**Versión 1.0**

# MARCO DE PRIVACIDAD DEL NIST: UNA HERRAMIENTA PARA MEJORAR LA PRIVACIDAD POR MEDIO DE LA GESTIÓN DE RIESGOS EMPRESARIALES, VERSIÓN 1.0

16 de enero de 2020

Esta publicación está disponible de forma gratuita en:
https://doi.org/10.6028/NIST.CSWP.01162020.



National Institute of Standards and Technology
U.S. Department of Commerce

# Resumen ejecutivo

Por más de dos décadas, la internet y las tecnologías de la información conexas han impulsado innovaciones, crecimiento económico y mejoras sin precedentes en los servicios sociales. Muchos de estos beneficios los potencian datos sobre personas que circulan por un ecosistema complejo. Por consiguiente, es posible que las personas no entiendan las consecuencias que podría acarrear para su privacidad la interacción con sistemas, productos y servicios. Al mismo tiempo, las organizaciones podrían no darse cuenta del alcance total de estas consecuencias para las personas, la sociedad o sus empresas; consecuencias que podrían afectar sus marcas, sus resultados finales y sus perspectivas de crecimiento futuras.

Después de seguir un proceso transparente, basado en el consenso de las partes interesadas privadas y públicas a fin de crear este instrumento facultativo, el Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés) publica este Marco de privacidad: una herramienta para mejorar la privacidad por medio de la gestión de riesgos empresariales (Marco de privacidad), que busca facilitar mejores prácticas de ingeniería de la privacidad compatibles con los conceptos de privacidad desde el diseño y ayudar a las organizaciones a proteger la privacidad de las personas. Con el Marco de privacidad, las organizaciones pueden:

- generar la confianza de los clientes promoviendo la toma de decisiones éticas en el diseño o en la implementación de productos y servicios que optimice el uso provechoso de datos, y minimizando las consecuencias adversas para la privacidad de las personas y la sociedad en conjunto;[1]
- asumir las obligaciones actuales en materia de cumplimiento, así como proteger productos y servicios contra la obsolescencia para cumplir estas obligaciones en un entorno tecnológico y normativo cambiante; y
- facilitar la comunicación acerca de las prácticas de privacidad con las personas, los socios comerciales, los evaluadores y las autoridades normativas.

Para aprovechar las ventajas de los datos y gestionar simultáneamente los riesgos de la privacidad de las personas, no bastan las soluciones únicas. Cuando se construye una casa, los propietarios deciden la distribución y el estilo confiando en que los cimientos están bien diseñados. La protección de la privacidad también debe considerar las preferencias individuales siempre que el diseño de los productos y servicios ya cuente con medidas eficaces para mitigar el riesgo a la privacidad. Por medio de un método basado en los riesgos y los resultados, el Marco de privacidad es suficientemente flexible para abordar diversas necesidades de privacidad, facilitar soluciones más innovadoras y eficaces que puedan lograr mejores resultados para las personas y las organizaciones, y mantenerse al día de las tendencias tecnológicas, como la inteligencia artificial y la internet de las cosas.

Este Marco de privacidad tiene la misma estructura que el Marco para la mejora de la seguridad cibernética en infraestructuras críticas (Marco de ciberseguridad) [1], lo que facilita el uso conjunto de ambos marcos. Al igual que el Marco de ciberseguridad, el Marco de privacidad se compone de tres partes: el Núcleo, los Perfiles y los Niveles de implementación. Cada componente fortalece la gestión de riesgos a la privacidad a través del vínculo entre los impulsores empresariales y de la misión, las funciones y responsabilidades de la organización, y las actividades de protección de la privacidad.

[1] No existe una norma objetiva para la toma de decisiones éticas. Esta se basa en las normas, los valores y las expectativas legales de una sociedad determinada.

- El Núcleo facilita la comunicación entre todos los niveles, desde el ejecutivo hasta el de implementación u operaciones, acerca de las actividades importantes de protección de la privacidad y los resultados deseados.
- Los Perfiles posibilitan la priorización de los resultados y de las actividades que satisfacen mejor los valores de la privacidad, las necesidades empresariales o de la misión, y los riesgos de la organización.
- Los Niveles de implementación contribuyen a la toma de decisiones y la comunicación sobre la suficiencia de los procesos y recursos de la organización para gestionar el riesgo a la privacidad.

En resumidas cuentas, el Marco de privacidad tiene como objeto ayudar a las organizaciones a crear mejores bases para la privacidad debido a que equipara los riesgos a la privacidad con su cartera más amplia de riesgos empresariales.

## Agradecimientos

Esta publicación nace de una iniciativa de colaboración entre el NIST y las partes interesadas, las cuales comprenden organizaciones y personas de los sectores público y privado. El Marco de privacidad del NIST fue elaborado con base en tres talleres públicos, una solicitud de información y una solicitud de comentarios, cinco seminarios web y cientos de interacciones directas con las partes interesadas.[2] El NIST reconoce y agradece a todos aquellos que han contribuido a esta publicación.

[2] Se puede encontrar un archivo completo de su elaboración en https://www.nist.gov/privacy-framework.

# Índice



# Lista de figuras



# Lista de tablas

# 1.0 Introducción al Marco de privacidad

Por más de dos décadas, la internet y las tecnologías de la información conexas han impulsado innovaciones, crecimiento económico y acceso sin precedentes a servicios sociales. Muchos de estos beneficios los potencian *datos* sobre *personas* que circulan por un ecosistema complejo. Por consiguiente, es posible que las personas no entiendan las consecuencias que podría acarrear para su privacidad la interacción con sistemas, productos y servicios. También es posible que las organizaciones no se den cuenta totalmente de estas consecuencias. No gestionar los *riesgos a la privacidad* puede tener consecuencias adversas directas a nivel individual y social, seguidas de efectos en las marcas, resultados finales y perspectivas de crecimiento futuras de las organizaciones. Encontrar maneras de seguir aprovechando las ventajas del *tratamiento de datos* y de proteger al mismo tiempo la privacidad de las personas es un problema que no se resuelve bien con soluciones únicas.

La privacidad es un reto, no solo por ser un concepto amplio que ayuda a salvaguardar valores importantes, como la autonomía y la dignidad humanas, sino también porque los medios para alcanzarla pueden variar.[3] Por ejemplo, la privacidad puede lograrse cuando se practica el retraimiento y se limita la observación, o cuando las personas controlan facetas de sus identidades (por ejemplo, su cuerpo, sus datos, su reputación).[4] Asimismo, la autonomía y la dignidad humanas no son constructos fijos ni cuantificables. Son conceptos que pasan por los filtros de la diversidad cultural y las diferencias individuales. Esta naturaleza amplia y cambiante de la privacidad dificulta la comunicación clara sobre los riesgos a la privacidad dentro de las organizaciones y entre estas, y con las personas. Lo que ha hecho falta es un lenguaje común y una herramienta práctica que sea suficientemente flexible para abordar las diversas necesidades de privacidad.

El presente Marco de privacidad: una herramienta para mejorar la privacidad por medio de la gestión de riesgos empresariales (Marco de privacidad) del NIST tiene como fin que las organizaciones de todo tamaño lo utilicen extensamente, sin considerar ningún tipo de tecnología, sector, ley o jurisdicción particular. Con la aplicación de un método común que se adapta a las funciones de cualquier organización en el *ecosistema de tratamiento de datos*, el objetivo del Marco de privacidad es ayudar a las organizaciones a gestionar los riesgos a la privacidad al:

- considerar la privacidad en el momento de diseñar e implementar los sistemas, productos y servicios que tienen un impacto sobre las personas;
- comunicar sus prácticas de privacidad; y
- fomentar la colaboración entre el personal de toda la organización (por ejemplo, entre los ejecutivos, los empleados del departamento legal y los del departamento de tecnología de la información [TI]) por medio de la creación de Perfiles, la selección de Niveles y el logro de resultados.

[3] La autonomía y la dignidad son conceptos que aborda la Declaración Universal de Derechos Humanos de las Naciones Unidas en https://www.un.org/es/universal-declaration-human-rights/.

[4] Hay muchas publicaciones que tratan de manera exhaustiva el trasfondo de la privacidad, o diferentes aspectos de este concepto. Para ver dos ejemplos, véase Solove, D. (2010). *Understanding Privacy*. Cambridge, Massachusetts: Harvard University Press. https://ssrn.com/abstract=1127888; y Selinger, E. y Hartzog, W. (2017) *Obscurity and Privacy* en J. Pitt y A. Shew. *Spaces for the Future: A Companion to Philosophy of Technology*, Nueva York, Nueva York: Taylor & Francis, capítulo 12, 1.ª ed., https://doi.org/10.4324/9780203735657.

## 1.1 Descripción del Marco de privacidad

Como se muestra en la **Figura** 1, el Marco de privacidad se compone de tres partes: el Núcleo, los Perfiles y los Niveles de implementación. Cada componente fortalece la forma en que las organizaciones gestionan los riesgos a la privacidad a través del vínculo entre los impulsores empresariales o de la misión, las funciones y responsabilidades de la organización, y las actividades de protección de la privacidad. Como se explica más adelante en la Sección 2:


**Figura 1: Núcleo, Perfiles y Niveles de implementación**

- El *Núcleo* es un conjunto de actividades de protección de la privacidad y de resultados que permite comunicar las actividades de protección de la privacidad priorizadas y los resultados a toda la organización, desde el nivel ejecutivo hasta el de implementación o de operaciones. El Núcleo se divide aún más en Categorías y Subcategorías clave, que comprenden resultados separados, para cada Función.
- Un *Perfil* representa las actividades o los resultados deseados actuales de una organización relativos a la privacidad. Para crear un Perfil, una organización puede analizar todos los resultados y las actividades en el Núcleo para determinar prioridades basándose en los impulsores empresariales o de la misión, las funciones en el ecosistema de tratamiento de datos, los tipos de tratamientos de datos y las necesidades de privacidad de las personas. Una organización puede crear o agregar Funciones, Categorías y Subcategorías, según sea necesario. Los Perfiles pueden utilizarse para identificar oportunidades de mejoramiento de la postura de privacidad al comparar un Perfil "actual" (el estado "tal como está") con un perfil "objetivo" (el estado "que debe ser"). Los perfiles se pueden emplear para hacer autoevaluaciones y para comunicar dentro de una organización, o entre organizaciones, la manera en que se gestionan los riesgos a la privacidad.
- Los *Niveles de implementación* ("Niveles") proporcionan un punto de referencia sobre la manera en que una organización percibe los riesgos a la privacidad y si cuenta con suficientes procesos y recursos establecidos para gestionar esos riesgos. Los Niveles reflejan una progresión de respuestas informales y reactivas a métodos ágiles que se basan en riesgos. Al seleccionar los Niveles, una organización deberá considerar sus Perfiles objetivo y la manera en que sus prácticas actuales de gestión de riesgos, el grado de integración de los riesgos a la privacidad en su cartera de gestión de riesgos empresariales, sus relaciones en el ecosistema de tratamiento de datos, la composición de su personal y el programa de capacitación puedan favorecer u obstaculizar el logro de estos Perfiles.

## 1.2 Gestión de riesgos a la privacidad

Si bien algunas organizaciones cuentan con un conocimiento sólido de la *gestión de riesgos a la privacidad,* todavía no se ha generalizado una interpretación común de muchos de los aspectos de este tema.[5] Para promover un conocimiento más amplio, en esta sección, se tratan conceptos y consideraciones que las organizaciones pueden utilizar para organizar, mejorar o comunicar la gestión de riesgos a la privacidad. En el Apéndice D, se proporciona información adicional sobre las prácticas clave de gestión de riesgos a la privacidad.

### 1.2.1 Gestión de los riesgos a la privacidad y la ciberseguridad

Desde su introducción en 2014, el Marco de ciberseguridad ha ayudado a las organizaciones a comunicarse y gestionar los riesgos a la ciberseguridad. [1] La gestión de riesgos a la ciberseguridad contribuye a la gestión de riesgos a la privacidad; sin embargo, no es suficiente, ya que los riesgos a la privacidad también pueden originarse por medios no relacionados con *incidentes de ciberseguridad*, como se ilustra en la **Figura 2.** Es importante tener un conocimiento general de los diversos orígenes de los riesgos a la ciberseguridad y a la privacidad a fin de determinar las soluciones más eficaces para abordar estos riesgos.

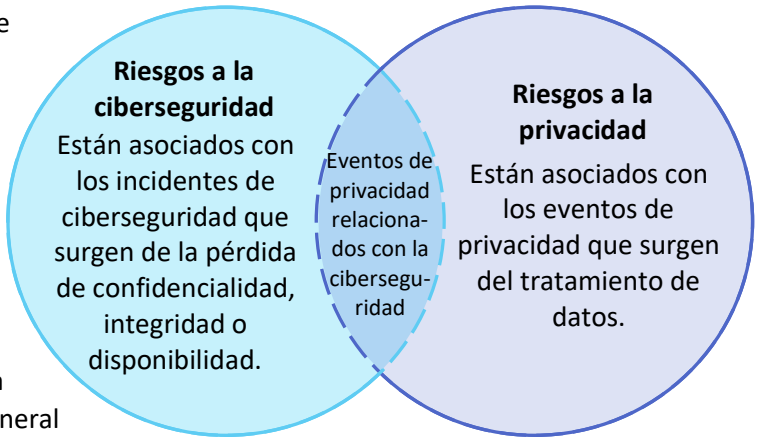


**Figura 2: Relación entre los riesgos a la ciberseguridad y a la privacidad**

El método del Marco de privacidad para los riesgos a la privacidad conlleva considerar los *eventos de privacidad* como posibles problemas que las personas podrían experimentar provenientes de las operaciones de sistemas, productos o servicios con datos en formato digital o no digital, durante un ciclo de vida completo: desde la recolección de los datos hasta su eliminación.

***Acción de datos***
Es una operación del ciclo de vida de los datos que incluye, entre otros, su recolección, retención, registro, generación, transformación, uso, revelación, uso compartido, transmisión y eliminación.

***Tratamiento de datos***
Es el conjunto colectivo de acciones de datos.

El Marco de privacidad describe estas operaciones de datos en singular como una *acción de datos*, y de manera colectiva como el tratamiento de datos. Los problemas que las personas pueden experimentar debido al tratamiento de datos se pueden expresar de varias maneras, pero el NIST los describe como problemas que van desde efectos relacionados con la dignidad (como la vergüenza o los estigmas) hasta perjuicios más tangibles (como la discriminación, la pérdida económica o el daño físico).[6]

---

5 Véase el *Summary Analysis of the Responses to the NIST Privacy Framework Request for Information* [Análisis resumido de las respuestas a la solicitud de información referente al Marco de privacidad del NIST] en la p. 7 de [2].

6 El NIST ha elaborado un catálogo ilustrativo de problemas que se usa en la evaluación de los riesgos a la privacidad. Véase la *NIST Privacy Risk Assessment Methodology* [Metodología del NIST para evaluación de los

La base de los problemas que las personas pueden experimentar es variable. Como se ilustra en la **Figura** 2, los problemas surgen como un efecto adverso del tratamiento de datos que las organizaciones llevan a cabo para cumplir con los objetivos de su misión o empresa. Un ejemplo de esto lo son las inquietudes que algunas comunidades tenían con respecto a la instalación de "contadores inteligentes". Estos eran parte de una iniciativa tecnológica nacional de la red eléctrica inteligente para aumentar la eficiencia energética.[7] La capacidad de estos contadores para recolectar, registrar y distribuir información muy detallada sobre el uso de la electricidad en el hogar podía proporcionar datos acerca del comportamiento de las personas dentro de sus hogares.[8] Los contadores estaban funcionando según lo previsto, pero el tratamiento de datos podía hacer que la gente se sintiera vigilada.

