RESOLUCIÓN FN/MP N° 1339 /2026

Santiago, 12 de junio de 2026

ANT.: Resolución FN/MP N° 501/2025, de 7 de marzo de 2025, que Aprueba Política de Gobernanza de Datos del Ministerio Público.

MAT: Aprueba nueva Política de Gobernanza de Datos del Ministerio Público.

CONSIDERANDO:

1° Que, conforme a lo dispuesto en los artículos 83 de la Constitución Política y 1° de la Ley N° 19.640, Orgánica Constitucional del Ministerio Público, corresponde a este organismo autónomo y jerarquizado, la función de dirigir en forma exclusiva la investigación de los hechos constitutivos de delitos, ejercer la acción penal pública y tomar las medidas que sean pertinentes y necesarias para proteger a las víctimas y testigos de los ilícitos.

2° Que, de conformidad con lo dispuesto en el artículo 91 de la Constitución Política de la República, el Fiscal Nacional tendrá la superintendencia directiva, correccional y económica del Ministerio Público, en conformidad a la ley orgánica constitucional respectiva.

3° Que, mediante la Ley N° 21.719, cuya entrada en vigor es el 1 de diciembre de 2026, conforme a lo dispuesto en su artículo primero transitorio, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, el legislador estableció un nuevo marco regulatorio en la materia. Dicho marco contempla un régimen especial para los organismos dotados de autonomía constitucional, entre ellos el Ministerio Público, contenido en el Título VIII de la ley, conforme al cual el tratamiento de datos de estos organismos se rige por su estatuto especial y por las disposiciones expresamente aplicables, sin sujeción al régimen administrativo común ni a la potestad fiscalizadora y sancionatoria ordinaria de la Agencia de Protección de Datos Personales.

4° Que, conforme a lo dispuesto en el artículo 54 de la Ley N° 21.719, el tratamiento de datos personales efectuado por organismos públicos dotados de autonomía constitucional, entre ellos el Ministerio Público, se encuentra sujeto a un régimen especial, siendo lícito el tratamiento de datos personales que estos realicen cuando resulte necesario para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y de acuerdo con sus leyes orgánicas. En dichas circunstancias, tales organismos tienen la calidad de responsables de los datos personales que tratan y no requieren el consentimiento de sus titulares para efectuar dicho tratamiento.

5° Que, en el marco del régimen especial previsto en el artículo 54, la Ley N° 21.719 precisa las disposiciones que resultan aplicables a los organismos públicos dotados de autonomía

constitucional, así como las condiciones bajo las cuales estos efectúan el tratamiento de datos personales en el ejercicio de sus funciones.

Asimismo, la propia ley contempla reglas especiales respecto del tratamiento de datos personales vinculado a actividades de prevención, investigación, detección o enjuiciamiento de infracciones penales, protección de víctimas y testigos, análisis criminal y reportabilidad de información criminal, atendida la naturaleza de dichas actividades y la necesidad de resguardar el adecuado cumplimiento de las funciones públicas involucradas.

6° Que, el referido artículo 54 dispone que las autoridades superiores de los organismos públicos dotados de autonomía constitucional deberán dictar las políticas, normas e instrucciones necesarias para dar cumplimiento a los principios y obligaciones establecidos en la ley, especialmente aquellas que permitan el ejercicio de los derechos de los titulares de datos personales y las que fijan los estándares o condiciones mínimas de control, seguridad y resguardo en el tratamiento de dichos datos. Asimismo, el artículo séptimo transitorio de la Ley N° 21.719 dispone que las instituciones señaladas en el artículo 54 deberán dictar las referidas políticas, normas, e instrucciones dentro de los dieciocho meses siguientes a la publicación de la ley en el Diario Oficial, lo cual tuvo lugar el 13 de diciembre de 2024.

7° Que, mediante Resolución FN/MP N° 501/2025, de 7 de marzo de 2025, se aprobó la Política de Gobernanza de Datos del Ministerio Público, instrumento que resulta necesario actualizar y adecuar al nuevo marco normativo y a las exigencias establecidas por la Ley N° 21.719.

8° Que, la actualización de la Política de Gobernanza de Datos del Ministerio Público resulta esencial para establecer directrices claras respecto a1 tratamiento de datos personales, asegurando que estos sean gestionados de conformidad con la normativa vigente y, especialmente, con las disposiciones de la Ley N° 21.719 y **VISTOS**, además, lo dispuesto en el artículo 13 de la Ley N° 19.640, Orgánica Constitucional del Ministerio Público.

RESUELVO:

Apruébese y póngase en vigencia, a contar de esta fecha, la nueva Política de Gobernanza de Datos del Ministerio Público, cuyo texto se adjunta como anexo a la presente resolución.

Anótese y comuníquese.

REPUBLICA DE CHILE
FISCAL NACIONAL
MINISTERIO PÚBLICO

ANGEL VALENCIA VÁSQUEZ
FISCAL NACIONAL

MNL/LFSD/AMP/rhc/mna

c.c:
- Gabinete Fiscal Nacional
- Fiscales Regionales
- Fiscal Jefe Fiscalía Supraterritorial
- Directores Ejecutivos Regionales
- Administrador Ejecutivo Fiscalía Supraterritorial
- Gerentes de División de la Fiscalía Nacional
- Directores y Jefes de Unidades de la Fiscalía Nacional

Política de Gobernanza de Datos

Ministerio Público

Junio de 2026

ÍNDICE

I. ANTECEDENTES

Los alcances de la transformación digital han convertido a los datos en un nuevo factor de producción y en un activo clave para la toma decisiones para que todo tipo de organizaciones, públicas y privadas, puedan valerse de ellos, a fin de diseñar mejores políticas, productos y servicios, que se ajusten con mayor precisión a las necesidades de la sociedad. Su aprovechamiento a nivel de gestión pública, en un primer nivel, mejora la toma de decisiones a partir de evidencia; y en un segundo nivel, produce beneficios para los ciudadanos, las organizaciones de la sociedad civil y el sector privado a partir de la apertura de los datos y procesos que aportan a la toma de decisiones de política y gestión pública.

