CSP · INGENIERÍA INDUSTRIAL UNIVERSIDAD DE CHILE

CENTRO DE SISTEMAS PÚBLICOS

**Ministerio de Seguridad Pública**

# Diseño del Sistema de Seguridad Pública

## Diseño de la arquitectura federada y del modelo de gobernanza de datos del Sistema Integrado de Información del Sistema de Seguridad Pública

**INFORME FINAL**

Marzo 2026

Trabajo realizado entre
Diciembre de 2025 y Febrero de 2026

CSP · INGENIERÍA INDUSTRIAL UNIVERSIDAD DE CHILE
CENTRO DE SISTEMAS PÚBLICOS

**Director del Proyecto**
Richard Weber H.

**Investigadores y Académicos**
Leonardo Basso S.
Carlos Castro G.
Sebastián Maldonado A.
Claudio Pizarro T.
Carla Vairetti M.

**Equipo de Analistas**
Nicolás Delgado A.
Felipe Palma C.
Antonia Lizana P.
Matías Cánepa

Ministerio de Seguridad Pública
Gobierno de Chile

**Contraparte Institucional y Técnica**
Fabián Gil M.
Jefe de Unidad Estratégica

Simón Maturana M., Florencia Signorini B.
Asesores Unidad Estratégica

# Resumen Ejecutivo

La seguridad pública en Chile atraviesa un escenario de alta complejidad, marcado por la coexistencia de múltiples amenazas, una creciente demanda ciudadana de respuestas coordinadas y eficaces, y un entramado institucional compuesto por actores diversos con competencias diferenciadas. En este contexto, la información confiable, oportuna e integrada se configura como un insumo crítico para la toma de decisiones estratégicas, el diseño de políticas públicas basadas en evidencia y la coordinación operativa del sistema. No obstante, la fragmentación histórica y la gestión descentralizada de los sistemas de información han limitado seriamente la capacidad del Estado para aprovechar el valor estratégico de los datos disponibles.

Para superar la fragmentación detectada y cumplir con el mandato de interoperabilidad de la Ley 21.730, el proyecto establece como requerimiento base el diseño de una arquitectura federada de información. Este modelo se justifica como la única solución viable para garantizar la integración de datos sin vulnerar la custodia original de las fuentes, permitiendo que las instituciones mantengan su autonomía legal y técnica.

Este diseño se encuentra alineado, además, con lo dispuesto en el Decreto Supremo N°55, que aprueba el Reglamento del Sistema de Seguridad Pública, particularmente en su letra b), al establecer mecanismos de coordinación e interoperabilidad entre los actores del sistema, resguardando el acceso controlado a la información y el respeto por las competencias y responsabilidades propias de cada institución.

Bajo este esquema, el sistema debiese actuar como un nodo articulador y soberano que facilita el acceso a la información en tiempo real desde sus orígenes, asegurando la escalabilidad del ecosistema (proyectado a 48 instituciones) y el estricto cumplimiento de los marcos de seguridad y reserva necesarios para la persecución penal y la seguridad pública.

El diagnóstico desarrollado en el marco de este informe confirma que el ecosistema informacional del Ministerio de Seguridad Pública (MSP) y del Centro Integrado de Coordinación Policial (CICPOL) funciona actualmente como una red distribuida de plataformas, sistemas y bases de datos organizadas bajo lógicas funcionales diversas. Si bien existen capacidades relevantes y experiencias parciales de integración, persisten barreras estructurales que dificultan la interoperabilidad efectiva, tales como la ausencia de estándares comunes a nivel ministerial, la heterogeneidad tecnológica entre instituciones, la dependencia de mecanismos manuales de intercambio y la inexistencia de una gobernanza transversal consolidada de datos.

A partir del diagnóstico técnico y normativo del ecosistema informacional, el informe desarrolla de manera progresiva la propuesta de arquitectura federada del Sistema Integrado de Información del Sistema de Seguridad Pública, abordando tanto su fundamento conceptual como las condiciones organizacionales y normativas necesarias para sostener una gobernanza interinstitucional de datos. Sobre esta base, se profundiza en el diseño técnico detallado del sistema, incluyendo la definición de procesos, el modelo semántico y los requerimientos tecnológicos habilitantes para su implementación.

El documento sintetiza los principales hallazgos derivados del diagnóstico y desarrolla la fundamentación normativa de la arquitectura federada propuesta, asegurando su estricta coherencia con el marco jurídico vigente. Asimismo, formula conclusiones y recomendaciones estratégicas orientadas a su materialización y presenta una hoja de ruta para la implementación progresiva del sistema, considerando etapas, prioridades, condiciones habilitantes y lineamientos para su ejecución.