En un mundo cada vez más conectado, algunos problemas pueden surgir simplemente de las interacciones de las personas con los sistemas, productos y servicios, incluso cuando los datos que se procesan no están directamente vinculados con personas identificables. Por ejemplo, las tecnologías de las ciudades inteligentes podrían utilizarse para influir en el comportamiento de las personas o modificarlo, como los lugares por donde se desplazan en la ciudad o la manera en que lo hacen.[9] También pueden surgir problemas cuando hay una pérdida de *confidencialidad*, *integridad* o *disponibilidad* en algún momento durante el tratamiento de datos, como en el caso de un robo de datos perpetrado por atacantes externos, o del acceso o uso no autorizado de datos cometido por empleados. La **Figura** 2 muestra estos tipos de eventos de privacidad relacionados con la ciberseguridad en el área donde se intersecan los riesgos a la privacidad y los riesgos a la ciberseguridad.

Una vez que una organización sea capaz de identificar la probabilidad de que surja algún problema particular del tratamiento de datos (a lo que el Marco de privacidad se refiere como una *acción problemática de datos*), podrá evaluar el impacto en caso de que suceda la acción problemática de datos. Esta evaluación del impacto es donde el riesgo a la privacidad y el *riesgo* a la organización se intersecan. Las personas sufren el impacto directo de los problemas de manera individual o colectiva (incluso a nivel social). Los problemas que afectan a las personas pueden repercutir en una organización y causar costos por incumplimiento, pérdida de ingresos porque los clientes ya no procuran sus productos y servicios, o perjuicios a la reputación externa de su marca o a su cultura interna. Las organizaciones suelen gestionar estos tipos de repercusiones a nivel de gestión de riesgos empresariales. Al vincular los problemas que afectan a las personas con estos impactos organizativos bien entendidos, las organizaciones pueden equiparar el riesgo a la privacidad con otros riesgos que gestionan en su cartera más amplia e impulsar una toma de decisiones más informada sobre la asignación de recursos para fortalecer los programas en materia de privacidad. La **Figura** 3 muestra esta relación entre los riesgos a la privacidad y los riesgos a la organización.

---

riesgos a la privacidad] [3]. Es posible que otras organizaciones hayan creado otras categorías para los problemas, o que los traten como consecuencias adversas o daños.

7 Véase, por ejemplo, el Informe interinstitucional o interno 7628 del NIST, *Guidelines for Smart Grid Cybersecurity: Volume 1 – Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements*, rev. 1, vol. 1. [Directrices para la ciberseguridad de la red eléctrica inteligente: Volumen 1 – Estrategia, arquitectura y requisitos de alto nivel de ciberseguridad de la red eléctrica inteligente] en la p. 26 de [4].

8 Véase el Informe interinstitucional o interno 8062 del NIST, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* [Una introducción a la ingeniería de la privacidad y a la gestión de riesgos en los sistemas federales] en la p. 2 de [5]. Véase el Apéndice E del Informe interinstitucional o interno 8062 del NIST para obtener información sobre tipos adicionales de riesgos a la privacidad asociados con los efectos adversos del tratamiento de datos en las personas.

9 Véase Newcombe, T. (2016). *Security, Privacy, Governance Concerns About Smart City Technologies Grow* en *Government Technology*. Disponible en http://www.govtech.com/Security-Privacy-Governance-Concerns-About-Smart-City-Technologies-Grow.html.

**El problema** surge del tratamiento de datos.

**La persona** sufre un impacto directo (por ejemplo, vergüenza, discriminación, pérdida económica).

**La organización** se ve afectada por el impacto resultante (por ejemplo, clientes que no la procuran, costos por incumplimiento, perjuicios a la reputación o a la cultura interna).

**Figura 3: Relación entre los riesgos a la privacidad y los riesgos a la organización**

### 1.2.2 Evaluación de los riesgos a la privacidad

La gestión de riesgos a la privacidad es un conjunto de procesos establecidos en toda la organización que le ayudan a entender cómo sus sistemas, productos y servicios podrían causar problemas a las personas, y cómo pueden concebir soluciones eficaces para gestionar esos riesgos. *La evaluación de los riesgos a la privacidad* es un subproceso mediante el cual se identifican y evalúan riesgos específicos a la privacidad. En general, las evaluaciones de los riesgos a la privacidad producen la información que puede ayudar a las organizaciones a sopesar los beneficios del tratamiento de datos frente a los riesgos, y a determinar la respuesta adecuada. Esto a veces se denomina "proporcionalidad".[10] Las organizaciones pueden optar por asignar prioridades y responder a los riesgos a la privacidad de diferentes formas, dependiendo del posible impacto en las personas y de las repercusiones en las organizaciones. Los procedimientos de la respuesta comprenden:[11]

- mitigar el riesgo (por ejemplo, las organizaciones podrían aplicar medidas técnicas o normativas a los sistemas, productos o servicios que reduzcan el riesgo a un grado mínimo aceptable);
- transferir o compartir el riesgo (por ejemplo, los contratos son un modo de compartir o transferir el riesgo a otras organizaciones, y los avisos de privacidad y mecanismos de consentimiento son un modo de compartir el riesgo con las personas);
- evitar el riesgo (por ejemplo, las organizaciones podrían determinar que los riesgos superan los beneficios, y renunciar al tratamiento de datos o darle fin); o
- aceptar el riesgo (por ejemplo, las organizaciones podrían determinar que los problemas para las personas son mínimos, o que es poco probable que ocurran, por lo tanto, los beneficios superarían los riesgos y no sería necesario invertir recursos en la mitigación).

Las evaluaciones de los riesgos a la privacidad son particularmente importantes porque, como se señaló anteriormente, la privacidad es una condición que salvaguarda valores múltiples. Los métodos para salvaguardar estos valores pueden ser diferentes y, además, estar en conflicto uno con el otro. En función de sus objetivos, si una organización intenta lograr la privacidad limitando la observación, esto podría dar lugar a la implementación de medidas como las arquitecturas de datos distribuidas o las técnicas criptográficas que mejoran la privacidad y ocultan datos incluso de la organización. Si una organización también intenta facilitar el control individual, las medidas podrían entrar en conflicto. Por ejemplo,

---

10 Véase *Necessity & Proportionality*. (2019), Supervisor Europeo de Protección de Datos. Disponible en https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en.

11 Véase la Publicación especial 800-39 del NIST, *Managing Information Security Risk: Organization, Mission, and Information System View* [Gestión de riesgos a la seguridad de la información: vista de la organización, la misión y el sistema de información] [6].

cuando una persona solicita acceso a datos, es posible que la organización no pueda presentarlos si los datos se han distribuido o cifrado de manera tal que la organización no puede acceder a ellos. Las evaluaciones de los riesgos a la privacidad permiten a una organización a conocer, en un contexto dado, los valores que deben protegerse, los métodos que deben emplearse y la manera de equilibrar la implementación de distintos tipos de medidas.

Por último, las evaluaciones de los riesgos a la privacidad ayudan a las organizaciones a distinguir entre el riesgo a la privacidad y el riesgo al cumplimiento. Identificar si el tratamiento de datos podría causar problemas a las personas, incluso cuando una organización pueda cumplir plenamente con las leyes o los reglamentos aplicables, podría ayudar con la toma de decisiones éticas en el diseño o la implementación de sistemas, productos y servicios. Aunque no existe una norma objetiva para tomar decisiones éticas, la toma de decisiones se basa en las normas, los valores y las expectativas legales de una sociedad dada. Esto facilita optimizar el uso provechoso de datos, minimizando las consecuencias adversas para la privacidad de las personas y la sociedad en conjunto. Igualmente, evita la pérdida de confianza que perjudica la reputación de las organizaciones, ralentiza la adopción o hace que no se procuren los productos y servicios.

Véase el Apéndice D para obtener más información sobre los aspectos operativos de la evaluación de los riesgos a la privacidad.

## 1.3 Descripción del documento

El resto de este documento contiene las secciones y los apéndices siguientes:

- La **Sección 2** describe los componentes del Marco de privacidad: el Núcleo, los Perfiles y los Niveles de implementación.
- La **Sección 3** presenta ejemplos de las maneras en que se puede usar el Marco de privacidad.
- La **sección Referencias** enumera las referencias del documento.
- El **Apéndice A** presenta el Núcleo del Marco de privacidad en formato tabular: Funciones, Categorías y Subcategorías.
- El **Apéndice B** comprende un glosario de términos seleccionados.
- El **Apéndice C** enumera las siglas que se utilizan en este documento.
- El **Apéndice D** considera las prácticas clave que contribuyen a la gestión exitosa de los riesgos a la privacidad.
- El **Apéndice E** define los Niveles de implementación.

# 2.0 Conceptos básicos del Marco de privacidad

El Marco de privacidad proporciona un lenguaje común para entender y gestionar los riesgos a la privacidad, y comunicarlos a las partes interesadas internas y externas. Es adaptable a las funciones de toda organización en el ecosistema de tratamiento de datos. Puede utilizarse para identificar y dar prioridad a las medidas que se tomen para reducir los riesgos a la privacidad. Además, es una herramienta que se emplea para alinear los métodos normativos, empresariales y tecnológicos con la gestión de esos riesgos.

## 2.1 Núcleo

Según se explica en el Apéndice A, el Núcleo proporciona un conjunto cada vez más pormenorizado de las actividades y los resultados que facilitan la comunicación sobre la gestión de los riesgos a la privacidad. Como muestra la **Figura** 4, el Núcleo comprende Funciones, Categorías y Subcategorías.

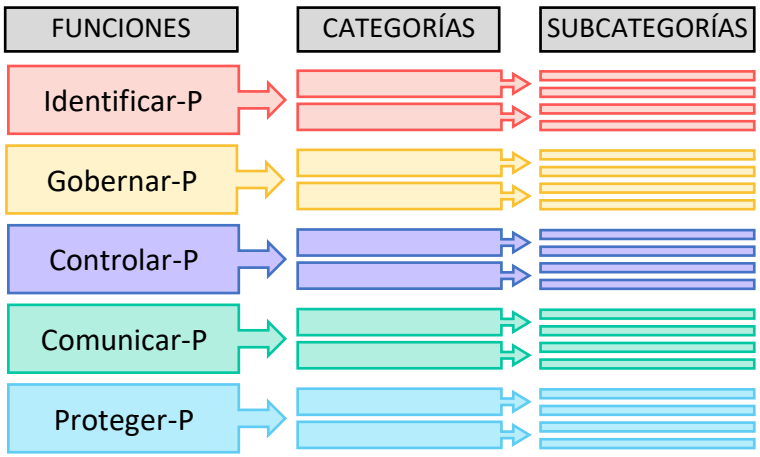


**Figura 4: Estructura del Núcleo del Marco de privacidad**

Los elementos del Núcleo funcionan en conjunto:

- Las *Funciones* organizan las actividades fundamentales de privacidad en su nivel más alto. Ayudan a una organización a expresar su gestión de riesgos a la privacidad entendiendo y manejando el tratamiento de datos, habilitando las decisiones de *gestión de riesgos*, determinando la manera de interactuar con las personas y mejorando con lo aprendido de actividades previas. No están diseñadas para constituir una ruta en serie, ni para llevar a un estado final deseado estático. Más bien, las Funciones se deben ejecutar de forma simultánea y continua para crear o mejorar una cultura operativa que aborde la naturaleza dinámica de los riesgos a la privacidad.
- Las *Categorías* son las subdivisiones de una Función en grupos de resultados de privacidad que están estrechamente vinculados con necesidades programáticas y actividades particulares.
- Las *Subcategorías* dividen aún más una Categoría en resultados específicos de actividades técnicas o de gestión. Proporcionan un conjunto de resultados que, aunque no sean exhaustivos, contribuyen al logro de los resultados en cada categoría.

Las cinco Funciones (Identificar-P, Gobernar-P, Controlar-P, Comunicar-P y Proteger-P) que se definen a continuación, pueden utilizarse para gestionar los riesgos a la privacidad que surgen del tratamiento de datos.[12] Proteger-P se centra específicamente en la gestión de los riesgos asociados con eventos de privacidad relacionados con la ciberseguridad (por ejemplo, *vulneraciones de la privacidad*). Aunque el Marco de ciberseguridad se destina a tratar todo tipo de incidente de ciberseguridad, puede emplearse para promover además la gestión de los riesgos asociados con eventos de


**Figura 5: Uso de las Funciones para gestionar los riesgos a la ciberseguridad y la privacidad**

[12] La "-P" al final del nombre de cada Función indica que la Función se deriva del Marco de privacidad. Se emplea para evitar que se confundan con las Funciones del Marco de ciberseguridad.

privacidad relacionados con la ciberseguridad mediante el uso de las siguientes Funciones: Detectar, Responder y Recuperar. De otro modo, las organizaciones podrían utilizar las cinco Funciones del Marco de ciberseguridad junto con las Funciones Identificar-P, Gobernar-P, Controlar-P y Comunicar-P para abordar colectivamente los riesgos a la privacidad y la ciberseguridad. La **Figura** 5 muestra el diagrama de Venn de la Sección 1.2.1 para indicar la manera en que las Funciones de ambos marcos pueden usarse en diversas combinaciones para gestionar diferentes aspectos de los riesgos a la privacidad y la ciberseguridad. Las cinco Funciones del Marco de privacidad se definen de la manera siguiente:

- *Identificar-P*: Define el conocimiento organizativo para gestionar el riesgo a la privacidad de las personas que surge del tratamiento de datos.

  Las actividades de la Función Identificar-P son fundamentales para el uso efectivo del Marco de privacidad. El inventario de las circunstancias en las que se procesan los datos, el conocimiento de los intereses relativos a la privacidad de las personas atendidas o afectadas directa o indirectamente por una organización, y las evaluaciones de riesgos permiten que una organización conozca el entorno empresarial en el que opera e identifique y dé prioridad a los riesgos a la privacidad.

- *Gobernar-P*: Define e implementa la estructura de gobernanza organizativa para facilitar el conocimiento continuo de las prioridades de gestión de riesgos de la organización basadas en el riesgo a la privacidad.

  La Función Gobernar-P es similarmente fundamental, pero se centra en las actividades a nivel organizativo, como el establecimiento de valores y políticas de la privacidad de la organización, la identificación de sus requisitos legales o normativos y el conocimiento de su *tolerancia al riesgo*, que permiten a una organización dirigir y priorizar sus esfuerzos de acuerdo con su estrategia de gestión de riesgos y sus necesidades empresariales.

- *Controlar-P*: Desarrolla e implementa actividades adecuadas para que las organizaciones o las personas puedan aplicar los datos con detalle suficiente y gestionar los riesgos a la privacidad.

  La Función Controlar-P contempla la gestión del tratamiento de datos desde el punto de vista de las organizaciones y las personas.

- *Comunicar-P*: Desarrolla e implementa actividades adecuadas por medio de las cuales las organizaciones y las personas pueden obtener un conocimiento confiable y participar en un diálogo acerca de la manera en que se procesan los datos y los riesgos a la privacidad conexos.

  La Función Comunicar-P reconoce la posibilidad de que tanto las organizaciones como las personas necesiten saber cómo se procesan los datos para gestionar con efectividad los riesgos a la privacidad.

- *Proteger-P*: Establece e implementa salvaguardias adecuadas para el tratamiento de datos.

  La Función Proteger-P abarca la protección de datos para evitar los eventos de privacidad relacionados con la ciberseguridad, es decir, la intersección de la gestión de los riesgos a la privacidad y los riesgos a la ciberseguridad.

## 2.2 Perfiles

Los Perfiles son una selección de Funciones, Categorías y Subcategorías específicas del Núcleo que la organización ha priorizado para ayudar a gestionar el riesgo a la privacidad. Los Perfiles se pueden usar para describir el estado actual y el estado objetivo deseado de actividades de privacidad específicas. El Perfil actual indica los resultados de privacidad que una organización logra actualmente, mientras que el Perfil objetivo indica los resultados necesarios para lograr las metas de la gestión de riesgos a la privacidad que se desean. Las diferencias entre ambos Perfiles le permiten a una organización identificar las diferencias, elaborar un plan de acción para mejoramiento y evaluar los recursos que se necesitarían (por ejemplo, dotación de personal, financiación) para lograr los resultados de privacidad. Esto constituye la base del plan de una organización para reducir el riesgo a la privacidad de una manera rentable y priorizada. Los Perfiles también pueden servir para comunicar el riesgo dentro de las organizaciones y entre estas, porque les ayudan a entender y comparar el estado actual y el estado deseado de los resultados de privacidad.