El Ministerio Público, en adelante la Fiscalía, es un organismo autónomo jerarquizado que, conforme a lo previsto en Capítulo VII de la Constitución Política de la República, está encargado de dirigir en forma exclusiva la investigación de los hechos constitutivos de delito, los que determinen la participación punible y los que acrediten la inocencia del imputado y, en su caso, ejercer la acción penal pública en la forma prevista por la Ley ante los tribunales, correspondiéndole de igual manera, la adopción de medidas para la protección de las víctimas y testigos. Es así que, en el cumplimiento de estas funciones, la institución ha identificado la necesidad de implementar mejoras técnicas al proceso de toma de decisiones, y de habilitar mejoras en base a gestión de la información.

Asimismo, el valor de la información para el logro del mandato Constitucional se torna cada vez más relevante, en el entendido de que el manejo de datos sustenta gran parte de la gestión institucional, instalando el desafío de convertir los datos en conocimiento, y la información en un activo estratégico para la Institución.

A mayor abundamiento, una de las directrices de la institución es el uso de la inteligencia para investigar el fenómeno delictual y para la protección de víctimas y testigos, desplegando capacidades avanzadas a nivel tecnológico y humano, impulsando un proceso de modernización tecnológica acelerada con foco en la operación. Todo lo anterior ubica a la información y los datos en un plano estratégico, relevando de manera lógica y consecuente la necesidad de administrar este activo estratégico de manera adecuada, garantizando que el

ecosistema de datos propicie la confianza, organización, seguridad y correcta utilización de los activos de datos en todo su ciclo de vida, lo que consecuentemente evidencia la necesidad de establecer la Gobernanza de Datos en la Fiscalía de Chile.

Gobernanza de Datos

Se entenderá la Gobernanza de Datos como la actividad organizacional que se ocupa de la definición de principios y prácticas alineadas a los objetivos institucionales y orientadas a potenciar los datos como activos organizacionales. De este modo, la presente Política aborda las definiciones anteriores, estableciendo los Principios que deben ser entendidos y acatados por todos los miembros de la organización, además de Prácticas de Gestión de Datos, y los Roles y Organización para abordar la Gestión de la Información.

II. MARCO NORMATIVO

La presente Política tiene en consideración al menos las siguientes leyes y normativas, las que regulan el tratamiento de los datos personales:

- Constitución Política de la República.
- Código Penal y Código Procesal Penal.
- OF. CIRC. N°711, de 11 de diciembre de 2023, del Ministerio de la Secretaría General de la Presidencia y del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, que establece lineamientos para el uso de herramientas de inteligencia artificial en el sector público.
- Decreto N° 12 del año 2025, del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación de Chile que aprueba actualización de la Política Nacional de Inteligencia Artificial.
- Ley N°20.285: Ley sobre el Acceso a la Información Pública.
- Ley N°19.640: Ley Orgánica Constitucional del Ministerio Público.
- Ley N°19.628, sobre Protección de la Vida Privada, vigente hasta el 1° de diciembre de 2026; y Ley N°21.719, que Regula la Protección y el Tratamiento de los Datos Personales y Crea la Agencia de Protección de Datos Personales, publicada en el Diario Oficial de 13 de diciembre de 2024 y cuya entrada en vigor opera desde el 1 de diciembre de 2026,

especialmente las disposiciones contenidas en:

- Artículo 3°, que establece los principios aplicables al tratamiento de datos personales.
- Artículo 14 sexies, en lo relativo a la obligación de registro interno de las vulneraciones de las medidas de seguridad y comunicación a los titulares afectados en las hipótesis correspondientes.
- Artículos 20, 21 y 22, respecto del tratamiento de datos personales por organismos públicos, y a las obligaciones aplicables a estos, en cuanto resulten compatibles con el régimen especial previsto para los organismos públicos dotados de autonomía constitucional y con las disposiciones especiales que regulan el tratamiento de datos personales efectuado con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, protección de víctimas y testigos, análisis criminal y reportabilidad de información criminal.
- Artículo 24 letra a), que establece el régimen especial aplicable al tratamiento, comunicación o cesión de datos personales, realizado por órganos públicos, efectuado con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, protección de víctimas y testigos, análisis criminal y reportabilidad de información criminal.
- Artículo 54, que establece la regla general del tratamiento de datos personales aplicable a organismos públicos dotados de autonomía constitucional y que dispone que las autoridades superiores de los organismos autónomos constitucionales deberán dictar las políticas, normas e instrucciones necesarias para dar cumplimiento a los principios y obligaciones establecidos en la ley, especialmente aquellas destinadas a garantizar el ejercicio de los derechos de los titulares y a fijar estándares o condiciones mínimas de control, seguridad y resguardo en el tratamiento de datos personales.
- Artículo 55, que regula el ejercicio de los derechos de los titulares de datos personales ante los organismos públicos dotados de autonomía constitucional y el mecanismo de reclamación ante la Corte de Apelaciones respectiva.