En su conjunto, el informe establece las bases conceptuales, normativas, organizacionales y técnicas necesarias para avanzar desde un ecosistema fragmentado hacia un sistema integrado de información en materia de seguridad pública, proporcionando un marco integral para su implementación y sostenibilidad en el tiempo.

# Índice

# Introducción

El Sistema de Seguridad Pública, en adelante el Sistema, se configura como un sistema interinstitucional permanente, creado para articular la acción del Estado en materia de prevención del delito, control, persecución penal, sanción y reinserción social, así como de atención y protección a víctimas. Su diseño responde a la necesidad de coordinar múltiples instituciones con mandatos legales diferenciados, escalas territoriales diversas y horizontes temporales distintos de intervención, en un contexto caracterizado por fenómenos de violencia y delito de naturaleza compleja y dinámica. Esta complejidad estructural hace inviable una gestión basada exclusivamente en lógicas sectoriales o jerárquicas tradicionales, requiriendo un esquema explícito de articulación interinstitucional y multinivel.

Desde el punto de vista institucional, el Sistema se sustenta en un marco normativo y estratégico jerárquicamente articulado. La Ley N° 21.730 establece el Ministerio de Seguridad Pública como órgano rector y reconoce explícitamente la existencia de un sistema interinstitucional orientado a objetivos comunes. Sobre esta base, el Reglamento del Sistema de Seguridad Pública, aprobado mediante el Decreto Supremo N° 55 de 2025, define la arquitectura de gobernanza, las instancias formales de coordinación, los roles de los distintos actores y las reglas básicas de funcionamiento del Sistema, organizándolo a través de dos subsistemas diferenciados —el Subsistema de Seguridad Pública y el Subsistema de Prevención del Delito—, cada uno administrado por su respectiva Subsecretaría bajo la dirección del Ministerio. Complementariamente, la Política Nacional de Seguridad Pública 2025–2031 fija el marco estratégico que orienta la acción del Sistema en el mediano plazo.

Este entramado normativo y estratégico define el qué debe perseguir el Sistema y quiénes participan en su conducción y ejecución, pero no determina por sí solo cómo debe operar en la práctica para transformar dichas orientaciones en decisiones consistentes, coordinación efectiva, ejecución territorial pertinente y control del desempeño. En sistemas interinstitucionales de esta naturaleza, la existencia de normas, políticas e instancias formales no garantiza, por sí misma, coherencia operativa ni resultados sostenidos. De allí surge la necesidad de diseñar explícitamente dispositivos institucionales que ordenen la conducción práctica del Sistema y habiliten el cumplimiento efectivo de los objetivos definidos por la Política Nacional.

En este contexto, el MSP ha impulsado el desarrollo de componentes estructurales orientados a materializar el funcionamiento integrado del Sistema. Entre ellos, el Modelo de Gestión ordena la articulación estratégica y operativa entre los subsistemas y sus actores. Sin embargo, para que este Modelo de Gestión pueda operar en la práctica, esto es, priorizar, ejecutar, controlar y ajustar acciones en el territorio, requiere imperativamente de un soporte tecnológico transversal que reduzca las asimetrías de información y dote de trazabilidad a la rendición de cuentas. Es para resolver esta necesidad operativa que el Modelo de Gobernanza de Datos establece las reglas, estándares y responsabilidades necesarias para asegurar que la información que circula entre las instituciones sea oportuna, interoperable, segura, íntegra y confiable. Ambos modelos constituyen dispositivos habilitantes complementarios e interdependientes: el primero estructura la conducción del Sistema y el

segundo asegura las condiciones informacionales para apalancar dicha conducción con decisiones basadas en evidencia.

En coherencia con este marco, el Sistema Integrado de Información del Sistema de Seguridad Pública (SIISSEP) se concibe como la expresión técnica y operativa del Modelo de Gobernanza de Datos, y ha sido diseñado estructuralmente para habilitar y dar soporte al funcionamiento del Modelo de Gestión. Al articular los flujos de información bajo criterios de interoperabilidad, seguridad, calidad y trazabilidad, el SIISSEP se convierte en el motor que permite a las instancias estratégicas, tácticas y operativas del Sistema evaluar desempeños y reaccionar ante contingencias o desviaciones. Si bien en su fase inicial contempla la integración de las dos Subsecretarías del Ministerio y del Centro Integrado de Coordinación Policial, su diseño responde a una lógica de plataforma institucional habilitante para el conjunto del Sistema, permitiendo la incorporación progresiva de otras entidades conforme a sus competencias, capacidades y marcos regulatorios aplicables.