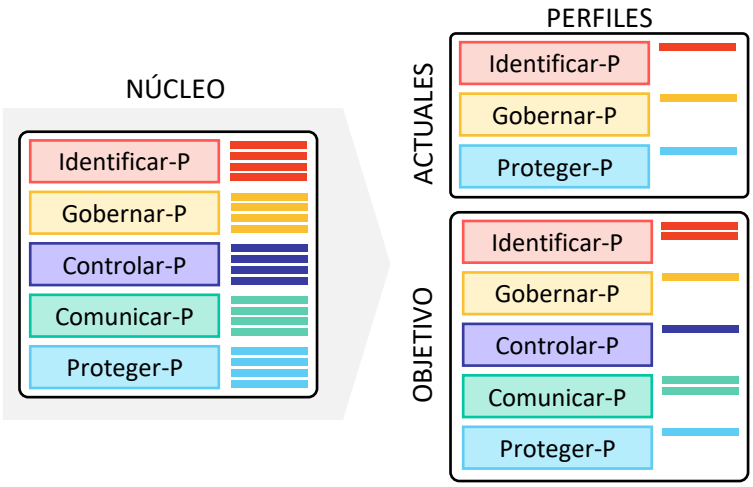


**Figura 6: Relación entre el Núcleo y los Perfiles**

El Marco de privacidad no prescribe ninguna plantilla de Perfiles para dar flexibilidad a la implementación. Según el método del Marco de privacidad basado en el riesgo, es posible que las organizaciones no necesiten lograr todos los resultados o actividades que se reflejan en el núcleo. Cuando una organización crea un Perfil, puede seleccionar o adaptar las Funciones, las Categorías y las Subcategorías a sus necesidades concretas, así como desarrollar sus propias Funciones, Categorías y Subcategorías adicionales que consideran los riesgos particulares de la organización. Una organización determina estas necesidades al tomar en cuenta los objetivos de su misión o empresa, sus valores de la privacidad y su tolerancia al riesgo; las funciones en el ecosistema de tratamiento de datos o en el sector industrial; los requisitos legales o normativos y mejores prácticas de la industria; las prioridades y los recursos de la gestión de riesgos; y las necesidades de privacidad de las personas atendidas o afectadas directa o indirectamente por los sistemas, productos o servicios de la organización.

Como se ilustra en la **Figura** 6, no hay ningún orden especificado para la creación de Perfiles. Una organización podría crear en primer lugar un Perfil objetivo para centrarse en los resultados de privacidad deseados y luego crear un Perfil actual para identificar las diferencias. O bien, una organización puede comenzar identificando sus actividades actuales y luego considerar la manera de modificar estas actividades para su Perfil objetivo. Una organización podría optar por crear Perfiles múltiples para diferentes funciones, sistemas, productos o servicios, o categorías de personas (por ejemplo, empleados, clientes) y priorizar mejor las actividades y los resultados en situaciones en las que existan diferentes grados de riesgos a la privacidad. Las organizaciones de un determinado sector industrial, o con funciones similares en el ecosistema de tratamiento de datos, pueden coordinarse entre ellas para crear Perfiles comunes.

## 2.3 Niveles de implementación

Los Niveles respaldan la toma de decisiones organizativa acerca de la manera de gestionar el riesgo a la privacidad al considerar la naturaleza de los riesgos a la privacidad que generan los sistemas, productos o servicios de la organización y la suficiencia de los procesos y los recursos que se implementan para gestionar dichos riesgos. Al seleccionar los Niveles, una organización deberá considerar sus Perfiles objetivo y la manera en que sus prácticas actuales de gestión de riesgos, el grado de integración de los riesgos a la privacidad en su cartera de gestión de riesgos empresariales, sus relaciones en el ecosistema de tratamiento de datos, la composición de su personal y el programa de capacitación puedan favorecer u obstaculizar el logro de estos Perfiles.

Existen cuatro Niveles bien definidos: Parcial (Nivel 1), Basado en riesgos (Nivel 2), Repetible (Nivel 3) y Adaptable (Nivel 4), que se describen en el Apéndice E. Los Niveles representan una progresión, aunque no es una progresión obligatoria. Si bien es probable que las organizaciones de Nivel 1 se beneficien de pasar al Nivel 2, no todas las organizaciones necesitan alcanzar los Niveles 3 o 4 (o también podrían centrarse únicamente en ciertas áreas de estos Niveles). La progresión a Niveles superiores es adecuada cuando los procesos o recursos de una organización en su Nivel actual no son suficientes para ayudar a gestionar los riesgos a la privacidad.

Una organización puede utilizar los Niveles para comunicarse internamente acerca de las asignaciones de recursos necesarias para avanzar a un Nivel superior, o como puntos de referencia generales para medir el progreso en su capacidad para gestionar los riesgos a la privacidad. Una organización también puede utilizar los Niveles para entender la escala de los recursos y los procesos de otras organizaciones en el ecosistema de tratamiento de datos y el modo en que se alinean con las prioridades de gestión de riesgos a la privacidad de la organización. No obstante, la implementación exitosa del Marco de privacidad se fundamenta en el logro de los resultados descritos en los Perfiles objetivo de una organización y no en la determinación de los Niveles.

# 3.0 Cómo utilizar el Marco de privacidad

Cuando el Marco de privacidad se utiliza como herramienta de gestión de riesgos, puede ayudar a una organización con sus medidas para optimizar el uso provechoso de los datos y con la elaboración de sistemas, productos y servicios innovadores, minimizando las consecuencias adversas para las personas. El Marco de privacidad puede ayudar a las organizaciones a responder esta pregunta fundamental: “¿Cómo estamos considerando los impactos sobre las personas a medida que perfeccionamos nuestros sistemas, productos y servicios?” El Marco de privacidad se puede emplear de manera flexible, de acuerdo con las necesidades particulares de una organización, aunque está diseñado para complementar las operaciones existentes de desarrollo de sistemas y negocios. La organización que lo implemente decidirá la manera de hacerlo. Por ejemplo, es posible que una organización ya cuente con procesos sólidos para gestionar los riesgos a la privacidad, pero, aun así, podría utilizar las cinco Funciones del Núcleo como una forma simplificada de analizar y articular cualquier diferencia. De otra manera, una organización que busque establecer un programa de privacidad puede usar las Categorías y las Subcategorías del Núcleo como referencia. Otras organizaciones podrían comparar los Perfiles o los Niveles para alinear las prioridades de la gestión de riesgos a la privacidad en las distintas funciones del ecosistema de tratamiento de datos. La diversidad de formas en que las organizaciones pueden emplear el Marco de privacidad debería desalentar la noción de que el “cumplimiento con el Marco de privacidad” es un concepto uniforme o referencial externamente. Las siguientes subsecciones presentan algunas opciones sobre las maneras de usar el Marco de privacidad.

## 3.1 Asignaciones a referencias informativas

Las referencias informativas son asignaciones a Subcategorías que contribuyen a la implementación, e incluyen asignaciones de herramientas, orientación técnica, normas, leyes, reglamentos y mejores prácticas. Las correspondencias que asignan las disposiciones de normas, leyes y reglamentos a las Subcategorías pueden ayudar a las organizaciones a determinar las actividades o los resultados a los que hay que dar prioridad para facilitar el cumplimiento. El Marco de privacidad es neutro en lo que a la tecnología se refiere, pero es compatible con la innovación tecnológica, puesto que cualquier organización o sector de la industria puede generar estas asignaciones a medida que evolucionan las necesidades tecnológicas y empresariales conexas. Al confiar en normas, directrices y prácticas basadas en un consenso, las herramientas y los métodos disponibles para lograr resultados de privacidad positivos pueden cruzar las fronteras y adaptarse a la naturaleza global de los riesgos a la privacidad. El empleo de normas existentes y emergentes habilitará a las economías de escala e impulsará el desarrollo de sistemas, productos y servicios que satisfagan las necesidades identificadas del mercado teniendo presentes las necesidades de privacidad de las personas.

Las deficiencias en las asignaciones también pueden emplearse para identificar los lugares donde las normas, directrices y prácticas adicionales o revisadas ayudarían a una organización a abordar necesidades emergentes. Una organización que implementa una Subcategoría determinada, o que crea una Subcategoría nueva, podría descubrir que no hay orientación suficiente para una actividad o resultado relacionados. Para hacer frente a esa necesidad, una organización podría colaborar con los líderes en el ámbito de la tecnología o con las entidades normativas para redactar, elaborar y coordinar normas, directrices o prácticas.

Se puede encontrar un repositorio de referencias informativas en https://www.nist.gov/privacy-framework. Estos recursos ayudan a las organizaciones con el uso del Marco de privacidad y el logro de mejores prácticas de privacidad.

## 3.2 Fortalecimiento de la responsabilidad

La responsabilidad se considera generalmente un principio clave de la privacidad, aunque, en teoría, no es un factor exclusivo de esta.[13] La responsabilidad se da en toda una organización y puede expresarse en diversos grados de abstracción, por ejemplo, como un valor cultural, como políticas y procedimientos de gobernanza, o como relaciones de trazabilidad entre los *requisitos de privacidad* y los *controles de privacidad*. La gestión de riesgos a la privacidad puede ser un medio para promover la responsabilidad en todos los niveles organizativos, ya que conecta a los ejecutivos sénior (las personas que pueden comunicar los valores de la privacidad y la tolerancia al riesgo de una organización) con el nivel de gerencia de procesos o negocios (las personas que pueden colaborar con la elaboración y la implementación de las políticas y los procedimientos de gobernanza que respaldan los valores de la privacidad de la organización). Estas políticas y procedimientos pueden comunicarse entonces a quienes se encuentran en el nivel de implementación u operaciones. Estas personas colaboran definiendo los requisitos de privacidad compatibles con la expresión de las políticas y los procedimientos en los sistemas, productos y servicios de una organización. El personal a nivel de implementación u operaciones también selecciona, implementa y evalúa los controles como medidas técnicas y políticas que cumplen con los requisitos de privacidad. Además, informa del progreso, las diferencias y las deficiencias, la gestión de incidentes, y los riesgos a


**Figura 7: Flujos de la comunicación y la colaboración nocional dentro de una organización**

[13] Véase, por ejemplo, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* [Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales] de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) (2013). Disponible en https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm; *ISO/IEC 29100:2011 – Information technology – Security techniques – Privacy framework* [Tecnología de la información – Técnicas de seguridad – Marco de privacidad] (ISO, Ginebra, Suiza) de la Organización Internacional de Normalización (ISO)/Comisión Electrotécnica Internacional (IEC, por sus siglas en inglés) (2011). Disponible en https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip; y *Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services* [Principios de la protección de la privacidad del consumidor: Principios de seguridad para las tecnologías y servicios automotrices] de la Alliance of Automobile Manufacturers, Inc. [Alianza de Fabricantes de Automóviles] y la Association of Global Automakers, Inc. [Asociación de Fabricantes Globales de Automóviles] (2014). Disponible en https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf.

la privacidad cambiantes para que el nivel de gerencia de procesos o negocios y los ejecutivos sénior puedan entender de mejor manera y responder adecuadamente.

La **Figura** 7 es una representación gráfica de la colaboración y la comunicación bidireccionales y de la forma en que pueden incorporarse los elementos del Marco de privacidad para facilitar el proceso. De esta manera, las organizaciones pueden utilizar el Marco de privacidad como una herramienta que fomente la responsabilidad. También pueden usar el Marco de privacidad junto con otros marcos y guías que proporcionen prácticas adicionales para lograr la responsabilidad dentro de las organizaciones y entre ellas.[14]

## 3.3 Establecimiento o mejoramiento de un programa de privacidad

Por medio de un modelo simple con las fases "preparar, establecer y proceder", el Marco de privacidad ayuda a crear un programa de privacidad nuevo o a mejorar un programa existente. A medida que una organización pase por estas fases, podrá utilizar referencias informativas para guiar la priorización o el logro de resultados. Véase la Sección 3.1 para obtener más información acerca de las referencias informativas. Además, se puede encontrar un repositorio en https://www.nist.gov/privacy-framework.

### Preparar

La gestión eficaz del riesgo a la privacidad requiere que una organización conozca su misión o entorno empresarial, su entorno legal, su tolerancia al riesgo, los riesgos a la privacidad generados por sus sistemas, productos o servicios, y las funciones que desempeña en el ecosistema de tratamiento de datos. Una organización hace uso de las Funciones Identificar-P y Gobernar-P para "estar preparada" cuando revisa las Categorías y Subcategorías y comienza a crear su Perfil actual y su Perfil objetivo.[15] Las actividades y los resultados, tales como el establecimiento de valores y políticas de privacidad de la organización, la determinación y expresión de la tolerancia al riesgo de la organización y la realización de evaluaciones de riesgos a la privacidad (véase el Apéndice D para obtener más información sobre las evaluaciones de riesgos a la privacidad), sientan una base para completar los Perfiles en la fase "Establecer".

***Un método simplificado para establecer o mejorar un programa de privacidad***

**Preparar:** usa las Funciones Identificar-P y Gobernar-P para estar "preparado".

**Establecer:** "establece" un plan de acción basado en las diferencias entre los Perfiles actuales y los Perfiles objetivo.

**Proceder:** "procede" con la implementación del plan de acción.

### Establecer

Una organización completa su Perfil actual al indicar cuáles resultados de las Categorías y Subcategorías de las Funciones restantes se están alcanzando. La indicación de que un resultado se alcanzó

[14] Véase, por ejemplo, la Publicación especial 800-37 del NIST, rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [Marco de gestión de riesgos para sistemas de información y organizaciones: un enfoque del ciclo de vida del sistema para la seguridad y la privacidad] [7]; y *Privacy Management Reference Model and Methodology (PMRM)* [Modelo de referencia y metodología para la gestión de la privacidad], versión 1.0 de la Organization for the Advancement of Structured Information Standards [Organización para la Mejora de las Normas de Información Estructuradas] (OASIS, por sus siglas en inglés) (2016) en https://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.pdf.

[15] Para obtener más información, véase la fase "Preparar" en la Sección 3.1 de la Publicación especial 800-37 del NIST, rev. 2 [7].

parcialmente ayuda al logro de los pasos subsiguientes porque proporciona información de referencia. Basada en las actividades que abarcan las funciones Identificar y Gobernar (como los valores y las políticas de la privacidad de la organización, la tolerancia al riesgo organizativo y los resultados de las evaluaciones de riesgos a la privacidad), la organización completa su Perfil objetivo centrado en la evaluación de las Categorías y Subcategorías que describe los resultados de privacidad deseados. Una organización también puede crear sus propias Funciones, Categorías y Subcategorías adicionales para considerar los riesgos organizativos particulares. Al crear un Perfil objetivo, también podría tener en cuenta las influencias y los requisitos de las partes interesadas externas, como clientes y socios empresariales. Una organización puede establecer Perfiles múltiples compatibles con sus diferentes líneas de negocio o procesos, los cuales podrían tener distintas necesidades empresariales y tolerancias al riesgo conexas.

Una organización compara el Perfil actual y el Perfil objetivo para determinar las diferencias. Además, crea un plan de acción priorizado para abordar las diferencias (que refleje los factores determinantes de la misión, los costos, beneficios y riesgos) y lograr los resultados en el Perfil objetivo. Una organización que utilice el Marco de ciberseguridad y el Marco de privacidad conjuntamente podrá crear planes de acción integrados. Luego, habrá de determinar los recursos, así como las necesidades de financiación y de personal, que se requieran para resolver las diferencias. Esto puede servir de base para la selección de un Nivel apropiado. El uso de los Perfiles de esta manera alienta a una organización a tomar decisiones informadas sobre las actividades de privacidad, contribuye a la gestión de riesgos y permite que la organización haga mejoras dirigidas y rentables.