- Toda otra ley, reglamento, o instrucción aplicable al Ministerio Público.

III. OBJETIVO DE LA POLÍTICA DE GOBERNANZA DE DATOS

Garantizar que los datos de la Fiscalía sean gestionados de manera consistente, segura, ética y conforme a la normativa aplicable, maximizando su valor estratégico y minimizando los riesgos a través del establecimiento de principios, prácticas y procedimientos para la gestión de datos de la institución relacionados con la dirección de la investigación penal, protección de víctimas, y testigos y atención de usuarios en general, procesos judiciales y gestión de apoyo administrativo.

IV. ALCANCE

Las definiciones de la presente Política aplican a todos los datos generados, almacenados, procesados y compartidos por la Fiscalía, tanto internos como externos. Incluye datos operativos, administrativos, financieros, de proveedores y otros interesados. Asimismo, se hará extensiva a todos los fiscales y funcionarios de la institución, que en el ejercicio de sus funciones accedan, conserven y/o gestionen información de la institución, y a aquellas personas naturales y jurídicas que por las funciones o prestación de servicios se relacionen con la institución en estas materias.

V. PRINCIPIOS

Los principios listados a continuación orientan el tratamiento de datos personales efectuado por el Ministerio Público y deberán aplicarse considerando la naturaleza de las funciones constitucionales y legales que le han sido encomendadas.

En el cumplimiento de dichas funciones, el Ministerio Público tratará datos personales de conformidad con el régimen jurídico previsto en la Ley N° 21.719, en particular, aquellas disposiciones aplicables a los organismos

dotados de autonomía constitucional (artículo 54), aquellas relativas al tratamiento de datos personales efectuado con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, protección de víctimas y testigos, análisis criminal y reportabilidad de información criminal (artículo 24, letra a), así como con las normas que regulan la reserva y secreto de las investigaciones penales (artículo 182 del Código Procesal Penal).

i. Licitud y lealtad

El Ministerio Público tratará los datos personales de manera lícita y leal. En ese contexto, el tratamiento de datos personales efectuado por la institución será lícito cuando resulte necesario para el cumplimiento de sus funciones legales y se realice dentro del ámbito de sus competencias, de conformidad con lo dispuesto en el artículo 54 de la Ley N.° 21.719.

En el ejercicio de dichas funciones, el Ministerio Público tendrá la calidad de responsable de los datos personales que trate y no requerirá el consentimiento del titular para efectuar dicho tratamiento, sin perjuicio de las demás obligaciones, principios y garantías establecidas en la ley.

ii. Legalidad

El Ministerio Público deberá asegurar que todas las actividades relacionadas con el tratamiento de datos personales cumplan con las leyes específicas, las políticas internas de la organización y los estándares técnicos aplicables en la materia.

iii. Finalidad

Los datos personales serán recolectados únicamente con fines específicos, explícitos y lícitos.

En tal sentido, el tratamiento de datos personales que realice el Ministerio Público, deberá ser compatible y limitarse a los fines que justificaron su obtención y/o encontrarse amparada por una habilitación legal expresa.

iv. Proporcionalidad

Los datos personales tratados por el Ministerio Público deberán limitarse a aquellos que resulten necesarios, adecuados y pertinentes para el cumplimiento de sus funciones constitucionales y legales.

Asimismo, serán conservados durante el tiempo necesario para el cumplimiento de los fines que justificaron su tratamiento, sin perjuicio de las excepciones establecidas por ley.

v. Calidad

El tratamiento de datos personales por parte del Ministerio Público debe ser veraz, completo, exacto, actualizado, comprobable y comprensible. Por lo anterior, no se realizará tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

vi. Responsabilidad y Probidad

El Ministerio Público es responsable de establecer y definir las funciones relacionadas a los datos, estableciendo los roles, funciones, procedimientos, accesos y uso de la información. Los funcionarios y fiscales de la institución son responsables de otorgarles a los mismos la debida utilización, sin perjuicio de la responsabilidad penal y/o disciplinaria que se derive del incumplimiento de este deber.

Asimismo, en el tratamiento de datos personales por parte de la Institución, se aplicará el principio de probidad en la función pública, el cual consiste en observar una conducta funcionaria intachable, un desempeño honesto y leal de la función o cargo con preeminencia del interés general sobre el particular.

Las infracciones que fiscales y funcionarios cometan con ocasión del tratamiento de datos personales serán conocidas y sancionadas conforme a las normas y procedimientos previstos en el Reglamento de Responsabilidad Administrativa de Fiscales y Funcionarios del Ministerio Público, en ejercicio de la potestad disciplinaria de las autoridades del órgano, de conformidad con lo dispuesto en el artículo 54, inciso segundo, parte final, de la Ley N° 21.719, sin perjuicio de las demás responsabilidades legales que pudieren corresponder.

La determinación de estas responsabilidades no queda sujeta a la intervención de la Agencia de Protección de Datos Personales, atendida la autonomía constitucional del Ministerio Público y el régimen especial que el artículo 54 de la Ley N° 21.719 establece para los organismos dotados de dicha autonomía.

vii. Seguridad de la Información

El Ministerio Público establecerá y aplicará las directrices de seguridad de la información que se requieran en términos de disponibilidad, integridad y confidencialidad de la información institucional y de los datos personales que trate.