En términos generales, el diseño del SIISSEP se orienta por cuatro principios fundamentales:

- **Disponibilidad oportuna de la información**, como condición para la toma de decisiones eficaces.
- **Seguridad, calidad e integridad de los datos**, resguardando su confiabilidad y trazabilidad.
- **Interoperabilidad técnica y semántica**, que facilite el intercambio entre plataformas institucionales diversas.
- **Claridad en los roles institucionales**, asegurando una gobernanza funcional de la información, con responsabilidades bien definidas de custodia, administración y uso.

En este sentido, el SIISSEP no constituye únicamente una solución tecnológica, sino el componente habilitante en materia de tecnologías de la información que apalanca las funciones transversales del Modelo de Gestión. Su diseño se concibe como parte integral del proceso de instalación progresiva del Sistema de Seguridad Pública, aportando a la consolidación de una infraestructura pública de información que hace operativamente posible la coordinación, el análisis estratégico y el ciclo de mejora continua alineados con los objetivos del Estado en materia de seguridad.

El Capítulo 1 desarrolla el diagnóstico del ecosistema informacional del Sistema de Seguridad Pública y sienta las bases conceptuales para el diseño del Sistema Integrado de Información. En este capítulo se presenta el marco normativo aplicable, el levantamiento y caracterización de los sistemas de información del Ministerio y de CICPOL, el análisis de interoperabilidad y las restricciones estructurales identificadas. Asimismo, se desarrolla y sistematiza la matriz técnico–normativa y se definen los estándares de interoperabilidad, seguridad, y calidad de datos que estructuran el funcionamiento del Sistema Integrado de Información.

El Capítulo 2 presenta el diseño técnico detallado del Sistema Integrado de Información bajo una arquitectura federada. Se desarrolla el modelo conceptual de federación, la definición de dominios de datos relevantes, la modelación de flujos de consulta y reglas de visibilidad, los procesos operativos asociados, los mecanismos de auditoría y trazabilidad, así como los requerimientos tecnológicos funcionales y no funcionales necesarios para su habilitación.

El Capítulo 3 aborda el diseño organizacional y normativo coherente con las obligaciones del MSP como órgano rector del Sistema. Se definen los roles y responsabilidades en la gobernanza del intercambio de información, los criterios para el tratamiento de datos sensibles, las políticas aplicables al uso y resguardo del dato y el modelo de coordinación interinstitucional que sustenta la arquitectura propuesta.

El Capítulo 4 desarrolla el plan de implementación del Sistema Integrado de Información, estableciendo la ruta de implementación de despliegue, las fases de incorporación institucional y los lineamientos para el desarrollo progresivo de capacidades técnicas y organizacionales.

Finalmente, el Capítulo 5 expone las conclusiones generales del estudio y formula recomendaciones estratégicas para la implementación gradual y sostenible del modelo propuesto, identificando brechas, riesgos y consideraciones críticas para su consolidación.

# Objetivos y Alcance del Proyecto

## Objetivo General del Proyecto

Diseñar el Sistema Integrado de Información del Sistema de Seguridad Pública (SIISSEP), comprendiendo su arquitectura tecnológica, su modelo de gobernanza de datos y los lineamientos de interoperabilidad que regulan su funcionamiento, como infraestructura institucional destinada a organizar, articular y regular los flujos de información del Sistema de Seguridad Pública, habilitando la interoperabilidad segura y eficiente entre las Subsecretarías del Ministerio de Seguridad Pública, CICPOL y las demás instituciones integrantes del Sistema, en conformidad con el mandato establecido en la Ley N° 21.730 y el marco normativo vigente.

Este diseño tiene por finalidad dotar al Ministerio de Seguridad Pública de un sistema y un marco de gobernanza que permitan superar la fragmentación informacional, fortalecer la coordinación interinstitucional y habilitar una gestión basada en evidencia, resguardando las autonomías institucionales y la custodia de los datos, y proyectando su integración progresiva conforme a las capacidades y condiciones habilitantes de cada institución.

## Objetivos Específicos

En coherencia con el objetivo general, el proyecto tiene por finalidad diagnosticar y sistematizar el ecosistema informacional del Ministerio de Seguridad Pública y del Centro Integrado de Coordinación Policial, mediante el mapeo de los sistemas de información, fuentes de datos, flujos y arquitecturas tecnológicas existentes, identificando las brechas técnicas, organizacionales y normativas que condicionan la interoperabilidad.

Sobre la base de dicho diagnóstico, se busca diseñar la arquitectura tecnológica del SIISSEP, definiendo sus componentes estructurales, capas de integración, servicios habilitantes y requerimientos funcionales y no funcionales necesarios para asegurar disponibilidad,

seguridad, eficiencia operativa e interoperabilidad entre las Subsecretarías del Ministerio y CICPOL.