### Proceder

Una vez que el plan de acción se haya “establecido”, la organización dará prioridad a las medidas que se aplicarán para resolver cualquier diferencia, para luego ajustar sus prácticas de privacidad actuales a fin de alcanzar el Perfil objetivo.[16]

Para que una organización evalúe y mejore continuamente su postura de privacidad, no tiene que seguir las fases en orden, sino en la secuencia que necesite. Por ejemplo, es posible que una organización descubra que la calidad de las evaluaciones de riesgos a la privacidad mejora cuando suele repetir la fase Preparar. Además, una organización puede vigilar el progreso mediante la actualización iterativa del Perfil actual o el Perfil objetivo para adaptarse a los riesgos cambiantes, y comparar más adelante el Perfil actual con el Perfil objetivo.

## 3.4 Aplicación al ciclo de vida de desarrollo de un sistema

El Perfil objetivo se puede alinear con las fases del ciclo de vida de desarrollo de un sistema (SDLC, por sus siglas en inglés), es decir, planificación, diseño, creación o compra, implementación, operación y desmantelamiento, para ayudar al logro de los resultados de privacidad priorizados.[17] Al comenzar con la fase de planificación, los resultados de privacidad priorizados podrán transformarse en las capacidades y los requisitos de privacidad del sistema, tomando en cuenta la probabilidad de que los requisitos evolucionen durante el resto del ciclo de vida. Un hito clave de la fase de diseño es la validación de que las capacidades y los requisitos de privacidad coinciden con las necesidades y la tolerancia al riesgo de una organización, como se expresa en el Perfil objetivo. Ese mismo Perfil objetivo

[16] La Publicación especial 800-37 del NIST, rev. 2, [7] ofrece más información sobre los pasos que deben seguirse en el plan de acción, incluidas la selección de control, la implementación y la evaluación para resolver toda diferencia.

[17] En el ciclo de vida de desarrollo de un sistema, las organizaciones pueden emplear una variedad de metodologías de desarrollo (por ejemplo, modelo en cascada, en espiral o ágil).

puede servir como una lista interna que deberá evaluarse cuando se ponga en marcha el sistema para verificar que se implementen todas las capacidades y los requisitos de privacidad. Los resultados de privacidad que el uso del Marco de privacidad determine deberán servir entonces de base para el funcionamiento continuo del sistema. Esto incluye la revaluación esporádica (con captura de resultados en un Perfil actual) para verificar que aún se cumpla con las capacidades y los requisitos de privacidad.

Las evaluaciones de riesgos a la privacidad suelen centrarse en el ciclo de vida de los datos, es decir, las etapas a través de las cuales pasan y que, a menudo, se caracterizan como creación o recolección, tratamiento, difusión, uso, almacenamiento y disposición. Esta última incluye la destrucción y la eliminación de los datos. La alineación del ciclo de vida de desarrollo de un sistema con el ciclo de vida de los datos, por medio de la identificación y el conocimiento de la manera en que se procesan los datos en todas las etapas del ciclo de vida de desarrollo de un sistema, ayuda a las organizaciones a gestionar mejor los riesgos a la privacidad y guía la selección e implementación de los controles de privacidad para cumplir con los requisitos de privacidad.

## 3.5 Uso en el ecosistema de tratamiento de datos

Un factor clave en la gestión de riesgos a la privacidad son las funciones que desempeña una entidad en el ecosistema de tratamiento de datos, las cuales pueden afectar no solo sus obligaciones legales, sino también las medidas que la entidad podría adoptar para gestionar los riesgos a la privacidad. Como se muestra en la **Figura** 8, el ecosistema de tratamiento de datos abarca una serie de entidades y funciones que pueden tener relaciones complejas y multidireccionales entre sí y con las personas. La complejidad aumenta cuando las entidades se apoyan en una cadena de subentidades (por ejemplo, los proveedores de servicios pueden tener el respaldo de una serie de proveedores de servicios, o los fabricantes pueden tener varios proveedores de componentes). La **Figura** 8 muestra las entidades como si tuvieran funciones distintas, pero algunas podrían desempeñar varias funciones, por ejemplo, una organización que preste servicios a otras organizaciones y venda productos al por menor a los consumidores. Las clasificaciones de las funciones que aparecen en la **Figura** 8 son nocionales. En la práctica, las funciones de una entidad pueden estar legalmente codificadas, por ejemplo, algunas leyes clasifican a las organizaciones como responsables de datos o procesadoras de datos, o bien las clasificaciones podrían derivarse de designaciones del sector industrial.


**Figura 8: Relaciones en el ecosistema de tratamiento de datos**

Cuando una entidad crea uno o más Perfiles pertinentes a sus funciones, puede usar el Marco de privacidad para considerar la manera en que gestionará el riesgo a la privacidad no solo con respecto a sus propias prioridades, sino también con respecto a la manera en que las medidas que adopte

afectarán la gestión de riesgos a la privacidad de otras entidades en el ecosistema de tratamiento de datos. Por ejemplo:

- Una organización que toma decisiones sobre la forma de recolectar y utilizar los datos de las personas podría utilizar un Perfil para comunicar los requisitos de privacidad a un proveedor de servicios externo (por ejemplo, un proveedor de servicios en la nube al que exporta los datos), y el proveedor de servicios externo que trate los datos podría utilizar su Perfil para demostrar las medidas que ha adoptado para procesar los datos de conformidad con sus obligaciones contractuales.
- Una organización podría comunicar su postura de privacidad por medio de un Perfil actual para informar resultados o para compararla con los requisitos de adquisición.
- Un sector de la industria establecerá tal vez un Perfil común que puedan usar sus miembros para personalizar sus propios Perfiles.
- Un fabricante puede emplear un Perfil objetivo para determinar las capacidades que debe incorporar en sus productos de manera tal que sus clientes comerciales puedan satisfacer las necesidades de privacidad de sus usuarios finales.
- Un programador puede usar un Perfil objetivo para considerar la manera de diseñar una aplicación que habilite salvaguardias de privacidad cuando se utilice en los entornos de los sistemas de otras organizaciones.

El Marco de privacidad proporciona un lenguaje común para comunicar los requisitos de privacidad con las entidades en el ecosistema de tratamiento de datos. La necesidad de esta comunicación puede tener particular relevancia cuando el ecosistema de tratamiento de datos cruza las fronteras nacionales, como en el caso de las transferencias internacionales de datos. Algunas de las prácticas organizativas compatibles con la comunicación son:

- determinación de los requisitos de privacidad;
- aprobación de los requisitos de privacidad por medio de acuerdos formales (por ejemplo, contratos, marcos entre varias partes);
- comunicación de la manera en que esos requisitos de privacidad se verificarán y validarán;
- verificación del cumplimiento de los requisitos de privacidad por medio de una variedad de metodologías de evaluación; y
- regulación y gestión de las actividades mencionadas.

## 3.6 Comunicación de las decisiones de compra

Dado que se puede usar un Perfil actual o un Perfil objetivo para generar una lista priorizada de requisitos de privacidad, estos Perfiles también pueden usarse como base para comunicar las decisiones sobre la compra de productos y servicios. Cuando una organización selecciona primero los resultados pertinentes a sus metas de privacidad, puede evaluar los sistemas, productos o servicios de sus socios comparándolos con esos resultados. Por ejemplo, si se compra un dispositivo para monitorear las condiciones ambientales de un bosque, la *capacidad de gestión* puede ser importante para ayudar a minimizar el tratamiento de datos sobre las personas que hacen uso del bosque. Esta capacidad debería hacer la comparación de una evaluación del fabricante con las Subcategorías aplicables en el Núcleo (por ejemplo, CT.DP-P4: Las configuraciones de sistemas o de dispositivos permiten la recolección o revelación selectivas de *elementos de datos*).

En los casos cuando no sea posible imponer al proveedor un conjunto de requisitos de privacidad, el objetivo debe ser tomar la mejor decisión de compra seleccionando entre varios proveedores, dada una lista cuidadosamente determinada de requisitos de privacidad. Esto suele significar que hay cierto grado de compensación, cuando se comparan varios productos o servicios con las diferencias conocidas en el Perfil. Si el sistema, producto o servicio que se adquirió no cumple con todos los objetivos descritos en el Perfil, la organización podría asumir el riesgo residual tomando medidas de mitigación u otras medidas de gestión.

## Referencias


[1] Instituto Nacional de Normas y Tecnología. (2018). Marco para la mejora de la seguridad cibernética en infraestructuras críticas, versión 1.1. (Instituto Nacional de Normas y Tecnología. Gaithersburg, Maryland). https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

[2] Instituto Nacional de Normas y Tecnología. (2019). *Summary Analysis of the Responses to the NIST Privacy Framework Request for Information* [Análisis resumido de las respuestas a la solicitud de información referente al Marco de privacidad del NIST]. (Instituto Nacional de Normas y Tecnología. Gaithersburg, Maryland). https://www.nist.gov/system/files/documents/2019/02/27/rfi_response_analysis_privacyframework_2.27.19.pdf

[3] Instituto Nacional de Normas y Tecnología. (2019). *NIST Privacy Risk Assessment Methodology* [Metodología del NIST para evaluación de los riesgos a la privacidad] (PRAM, por sus siglas en inglés). (Instituto Nacional de Normas y Tecnología. Gaithersburg, Maryland). https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources

[4] *The Smart Grid Interoperability Panel—Smart Grid Cybersecurity Committee* [Panel de interoperabilidad de la red eléctrica inteligente—Comisión de ciberseguridad de la red eléctrica inteligente] (2014). *Guidelines for Smart Grid Cybersecurity: Volume 1* [Directrices para la ciberseguridad de la red eléctrica inteligente: Volumen 1]. *Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements* [Estrategia, arquitectura y requisitos de alto nivel de ciberseguridad de la red eléctrica inteligente]. (Instituto Nacional de Normas y Tecnología. Gaithersburg, Maryland). Informe interinstitucional o interno 7628 del NIST, rev. 1, vol. 1. https://doi.org/10.6028/NIST.IR.7628r1

[5] Brooks, S. W., García, M. E., Lefkovitz N. B., Lightman S. y Nadeau, E. M. (2017). *An Introduction to Privacy Engineering and Risk Management in Federal Systems* [Una introducción a la ingeniería de la privacidad y a la gestión de riesgos en los sistemas federales]. (Instituto Nacional de Normas y Tecnología. Gaithersburg, Maryland). Informe interinstitucional o interno 8062 del NIST. https://doi.org/10.6028/NIST.IR.8062

[6] Iniciativa de transformación del grupo de trabajo conjunto (2011). *Managing Information Security Risk: Organization, Mission, and Information System View* [Gestión de riesgos a la seguridad de la información: vista de la organización, la misión y el sistema de información]. (Instituto Nacional de Normas y Tecnología. Gaithersburg, Maryland). Publicación especial 800-39 del NIST. https://doi.org/10.6028/NIST.SP.800-39

[7] Grupo de Trabajo conjunto (2018). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [Marco de gestión de riesgos para sistemas de información y organizaciones: un enfoque del ciclo de vida del sistema para la seguridad y la privacidad]. (Instituto Nacional de Normas y Tecnología. Gaithersburg, Maryland). Publicación especial 800-37 del NIST, rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[8] Grassi, P. A., García, M. E., Fenton, J. L. (2017). *Digital Identity Guidelines* [Directrices de identidad digital]. (Instituto Nacional de Normas y Tecnología. Gaithersburg, Maryland). Publicación especial 800-63-3 del NIST. Incluye actualizaciones a partir del 1 de diciembre de 2017. https://doi.org/10.6028/NIST.SP.800-63-3

[9] Oficina de Administración y Presupuesto (OMB, por sus siglas en inglés) (2017). *Preparing for and Responding to a Breach of Personally Identifiable Information* [Preparación contra una

vulneración de la información de identificación personal, y respuesta]. (La Casa Blanca. Washington, DC). Memorando M-17-12 de la OMB, 3 de enero de 2017. Disponible en https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf.

[10] Iniciativa de transformación del grupo de trabajo conjunto (2013). *Security and Privacy Controls for Federal Information Systems and Organizations* [Controles de seguridad y privacidad para sistemas y organizaciones de información federales]. (Instituto Nacional de Normas y Tecnología. Gaithersburg, Maryland). Publicación especial 800-53 del NIST, rev. 4. Incluye actualizaciones a partir del 22 de enero de 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[11] Grassi, P. A., Lefkovitz, N. B., Nadeau, E. M., Galluzzo, R. J. y Dinh, A. T. (2018). *Attribute Metadata: A Proposed Schema for Evaluating Federated Attributes* [Metadatos de atributos: un esquema propuesto para evaluar los atributos federados]. (Instituto Nacional de Normas y Tecnología. Gaithersburg, Maryland). Informe interinstitucional o interno 8112 del NIST. https://doi.org/10.6028/NIST.IR.8112

[12] Iniciativa de transformación del grupo de trabajo conjunto. (2012) *Guide for Conducting Risk Assessments* [Guía para efectuar evaluaciones de riesgos]. (Instituto Nacional de Normas y Tecnología. Gaithersburg, Maryland). Publicación especial 800-30 del NIST, rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[13] "Definiciones", título 44 del *Código de los EE. UU.*, sección 3542. Ed. 2011. https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3542

# Apéndice A: Núcleo del Marco de privacidad

Este apéndice presenta el Núcleo: una tabla de Funciones, Categorías y Subcategorías que describen actividades y resultados específicos de utilidad para la gestión de riesgos a la privacidad cuando los sistemas, productos y servicios procesan datos.

## Nota para los usuarios

**Método basado en riesgos:**

- **El Núcleo no es una lista de control de las acciones que se deben llevar a cabo. Una organización selecciona las Subcategorías de acuerdo con su estrategia de riesgos para proteger la privacidad de las personas, como se indica en las definiciones de la Categoría.** Es posible que una organización no necesite lograr todos los resultados o actividades que se reflejan en el Núcleo. Se prevé que una organización utilice Perfiles para seleccionar y dar prioridad a las Funciones, Categorías y Subcategorías que satisfagan mejor sus necesidades específicas al tomar en cuenta sus metas; las funciones en el ecosistema de tratamiento de datos o en el sector industrial; los requisitos legales o normativos y mejores prácticas de la industria; las prioridades de la gestión de riesgos; y las necesidades de privacidad de las personas atendidas o afectadas directa o indirectamente por los sistemas, productos o servicios de la organización.
- No es obligatorio lograr el resultado total. Una organización puede usar sus Perfiles para expresar el logro parcial de un resultado, dado que es posible que todos los aspectos de un resultado sean pertinentes para su gestión del riesgo a la privacidad, o bien, una organización puede usar un Perfil objetivo para expresar un aspecto de un resultado para el cual no tiene actualmente la capacidad de lograr.
- Podría ser necesario considerar una combinación de varios resultados para gestionar adecuadamente el riesgo a la privacidad. Por ejemplo, una organización que responda a las solicitudes de las personas para acceder a los datos podría seleccionar para su Perfil tanto la Subcategoría CT.DM-P1: “Se puede acceder a los elementos de datos para su revisión”, como la Categoría PR.AC-P: “Gestión y autenticación de la identidad y control del acceso a esta” para garantizar que solo la persona a la que conciernen los datos tenga acceso.

**Implementación:** El formato tabular del Núcleo no pretende sugerir un orden de implementación específico, ni supone que existe un grado de importancia entre las Funciones, Categorías y Subcategorías. La implementación puede ser no secuencial, simultánea o iterativa, según la etapa del ciclo de vida de desarrollo de sistema, el estado del programa de privacidad, la escala del personal o las funciones de una organización en el ecosistema de tratamiento de datos. Aunque el Núcleo no es exhaustivo, es extensible, y esto permite a las organizaciones, sectores y otras entidades adaptar o agregar Funciones, Categorías y Subcategorías adicionales a sus Perfiles.