Dichas medidas deberán ser apropiadas y proporcionales a la naturaleza de los datos tratados, así como a los fines del tratamiento con el objeto de prevenir su tratamiento no autorizado o ilícito, así como su perdida, filtración, daño accidental o destrucción.

viii. Transparencia e información

El Ministerio Público promoverá la transparencia en los procesos de gobierno, administración y tratamiento de datos personales, en los términos previstos por la legislación vigente y con pleno resguardo de la autonomía constitucional del órgano.

Lo anterior se entiende sin perjuicio de las limitaciones derivadas del régimen especial aplicable al tratamiento de datos efectuado con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, de acuerdo a lo dispuesto en la letra a) del art. 24 de la Ley N° 21.719 así como de las normas legales que establecen reserva o secreto respecto de determinada información, en especial la del art. 182 del Código Procesal Penal.

ix. Confidencialidad

El Ministerio Público como responsable del tratamiento de datos personales, así como el personal que tenga acceso a ellos, deberá guardar secreto o confidencialidad acerca de los mismos.

Para dichos efectos, la Fiscalía establecerá controles y medidas adecuadas para preservar el secreto o confidencialidad.

x. Trazabilidad

Los reportes de información, tanto internos o de uso público, deben ser trazables desde sus fuentes de origen, proceso por el que se permite conocer todas las etapas, ubicaciones o cambios por los que han pasado los datos en el contexto de una actividad de tratamiento o requerimientos específicos.

xi. Auditabilidad

Las decisiones relacionadas a datos, procesos y controles podrán ser auditables, por la División de Probidad e Integridad y Auditoría Interna de la Fiscalía Nacional, y deberán ser respaldadas con la documentación correspondiente, de conformidad a la autonomía propia de la Fiscalía.

VI. DERECHOS DE LOS TITULARES DE DATOS Y SU EJERCICIO

El tratamiento de datos personales que realice el Ministerio Público debe respetar los derechos y libertades de las personas y quedará sujeto a las disposiciones de la ley N° 21.719.

En tal sentido, y en cuanto al ejercicio de los derechos de acceso, rectificación, supresión, oposición, portabilidad y bloqueo de datos personales, se estará a lo dispuesto en el artículo 4 y siguientes de la referida norma, en lo que sea pertinente y aplicable al Ministerio Público.

Con todo, el tratamiento de datos personales vinculados a actividades de prevención, investigación, detección o enjuiciamiento de infracciones penales, protección de víctimas y testigos, análisis criminal o reportabilidad de información criminal, se regirá por las disposiciones especiales contenidas en el artículo 24 letra a) de la Ley N° 21.719, el secreto de las actuaciones de la investigación penal, consagrado en el art. 182 del Código Procesal Penal, y el secreto establecido en otras disposiciones legales, como la Ley N° 20.000 y Ley N° 19.913, entre otras.

Las solicitudes deberán presentarse a través de los canales institucionales habilitados y dispuestos para para estos efectos y serán tramitadas por la unidad que se determine mediante las instrucciones internas correspondientes, de acuerdo con el procedimiento y los plazos establecidos en la ley. Los canales señalados estarán dispuestos en la página web institucional.

Las solicitudes deberán contener a lo menos, los antecedentes necesarios para identificar a su titular o a su representante, individualizar los datos personales o tratamientos respecto de los cuales se ejerce el derecho correspondiente y proporcionar un medio para la recepción de la respuesta, de conformidad con lo dispuesto en el art. 11 de la Ley N° 21.719.

El Ministerio Público adoptará las medidas necesarias para garantizar una tramitación racional y justa de las solicitudes que se formulen en ejercicio de estos derechos.

De conformidad con lo dispuesto en el artículo 23 letras a) y b) de la Ley N.° 21.719, el Ministerio Público no acogerá las solicitudes cuando con ello se impida o entorpezca el cumplimiento de sus funciones investigativas, de protección a víctimas y testigos o sancionatorias, o cuando se afecte el carácter secreto de la información establecido por la ley.

El tratamiento de datos personales vinculados a actividades de prevención, investigación, detección o enjuiciamiento de infracciones penales, protección de víctimas y testigos, análisis criminal o reportabilidad de información criminal, se regirá por las disposiciones especiales contenidas en el artículo 24 letra a) de la Ley N.° 21.719 y el secreto de la investigación consagrado en el art. 182 del Código Procesal Penal.

VII. PRÁCTICAS DE GESTIÓN DE DATOS

El tratamiento de datos personales que realice la institución quedará sujeto a los siguientes propósitos:

i. Registrar la información de Datos Personales en las Bases de Datos de carácter administrativo de la institución, con la finalidad de Vincular personal, desarrollar procesos de contratación, adquisición de bienes u otros procesos de apoyo a la gestión y/o estratégicos.
ii. Registrar la información de Datos Personales en las Bases de Datos (operativas) de la Institución, con la finalidad de analizar, evaluar y generar datos estadísticos para la supervisión y seguimiento de la gestión institucional.
iii. Desarrollar las investigaciones penales y/o disciplinarias por hechos que lleguen a conocimiento de la Institución por denuncia, querella, oficio, entre otros medios, bajo el estricto cumplimiento de las normas procesales.
iv. Brindar protección a víctimas y testigos durante su participación en el proceso penal.
v. Producir Investigación y Desarrollo (I+D) tendientes a apoyar la operación, la investigación penal y la protección de víctimas y testigos
vi. Remitir información a entidades del sistema penal, judiciales, organismos auxiliares o entidades internacionales por solicitud expresa de las mismas, y bajo los principios de colaboración interinstitucional, circulación restringida y restricciones legales y reglamentarias asociadas al artículo 182 del Código Procesal Penal y a la Instrucción General que imparta criterios de actuación en la etapa de investigación del proceso penal (actualmente, Oficio FN N.° 060/2014, o la instrucción que lo reemplace).