Asimismo, el proyecto se orienta a definir los estándares de interoperabilidad, seguridad y calidad de datos aplicables al sistema integrado, asegurando consistencia técnica, trazabilidad y cumplimiento del marco normativo vigente.

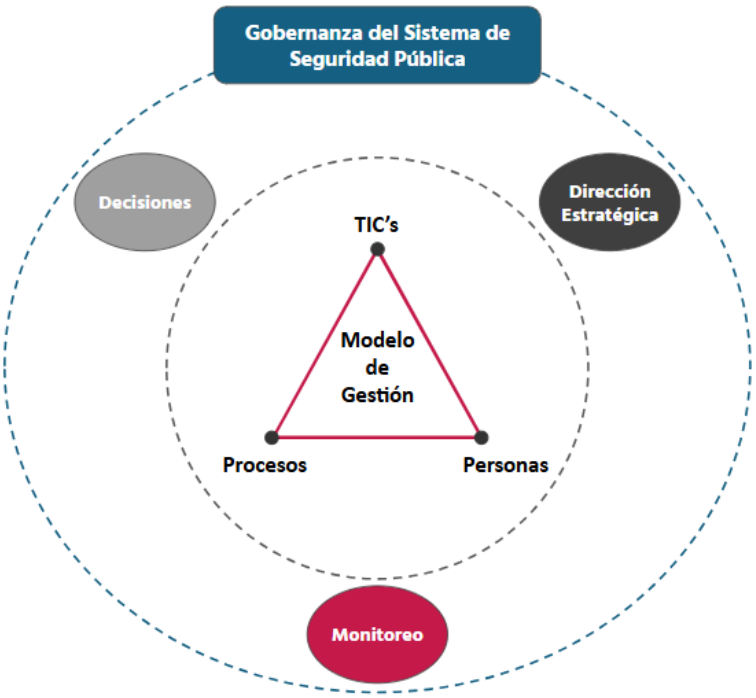
De manera complementaria, se propone formular el modelo de gobernanza de datos del SIISSEP, estableciendo roles, responsabilidades y mecanismos de gestión que regulen la administración, el uso y la custodia de la información en el ámbito ministerial y en su articulación con CICPOL.

En línea con el mandato de interoperabilidad y el respeto a las autonomías institucionales, se busca desarrollar el modelo conceptual de integración de datos entre instituciones, resguardando la distribución de la custodia de la información y asegurando condiciones de consulta y acceso compatibles con el marco legal aplicable.

Finalmente, el proyecto contempla diseñar el plan de crecimiento modular e integración progresiva del SIISSEP, definiendo fases de incorporación institucional, criterios de priorización y condiciones habilitantes para su escalabilidad hacia otras entidades del Sistema de Seguridad Pública, así como identificar las capacidades técnicas y organizacionales requeridas para su operación y sostenibilidad en el tiempo.

Este Sistema Integrado de Información del Sistema de Seguridad Pública da soporte al Modelo de Gestión del Sistema de Seguridad Pública que fue desarrollado en el proyecto “Diseño del Sistema de Seguridad Pública: Modelo de Gestión y Estrategia Bienal” y se visualiza en la siguiente figura.

**Figura 1**: Modelo de Gestión del Sistema de Seguridad Pública




**Fuente**: Informe Final "Diseño del Sistema de Seguridad Pública: Modelo de Gestión y Estrategia Bienal"

Todas las tareas de la Gobernanza del Sistema de Seguridad Pública (Dirección Estratégica, Decisiones, Monitoreo) requieren de un soporte tecnológico adecuado proveyendo información integrada que asegure interoperabilidad, seguridad y calidad de los datos almacenados y acceso oportuno.

## Alcance del Presente Informe

El presente documento corresponde al informe final del diseño del SIISSEP. Su alcance comprende la formulación integral de la arquitectura tecnológica y del modelo de gobernanza de datos destinados a organizar, articular y regular los flujos de información del Sistema de Seguridad Pública, habilitando la interoperabilidad segura y eficiente entre las dos Subsecretarías del Ministerio de Seguridad Pública, el Centro Integrado de Coordinación Policial (CICPOL) y, de manera progresiva, las demás instituciones integrantes del Sistema, en conformidad con la Ley N° 21.730 y el marco normativo vigente.

En este marco, el informe abarca las siguientes dimensiones:

**Diagnóstico del ecosistema informacional:** Levantamiento y sistematización de los sistemas de información, fuentes de datos, flujos y arquitecturas tecnológicas existentes en el Ministerio de Seguridad Pública y en CICPOL, identificando brechas técnicas, organizacionales y normativas que condicionan la interoperabilidad.

**Definición de estándares transversales:** Formulación de los estándares de interoperabilidad, seguridad y calidad de datos requeridos para estructurar el intercambio de información bajo criterios de consistencia técnica, trazabilidad y cumplimiento normativo.