**Funciones:**

- **Funciones del ecosistema:** El Núcleo tiene por objeto ser utilizable por toda organización o entidad, independientemente de sus funciones en el ecosistema de tratamiento de datos. Si bien el Marco de privacidad no clasifica las funciones de los ecosistemas, una organización debe revisar el Núcleo desde su punto de vista en el ecosistema. Las funciones de una organización pueden estar legalmente codificadas, por ejemplo, algunas leyes clasifican a organizaciones como responsables de datos o procesadoras de datos, o bien las clasificaciones podrían derivarse de designaciones del sector industrial. Dado que los elementos del Núcleo no se

asignan por función del ecosistema, una organización puede utilizar sus Perfiles para seleccionar Funciones, Categorías y Subcategorías que sean pertinentes a sus funciones.

- **Funciones organizativas:** Las distintas partes del personal de una organización pueden asumir la responsabilidad de Categorías o Subcategorías diferentes. Por ejemplo, el departamento legal podría hacerse responsable de llevar a cabo actividades de conformidad con "políticas, procesos y procedimientos de la gobernanza", mientras que el departamento de tecnología de la información podría trabajar en "inventario y asignaciones". En el mejor de los casos, el Núcleo promueve la colaboración de la organización para crear Perfiles y lograr resultados.

**Escalabilidad:** Ciertos aspectos de los resultados podrían estar redactados de forma ambigua. Por ejemplo, los resultados podrían incluir términos como "comunicado" o "revelado", sin indicar quién recibió las comunicaciones o revelaciones. La ambigüedad es deliberada para permitir que una amplia gama de organizaciones con diferentes casos de uso determine lo que es apropiado o que se requiere en un contexto dado.

**Repositorio de recursos:** Se pueden encontrar recursos independientes que ofrecen más información acerca de la manera de priorizar o lograr resultados en https://www.nist.gov/privacy-framework.

**Alineación del Marco de ciberseguridad:**

- Como se indica en la Sección 2.1, las organizaciones pueden usar las cinco Funciones del Marco de privacidad (Identificar-P, Gobernar-P, Controlar-P, Comunicar-P y Proteger-P) para gestionar los riesgos a la privacidad que surgen del tratamiento de datos. Proteger-P se centra específicamente en la gestión de los riesgos asociados con eventos de privacidad relacionados con la ciberseguridad (por ejemplo, vulneraciones de la privacidad). Para hacer aún más compatible la gestión de los riesgos asociados con los eventos de privacidad relacionados con la seguridad, las organizaciones podrían optar por usar las Funciones Detectar, Responder y Recuperar del Marco de ciberseguridad. Por este motivo, estas funciones se incluyen en la **Tabla** 1**,** pero se muestran con fondo gris. De otro modo, las organizaciones podrían utilizar las cinco Funciones del Marco de ciberseguridad junto con las Funciones Identificar-P, Gobernar-P, Controlar-P y Comunicar-P para abordar colectivamente los riesgos a la privacidad y la seguridad. Véase en la **Figura** 5 un ejemplo ilustrado de la manera en que las Funciones de ambos marcos pueden utilizarse en diversas combinaciones para gestionar diferentes aspectos de los riesgos a la privacidad y la ciberseguridad.
- Es posible que ciertas Funciones, Categorías o Subcategorías sean idénticas a las del Marco de ciberseguridad, o se hayan adaptado de este. La leyenda siguiente se puede usar para identificar esta relación en la **Tabla** 2. Se pueden encontrar las correspondencias completas entre los dos marcos en el repositorio de recursos en https://www.nist.gov/privacy-framework.

La Función, la Categoría o la Subcategoría se alinean con el Marco de ciberseguridad, pero el texto se ha adaptado para el Marco de privacidad.

La Categoría o la Subcategoría es idéntica a la del Marco de ciberseguridad.

**Identificadores del Núcleo:** Para facilitar el uso, cada componente del Núcleo recibe un identificador único. Cada una de las Funciones y de las Categorías tiene un identificador alfabético único, como se muestra en la **Tabla** 1. Las Subcategorías en cada Categoría tienen un número que se agrega al identificador alfabético. El identificador único de cada Subcategoría se incluye en la **Tabla** 2.

**Tabla 1: Identificadores únicos de las Funciones y las Categorías del Marco de privacidad**

| Identificador único de la Función | Función | Identificador único de la Categoría | Categoría |
|---|---|---|---|
| **ID-P** | Identificar-P | ID.IM-P | Inventario y asignaciones |
| | | ID.BE-P | Entorno empresarial |
| | | ID.RA-P | Evaluación de riesgos |
| | | ID.DE-P | Gestión de riesgos al ecosistema de tratamiento de datos |
| **GV-P** | Gobernar-P | GV.PO-P | Políticas, procesos y procedimientos de la gobernanza |
| | | GV.RM-P | Estrategia de gestión de riesgos |
| | | GV.AT-P | Conocimiento y capacitación |
| | | GV.MT-P | Vigilancia y revisión |
| **CT-P** | Controlar-P | CT.PO-P | Políticas, procesos y procedimientos del tratamiento de datos |
| | | CT.DM-P | Gestión de tratamiento de datos |
| | | CT.DP-P | Tratamiento desasociado |
| **CM-P** | Comunicar-P | CM.PO-P | Políticas, procesos y procedimientos de la comunicación |
| | | CM.AW-P | Conocimiento del tratamiento de datos |
| **PR-P** | Proteger-P | PR.PO-P | Políticas, procesos y procedimientos de la protección de datos |
| | | PR.AC-P | Gestión y autenticación de la identidad y control del acceso a esta |
| | | PR.DS-P | Seguridad de datos |
| | | PR.MA-P | Mantenimiento |
| | | PR.PT-P | Tecnología protectora |
| **DE** | Detectar | DE.AE | Anomalías y eventos |
| | | DE.CM | Vigilancia continua de la seguridad |
| | | DE.DP | Procesos de detección |
| **RS** | Responder | RS.RP | Planificación de la respuesta |
| | | RS.CO | Comunicaciones |
| | | RS.AN | Análisis |
| | | RS.MI | Mitigación |
| | | RS.IM | Mejoramientos |
| **RC** | Recuperar | RC.RP | Planificación de la recuperación |
| | | RC.IM | Mejoramientos |
| | | RC.CO | Comunicaciones |

**Tabla 2: Núcleo del Marco de privacidad**

| Función | Categoría | Subcategoría |
|---|---|---|
| **IDENTIFICAR-P (ID-P):** Define el conocimiento organizativo para gestionar el riesgo a la privacidad de las personas que surge del tratamiento de datos. | **Inventario y asignaciones (ID.IM-P):** Se conoce el tratamiento de datos por sistemas, productos o servicios, y este tratamiento es la base de la gestión de riesgos a la privacidad. | **ID.IM-P1:** Se inventarían los sistemas, productos o servicios que procesan datos. |
| | | **ID.IM-P2:** Se inventarían los propietarios u operadores (por ejemplo, la organización o terceros, como proveedores de servicios, socios, clientes y desarrolladores) y sus funciones con respecto a los sistemas, productos, servicios y componentes (por ejemplo, internos o externos) que procesan datos. |
| | | **ID.IM-P3:** Se inventarían las categorías de personas (por ejemplo, clientes, empleados, posibles empleados o consumidores) cuyos datos se están procesando. |
| | | **ID.IM-P4:** Se inventarían las acciones de datos de los sistemas, productos o servicios. |
| | | **ID.IM-P5:** Se inventarían los propósitos de las acciones de datos. |
| | | **ID.IM-P6:** Se inventarían los elementos de datos en las acciones de datos. |
| | | **ID.IM-P7:** Se identifica el entorno de tratamiento de datos (por ejemplo, ubicación geográfica, internamente, en la nube, de terceros). |
| | | **ID.IM-P8:** El tratamiento de datos se asigna, ilustrando las acciones de datos y los elementos de datos conexos para los sistemas, productos o servicios, incluidos los componentes, las funciones de los propietarios u operadores de los componentes y las interacciones de personas o de terceros con los sistemas, productos o servicios. |
| | **Entorno empresarial (ID.BE-P):** Se conocen y priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización, y esta información es la base de las decisiones sobre funciones, responsabilidades y de la gestión de riesgos a la privacidad. | **ID.BE-P1:** Se identifican y comunican las funciones de la organización en el ecosistema de tratamiento de datos. |
| | | **ID.BE-P2:** Se establecen y comunican las prioridades de la misión, los objetivos y las actividades de la organización. |
| | | **ID.BE-P3:** Se identifican los sistemas, productos o servicios compatibles con las prioridades de la organización y se comunican los requisitos clave. |

| Función | Categoría | Subcategoría |
|---|---|---|
| | **Evaluación de riesgos (ID.RA-P):** La organización conoce los riesgos a la privacidad de las personas y la manera en que dichos riesgos a la privacidad pueden repercutir en las operaciones organizativas, así como en su misión, funciones, otras prioridades de la gestión de riesgos (por ejemplo, el cumplimiento, las finanzas), reputación, empleados y cultura. | **ID.RA-P1:** Se identifican los factores contextuales relacionados con los sistemas, productos o servicios, al igual que las acciones de datos (por ejemplo, la información demográfica de las personas y sus intereses o percepciones relacionados con la privacidad, la confidencialidad o los tipos de datos, y la visibilidad del tratamiento de datos para las personas y los terceros). |
| | | **ID.RA-P2:** Se identifican y evalúan las entradas y salidas de análisis de datos para determinar el sesgo. |
| | | **ID.RA-P3:** Se identifican las posibles acciones problemáticas de datos y los problemas conexos. |
| | | **ID.RA-P4:** Se emplean las acciones problemáticas de datos, las probabilidades y los impactos para determinar y priorizar los riesgos. |
| | | **ID.RA-P5:** Se identifican, priorizan e implementan las respuestas a los riesgos. |
| | **Gestión de riesgos al ecosistema de tratamiento de datos (ID.DE-P):** Se establecen y utilizan las prioridades, restricciones, tolerancia al riesgo y suposiciones de la organización para ayudar a las decisiones relativas al riesgo asociadas con la gestión de riesgos a la privacidad y con los terceros en el ecosistema de tratamiento de datos. La organización ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos a la privacidad en el ecosistema de tratamiento de datos. | **ID.DE-P1:** Las partes interesadas de la organización identifican, establecen, evalúan, gestionan y acuerdan las políticas, los procesos y los procedimientos de la gestión de riesgos al ecosistema de tratamiento de datos. |
| | | **ID.DE-P2:** Se identifican, priorizan y evalúan, mediante un proceso de evaluación de riesgos a la privacidad, las partes del ecosistema de tratamiento de datos (por ejemplo, proveedores de servicios, clientes, socios, fabricantes de productos y desarrolladores de aplicaciones). |
| | | **ID.DE-P3:** Se celebran contratos con las partes del ecosistema de tratamiento de datos para implementar medidas adecuadas destinadas al cumplimiento de los objetivos del programa de privacidad de una organización. |
| | | **ID.DE-P4:** Se emplean marcos de interoperabilidad o métodos similares de varias partes para gestionar los riesgos a la privacidad del ecosistema de tratamiento de datos. |

| | Función | Categoría | Subcategoría |
|---|---|---|---|
| | | | **ID.DE-P5:** Se evalúan de manera habitual las partes del ecosistema de tratamiento de datos por medio de auditorías, resultados de pruebas u otros tipos de evaluaciones para verificar que cumplan con sus obligaciones contractuales, con el marco de interoperabilidad u otras obligaciones. |
| | **GOBERNAR-P (GV-P):** Define e implementa la estructura de gobernanza organizativa para facilitar el conocimiento continuo de las prioridades de gestión de riesgos de la organización basadas en el riesgo a la privacidad. | **Políticas, procesos y procedimientos de la gobernanza (GV.PO-P):** Se conocen las políticas, los procesos y los procedimientos para gestionar y vigilar los requisitos normativos, legales, de riesgo, ambientales y operativos de la organización, y en estos se basa la gestión de riesgos a la privacidad. | **GV.PO-P1:** Se establecen y comunican los valores y las políticas de la privacidad de la organización (por ejemplo, las condiciones sobre el tratamiento de datos, como los usos o los períodos de retención de datos, y las prerrogativas de las personas con respecto al tratamiento de estos). |
| | | | **GV.PO-P2:** Se establecen e implementan procesos para infundir los valores de la privacidad de la organización a la elaboración y las operaciones del sistema, producto o servicio. |
| | | | **GV.PO-P3:** Se establecen las funciones y las responsabilidades del personal con respecto a la privacidad. |
| | | | **GV.PO-P4:** Se coordinan las funciones y las responsabilidades de la privacidad, y se alinean con los terceros que tengan un interés (por ejemplo, proveedores de servicios, clientes y socios). |
| | | | **GV.PO-P5:** Se conocen y gestionan los requisitos legales, normativos y contractuales relativos a la privacidad. |
| | | | **GV.PO-P6:** Las políticas, los procesos y los procedimientos de la gestión de riesgos y la gobernanza abordan los riesgos a la privacidad. |
| | | **Estrategia de gestión de riesgos (GV.RM-P):** Se establecen las prioridades, restricciones, tolerancia al riesgo y suposiciones de la organización, y se aplican para facilitar las decisiones operativas sobre el riesgo. | **GV.RM-P1:** Las partes interesadas de la organización establecen, gestionan y acuerdan los procesos de la gestión de riesgos. |
| | | | **GV.RM-P2:** Se determina y expresa claramente la tolerancia al riesgo de la organización. |
| | | | **GV.RM-P3:** La determinación de la tolerancia al riesgo de la organización se basa en sus funciones en el ecosistema de tratamiento de datos. |
| | | **Conocimiento y capacitación (GV.AT-P):** El personal de la organización y los | **GV.AT-P1:** Se informa y capacita a los empleados con respecto a sus funciones y responsabilidades. |

| | Función | Categoría | Subcategoría |
|---|---|---|---|
| | | terceros que participan en el tratamiento de datos reciben educación para tener conocimiento de la privacidad, y capacitación para cumplir con sus obligaciones y responsabilidades relacionadas con la privacidad, de acuerdo con las políticas, procesos, procedimientos y acuerdos conexos, y los valores de la privacidad de la organización. | **GV.AT-P2:** Los ejecutivos sénior conocen sus funciones y responsabilidades. |
| | | | **GV.AT-P3:** El personal de privacidad conoce sus funciones y responsabilidades. |
| | | | **GV.AT-P4:** Los terceros (por ejemplo, proveedores de servicios, clientes y socios) conocen sus funciones y responsabilidades. |
| | | **Vigilancia y revisión (GV.MT-P):** Se conocen las políticas, los procesos y los procedimientos para la revisión continua de la postura de privacidad de la organización, y en estos se basa la gestión de riesgos a la privacidad. | **GV.MT-P1:** El riesgo a la privacidad se evalúa de forma continua, al igual que los factores clave que comprenden el entorno empresarial de la organización (por ejemplo, la introducción de nuevas tecnologías), la gobernanza (por ejemplo, las obligaciones legales y la tolerancia al riesgo), el tratamiento de datos y los cambios en los sistemas, productos o servicios. |
| | | | **GV.MT-P2:** Se revisan los valores, las políticas y la capacitación en materia de privacidad, y se comunica toda actualización. |
| | | | **GV.MT-P3:** Se establecen e implementan políticas, procesos y procedimientos para evaluar el cumplimiento con los requisitos legales y las políticas de privacidad. |
| | | | **GV.MT-P4:** Se establecen e implementan políticas, procesos y procedimientos para comunicar el progreso en la gestión de riesgos a la privacidad. |
| | | | **GV.MT-P5:** Se establecen e implementan políticas, procesos y procedimientos para recibir, analizar y responder a las acciones problemáticas de datos reveladas a la organización provenientes de fuentes internas y externas (por ejemplo, descubrimientos internos, investigadores de privacidad, eventos profesionales). |
| | | | **GV.MT-P6:** Las políticas, los procesos y los procedimientos incorporan las lecciones aprendidas de las acciones problemáticas de datos. |