En este contexto y definido el propósito del tratamiento datos, se establecen las Prácticas de Gestión de Datos, las que se centrarán en la protección, actualización, calidad y uso ético de datos, permitiendo a través de estas definiciones el controlar la gestión de los activos de información institucionales, determinar cómo se toman las decisiones sobre los datos, el comportamiento esperado de las personas de la institución, y los procesos respecto de éstos. Las prácticas que se desarrollarán e implementarán serán al menos las siguientes:

- Prácticas de protección de datos personales
- Prácticas de actualización de datos
- Prácticas de calidad de datos
- Prácticas de ética en el uso de los datos
- Prácticas de gestión de incidentes
- Prácticas de catalogación de los datos

VIII. ROLES Y ORGANIZACIÓN

i. Comité Directivo de Gobierno de Datos:

Se establece la conformación de un Comité Directivo de Gobierno de Datos, cuya función es asegurar que la gobernanza de datos al interior del Ministerio Público se encuentre alineada con los objetivos estratégicos, y estará compuesto por Dirección Ejecutiva Nacional, por las Gerencias de la División de Estudios, Evaluación y Análisis avanzado de datos, División de Informática, División de Atención a las Víctimas y Testigos, División de Planificación, Control de la Gestión y Supervisión, y la Jefatura de Unidad de Asesoría Jurídica.

Las funciones principales del Comité son:

- Definir la estrategia y visión de datos
- Evaluar y aprobar las prácticas de Gestión de Datos
- Priorización estratégica
- Supervisar el desempeño de la gobernanza de datos
- Resolución de conflictos en la implementación de políticas, prácticas y estándares
- Aprobar y evaluar la implementación de la Gobernanza de Datos en la Institución y su Plan anual.

ii. Comité Ejecutivo de Gobierno de Datos:

Para la ejecución e implementación operativa de lo dispuesto en la presente Política, se designará un Comité Ejecutivo de Gobierno de Datos cuyos

integrantes, duración y tareas específicas serán establecidas por Resolución del Sr. Fiscal Nacional.

IX. ESTRATEGIA DE GOBIERNO DE DATOS

Con el objetivo de establecer un marco de orientación estratégica para la implementación de la Gobernanza de Datos al interior del Ministerio Público, se anexa a la presente Política, el documento "Estrategia de Gobierno de Datos" estableciendo en el mismo un contexto y ruta de trabajo para su implementación.

ANEXO

ESTRATEGIA DE GOBERNANZA DE DATOS

El presente documento tiene como propósito establecer un marco de orientación estratégica para la implementación de la Gobernanza de Datos de la Fiscalía, a partir de las definiciones realizadas en la Política de Gobernanza de Datos de la institución, y que permita proyectar un contexto y una ruta de trabajo para su implementación.

a) MISIÓN

Posicionar los datos que maneja la Institución como activos organizacionales estratégicos para la consecución de su propósito y misión, relevando la importancia de un manejo seguro, lícito y ético en todo el ciclo de los datos, desde su creación hasta su archivo o eliminación.

b) VISIÓN

Ser una institución que comprende, conoce, gestiona y posiciona los datos como un activo fundamental en la consecución de su propósito y misión institucional y sus lineamientos estratégicos, aportando a la mejora continua de sus procesos a través del manejo seguro, lícito y ético del ciclo de vida de los activos de datos.

c) MARCO DE TRABAJO

La Institución define trabajar en base al marco de trabajo DAMA (Data-Managment)[1] el cual establece once prácticas o ámbitos de trabajo para la gestión de la información, y entrega una guía para avanzar en cada uno de los ámbitos. En la Institución, la adopción de esta guía se materializará a través del Plan Anual de Gobernanza de Datos, el cual deberá establecer las acciones a trabajar en cada ámbito, definiendo una priorización en base a brechas y riesgos de

[1] Dama International, 2025. Disponible en: https://dama.org/learning-resources/dama-data-management-body-of-knowledge-dmbok/

seguridad, legalidad y ética asociados a dichas brechas. Los ámbitos del marco de trabajo DAMA son los siguientes:

- Gobernanza de Datos: se ocupa de la definición de visión, políticas y estrategias, alineadas a los objetivos institucionales, orientadas a potenciar los datos como activos organizacionales.
- Arquitectura de Datos: se encarga de establecer los dominios, inventarios y modelos de información. También los diseños de las plataformas para gestionar los datos.
- Modelado y Diseño de Datos: diseña los modelos de datos que se implementan en la arquitectura definida.
- Almacenamiento y Operación de Datos: se encarga de la implementación y operación de las plataformas de gestión de datos.
- Seguridad de datos: se encarga de todo lo relativo a la privacidad, confidencialidad y a garantizar un acceso apropiado a los datos.
- Integración e Interoperabilidad de datos: responsable de definir la integración y transferencia de los datos ya sea al interior de la organización o hacia/desde el exterior.
- Documentos y Contenidos: establece las reglas aplicables a los datos no estructurados como documentos y otros contenidos.
- Datos Maestros y de Referencia: buscan generar una estandarización de las codificaciones y de la centralización de la información más relevante.
- Data Warehousing & BI: se ocupan de lo referente a inteligencia de negocio (BI) y analítica de datos.
- Metadatos: busca proporcionar y administrar la información sobre los datos como catálogos y diccionarios.
- Calidad de Datos: mecanismos a través de los cuales se define, controla y mejora la calidad de los datos.