**Diseño técnico de la arquitectura federada:** Desarrollo del modelo conceptual y operativo del SIISSEP, incluyendo la definición de dominios de datos, flujos de consulta, reglas de visibilidad, mecanismos de auditoría y requerimientos funcionales y no funcionales necesarios para su habilitación, bajo una lógica de integración federada y escalable.

**Modelo de Gobernanza de Datos:** Definición del marco organizacional y normativo que regula la administración, custodia y uso de la información compartida, estableciendo roles, responsabilidades y mecanismos de coordinación interinstitucional coherentes con las obligaciones del Ministerio como órgano rector del Sistema.

**Plan de implementación y crecimiento modular:** Formulación de una hoja de ruta para la implementación progresiva del SIISSEP, definiendo fases de incorporación institucional, criterios de priorización, condiciones habilitantes y capacidades técnicas y organizacionales necesarias para su sostenibilidad.

No forman parte del alcance del presente informe:

- El desarrollo de código, programación, adquisición de licenciamiento, contratación de infraestructura o despliegue en producción de las soluciones tecnológicas diseñadas.
- La implementación operativa del sistema.

# Metodología

La metodología para el diseño de la arquitectura tecnológica del Sistema Integrado de Información se estructura como un enfoque técnico, colaborativo y progresivo, orientado a traducir los lineamientos estratégicos del sector en un diseño arquitectónico técnicamente consistente y viable desde el punto de vista tecnológico, y al mismo tiempo implementable dentro de las capacidades operativas, normativas e institucionales existentes.

Este enfoque metodológico se basa en el supuesto de que el diseño de una arquitectura institucional de integración de información requiere, como condición habilitante, un diagnóstico empírico y actualizado de las capacidades tecnológicas, operativas, normativas y organizacionales de cada nodo institucional, en particular del nodo central. En este marco, la metodología busca reducir la brecha entre los mandatos legales y de planificación vigentes y las condiciones efectivas de interoperabilidad actualmente presentes en las subsecretarías del Ministerio de Seguridad Pública y en CICPOL.

Como insumo de base, se consideran los antecedentes del Diagnóstico Estratégico del Sistema de Seguridad Pública desarrollado por el Instituto de Sistemas Complejos de Ingeniería (ISCI), el cual identificó brechas relevantes en materia de gobernanza de datos e interoperabilidad. Dado el carácter predominantemente estratégico de dicho diagnóstico, la metodología contempla la realización de un levantamiento técnico de segundo nivel, específicamente orientado al diseño de la arquitectura del SIISSEP.

Para estos efectos, se diseñaron y aplicaron matrices de caracterización técnica, construidas a partir de los insumos existentes de la Unidad Estratégica del Ministerio y de las matrices utilizadas en el diagnóstico ISCI. Estas matrices permiten sistematizar información clave sobre los sistemas de información y los flujos de datos de las instituciones participantes, incorporando dimensiones tales como el origen y formato de los datos, la frecuencia de actualización, los mecanismos de acceso, los usos operativos, los responsables de custodia y los procesos de transformación.

El levantamiento se desarrolla mediante sesiones de trabajo presenciales con las instituciones responsables, las cuales cumplen un doble propósito: por una parte, recopilar información técnica detallada y validada; y por otra, generar una comprensión compartida respecto del rol del Ministerio de Seguridad Pública como articulador del sistema y de la lógica de funcionamiento de una arquitectura federada. Estas instancias permiten validar las dimensiones consideradas y ajustar el enfoque del levantamiento según la naturaleza específica de cada flujo de información.

Posteriormente, las matrices son remitidas formalmente a los equipos técnicos de cada Subsecretaría y de CICPOL para su completitud y validación, asegurando que la información recopilada refleje adecuadamente las condiciones técnicas, operativas y normativas de cada entidad.

Sobre la base de este levantamiento, la metodología contempla un análisis técnico integrado orientado a identificar compatibilidades, restricciones normativas y condiciones habilitantes para el diseño de la arquitectura federada y del modelo de gobernanza de datos del SIISSEP. Los resultados de este análisis constituyen el insumo principal para la formulación de las definiciones conceptuales presentadas en este informe y para el desarrollo posterior de los normativos, organizacionales, técnicos y tecnológicos en las siguientes fases del proyecto.

Finalmente, este levantamiento técnico se concibe como un insumo crítico para:

- Asegurar la compatibilidad del modelo de federación con los sistemas de información existentes;
- Identificar las restricciones normativas efectivas que inciden en el intercambio y la visibilidad de los datos; y
- Definir estándares de interoperabilidad, seguridad y calidad que sean aplicables a las fuentes reales del Sistema de Seguridad Pública.