| | Función | Categoría | Subcategoría |
|---|---|---|---|
| | | | **GV.MT-P7:** Se establecen e implementan políticas, procesos y procedimientos para recibir, dar seguimiento y responder a quejas, inquietudes y preguntas de las personas sobre las prácticas de privacidad de la organización. |
| | **CONTROL-P (CT-P):** Desarrolla e implementa actividades adecuadas para que las organizaciones o las personas puedan aplicar los datos con detalle suficiente y gestionar los riesgos a la privacidad. | **Políticas, procesos y procedimientos del tratamiento de datos (CT.PO-P):** Se establecen y emplean políticas, procesos y procedimientos para gestionar el tratamiento de datos (por ejemplo, el propósito, el alcance, las funciones y las responsabilidades en el ecosistema de tratamiento de datos, y el compromiso de gestión) de acuerdo con la estrategia de riesgos de la organización para proteger la privacidad de las personas. | **CT.PO-P1:** Se establecen e implementan políticas, procesos y procedimientos para autorizar el tratamiento de datos (por ejemplo, decisiones organizativas, consentimiento de las personas), y la revocación y conservación de autorizaciones. |
| | | | **CT.PO-P2:** Se establecen e implementan políticas, procesos y procedimientos para habilitar la revisión, transferencia, uso compartido, revelación, modificación y eliminación de datos (por ejemplo, para mantener la calidad de los datos y gestionar la retención de estos). |
| | | | **CT.PO-P3:** Se establecen e implementan políticas, procesos y procedimientos para habilitar las preferencias y solicitudes de las personas referentes al tratamiento de datos. |
| | | | **CT.PO-P4:** Se alinea e implementa un ciclo de vida de datos para gestionar los datos con el ciclo de vida de desarrollo de un sistema para gestionar los sistemas. |
| | | **Gestión de tratamiento de datos (CT.DM-P):** Los datos se gestionan de acuerdo con la estrategia de riesgos de la organización para proteger la privacidad de las personas, aumentar la capacidad de gestión y habilitar la implementación de principios de privacidad (por ejemplo, la participación individual, la calidad de datos y la minimización de estos). | **CT.DM-P1:** Se puede acceder a los elementos de datos para su revisión. |
| | | | **CT.DM-P2:** Se puede acceder a los elementos de datos para su transmisión o revelación. |
| | | | **CT.DM-P3:** Se puede acceder a los elementos de datos para su modificación. |
| | | | **CT.DM-P4:** Se puede acceder a los elementos de datos para su eliminación. |
| | | | **CT.DM-P5:** Los datos se destruyen de acuerdo con la política. |
| | | | **CT.DM-P6:** Los datos se transmiten usando formatos estandarizados. |
| | | | **CT.DM-P7:** Se establecen e implementan mecanismos para transmitir permisos de tratamiento y valores de datos relacionados con los elementos de datos. |

| | Función | Categoría | Subcategoría |
|---|---|---|---|
| | | | **CT.DM-P8:** Los asientos de auditorías o registros se determinan, documentan, implementan y revisan de conformidad con la política, e incorporan el principio de minimización de datos. |
| | | | **CT.DM-P9:** Se prueban y evalúan las medidas técnicas implementadas para gestionar el tratamiento de datos. |
| | | | **CT.DM-P10:** Las preferencias de privacidad de las partes interesadas se incluyen en los objetivos del diseño algorítmico y los resultados se evalúan con respecto a estas preferencias. |
| | | **Tratamiento desasociado (CT.DP-P):** Las soluciones referentes al tratamiento de datos aumentan la capacidad para desasociar de acuerdo con la estrategia de riesgos de la organización para proteger la privacidad de las personas y habilitar la implementación de los principios de privacidad (por ejemplo, la minimización de datos). | **CT.DP-P1:** Los datos se procesan para limitar la capacidad de observación y vinculación (por ejemplo, acciones de datos que se efectúan en dispositivos locales, criptografía que conserva la privacidad). |
| | | | **CT.DP-P2:** Los datos se procesan para limitar la identificación de las personas (por ejemplo, técnicas de privacidad para eliminar la identificación, creación de tokens). |
| | | | **CT.DP-P3:** Los datos se procesan para limitar la formulación de inferencias sobre el comportamiento o las actividades de las personas (por ejemplo, tratamiento de datos no centralizado, arquitecturas distribuidas). |
| | | | **CT.DP-P4:** Las configuraciones de sistemas o de dispositivos permiten la recolección o la revelación selectiva de elementos de datos. |
| | | | **CT.DP-P5:** Los valores de atributo sustituyen las referencias de atributo. |
| | **COMUNICAR-P (CM-P):** Desarrolla e implementa actividades adecuadas por medio de las cuales las organizaciones y las personas pueden obtener un conocimiento confiable y | **Políticas, procesos y procedimientos de la comunicación (CM.PO-P):** Se establecen y emplean políticas, procesos y procedimientos para aumentar la transparencia de las prácticas del tratamiento de datos de la organización (por ejemplo, el propósito, el alcance, las funciones y las responsabilidades en el ecosistema de tratamiento de datos, y el compromiso de la gestión), y los riesgos a la privacidad conexos. | **CM.PO-P1:** Se establecen e implementan políticas, procesos y procedimientos de transparencia para comunicar los propósitos, las prácticas y los riesgos a la privacidad conexos relativos al tratamiento de datos. |
| | | | **CM.PO-P2:** Se establecen funciones y responsabilidades (por ejemplo, las relaciones públicas) para comunicar los propósitos, las prácticas y los riesgos a la privacidad conexos relativos al tratamiento de datos. |

| | Función | Categoría | Subcategoría |
|---|---|---|---|
| | participar en un diálogo acerca de la manera en que se procesan los datos y los riesgos a la privacidad conexos. | **Conocimiento del tratamiento de datos (CM.AW-P):** Las personas y las organizaciones cuentan con conocimientos confiables sobre las prácticas del tratamiento de datos y los riesgos a la privacidad conexos, y se establecen y emplean mecanismos eficaces para aumentar la previsibilidad de acuerdo con la estrategia de riesgos de la organización para proteger la privacidad de las personas. | **CM.AW-P1:** Se establecen e implementan mecanismos (por ejemplo, avisos, informes internos o públicos) para comunicar los propósitos, las prácticas y los riesgos a la privacidad conexos relativos al tratamiento de datos, así como las opciones para habilitar las preferencias y solicitudes de las personas referentes al tratamiento de datos. |
| | | | **CM.AW-P2:** Se establecen e implementan mecanismos para recibir retroalimentación de las personas (por ejemplo, encuestas o grupos de discusión) acerca del tratamiento de datos y los riesgos a la privacidad conexos. |
| | | | **CM.AW-P3:** El diseño del sistema, producto o servicio habilita la visibilidad del tratamiento de datos. |
| | | | **CM.AW-P4:** Se conservan registros de revelación y uso compartido de datos, a los que se puede acceder para su revisión, transmisión o revelación. |
| | | | **CM.AW-P5:** Las correcciones o eliminaciones de datos pueden comunicarse a las personas o las organizaciones (por ejemplo, fuentes de datos) en el ecosistema de tratamiento de datos. |
| | | | **CM.AW-P6:** Se conservan la proveniencia y el linaje de los datos a los que se puede acceder para su revisión, transmisión o revelación. |
| | | | **CM.AW-P7:** Se notifica a las personas y organizaciones afectadas de una vulneración de la privacidad o de un evento de privacidad. |
| | | | **CM.AW-P8:** Para abordar los efectos de las acciones problemáticas de datos, se proporciona a las personas mecanismos de mitigación (por ejemplo, vigilancia de crédito, retiro de consentimiento, modificación o eliminación de datos). |
| | **PROTEGER-P (PR-P):** Establece e implementa salvaguardias adecuadas para | **Políticas, procesos y procedimientos de la protección de datos (PR.PO-P):** Se establecen y emplean políticas (por ejemplo, el propósito, el alcance, las funciones y las responsabilidades en el ecosistema de tratamiento de datos, y el compromiso de gestión), procesos y | **PR.PO-P1:** Se crea y mantiene una configuración básica de la tecnología de la información que incorpora principios de seguridad (por ejemplo, el concepto de funcionalidad mínima). |
| | | | **PR.PO-P2:** Se establecen e implementan los procesos de control de cambios de configuración. |
| | | | **PR.PO-P3:** Se hacen, conservan y prueban copias de seguridad de la información. |

| Función | Categoría | Subcategoría |
|---|---|---|
| el tratamiento de datos. | procedimientos de seguridad y privacidad para gestionar la protección de datos. | **PR.PO-P4:** Se cumple con las políticas y los reglamentos relativos al entorno operativo físico de los recursos organizativos. |
| | | **PR.PO-P5:** Se mejoran los procesos de protección. |
| | | **PR.PO-P6:** Se comparte la efectividad de las tecnologías de protección. |
| | | **PR.PO-P7:** Se establecen, implementan y gestionan los planes de respuesta (de respuesta a incidentes y de continuidad de la empresa) y los planes de recuperación (de recuperación de incidentes y de recuperación de desastres). |
| | | **PR.PO-P8:** Se prueban los planes de respuesta y de recuperación. |
| | | **PR.PO-P9:** Se incluyen los procedimientos de privacidad en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, verificación de personal). |
| | | **PR.PO-P10:** Se elabora e implementa un plan de gestión de vulnerabilidades. |
| | **Gestión y autenticación de la identidad y control del acceso a esta (PR.AC-P):** El acceso a los datos y dispositivos se limita a las personas, los procesos y los dispositivos autorizados, y se gestiona de acuerdo con el riesgo evaluado que representa el acceso no autorizado. | **PR.AC-P1:** Se emiten, gestionan, verifican, revocan y auditan identidades y credenciales para las personas, los procesos y los dispositivos autorizados. |
| | | **PR.AC-P2:** Se gestiona el acceso físico a los datos y los dispositivos. |
| | | **PR.AC-P3:** Se gestiona el acceso remoto. |
| | | **PR.AC-P4:** Se gestionan los permisos y las autorizaciones para lograr acceso, y se incorporan los principios de privilegios mínimos y separación de funciones. |
| | | **PR.AC-P5:** Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red). |
| | | **PR.AC-P6:** Las personas y los dispositivos se comprueban, se vinculan con las credenciales y se autentican de acuerdo con el riesgo de la transacción (por ejemplo, los riesgos a la privacidad y la seguridad de las personas, y otros riesgos de la organización). |
| | **Seguridad de datos (PR.DS-P):** Los datos se gestionan de acuerdo con | **PR.DS-P1:** Se protegen los datos en reposo. |
| | | **PR.DS-P2:** Se protegen los datos en tránsito. |

| Función | Categoría | Subcategoría |
|---|---|---|
| | la estrategia de riesgos de la organización para proteger la privacidad de las personas y mantener la confidencialidad, integridad y disponibilidad de los datos. | **PR.DS-P3:** Los sistemas, productos o servicios y datos conexos se gestionan formalmente durante la eliminación, las transferencias y la disposición. |
| | | **PR.DS-P4:** Se mantiene una capacidad adecuada para garantizar la disponibilidad. |
| | | **PR.DS-P5:** Se implementan protecciones contra las pérdidas de datos. |
| | | **PR.DS-P6:** Se utilizan mecanismos de comprobación de integridad para verificar la integridad del software, el firmware y la información. |
| | | **PR.DS-P7:** Los entornos de desarrollo y de pruebas son independientes del entorno de producción. |
| | | **PR.DS-P8:** Se utilizan mecanismos de comprobación de integridad para verificar la integridad del hardware. |
| | **Mantenimiento (PR.MA-P):** El mantenimiento del sistema y sus reparaciones se efectúan de acuerdo con las políticas, los procesos y los procedimientos. | **PR.MA-P1:** El mantenimiento y la reparación de los recursos organizativos se hacen y registran con herramientas aprobadas y controladas. |
| | | **PR.MA-P2:** Se aprueba, registra y efectúa el mantenimiento remoto de los recursos organizativos de manera que se evite el acceso no autorizado. |
| | **Tecnología de protección (PR.PT-P):** Las soluciones de seguridad técnica se gestionan para garantizar la seguridad y la resiliencia de los sistemas, productos o servicios y los datos conexos, conforme a las políticas, procesos, procedimientos y acuerdos correspondientes. | **PR.PT-P1:** Los medios extraíbles están protegidos y su uso se restringe de acuerdo con la política. |
| | | **PR.PT-P2:** El principio de funcionalidad mínima se incorpora configurando los sistemas para proporcionar solo las capacidades esenciales. |
| | | **PR.PT-P3:** Se protegen las comunicaciones y las redes de control. |
| | | **PR.PT-P4:** Se implementan mecanismos (por ejemplo, a prueba de errores, de equilibrio de carga, de intercambio directo) para cumplir con los requisitos de resiliencia en situaciones normales y adversas. |

# Apéndice B: Glosario

En este apéndice, se definen términos seleccionados que se usan a los fines de esta publicación.

| | |
|---|---|
| **acción de datos** (adaptado del Informe interinstitucional o interno 8062 del NIST [5]) | Operación del ciclo de vida de datos de un sistema, producto o servicio que incluye, entre otros, la recolección, retención, registro, generación, transformación, uso, revelación, uso compartido, transmisión y eliminación. |
| **acción de datos problemática** (adaptado del Informe interinstitucional o interno 8062 del NIST [5]) | Acción de datos que podría causar un efecto adverso para las personas. |
| **capacidad de gestión** (adaptado del Informe interinstitucional o interno 8062 del NIST [5]) | Suministro de la capacidad para la administración detallada de datos, que incluye su modificación, eliminación y revelación selectiva. |
| **capacidad para desasociar** (adaptado del Informe interinstitucional o interno 8062 del NIST [5]) | Habilitación del tratamiento de datos o de eventos sin que se asocien a personas o dispositivos más allá de los requisitos operativos del sistema. |
| **Categoría** | Subdivisión de una Función en grupos de resultados de privacidad estrechamente vinculados con las necesidades programáticas y actividades particulares. |
| **Comunicar-P (Función)** | Desarrolla e implementa actividades adecuadas por medio de las cuales las organizaciones y las personas pueden obtener un conocimiento confiable y participar en un diálogo acerca de la manera en que se procesan los datos y los riesgos a la privacidad conexos. |
| **confidencialidad** (título 44 del Código de EE. UU. [13]) | Conservación de las restricciones autorizadas del acceso a información y de su revelación, que incluye medios para proteger la privacidad personal y la información de propiedad exclusiva. |
| **Controlar-P (Función)** | Desarrolla e implementa actividades adecuadas para que las organizaciones o las personas puedan aplicar los datos con detalle suficiente y gestionar los riesgos a la privacidad. |
| **controles de privacidad** (adaptado de la Publicación especial 800-37 del NIST [7]) | Salvaguardias administrativas, técnicas y físicas que se emplean dentro de una organización para satisfacer los requisitos de privacidad. |
| **datos** | Representación de la información en formato digital y no digital. |