d) DESCRIPCIÓN DE PRÁCTICAS DE GESTIÓN DE DATOS

En este contexto y definido el propósito de tratamiento datos declarado en la Política de Gobernanza de Datos, se establecen las Prácticas de Gestión de Datos, las que se centrarán en la protección, actualización, calidad y uso ético de datos, permitiendo a través de estas definiciones el controlar la gestión de los

activos de información institucionales, determinar cómo se toman las decisiones sobre los datos, el comportamiento esperado de las personas de la institución, y los procesos respecto de éstos. Se describen a continuación las prácticas de gestión de datos que se definirán e implementarán en la Institución:

a) Prácticas de Protección de Datos Personales:

i. Prevención de fuga de datos.

- Bloqueo de Puertos: con el objetivo de prevenir la fuga de datos, la institución podrá bloquear de forma centralizada el acceso y conectividad de dispositivos no autorizados en las estaciones de trabajo (PC), tales como pendrive o discos duros externos.
- Prohibición de envío de información por medios no autorizados: El envío o entrega de información con datos personales solo podrá realizarse a través de los medios y mecanismos previamente autorizados.

ii. Transmisión y recepción segura de datos

- Mecanismos regulares de transmisión y recepción de archivos con datos: la Fiscalía definirá cuáles serán los mecanismos regulares para la transmisión y recepción de archivos con datos, dependiendo de la clasificación de los datos, formato del archivo, tipo de archivo y canal de transmisión más idóneo para este proceso. Estos mecanismos deberán ser revisados de forma periódica, de manera de hacer los ajustes necesarios de acuerdo con las necesidades de la institución.
- Mecanismos excepcionales de transmisión y recepción de archivos con datos: en los casos que la transmisión y recepción de archivos con datos no se pueda realizar mediante los canales regulares, la institución definirá mecanismos excepcionales para este proceso, mecanismos que deben estar claramente documentados y autorizados. Estos mecanismos deberán ser revisados de forma periódica, de manera de hacer los ajustes necesarios de acuerdo con las necesidades de la institución.
- Interconexiones: para los procesos de transmisión y recepción de datos se fomentará, en los casos que corresponda y en los cuales exista la disponibilidad técnica, el establecimiento de interconexiones mediante

canales de comunicación dedicados y encriptados. (Validar si se debe indicar que estas interconexiones deben estar amparadas por convenios de colaboración).

iii. Acceso a los datos personales almacenados y administrados por la Fiscalía.

- Solicitudes de Acceso, conforme lo dispuesto en la Ley N° 21.719.
- Acceso a datos personales en el marco del desarrollo de aplicaciones o sistemas.
- Proporcionalidad en el acceso a los datos personales, lo que quiere decir que los funcionarios y fiscales de la Institución podrán acceder a datos personales almacenados en los sistemas y bases de datos institucionales, de acuerdo a las funciones que deba cumplir, en sintonía con el principio de proporcionalidad definido y regulado en la Ley N° 21.719.

iv. Disociación de datos: es el proceso mediante el cual se busca que un dato no pueda asociarse a una persona específica o determinable, para lo cual se definen dos procedimientos:

- Anonimización: se definirá un procedimiento que establezca los criterios y aplicación de un proceso de anonimización sobre los datos personales que mantiene la institución. Este procedimiento deberá garantizar que un dato personal o sensible no pueda vincularse o asociarse a una persona, caso o procedimiento determinado, ni permitir su identificación, dado que se ha destruido o eliminado el nexo con la información que vincula, asocia o identifica. Un dato anonimizado deja de ser un dato personal o sensible.
- Seudonimización: tratamiento de datos personales que se efectúa de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona natural identificada o identificable.

v. Acceso restringido por perfil

Los usuarios de plataformas institucionales que registran o utilizan registros calificados como datos personales podrán acceder a dichos sistemas sólo mediante una autenticación personal, con usuario y clave, de carácter personal e intransferible.

vi. Documentación

La documentación de las bases de datos deberá seguir criterios de alto estándar en materia de gobierno de datos:

- Las División de la Fiscalía Nacional encargada del gobierno de datos deberá elaborar la documentación y metadatos necesarios que permitan su comprensión, uso adecuado y replicabilidad.
- La documentación de las bases de datos y sistemas informáticos vinculados al quehacer del Ministerio Publico debe contener, en los casos que corresponda, todos o algunos de los siguientes elementos: (a) diccionario de datos, (b) metadatos. (c) modelamiento de proceso para su elaboración, en los casos en que corresponda, (d) programación, (e) código o vínculo al repositorio donde se almacena el código que permite su generación, (f) Modelo de datos, (g) Control de versiones.

b) Prácticas de actualización de datos:

i. Periodicidad. la periodicidad de la actualización de los datos dependerá de su objetivo y las necesidades institucionales. Cada proceso de trabajo que requiere actualización de datos deberá requerir y documentar la periodicidad de su actualización.

