El Reglamento General establece una serie de medidas para cumplir con este principio, entre las que se destacan: aplicar la protección de datos desde el diseño y por defecto (art. 25); realizar un registro de actividades de tratamiento (art. 30); establecer medidas de seguridad (art. 32); realizar notificaciones de violaciones de seguridad a la autoridad de control y a los interesados (arts. 33 y 34); elaborar una evaluación de impacto en la protección de datos (art. 35) y la designación de un delegado de protección de datos (art. 37).

110. De las medidas acabadas de citar y refiriéndonos solo a una de ellas, la evaluación de impacto en la protección de datos, incorporada por el Reglamento General, es obligatoria (art. 35, incisos 1, 3 y 4) cuando el tratamiento entrañe un alto riesgo para las libertades y derechos de los titulares de la información[28]; lo que resultará particularmente pertinente cuando se introduce una nueva tecnología para el tratamiento de los datos de las personas físicas.

111. La oportunidad en que el responsable debe realizar dicha evaluación es previa a la realización del tratamiento de los datos personales, de tal forma que ayude en la toma de decisiones correspondientes y en coherencia con la protección de datos desde el diseño y por defecto[29].

112. El principio de responsabilidad proactiva, exige a las organizaciones que analicen qué datos tratan, con qué finalidad lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de esta información, deben determinar expresamente la forma en que aplicarán las medidas que el Reglamento General exige,

[28] Artículo 35 del Reglamento General: "3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:
a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o c) observación sistemática a gran escala de una zona de acceso público."

[29] Directrices sobre la evaluación de impacto relativa a la protección de datos y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679.WP.248. Abril 2017. Pág. 16.

asegurándose que esas medidas y procedimientos sean los adecuados para cumplir con la protección de datos; así como de que pueden demostrarlo ante los interesados y la autoridad de control. Este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo[30].

113. En la misma línea, los Principios de la OEA hace hincapié en adoptar, implementar y demostrar medidas de seguridad, enfocando la responsabilidad a la seguridad de los datos personales, y también a las comunicaciones y transferencias internacionales de datos, debiendo los responsables asumir la tarea de asegurar un grado continuo de protección acorde con los principios establecidos en dicho instrumento (principio 10).

114. Las Directrices OCDE imponen la responsabilidad de cumplir con las normas y decisiones sobre la protección de la privacidad al responsable, debiendo ajustar su conducta a los principios establecidos (art. 14).

115. El Marco de privacidad APEC regula este principio enfocándose principalmente en las transferencias de datos (art. 32). Es así que cuando la información personal se va a transferir a otra persona u organización, tanto a nivel nacional como internacional, los responsables deben obtener el consentimiento del titular; o garantizar que el destinatario protegerá la información de manera coherente cuando no obtenga el consentimiento, adoptando medidas razonables para garantizar que la misma esté protegida después de su transferencia y acorde con los principios.

116. En el Convenio 108 modernizado, se establece que los responsables o encargados deberán implementar medidas técnicas y organizacionales que tomen en cuenta las implicancias del derecho a la protección de datos personales en todas las etapas del tratamiento (arts. 10.1 y 10.3). En el informe explicativo del Convenio, se indican ciertas medidas que el responsable o encargado podrá tener que tomar, entre las que mencionan las siguientes: capacitar empleados; establecer procedimientos de notificación adecuados; indicar cuándo deben eliminarse los datos; establecer disposiciones contractuales específicas delegando el tratamiento con el fin de hacer cumplir con el Convenio; así como establecer procedimientos internos que permitan verificar y demostrar el cumplimiento[31].

117. Finalmente, cabe destacar que, en todos los documentos normativos internacionales analizados, se prevé específicamente este principio, a excepción de los Principios rectores de las Naciones Unidas; y únicamente los Estándares Iberoamericanos y el Reglamento General establecen mecanismos o medidas a adoptar para el cumplimiento del mismo, tal como puede apreciarse en el cuadro 7 a continuación.

[30] Agencia Española de Protección de Datos Personales, "¿Qué es el principio de responsabilidad proactiva?", https://www.aepd.es/es/preguntas-frecuentes/2-rgpd/3-principios-relativos-al-tratamiento/FAQ-0208-que-es-el-prinipio-de-responsabilidad-proactiva.

[31] Traducción Núm. 058/2019. Informe Explicativo del Convenio, *Artículo 10, No. 85.* Disponible en: https://rm.coe.int/informe-explicativo-de-convenio/1680968479.