| | |
|---|---|
| **disponibilidad** (título 44 del Código de EE. UU. [13]) | Garantía de acceso oportuno y confiable a la información y de su uso. |
| **ecosistema de tratamiento de datos** | Relaciones complejas e interconectadas entre las entidades que participan en la creación o la implementación de sistemas, productos o servicios, o cualquier componente de estos que procese datos. |
| **elemento de datos** | Parte más pequeña de datos, con nombre, que transmite información pertinente. |
| **evaluación de riesgos a la privacidad** | Subproceso de la gestión de riesgos a la privacidad para identificar y evaluar riesgos específicos a la privacidad. |
| **evento de privacidad** | Ocurrencia real o posible de acciones problemáticas de datos. |
| **Función** | Componente del Núcleo que proporciona el nivel más alto de estructura para organizar las actividades de privacidad básicas en Categorías y Subcategorías. |
| **gestión de riesgos** | Proceso de identificación, evaluación y respuesta a riesgos. |
| **gestión de riesgos a la privacidad** | Conjunto de procesos en toda la organización para identificar, evaluar y responder a los riesgos a la privacidad. |
| **Gobernar-P (Función)** | Define e implementa la estructura de gobernanza organizativa para facilitar el conocimiento continuo de las prioridades de gestión de riesgos de la organización basadas en el riesgo a la privacidad. |
| **Identificar-P (Función)** | Define el conocimiento organizativo para gestionar el riesgo a la privacidad de las personas que surge del tratamiento de datos. |
| **incidente de ciberseguridad** (Marco para la mejora de la seguridad cibernética en infraestructuras críticas [1]) | Evento de ciberseguridad del que se determinó que tiene un impacto en la organización, lo que genera la necesidad de respuesta y recuperación. |
| (Memorando 17-12 de la OMB [9]) | Suceso que (1) pone en peligro real o inminente, sin autoridad legal, la integridad, la confidencialidad o la disponibilidad de información o de un sistema de información; o (2) infringe o amenaza de manera inminente con infringir la ley, las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptable. |
| **integridad** (título 44 del Código de EE. UU. [13]) | Protección contra la modificación o destrucción indebidas de la información; incluye garantía de la autenticidad de la información sin rechazarla. |

| | |
|---|---|
| **linaje** | Historial del tratamiento de un elemento de datos que puede incluir flujos de datos punto a punto y las acciones de datos efectuadas en el elemento de datos. |
| **metadatos** (adaptado de la Publicación especial 800-53 del NIST [10]) | Información que describe las características de los datos. Esto puede incluir, por ejemplo, los metadatos estructurales que describen las estructuras de los datos (es decir, el formato, la sintaxis y la semántica de los datos) y los metadatos descriptivos que describen el contenido de los datos. |
| **Nivel de implementación** | Proporciona un punto de referencia sobre la manera en que una organización percibe los riesgos a la privacidad y si cuenta con suficientes procesos y recursos establecidos para gestionar esos riesgos. |
| **Núcleo** | Conjunto de actividades y resultados relativos a la protección de la privacidad. El Núcleo del Marco consta de tres elementos: Funciones, Categorías y Subcategorías. |
| **Perfil** | Selección de Funciones, Categorías y Subcategorías específicas del Núcleo que una organización ha priorizado para ayudar a gestionar el riesgo a la privacidad. |
| **persona** | Una sola persona o un grupo de personas, incluso en un nivel social. |
| **previsibilidad** (adaptado del Informe interinstitucional o interno 8062 del NIST [5]) | Habilitación de suposiciones confiables de personas, propietarios y operadores acerca de datos y de su tratamiento por medio de un sistema, producto o servicio. |
| **Proteger-P (Función)** | Establece e implementa salvaguardias adecuadas para el tratamiento de datos. |
| **proveniencia** (adaptado del Informe interinstitucional o interno 8112 del NIST [11]) | Metadatos concernientes al origen o la fuente de datos especificados. |
| **referencia de atributo** (Publicación especial 800-63-3 del NIST [8]) | Declaración que confirma una propiedad de un suscriptor sin contener necesariamente información identificativa, independiente del formato. Por ejemplo, para el atributo “fecha de nacimiento”, una referencia podría ser “mayor de 18 años” o “nació en diciembre”. |
| **requisito de privacidad** | Especificación para que la funcionalidad de un sistema, producto o servicio logre los resultados de privacidad deseados de las partes interesadas. |
| **riesgo** (Publicación especial 800-30 del NIST [12]) | Medida en que una entidad es amenazada por una posible circunstancia o evento. Es normalmente una función de (1) los efectos adversos que tendría la circunstancia o el evento si llegaran a ocurrir; y (2) la probabilidad de que ocurran. |

| | |
|---|---|
| **riesgos a la privacidad** | Probabilidad de que las personas experimenten problemas que surgen del tratamiento de datos, y el impacto de estos en caso de que ocurran. |
| **Subcategoría** | Divisiones adicionales de una Categoría en resultados específicos de actividades técnicas o de gestión. |
| **tolerancia al riesgo** (Publicación especial 800-39 del NIST [6]) | Nivel de riesgo o grado de incertidumbre que las organizaciones consideran aceptable. |
| **tratamiento** | Véase *tratamiento de datos*. |
| **tratamiento de datos** (adaptado del Informe interinstitucional o interno 8062 del NIST [5]) | Conjunto colectivo de acciones de datos (es decir, el ciclo de vida completo de datos que incluye, entre otros, la recolección, retención, registro, generación, transformación, uso, revelación, uso compartido, transmisión y eliminación). |
| **valor de atributo** (Publicación especial 800-63-3 del NIST [8]) | Declaración completa que confirma una propiedad de un suscriptor, independiente del formato. Por ejemplo, para el atributo de “fecha de nacimiento”, un valor podría ser “1/12/1980” o “1 de diciembre de 1980”. |
| **vulneración de la privacidad** (adaptado del Memorando M-17-12 de la OMB [9]) | Pérdida de control, puesta en peligro, revelación no autorizada, adquisición no autorizada o cualquier suceso similar en el que (1) una persona que no sea el usuario autorizado accede o es posible que acceda a datos; o (2) un usuario autorizado accede a datos con un fin distinto al que se autoriza. |

# Apéndice C: Siglas

En este apéndice, se definen las siglas seleccionadas que se usan en esta publicación.

| | |
|---|---|
| IEC | International Electrotechnical Commission [Comisión Electrotécnica Internacional] |
| IR | Interagency or Internal Report [Informe interinstitucional o interno] |
| ISO | International Organization for Standardization [Organización Internacional de Normalización] |
| NIST | National Institute of Standards and Technology [Instituto Nacional de Normas y Tecnología] |
| OASIS | Organization for the Advancement of Structured Information Standards [Organización para la Mejora de las Normas de Información Estructuradas] |
| OECD | Organisation for Economic Co-operation and Development [Organización para la Cooperación y el Desarrollo Económicos] |
| OMB | Office of Management and Budget [Oficina de Administración y Presupuesto] |
| PMRM | Privacy Management Reference Model and Methodology [Modelo de referencia y metodología para la gestión de la privacidad] |
| PRAM | Privacy Risk Assessment Methodology [Metodología para evaluación de los riesgos a la privacidad] |
| RFC | Request for Comment [solicitud de comentarios] |
| RFI | Request for Information [solicitud de información, SDI] |
| SDLC | System Development Life Cycle [ciclo de vida de desarrollo de un sistema] |
| SP | Special Publication [Publicación especial] |
| TI | tecnología de la información |

# Apéndice D: Prácticas de gestión de riesgos a la privacidad

La Sección 1.2 presenta una serie de consideraciones en torno a la gestión de riesgos a la privacidad que comprende la relación entre la ciberseguridad y el riesgo a la privacidad, y la función que desempeña la evaluación de riesgos a la privacidad. En este apéndice, se consideran algunas de las prácticas clave que contribuyen a una gestión exitosa de los riesgos a la privacidad, entre otras: organización de los recursos preparatorios, determinación de las capacidades de privacidad, definición de los requisitos de privacidad, realización de evaluaciones de los riesgos a la privacidad, establecimiento de la trazabilidad de los requisitos de privacidad y vigilancia en busca de riesgos a la privacidad cambiantes. Se incluyen referencias a las Categorías y Subcategorías para facilitar el uso del Núcleo en la aplicación de estas prácticas; estas referencias aparecen entre paréntesis.

## Organización de recursos preparatorios

Los recursos adecuados facilitan la toma de decisiones informadas sobre los riesgos a la privacidad en todos los niveles de una organización. En términos prácticos, la responsabilidad de la elaboración de los diversos recursos puede estar asignada a diferentes componentes de una organización. Por lo tanto, es posible que un componente de una organización que dependa de ciertos recursos descubra que los recursos no existen o que no pueden abordar suficientemente la privacidad. En estas circunstancias, el componente dependiente puede considerar el propósito del recurso y buscar la información a través de otras fuentes, o bien tomar la mejor decisión posible con la información disponible. En resumen, los recursos buenos son útiles, pero ninguna deficiencia deberá impedir que los componentes de una organización tomen las mejores decisiones sobre riesgos según sus capacidades.

Si bien los siguientes recursos no son exhaustivos, sientan la base para una mejor toma de decisiones.

- **Asignaciones de las funciones relacionadas con la gestión de riesgos** (GV.PO-P3, GV.PO-P4)

  Establecer y habilitar el conocimiento en la organización acerca de quiénes son los encargados de rendir cuentas y de la gestión de riesgos a la privacidad, así como otras tareas de la gestión de riesgos, contribuye a optimizar la coordinación y la responsabilidad de la toma de decisiones. Además, una amplia gama de perspectivas puede mejorar el proceso de identificación, evaluación y respuesta a los riesgos a la privacidad. Un equipo diverso y multidisciplinario ayuda a definir una variedad más completa de riesgos a la privacidad de las personas y a seleccionar un conjunto más amplio de mitigaciones. La determinación de las funciones que se deben incluir en los análisis de la gestión de riesgos depende del contexto y la composición de la organización, aunque la colaboración entre los programas de privacidad y ciberseguridad de una organización será importante. Si se asignan varias funciones a una persona, deberá considerarse la gestión de posibles conflictos de intereses.

- **Estrategia de gestión de riesgos empresariales** (GV.RM-P)

  La estrategia de gestión de riesgos empresariales de una organización ayuda a alinear la misión y los valores organizativos con su tolerancia al riesgo, suposiciones, restricciones y prioridades. Es probable que las limitaciones de recursos para lograr los objetivos empresariales o de la misión y para gestionar una cartera amplia de riesgos requieran compensaciones. Permitir que el personal que participa en el proceso de gestión de riesgos a la privacidad conozca mejor la tolerancia al riesgo de una organización debe ayudar a orientar las decisiones sobre la manera de asignar los recursos y a mejorar las decisiones en torno a la respuesta al riesgo.

- **Partes interesadas clave** (GV.PO-P4, ID.DE-P)

  Las partes interesadas en la privacidad son aquellas que prestan atención a los resultados de la privacidad del sistema, producto o servicio, o que se preocupan por estos. Por ejemplo, es probable que los intereses legales se centren en que el sistema, producto o servicio funcione de una manera que haga que la organización no cumpla con las leyes o los reglamentos sobre privacidad o con sus acuerdos comerciales. A los propietarios de negocios que desean maximizar su uso les podría inquietar la pérdida de confianza en el sistema, producto o servicio como consecuencia de una privacidad deficiente. Las personas cuyos datos se procesan o que interactúan con el sistema, producto o servicio estarán interesadas en no experimentar problemas ni consecuencias adversas. Entender a las partes interesadas y los tipos de resultados de privacidad que les atraen facilitará el diseño de sistemas, productos o servicios que atiendan debidamente sus necesidades.

- **Requisitos de privacidad a nivel organizativo** (GV.PO-P)

  Los requisitos de privacidad a nivel organizativo se emplean para expresar las obligaciones legales, los valores de privacidad y las políticas que una organización prevé cumplir. Conocer estos requisitos es fundamental para garantizar que el diseño de sistemas, productos o servicios cumpla con sus obligaciones. Los requisitos de privacidad a nivel organizativo se pueden derivar de diversas fuentes, entre otras:

  - el entorno legal (por ejemplo, leyes, reglamentos, contratos);
  - las políticas organizativas o los valores culturales;
  - las normas pertinentes; y
  - los principios de privacidad.

- **Artefactos de diseño del sistema, producto o servicio** (ID.BE-P3)

  Los artefactos de diseño pueden adoptar muchas formas, como arquitecturas de diseño de sistemas o diagramas de flujo de datos, y ayudan a una organización a determinar la manera en que funcionarán sus sistemas, productos y servicios. Por lo tanto, contribuyen a que los programas de privacidad sepan cómo necesitan funcionar los sistemas, productos y servicios para que los controles o las medidas que mitigan los riesgos a la privacidad se seleccionen e implementen de forma que mantengan la funcionalidad y protejan la privacidad al mismo tiempo.

- **Mapas de datos** (ID.IM-P)

  Los mapas de datos ilustran el tratamiento de datos y las interacciones de las personas con los sistemas, productos y servicios. Un mapa de datos muestra el entorno del tratamiento de datos e incluye los componentes mediante los cuales se procesan los datos o con los que interactúan las personas, los propietarios u operadores de los componentes, las acciones de datos discretos y los elementos de datos específicos que se procesan. Los mapas de datos se pueden ilustrar de diferentes maneras y el nivel de detalle varía en función de las necesidades de una organización. Un mapa de datos puede superponerse a los artefactos de diseño existentes del sistema, producto o servicio por conveniencia o facilidad de comunicación entre los componentes de la organización. Como se explica a continuación, un mapa de datos es un artefacto importante en la evaluación de los riesgos a la privacidad.

## Determinación de las capacidades de privacidad

Las capacidades de privacidad se pueden usar para describir la propiedad o característica del sistema, producto o servicio que logra el resultado de privacidad deseado (por ejemplo, "el servicio facilita la minimización de datos"). La confidencialidad, integridad y disponibilidad de los objetivos de seguridad, junto con los requisitos de seguridad, sirven de base a las capacidades de seguridad de un sistema, producto o servicio. Como se establece en la **Tabla** 3, un conjunto adicional de objetivos de ingeniería de la privacidad es útil para determinar las capacidades de privacidad. Asimismo, una organización podría utilizar los objetivos de ingeniería de la privacidad como un recurso de priorización de alto nivel. La presencia de sistemas, productos o servicios con poca previsibilidad, capacidad de gestión o capacidad para desasociar puede indicar un mayor riesgo a la privacidad y, por lo tanto, merece una evaluación más completa de los riesgos a la privacidad.

Al determinar las capacidades de privacidad, una organización podría considerar cuáles de sus objetivos de seguridad y de ingeniería de la privacidad son más importantes con respecto a sus necesidades empresariales o de la misión, la tolerancia al riesgo y los requisitos de privacidad a nivel organizativo (véase arriba "Organización de recursos preparatorios"). Es posible que no todos los objetivos sean igualmente importantes, o que se necesiten compensaciones entre ellos. Si bien las capacidades de privacidad sirven de base a la evaluación de riesgos a la privacidad y facilitan las decisiones acerca de la priorización de los riesgos, esas capacidades también pueden basarse en la evaluación de riesgos y modificarse para respaldar la gestión de riesgos a la privacidad específicos o para abordar cambios al entorno, así como cambios en el diseño del sistema, producto o servicio.