ii. Control de versiones de los procedimientos de generación de datos: los procesos de generación de datos deberán estar documentados siguiendo lineamientos establecidos que permitan la trazabilidad de las distintas versiones e intervenciones. La documentación deberá estar disponible de forma accesible y oportuna, en la página institucional, y se deberá procurar su actualización anual.

c) Prácticas de calidad de datos:

Los datos contenidos en las respectivas bases generadas por una División, Unidad Especializada, Unidad de Apoyo, Fiscalía Regional o Fiscalía Local deberán ser sometidas a procesos de verificación de su calidad para satisfacer las necesidades y expectativas de sus usuarios, teniendo en consideración, al menos, las siguientes dimensiones:

- **Exactitud**: Grado en que los datos representan correctamente las entidades, en comparación con fuentes de datos que han sido verificadas como exactas.
- **Completitud:** Se deben indicar todos los filtros o criterios de selección y exclusión aplicados a los datos para la obtención del conjunto resultado.
- **Consistencia:** Representación estable de los valores de los datos entre conjuntos de datos, en el tiempo, al interior de un conjunto de datos, entre otras, según corresponda.
- **Oportunidad:** Volatilidad esperada de los datos, es decir, qué tan frecuentemente cambian y las razones de dicho cambio.

d) Prácticas de ética en el uso de los datos:

- Prácticas de Transparencia y rendición de cuentas
- Prácticas de Igualdad no discriminación
- Prácticas de Trazabilidad

e) Prácticas para la Gestión de Incidentes y Vulneraciones de Seguridad de Datos Personales

i. Detección y gestión de incidentes

El Ministerio Público, a través de la División encargada conforme el Reglamento respectivo, adoptará las medidas necesarias para detectar, gestionar y dar respuesta a los incidentes y vulneraciones de seguridad que comprometan o puedan comprometer la integridad, confidencialidad o disponibilidad de los datos personales que trate en el ejercicio de sus funciones.

La gestión de incidentes deberá orientarse a la identificación de sus causas, la evaluación de sus efectos y la adopción de medidas destinadas a mitigar sus consecuencias y prevenir su reiteración.

Cuando un incidente constituya una vulneración de seguridad de datos personales, se aplicarán adicionalmente las medidas de registro interno y comunicación a los titulares afectados previstas en la presente Política.

ii. Registro interno de vulneraciones de seguridad

El Ministerio Público mantendrá un registro interno de las vulneraciones de seguridad que afecten a los datos personales que trate, de conformidad con lo dispuesto en el artículo 14 sexies, inciso segundo, de la Ley N.° 21.719. La designación de este encargado se efectuará mediante la resolución del Fiscal Nacional que dicte al efecto.

Dicho registro deberá contener, a lo menos, la naturaleza de las vulneraciones sufridas, sus efectos, las categorías de datos comprometidos, el número aproximado de titulares afectados y las medidas adoptadas para gestionar la vulneración y prevenir incidentes futuros.

El registro tendrá carácter interno y constituirá un mecanismo de control, seguimiento, evaluación de las medidas de seguridad y adopción de medidas de corrección.

iii. Comunicación a titulares afectados

Como parte de las medidas destinadas a resguardar los derechos de los titulares de datos personales, el Ministerio Público comunicará a los titulares de datos las vulneraciones de seguridad que afecten datos personales sensibles, datos relativos a niños y niñas menores de catorce años o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial.

La comunicación deberá efectuarse utilizando los medios que dispone la ley, en un lenguaje claro y sencillo, debiendo singularizar los datos afectados, las

posibles consecuencias de las vulneraciones de seguridad y las medidas de solución o resguardo aplicadas.

Con todo, dicha comunicación será aplicable solo respecto de los tratamientos de datos personales efectuados para fines de gestión institucional, administrativa y de apoyo a la operación del Ministerio Público, quedando excluidos los tratamientos de datos personales vinculados a actividades de prevención, investigación, detección o enjuiciamiento de infracciones penales, protección de víctimas y testigos, análisis criminal y reportabilidad de información criminal; de conformidad con lo establecido en el artículo 24 letra a) de la Ley N.° 21.719, art. 182 del Código Procesal Penal referido al régimen de reserva de la investigación y por las demás disposiciones legales aplicables.

iv. Vinculación con la Agencia de Protección de Datos Personales

El deber de reportar vulneraciones de seguridad a la Agencia de Protección de Datos Personales, previsto en el artículo 14 sexies, inciso primero, de la Ley N.° 21.719, no resulta exigible al Ministerio Público. Lo anterior obedece a que dicho deber se inserta en el régimen de fiscalización y responsabilidad administrativa que la ley estructura en torno a la potestad supervisora de la Agencia, régimen del que el Ministerio Público se encuentra excluido en virtud del artículo 54 de la misma ley. En consecuencia, la Agencia carece de competencia fiscalizadora y sancionatoria respecto del Ministerio Público, lo que priva de objeto y de eficacia al reporte que dicha norma contempla.

Refuerza lo anterior el diseño del Título VIII de la ley, que revela una decisión del legislador de no someter a los organismos autónomos constitucionales al régimen de fiscalización externa, radicando en cambio el cumplimiento de la ley en la regulación interna y en la potestad disciplinaria de sus propias autoridades.