Cuadro 7

**Principio de responsabilidad y mecanismos para su cumplimiento**

| | *Convenio modernizado del Consejo de Europa para la protección de las personas con respecto al tratamiento de datos personales* | *Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales de las Naciones Unidas* | *Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos* | *Reglamento General de Protección de Datos de la Unión Europea* | *- Directrices para la protección de la privacidad y los flujos transfronterizos de datos personales de la OCDE* | *Marco de privacidad de la APEC* | *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, con anotaciones, de la OEA* |
|---|---|---|---|---|---|---|---|
| | *Artículo(s)* | *Artículo(s)* | *Artículo(s)* | *Artículo(s)* | *Párrafo* | *Principio* | *Principio* |
| Prevé específicamente el principio de responsabilidad | 10.1 | | 20 | 5.2 | 14 | 32 | 10 |
| Establece mecanismos o medidas a adoptar para cumplir con el principio | | | 20.3 | 5.1, 24, 25, 30, 32, 33, 34, 35 y 37 | | | |

118. En buena cuenta, este principio de responsabilidad, tiende a reforzar y hacer que el deber del cumplimiento de los principios y de toda la normativa sobre protección de datos y privacidad, que le corresponde observar a los responsables y encargados, en todas las actividades de tratamiento que realicen, pase a contar con elementos objetivos en los que el cumplimiento real se sustente y se cumplan los fines legítimos, en un clima de confianza y respeto de los derechos fundamentales involucrados.

## Principio de seguridad

119. La seguridad es fundamental para la protección de datos; no puede existir protección de datos sin seguridad.

120. Para cumplir con este principio se deben identificar, evaluar y documentar los riesgos que puedan producirse durante el ciclo de vida de los datos, con el fin de implementar las medidas de seguridad necesarias y poder garantizar la confidencialidad, integridad y disponibilidad de los datos personales, evitando la materialización de riesgos.

121. Todos los documentos normativos internacionales analizados incluyen este principio, de manera más o menos descriptiva, indicando la necesidad de establecer medidas de seguridad apropiadas, suficientes, oportunas, razonables o adecuadas para prevenir diferentes tipos de riesgos tales como, el acceso no autorizado, pérdida, modificación, destrucción o divulgación de los datos personales, entre otros [32].

122. En el cuadro 8 se detallan los tipos de medidas de seguridad y de riesgos especificados en cada uno de los documentos normativos internacionales. También se observa en cuál de ellos se establecen pautas, para determinar las medidas y la obligación de notificar vulneraciones de seguridad.

[32] Toda esta información surge del cuadro presentado en este acápite, donde podemos apreciar los tipos de medidas de seguridad y de riesgos, de los artículos ahí mencionados (artículo 7.1 del Convenio 108 modernizado; artículo 7 de los Principios Rectores de las Naciones Unidas; artículo 21.1 de los Estándares Iberoamericanos; artículo 5.1 f) del Reglamento General; párrafo 11 de las Directrices OCDE; artículo 28 del Marco de privacidad APEC; Principio 6 de los Principios de la OEA).

Cuadro 8
**Principio de seguridad**

| | *Convenio modernizado del Consejo de Europa para la protección de las personas con respecto al tratamiento de datos personales* | *Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales de las Naciones Unidas* | *Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos* | *Reglamento General de Protección de Datos de la Unión Europea* | *Directrices para la protección de la privacidad y los flujos transfronterizos de datos personales de la OCDE* | *Marco de privacidad de la APEC* | *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, con anotaciones, de la OEA* |
|---|---|---|---|---|---|---|---|
| Tipo de medidas de seguridad | Medidas de seguridad apropiadas<br>Art. 7.1 | Medidas apropiadas<br>Art. 7 | Medidas de carácter administrativo, físico y técnico suficientes<br>Art. 21.1 | Medidas técnicas y organizativas apropiadas<br>Art. 5.1-f) | Medidas de seguridad razonables<br>párr. 11 | Medidas apropiadas<br>Art. 28 | Salvaguardias de seguridad técnicas, administrativas u organizacionales razonables y adecuadas<br>Principio 6 |
| Tipo de riesgo | Riesgos como acceso accidental o no autorizado, destrucción, pérdida, uso, modificación o divulgación de datos personales<br>Art. 7.1 | Riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informático<br>Art. 7 | Daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales<br>Art. 22.1 | Tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental<br>Art. 5.1f) | Riesgos como pérdida o acceso no autorizado, destrucción, uso, modificación o divulgación de datos<br>párr. 11 | Pérdida o acceso no autorizado; destrucción, uso, modificación o divulgación no autorizada; u otro uso indebido<br>Art. 28 | Tratamientos no autorizados o ilegítimos, incluyendo el acceso, pérdida, destrucción, daños o divulgación, aun cuando éstos ocurran de manera accidental<br>Principio 6 |
| Pautas para determinar las medidas | | | Art. 21.2 | Art. 32 | | Art. 28 | |
| Notificación de vulneraciones de seguridad a la Autoridad de Control | Art. 7.2 | | Art. 22 | Art. 33 | párr. 15 c) | Art. 54 | |
| Notificación de vulneraciones de seguridad a los titulares afectados | | | Art 22 | Art 34 | párr. 15 c) | Art. 54 | |

123. Las medidas de seguridad deben ser proporcionales a la magnitud del riesgo, deben revisarse y actualizarse periódicamente, pudiendo también auditarse, para mejorarlas e impedir que se vuelvan obsoletas[33].