**Tabla 3: Objetivos de ingeniería de la privacidad y de seguridad**[18]

| | **Objetivo** | **Definición** | **Funciones principales conexas del Núcleo del Marco de privacidad** |
|---|---|---|---|
| **Objetivos de ingeniería de la privacidad** | Previsibilidad | Habilitación de suposiciones confiables de personas, propietarios y operadores acerca de datos y de su tratamiento por medio de un sistema | Identificar-P, Gobernar-P, Controlar-P, Comunicar-P, Proteger-P |
| | Capacidad de gestión | Suministro de la capacidad para la administración detallada de datos, que incluye su recolección, modificación, eliminación y revelación selectiva | Identificar-P, Gobernar-P, Controlar-P |
| | Capacidad para desasociar | Habilitación del tratamiento de datos o de eventos sin que se asocien a personas o dispositivos más allá de los requisitos operativos del sistema | Identificar-P, Gobernar-P, Controlar-P |

[18] Los objetivos de ingeniería de la privacidad se han adaptado del Informe interinstitucional o interno 8062 del NIST [5]. Los objetivos de seguridad provienen de la Publicación especial 800-37 del NIST, rev. 2 [7].

| | | | |
|---|---|---|---|
| **Objetivos de seguridad** | Confidencialidad | Conservación de las restricciones autorizadas del acceso a información y de su revelación que incluye medios para proteger la privacidad personal e información de propiedad exclusiva | Identificar-P, Gobernar-P, Proteger-P |
| | Integridad | Protección contra la modificación o destrucción indebidas de la información; incluye garantía de la autenticidad de la información sin rechazarla | Identificar-P, Gobernar-P, Proteger-P |
| | Disponibilidad | Garantía de acceso oportuno y confiable a la información y de su uso | Identificar-P, Gobernar-P, Proteger-P |

## Definición de los requisitos de privacidad

Los requisitos de privacidad especifican la forma en que un sistema, producto o servicio necesita funcionar para lograr los resultados de privacidad que las partes interesadas desean (por ejemplo, "la aplicación está configurada para permitir que los usuarios seleccionen elementos de datos específicos"). Para definir los requisitos de privacidad, se consideran los requisitos de privacidad a nivel organizativo (véase arriba "Organización de recursos preparatorios") y los resultados de una evaluación de los riesgos a la privacidad. Este proceso ayuda a una organización a responder a dos preguntas: 1) ¿Qué *puede* hacer un sistema, producto o servicio con el tratamiento de datos y las interacciones con las personas? 2) ¿Qué *debería* hacer? Luego, la organización puede asignar recursos para diseñar un sistema, producto o servicio de manera que cumpla con los requisitos definidos. En última instancia, definir los requisitos de privacidad puede influir en el desarrollo de sistemas, productos y servicios que sean más conscientes de la privacidad de las personas y que se basen en decisiones informadas sobre riesgos.

## Realización de evaluaciones de los riesgos a la privacidad

Llevar a cabo una evaluación de riesgos a la privacidad ayuda a una organización a identificar los riesgos a la privacidad generados por el sistema, producto o servicio, y a priorizarlos para poder tomar decisiones informadas sobre la manera de responder a esos riesgos (ID.RA-P, GV.RM-P). Las metodologías para hacer las evaluaciones de riesgos a la privacidad pueden variar; sin embargo, las organizaciones deberán considerar las siguientes características:[19]

- **Modelo de riesgo** (ID.RA-P, GV.MT-P1)

  Los modelos de riesgo definen los factores de riesgo que se deben evaluar y las relaciones entre estos.[20] Si una organización no emplea un modelo de riesgo predefinido, debe definir claramente los factores de riesgo

  **Factores de riesgos a la privacidad:**
  acción problemática de datos | probabilidad | impacto

[19] El NIST elaboró una *Privacy Risk Assessment Methodology* [Metodología para evaluación de los riesgos a la privacidad] (PRAM, por sus siglas en inglés) que ayuda a las organizaciones a identificar, evaluar y responder a los riesgos a la privacidad. Consiste en un conjunto de hojas de trabajo disponibles en [3].

[20] Véase la Publicación especial 800-30 del NIST, rev. 1, p. 8, *Guide for Conducting Risk Assessments* [Guía para efectuar evaluaciones de riesgos] [12].

que evaluará y las relaciones entre estos factores. Aunque la ciberseguridad aplica un modelo de riesgo ampliamente utilizado que se basa en los factores de riesgos de amenazas, vulnerabilidades, probabilidad e impacto, no existe un modelo de riesgos a la privacidad con aceptación común. El NIST elaboró un modelo de riesgos a la privacidad para calcular el riesgo con base en la probabilidad de una acción problemática de datos multiplicada por el impacto de una acción problemática de datos. Cada uno de los tres factores de riesgos se explica a continuación.

- Una acción problemática de datos es toda acción que un sistema ejecuta para procesar datos que podrían ocasionar un problema para las personas. Las organizaciones toman en cuenta el tipo de problemas que son importantes para las personas. Los problemas pueden adoptar cualquier forma y considerar las experiencias de las personas.[21]
- La probabilidad se define como un análisis contextual de que una acción de datos podría causar un problema a un conjunto representativo de personas. El contexto puede incluir factores organizativos (por ejemplo, ubicación geográfica, percepción pública acerca de las organizaciones participantes con respecto a la privacidad), factores del sistema (por ejemplo, la naturaleza y los antecedentes de las interacciones de las personas con el sistema, la visibilidad del tratamiento de datos para las personas y terceros) o factores individuales (por ejemplo, datos demográficos de las personas, sus intereses o percepciones con respecto a la privacidad, confidencialidad de los datos).[22] Un mapa de datos es de utilidad para este análisis contextual (véase “Organización de recursos preparatorios”).
- El impacto es un análisis de los costos si llegara a ocurrir el problema. Como se indica en la Sección 1.2, las organizaciones no experimentan estos problemas directamente. Además, las experiencias de las personas podrían ser subjetivas. Por lo tanto, puede ser difícil evaluar con precisión el impacto. Las organizaciones deben considerar los mejores medios para incorporar el impacto en las personas a fin de dar prioridad y responder adecuadamente a los riesgos a la privacidad.[23]

- **Método de evaluación**

  El método de evaluación es el mecanismo mediante el cual se priorizan los riesgos identificados. Los métodos de evaluación se pueden clasificar como cuantitativos, semicuantitativos o cualitativos.[24] [25]

- **Priorización de riesgos** (ID.RA-P4)

[21] Como parte de la PRAM, el NIST creó un catálogo ilustrativo de acciones problemáticas de datos y de problemas que se deben considerar [3]. Es posible que otras organizaciones hayan establecido conjuntos de problemas adicionales, o que se refieran a estos como consecuencias adversas o daños.

[22] Véase la PRAM del NIST para obtener más información sobre factores contextuales. Ídem en la Hoja de trabajo 2.

[23] La PRAM del NIST usa los costos organizativos (por ejemplo, los costos por incumplimiento, los costos comerciales directos y los costos relativos a la reputación y a la cultura interna) como factores determinantes para considerar la manera de evaluar el impacto individual. Ídem en la Hoja de trabajo 3, pestaña Impacto.

[24] Véase la Publicación especial 800-30 del NIST, rev. 1, p. 14: *Guide for Conducting Risk Assessments* [Guía para efectuar evaluaciones de riesgos] [12]

[25] La PRAM del NIST aplica un método semicuantitativo que se basa en una escala del uno al diez.

Dados los límites aplicables de los recursos de una organización, las organizaciones priorizan los riesgos para facilitar la comunicación acerca de la manera de responder.[26]

- **Respuesta a los riesgos** (ID.RA-P5)

  Como se describe en la Sección 1.2.2, los procedimientos de la respuesta comprenden mitigar, transferir o compartir, evitar o aceptar.[27]

## Establecimiento de la trazabilidad de los requisitos de privacidad

Una vez que una organización haya determinado los riesgos que debe mitigar, podrá afinar los requisitos de privacidad y luego seleccionar e implementar los controles (es decir, las salvaguardias técnicas, físicas o de políticas) para satisfacer estos requisitos.[28] Una organización puede usar una variedad de fuentes para seleccionar los controles, como la Publicación especial 800-53 del NIST, *Security and Privacy Controls for Information Systems and Organizations.* [Controles de seguridad y privacidad para sistemas de información y organizaciones].[29] Después de la implementación, la organización evalúa iterativamente la efectividad de los controles para satisfacer los requisitos de privacidad y gestionar los riesgos a esta. De esta manera, una organización establece la trazabilidad entre los controles y los requisitos de privacidad, y demuestra la rendición de cuentas entre sus sistemas, productos y servicios y sus metas organizativas de privacidad.

## Vigilancia de los cambios

La gestión de riesgos a la privacidad no es un proceso estático. Una organización vigila la manera en que los cambios en su entorno empresarial (incluidas las nuevas leyes y reglamentos, así como las tecnologías emergentes) y los cambios correspondientes en sus sistemas, productos y servicios podrían afectar los riesgos a la privacidad, y aplica de forma iterativa las prácticas que aparecen en este apéndice para hacer los ajustes correspondientes. (GV.MT-P1)

---

[26] La PRAM del NIST proporciona varias representaciones de la priorización, incluido un mapa térmico. Véase [3] la Hoja de trabajo 3.

[27] La PRAM del NIST ofrece un proceso para responder a los riesgos a la privacidad priorizados. Ídem en la Hoja de trabajo 4.

[28] Véase la Publicación especial 800-37 del NIST, rev. 2 [7].

[29] Véase la Publicación especial actualizada 800-53 del NIST [10].

# Apéndice E: Definiciones de los Niveles de implementación

Los cuatro Niveles que se resumen a continuación se definen con cuatro elementos:

## Nivel 1: Parcial

- **Proceso de gestión de riesgos a la privacidad.** Las prácticas de la gestión de riesgos a la privacidad de la organización no se han formalizado, y el riesgo se gestiona según el caso, a veces, de manera reactiva. Es posible que la priorización de las actividades de privacidad no se base directamente en las prioridades de gestión de riesgos, las evaluaciones de riesgos a la privacidad ni los objetivos empresariales o de la misión de la organización.
- **Programa integrado de gestión de riesgos a la privacidad.** Existe un conocimiento limitado de los riesgos a la privacidad a nivel organizativo. La organización implementa la gestión de riesgos a la privacidad de forma irregular y caso por caso debido a experiencia o información diversa obtenida de fuentes externas. Es posible que la organización no cuente con procesos que permitan el intercambio interno de información sobre el tratamiento de datos y los riesgos a la privacidad resultantes.
- **Relaciones en el ecosistema de tratamiento de datos.** Existe un conocimiento limitado de las funciones de una organización en el ecosistema más amplio con respecto a otras entidades (por ejemplo, compradores, proveedores, proveedores de servicios, socios comerciales, socios). La organización no cuenta con procesos para identificar la manera en que los riesgos a la privacidad pueden proliferar en todo el ecosistema, ni para comunicar los riesgos o requisitos de privacidad a otras entidades del ecosistema.
- **Personal.** Algunos empleados pueden tener un conocimiento limitado de los riesgos a la privacidad o de los procesos de gestión de riesgos a la privacidad; sin embargo, no tienen responsabilidades de privacidad específicas. La capacitación en materia de privacidad se ofrece según se necesita y el contenido no refleja las mejores prácticas actuales.

## Nivel 2: Basado en riesgos

- **Proceso de gestión de riesgos a la privacidad.** La administración aprueba las prácticas de gestión de riesgos, pero es posible que no se establezcan como política en toda la organización. La priorización de las actividades de privacidad se basa directamente en las prioridades de gestión de riesgos, las evaluaciones de riesgos a la privacidad o los objetivos empresariales o de la misión de la organización.
- **Programa integrado de gestión de riesgos a la privacidad.** Existe un conocimiento de los riesgos a la privacidad a nivel organizativo, pero no se ha establecido un método en toda la organización para gestionar los riesgos a la privacidad. La información sobre el tratamiento de datos y los riesgos a la privacidad resultantes se intercambia dentro de la organización de manera informal. La consideración de la privacidad en los objetivos y programas organizativos puede darse en algunos de los niveles de la organización, pero no en todos. Se hace la evaluación de riesgos a la privacidad, pero no suele repetirse.
- **Relaciones en el ecosistema de tratamiento de datos.** Existe cierto conocimiento de las funciones de una organización en el ecosistema más amplio con respecto a otras entidades (por ejemplo, compradores, proveedores, proveedores de servicios, socios comerciales, socios). La organización es consciente de los riesgos al ecosistema de privacidad asociados con los

productos y servicios que proporciona y utiliza, pero no actúa de manera uniforme o formal ante esos riesgos.

- **Personal.** Hay empleados que tienen responsabilidades de privacidad específicas, pero es posible que también tengan responsabilidades que no competen a la privacidad. La capacitación en materia de privacidad se ofrece periódicamente al personal de privacidad, aunque no se cuenta con un proceso uniforme para actualizar las mejores prácticas.

## Nivel 3: Repetible

- **Proceso de gestión de riesgos a la privacidad.** Las prácticas de la gestión de riesgos de la organización se han aprobado y expresado formalmente como política. Las prácticas de privacidad de la organización se actualizan periódicamente en función de la aplicación de los procesos de gestión de riesgos a los cambios en los objetivos empresariales o de la misión y a un panorama cambiante de riesgos, políticas y tecnología.
- **Programa integrado de gestión de riesgos a la privacidad.** Se aplica un método en toda la organización para gestionar los riesgos a la privacidad. Se definen, implementan según lo previsto y se revisan las políticas, los procesos y los procedimientos basados en el riesgo. Se han establecido métodos uniformes para responder eficazmente a los cambios en el riesgo. La organización vigila de forma sistemática y precisa los riesgos a la privacidad. Los ejecutivos sénior de la privacidad y de otros ámbitos se comunican periódicamente con respecto a los riesgos a la privacidad y comprueban que se considere la privacidad en todas las líneas de operación de la organización.
- **Relaciones en el ecosistema de tratamiento de datos.** La organización conoce sus funciones, dependencias y dependientes en el ecosistema más amplio y puede contribuir a que la comunidad tenga mayor conocimiento de los riesgos. La organización es consciente de los riesgos al ecosistema de privacidad asociados con los productos y servicios que proporciona y utiliza. Además, por lo general actúa formalmente ante esos riesgos por medio de mecanismos, como acuerdos escritos, para comunicar los requisitos de privacidad, las estructuras de gobernanza y la implementación y vigilancia de las políticas.
- **Personal.** El personal que se dedica a la privacidad posee los conocimientos y las habilidades para desempeñar sus funciones y responsabilidades. Se ofrece capacitación en materia de privacidad periódica y actualizada a todo el personal.

## Nivel 4: Adaptable

- **Proceso de gestión de riesgos a la privacidad.** La organización adapta sus prácticas de privacidad según las lecciones aprendidas de los eventos de privacidad y la identificación de nuevos riesgos a la privacidad. Por medio de un proceso de mejoramiento continuo que incorpora tecnologías y prácticas avanzadas de privacidad, la organización se adapta activamente a un panorama cambiante de políticas y tecnología, y responde de manera oportuna y efectiva a los riesgos a la privacidad en evolución.
- **Programa integrado de gestión de riesgos a la privacidad.** Se aplica un método en toda la organización para gestionar los riesgos a la privacidad mediante el uso de políticas, procesos y procedimientos basados en riesgos para abordar las acciones problemáticas de datos. La relación entre el riesgo a la privacidad y los objetivos de la organización se conoce claramente y se considera durante la toma de decisiones. Los ejecutivos sénior vigilan el riesgo a la privacidad en el mismo contexto de los riesgos a la ciberseguridad, los riesgos financieros y demás riesgos

organizativos. El presupuesto de la organización se basa en el conocimiento del entorno del riesgo actual y del previsto, y en la tolerancia al riesgo. Las unidades empresariales implementan la visión ejecutiva y analizan los riesgos a nivel de sistema en el contexto de las tolerancias al riesgo de la organización. La gestión de riesgos a la privacidad forma parte de la cultura organizativa y evoluciona con las lecciones aprendidas y el conocimiento continuo del tratamiento de datos y de los riesgos a la privacidad resultantes. La organización puede considerar con rapidez y eficiencia los cambios en los objetivos empresariales y de la misión en la forma en que se asumen y comunican los riesgos.

- **Relaciones en el ecosistema de tratamiento de datos.** La organización conoce sus funciones, dependencias y dependientes en el ecosistema más amplio y contribuye a que la comunidad tenga mayor conocimiento de los riesgos. La organización usa la información en tiempo real, o casi en tiempo real, para entender y actuar consecuentemente ante los riesgos del ecosistema de privacidad asociados con los productos y servicios que proporciona y utiliza. Además, se comunica de manera proactiva, empleando mecanismos formales (por ejemplo, acuerdos) e informales para entablar y mantener relaciones sólidas en el ecosistema.
- **Personal.** La organización cuenta con conjuntos de habilidades especializadas en privacidad en toda la estructura organizativa, y el personal que tiene perspectivas diversas contribuye a la gestión de los riesgos a la privacidad. Se ofrece capacitación periódica y especializada en materia de privacidad a todo el personal. El personal de todos los niveles conoce los valores de la privacidad de la organización y su función en el mantenimiento de esos valores.