Confirma esta conclusión el artículo 55 de la ley, conforme al cual el titular de datos que se vea agraviado por la denegación injustificada o arbitraria del ejercicio de sus derechos, o por la infracción de los principios y deberes establecidos en la ley, puede reclamar directamente ante la Corte de

Apelaciones respectiva. De este modo, el control externo de las actuaciones del Ministerio Público en materia de tratamiento de datos personales está radicado exclusivamente en los tribunales de justicia.

A mayor abundamiento, el reporte externo de un incidente de seguridad a la Agencia podría comprometer el secreto de la investigación consagrado en el artículo 182 del Código Procesal Penal, toda vez que la comunicación a un organismo externo de información relativa a vulneraciones que afecten datos de investigaciones en curso o terminadas, víctimas protegidas o testigos bajo reserva generaría un flujo de información incompatible con las funciones constitucionales del Ministerio Público.

Lo anterior es sin perjuicio de la facultad del Ministerio Público de requerir voluntariamente la asistencia técnica de la Agencia de Protección de Datos Personales en los términos del artículo 54, inciso segundo, y artículo 30 bis letra i) de la Ley N.° 21.719.

f) Prácticas para la Catalogación de los datos

El catálogo de datos es un repositorio centralizado que documenta de manera estructurada los conjuntos de datos claves del Ministerio Publico, es decir aquellos vinculados con el cumplimiento de la misión y objetivos fundamentales de la Fiscalía, capturando metadatos, entre otros, para facilitar la comprensión, organización y acceso seguro, actualizándose de manera regular para garantizar la calidad y disponibilidad de los datos clave, conforme lo definido por la institución en los diversos instrumentos atingentes.

Glosario

En el presente apartado se da cuenta de las principales definiciones o conceptos técnicos utilizados en la presente Política:

Dato: Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa. Los datos describen hechos empíricos, sucesos y entidades, son considerados activos transversales para el funcionamiento de diversos procesos y operaciones de entidades públicas y privadas.

Datos Personales. Información relativa a una persona física identificada o identificable.

Datos Sensibles: Son aquellos que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como el origen étnico o racial, la afiliación política, sindical o gremial, la situación socioeconómica, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la orientación sexual y a la identidad de género de una persona natural.

Datos misionales: son datos contenidos en los sistemas de información misionales de la Institución (gestión de denuncias y análisis de información, investigación y judicialización, protección y asistencia, análisis criminal).

Datos de procesos de apoyo: Son los datos dentro de los procesos estratégicos (planificación estratégica, comunicación y relacionamiento institucional), y apoyo a la gestión (gestión de personas, gestión TIC, gestión documental, gestión de bienes, gestión financiera, gestión de contratos), así como aquellos de procesos de seguimiento, control y mejora (mejora continua y auditoría).

Datos estructurados: es aquel que se organiza y formatea de una manera específica, siguiendo un modelo predefinido.

Datos No estructurados: son aquellos que no tienen una organización fija. Son como un texto libre, donde la información no se encuentra en campos específicos.

Fuentes de acceso público: todas aquellas bases de datos o conjuntos de datos personales, cuyo acceso o consulta puede ser efectuada en forma lícita por cualquier persona, tales como el Diario Oficial, medios de comunicación o los registros públicos que disponga la ley. El tratamiento de datos personales provenientes de fuentes de acceso público se someterá a las disposiciones de la ley.

Anonimización: Corresponde a un procedimiento irreversible por el cual un dato personal no puede vincularse o asociarse a una persona determinada ni permitir su identificación.

Infraestructura de Datos: Es el conjunto de recursos compartidos, dinámicos y estandarizados, dispuestos por diferentes actores, que habilita la provisión permanente de datos para su aprovechamiento y generación de valor para la gestión institucional.

Meta Datos: son datos que describen otros datos, que se orientan a facilitar la búsqueda, organización y entendimiento de la información.

Tratamiento de datos: Cualquier operación o conjunto de operaciones de carácter automatizado o no, que permitan la recolección, procesamiento, almacenamiento, comunicación, transmisión o uso de datos personales o conjuntos de datos personales.

Ciclo de Vida Del Dato:

El ciclo de vida del dato se refiere a las etapas que atraviesan los datos desde su creación hasta su eliminación. Este ciclo comienza con la generación de datos, donde se recopilan datos a través de diversas fuentes. En esta fase, es crucial asegurar la calidad y la relevancia de los datos, ya que sentarán las bases para las etapas posteriores. La recolección puede implicar tanto datos estructurados como no estructurados, y es fundamental establecer métodos adecuados para su captura.

Una vez que los datos han sido generados, entran en la fase de almacenamiento y gestión. Aquí, los datos se organizan y almacenan en bases de datos o sistemas de almacenamiento, donde se implementan medidas de seguridad para proteger la información. Durante esta etapa, se pueden realizar procesos de limpieza y transformación de datos para mejorar su calidad y facilitar su análisis. La gestión de datos también incluye la catalogación y el mantenimiento de metadatos, lo que permite a los usuarios localizar y utilizar los datos de manera eficiente.

Finalmente, los datos pasan por la fase de análisis y utilización, donde se extrae y/o genera información, que permite un proceso de toma de decisiones basada en la información disponible o generada. Esta etapa puede incluir la visualización de datos, la generación de informes y la aplicación de técnicas de análisis avanzado, como el aprendizaje automático. Una vez que los datos han cumplido su propósito, se procede a su archivado o eliminación, dependiendo de las políticas de la organización y las regulaciones aplicables.

La gestión adecuada del ciclo de vida del dato es esencial para maximizar su valor y garantizar la conformidad con las normativas de protección de datos.