# 1. Diagnóstico y diseño conceptual en el marco de la Ley 21.730

Este capítulo articula el marco normativo, el diagnóstico del ecosistema informacional y la definición de estándares que orientan el diseño conceptual del Sistema Integrado de Información del Sistema de Seguridad Pública. Su propósito es establecer una línea base clara que vincule el mandato de interoperabilidad definido por la Ley N° 21.730 con el estado actual de los flujos, sistemas e infraestructuras existentes.

En el apartado 1.1 se expone el marco normativo aplicable, delimitando las habilitaciones, principios y restricciones que condicionan el tratamiento e intercambio de datos en el Sistema. En el apartado 1.2 se presenta el levantamiento y caracterización de los sistemas, fuentes de datos y flujos de información del Ministerio y de CICPOL. En el apartado 1.3 se analiza la infraestructura tecnológica y su nivel de madurez institucional. En el apartado 1.4 se examina la interoperabilidad y las restricciones estructurales identificadas, incluyendo la aplicación de la Matriz de Interoperabilidad Técnico-Normativa. Finalmente, en el apartado 1.5 se establecen los estándares de interoperabilidad, seguridad y calidad de datos que deberán orientar el diseño del sistema en el capítulo siguiente.

## 1.1. Marco normativo y diagnóstico del ecosistema informacional

### 1.1.1. Marco normativo aplicable

El marco normativo que incide sobre el Sistema de Información del Sistema de Seguridad Pública es de carácter multinivel y jerárquico, combinando leyes habilitantes de organización institucional, normas generales de protección de datos personales, reglamentos específicos del Sistema de Seguridad Pública y políticas internas de gobernanza y gestión de la información.

La Ley N° 21.730, que crea el Ministerio de Seguridad Pública, constituye el fundamento legal del Sistema de Seguridad Pública al reconocer su existencia como un sistema interinstitucional permanente y establecer al Ministerio como su órgano rector. La ley define las funciones y atribuciones del Ministerio en materia de conducción y coordinación de la política de seguridad pública, fija los principios generales que orientan el funcionamiento del Sistema y consagra la coordinación interinstitucional como eje de su actuación. En el ámbito informacional, faculta al Ministerio para requerir antecedentes a otros órganos del Estado en materias de su competencia, estableciendo límites al tratamiento de datos personales y disponiendo que los sistemas de análisis ministerial no deben permitir la singularización de personas determinadas, en conformidad con la normativa vigente en materia de protección de datos.

En materia de protección de datos personales, el Sistema de Información se rige actualmente por la Ley N° 19.628, sobre protección de la vida privada, la cual establece los principios generales de licitud, finalidad, proporcionalidad, calidad y seguridad del dato aplicables al tratamiento de datos personales por organismos públicos. Paralelamente, la Ley N° 21.719, que moderniza el régimen de protección de datos personales y crea la Agencia de Protección de Datos, introduce un estándar reforzado de obligaciones, tales como la responsabilidad proactiva, la seguridad por diseño y por defecto, y el tratamiento diferenciado de datos sensibles.

Las disposiciones sustantivas de la Ley N° 21.719 contemplan una entrada en vigencia diferida, encontrándose plenamente aplicables a partir del 1 de diciembre de 2026. Durante el período de transición, el marco plenamente exigible corresponde a la Ley N° 19.628, sin perjuicio de que el diseño y evolución del Sistema de Información deban considerar los estándares reforzados establecidos por la Ley N° 21.719, a fin de asegurar su coherencia jurídica y sostenibilidad en el mediano plazo.

Desde el punto de vista reglamentario, el Decreto Supremo N° 55, que reglamenta el Sistema de Seguridad Pública, desarrolla las disposiciones de la Ley N° 21.730, regulando el funcionamiento del Sistema, los mecanismos de intercambio de información, las condiciones de acceso a los datos y los principios aplicables a su tratamiento. Este reglamento constituye la principal referencia normativa para la operación del Sistema de Información, estableciendo exigencias de interoperabilidad, trazabilidad, confidencialidad, formalización de los intercambios y deberes de secreto.

Complementariamente, la Política Nacional de Seguridad Pública establece el marco estratégico que orienta la consolidación de un sistema integrado de información, promoviendo la toma de decisiones basada en evidencia y la articulación entre las distintas instituciones que conforman el Sistema. Como instrumento mandatado por la Ley N° 21.730 y aprobado mediante decreto supremo, esta Política establece directrices programáticas concretas para el ecosistema de datos, entre las que destacan: el imperativo de interoperabilidad resguardando la confidencialidad de datos sensibles, el mandato de diseñar un sistema integrado con altos estándares de ciberseguridad (Línea de Acción 1), y el establecimiento de un sistema de gobernanza, registro de acceso y auditoría que asegure la trazabilidad de la información (Línea de Acción 5).