124. En el caso de los Principios de la OEA se establece que dichas medidas de seguridad deberían ser objeto de auditoría y actualización permanente (principio 6), mientras que los Estándares Iberoamericanos indican que el responsable llevará a cabo acciones que garanticen el monitoreo, revisión, mantenimiento y mejora continua de las medidas de seguridad aplicables al tratamiento de los datos personales, de manera periódica (art. 21.3). El Marco de privacidad APEC por su parte, menciona que las medidas de seguridad deberían estar sujetas a revisión y reevaluación periódica (art. 28).

125. Ciertos documentos normativos internacionales regulan la obligación de notificar las vulneraciones de seguridad a la autoridad de control, como el Convenio 108 modernizado (art. 7.2), los Estándares Iberoamericanos (art. 22), Reglamento General (art. 33), las Directrices OCDE (párr. 15.c)) y el Marco de privacidad APEC (art. 54). Asimismo, estos documentos normativos internacionales, con excepción del Convenio 108 modernizado, establecen también la obligación de informar las vulneraciones de seguridad a los titulares afectados.

126. Debemos poner de relieve la importancia que tienen las notificaciones a las autoridades de control o eventualmente a los titulares afectados. Por un lado, permiten que dicha autoridad sea capaz de supervisar que se tomen las medidas apropiadas al encontrarse frente a una vulneración de la seguridad y que la misma se contenga en el menor tiempo posible; y por otro lado, asegura que los titulares afectados por la brecha de seguridad sean conscientes de que ocurrió la misma y de los daños que podrían ocasionarse como consecuencia.

127. La Agencia Española de Protección de Datos señala que el principio de seguridad en el Reglamento General “impone a quienes tratan datos el necesario análisis de riesgos orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, disponibilidad y confidencialidad de los datos personales que traten”[34].

128. Los Estándares Iberoamericanos de Protección (art. 21.2), el Reglamento General (art. 32) y el Marco de privacidad APEC (art. 28), establecen pautas o factores para determinar las medidas de seguridad a tomar, como se analiza a continuación, pero ninguno de ellos establece cuáles son las medidas específicas a aplicar, puesto que ello sería imposible de determinar de forma que no se vuelva obsoleto.

129. El Reglamento General indica que el responsable y el encargado tendrán en cuenta los siguientes factores para determinar las medidas apropiadas con el fin de garantizar un nivel de seguridad adecuado al riesgo: “el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas” (art. 32).

130. En la misma línea, en los Estándares Iberoamericanos consideran dichos factores y agrega los siguientes: “las transferencias internacionales que se realicen o pretendan realizar”, “el número de titulares”, “las posibles consecuencias que se derivarían de una vulneración para los titulares y las vulneraciones previas ocurridas” (art. 21.2).

[33] Principio 6 de los Principios de la OEA.

[34] Agencia Española de Protección de Datos, “Principios”, 25 de noviembre de 2021, https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios.

131. En el Marco de privacidad APEC se menciona que las medidas de seguridad deben ser proporcionales a la probabilidad y severidad del daño que podría producirse, a la sensibilidad de la información y al contexto en el que es guardada (art. 28). A diferencia de los demás documentos normativos internacionales, solo considera al responsable como obligado a establecer y mantener las medidas de seguridad, teniendo en cuenta los factores señalados, sin considerar al encargado del tratamiento.

132. En los Principios de la OEA, el principio de seguridad no se pronuncia en el sentido señalado precedentemente. Sin embargo, los Principios Anotados establecen que "las medidas adoptadas para proteger los datos personales deberían ser elegidas tomando en cuenta, entre otros factores: i) la posible afectación a los derechos de los titulares, en particular, el posible valor de los datos para una tercera persona no autorizada para su tratamiento; ii) los costos de su implementación; iii) las finalidades del tratamiento, y iv) la naturaleza de los datos personales tratados, en especial los Datos Sensibles" (principio 6, anotado).

133. De los documentos normativos internacionales analizados, el Reglamento General es el único que brinda ejemplos de medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado al riesgo, a saber: "a) la seudonimización y el cifrado de datos personales; b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; y d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento" (art. 32.1).

134. Asimismo, en el artículo 32.3 del Reglamento General se establece que la adhesión a un código de conducta o a un mecanismo de certificación podrá servir para demostrar el cumplimiento de estos requisitos.

135. Todo responsable o encargado debe tomar medidas para garantizar la seguridad y proteger los datos personales contra riesgos como el acceso no autorizado, pérdida, modificación, destrucción, divulgación o daño. Si no se toman dichas medidas de seguridad, la información personal se torna vulnerable a los riesgos mencionados, lo que puede transformarse en graves perjuicios a los derechos de los titulares de los datos. Por ello, todos los documentos normativos internacionales analizados consideran la necesidad de establecer diferentes tipos de medidas para los riesgos que podrían ocasionarse; e incluso, en algunos casos, dan pautas para determinar las medidas de seguridad adecuadas, sin señalar las medidas específicas a aplicar, en atención a que el avance de las tecnologías y sus eventuales vulneraciones nunca podrían ser acompañados de la correspondiente actualización de las normas.

136. La diversidad de las tecnologías, así como su dinámica transformación que aumenta sus capacidades de recolección y procesamiento de datos, deben ser tomadas en cuenta para evaluar con responsabilidad y ética, los riesgos y las medidas de seguridad adecuadas, por parte de los responsables de los tratamientos, en relación a la habilitación que legítimamente tienen en su calidad de tales, así como a la necesidad incuestionable de guardar la debida confidencialidad de los datos personales que están siendo tratados bajo su responsabilidad.

137. Garantizar integridad, disponibilidad y confidencialidad de los datos personales es una tarea primordial y una responsabilidad que recae en los responsables y encargados del tratamiento, para evitar graves vulneraciones a los derechos de los titulares de los datos; no obstante, de producirse ello, tengan el menor impacto posible en sus derechos; debiendo establecerse asimismo, pautas a seguir cuando las mismas

suceden, como las notificaciones obligatorias a la autoridad de control y a los titulares de los derechos afectados.

# III. Conclusiones

138. Los principios rectores de la privacidad y de la protección de datos personales constituyen parte estructural de los sistemas jurídicos sobre la materia. Son pautas de interpretación y ayudas para completar vacíos en la legislación. Comprometen a los responsables y a los encargados a actuar de manera adecuada en el tratamiento de los datos personales.

139. La legalidad debe ser el cauce por el que deben discurrir todas las actividades del tratamiento durante todo el ciclo de vida de los datos personales y tiene como requisito base la configuración de algunas de las causales legitimantes establecidas en la normativa que sea de aplicación.

140. El principio de consentimiento está íntimamente unido al de legalidad, siendo la causa habilitante para el tratamiento de los datos personales más común, internacionalmente reconocida.

141. El principio de transparencia debe observarse independientemente de cuál sea la base jurídica que legitima el tratamiento.

142. El principio de finalidad se encuentra establecido en todos los documentos normativos analizados. La finalidad debe ser: explícita, específica, legítima y pertinente. Funcionará como delimitadora de las actividades de tratamiento a las que serán sometidos los datos personales.

143. La lealtad exige que la información personal sea tratada respetando de manera fiel todos los términos y condiciones que habilitaron su recopilación y utilizando medios para el tratamiento que faciliten dicho objetivo.

144. Por el principio de proporcionalidad los datos personales, así como las actividades de tratamiento a los que aquellos sean sometidos, deben limitarse únicamente al cumplimiento de los fines legítimos para los cuales fueron recopilados.

145. La calidad de la información personal que esté siendo objeto de tratamiento, resulta vital para el buen logro de las finalidades que autorizaron su recopilación, así como su posterior tratamiento.

146. El principio de responsabilidad tiende a reforzar y hacer que el deber del cumplimiento de los principios y de la normativa pase a contar con elementos objetivos en los que el cumplimiento real se sustente y se logren los fines legítimos, en un clima de confianza y respeto de los derechos fundamentales involucrados.

147. No habrá protección de datos ni respeto a la privacidad sin seguridad. Garantizar la integridad, disponibilidad y confidencialidad de los datos personales es una tarea primordial y una gran responsabilidad. La diversidad de las tecnologías, así como su dinámica transformación, deben ser tomadas en cuenta para evaluar con responsabilidad y ética, los riesgos y las medidas de seguridad adecuadas.

148. Existen muchos puntos comunes, a la hora en que los documentos normativos internacionales desarrollan los principios de la privacidad y de la protección de datos personales.

149. Los elementos comunes identificados, pueden servir de base para avanzar hacia un consenso global que permitirá hacer frente, de manera conjunta y adecuada, a los distintos retos que se presentan en el tratamiento de los datos que conciernen a las personas, tales como los relacionados con la transferencia internacional de datos, el

uso de las tecnologías de la información y de las comunicaciones, la inteligencia artificial, en tanto los derechos humanos merecen igual respeto en entornos virtuales como presenciales.

150. Es menester continuar avanzando hacia un equilibrio entre los distintos intereses involucrados en el tratamiento de datos personales en la era global y digital en la que nos encontramos, en pos de la cooperación y la armonización normativa.