Finalmente, el marco normativo se complementa con instrumentos de carácter interno, destacando la Política de Gobernanza de Datos del Sistema de Seguridad Pública, la cual desarrolla el marco de gobernanza aplicable al SIISSEP a lo largo de todo el ciclo de vida de los datos. Esta política consolida un modelo de gestión de la información que articula las responsabilidades del Ministerio y de las instituciones integrantes del Sistema, en coherencia con lo dispuesto en el Decreto Supremo N° 55. Asimismo, define roles, responsabilidades y estándares comunes de interoperabilidad, calidad, oportunidad y seguridad de los datos, estableciendo una estructura estratégica y operativa guiada por un Comité de Gobernanza de Datos. A través de este instrumento se mandata una gestión de riesgos basada en estándares internacionales, el uso ético y responsable de la información (Sunstein 2023) y la aplicación de mecanismos de anonimización o seudonimización cuando corresponda, habilitando además la dictación de instrumentos técnicos derivados necesarios para ejecutar el intercambio seguro y trazable de datos entre los órganos del Sistema.

### 1.1.2. Mapeo y caracterización de los sistemas de información, fuentes de datos y arquitecturas tecnológicas del MSP y de CICPOL

#### 1.1.2.1. Flujos de información

El levantamiento de información efectuado mediante matrices permitió caracterizar de manera estructurada las prácticas efectivas de gestión y circulación de datos en el Ministerio de Seguridad Pública y su entorno interinstitucional. Más que elaborar un inventario exhaustivo de sistemas o bases de datos, el análisis se orientó a comprender cómo las distintas divisiones y departamentos gestionan la información en la práctica, considerando el objetivo de uso, los soportes tecnológicos disponibles, el origen de los datos, los mecanismos de intercambio, los formatos empleados y las modalidades de procesamiento interno, exclusivamente sobre la base de antecedentes efectivamente levantados.

El foco del ejercicio se concentró en aquellas unidades que, por la naturaleza de sus funciones, operan como principales nodos de manejo de información estructurada y de alcance transversal, cuyos flujos resultan especialmente relevantes para la conducción estratégica y el análisis del Sistema en su etapa inicial de implementación. Ello no implica desconocer que otras divisiones desarrollan funciones sustantivas, sino delimitar analíticamente el alcance del diagnóstico en función de su incidencia en la arquitectura informacional del Sistema.

## Subsecretaría de Seguridad Pública

### División de Seguridad y Orden Público (DSOP – GSTOP)

El objetivo de la gestión de información en la División de Seguridad y Orden Público es el seguimiento institucional del funcionamiento del sistema STOP y el monitoreo de compromisos interinstitucionales, con el fin de apoyar el análisis estratégico y la toma de decisiones de la autoridad ministerial. La plataforma utilizada para estos fines corresponde al sistema institucional GSTOP, que opera como un sistema centralizado de registro y consulta estructurada.

Las instituciones que ingresan información son los equipos de los niveles regionales y comunales, quienes registran antecedentes mediante mecanismos de captura estructurada directamente en la plataforma. Las instituciones que reciben información corresponden a la propia División y al nivel central de la Subsecretaría, que utilizan los datos consolidados para la elaboración de informes periódicos y el seguimiento de compromisos institucionales.

En cuanto al formato de entrega de datos, el ingreso se realiza mediante registro estructurado en la plataforma, complementado con extracciones periódicas de bases en formato Excel para su análisis interno. Este esquema configura un flujo formalizado de captura sistémica con procesamiento posterior sobre copias estructuradas, donde predomina el análisis interno por sobre mecanismos de interoperabilidad dinámica con otras plataformas institucionales.

### Departamento de Orden Público y Eventos Masivos

El objetivo de la gestión de información del Departamento de Orden Público y Eventos Masivos es administrar y controlar antecedentes asociados a prohibiciones de acceso a recintos deportivos, así como generar reportes operativos y estadísticos vinculados a eventos masivos. La plataforma utilizada no corresponde a un sistema interoperable externo, sino a bases de datos internas propias que se alimentan mediante un esquema de gestión documental y digitación manual.

Las instituciones que ingresan información son principalmente juzgados con competencia penal, juzgados de policía local, clubes deportivos y entidades organizadoras, que remiten resoluciones judiciales y antecedentes asociados a medidas de prohibición. Las instituciones que reciben información son el propio Departamento, que utiliza estos registros para el control operativo y la elaboración de reportes, y, cuando corresponde, actores relevantes del sistema deportivo a quienes se comunica información consolidada.

Respecto del formato de entrega de datos, la información es recibida mayoritariamente en documentos PDF enviados a través de correo electrónico formal. Posteriormente, estos antecedentes son sistematizados en bases estructuradas internas, configurando un flujo que combina recepción documental, procesamiento manual y redistribución funcional, sin integración sistémica automatizada con los organismos de origen.

**División de Control y Planificación de las Policías**

El objetivo de la gestión de información en la División de Control y Planificación de las Policías es la administración de los procesos de postulación y selección asociados a programas de cooperación y formación policial internacional, organizando y evaluando antecedentes que permitan adoptar decisiones fundadas respecto de la asignación de cupos y becas. La plataforma utilizada corresponde a una plataforma web institucional, a través de la cual se gestionan las postulaciones.

Las instituciones que ingresan información son los propios postulantes, principalmente policías extranjeros, quienes registran antecedentes personales y administrativos en formato estructurado, junto con la documentación de respaldo exigida en PDF. Las instituciones que reciben información son los equipos evaluadores de la División, responsables de revisar, verificar requisitos y seleccionar las postulaciones.

En cuanto al formato de entrega de datos, el intercambio combina el ingreso estructurado en la plataforma con la carga de documentos adjuntos en PDF, generando además notificaciones automáticas por correo electrónico para su gestión interna. El procesamiento se realiza mediante revisión manual de antecedentes y apoyo en planillas Excel para consolidar resultados. Si bien la plataforma permite generar reportes agregados, el tratamiento de la información se apoya principalmente en procesos de revisión y análisis posterior, más que en transformaciones automatizadas de los datos.

**Departamento de Modernización de las Policías**

El objetivo de la gestión de información en el Departamento de Modernización de las Policías es el seguimiento, evaluación y control del avance de los planes estratégicos y de gestión operativa de las instituciones policiales, en el marco del ejercicio de supervisión y control civil. La plataforma utilizada combina una plataforma institucional de reporte, actualmente en implementación progresiva, con un esquema tradicional de gestión documental.

Las instituciones que ingresan información son Carabineros de Chile y la Policía de Investigaciones, que reportan periódicamente antecedentes vinculados a objetivos estratégicos, planes de desarrollo institucional, productos e indicadores de desempeño. Las instituciones que reciben información corresponden al propio Departamento y a las autoridades ministeriales encargadas de la evaluación y toma de decisiones.

Respecto del formato de entrega de datos, el flujo es mixto: se materializa tanto mediante el envío de reportes en formato PDF a través de oficios formales como mediante el ingreso estructurado de información en la plataforma. En ambos casos, los antecedentes son posteriormente exportados a planillas Excel para su análisis interno, evaluación de cumplimiento y consolidación, configurando un esquema donde el procesamiento posterior constituye el eje central para fines estratégicos.

### Departamento de Análisis Criminal

El objetivo de la gestión de información en el Departamento de Análisis Criminal es la consolidación, integración y análisis de información proveniente de múltiples instituciones externas, con el propósito de apoyar el monitoreo permanente y la elaboración de análisis estratégicos en distintos ámbitos de la seguridad pública. La plataforma utilizada se basa en repositorios locales y en herramientas de procesamiento estadístico que permiten integrar y estandarizar datos de origen diverso.

Las instituciones que ingresan información corresponden a distintas entidades del sistema, entre ellas policías y otros organismos sectoriales, que remiten antecedentes vinculados a homicidios, armas, drogas y otros fenómenos delictivos. Las instituciones que reciben información son la propia unidad de análisis, que consolida y procesa los datos, y posteriormente las autoridades y equipos técnicos que consumen los reportes elaborados.

En cuanto al formato de entrega de datos, el intercambio se caracteriza por la recepción de información en formatos heterogéneos, principalmente archivos Excel y PDF, transferidos mediante correo institucional, mensajería y oficios formales. El procesamiento implica la limpieza, estandarización y armonización de variables para construir bases integradas de alcance nacional, configurando un esquema donde el valor analítico se genera fundamentalmente a partir del tratamiento posterior de integración multifuente, más que mediante esquemas automatizados de interoperabilidad sistémica.

### División de Crimen Organizado (DCOTSF – SIREGARD)

El objetivo de la gestión de información en la División de Crimen Organizado se orienta a la identificación, registro y control de personas naturales o jurídicas vinculadas al comercio, almacenamiento y traslado de sustancias químicas controladas, en el marco de las funciones de fiscalización y supervisión regulatoria. La plataforma utilizada corresponde al sistema institucional SIREGARD, que opera como registro estructurado para la gestión de autorizaciones y control de actividades reguladas.

Las instituciones que ingresan información son los particulares e instituciones públicas sujetas a la regulación, quienes registran antecedentes directamente en el sistema conforme a las exigencias normativas vigentes. Las instituciones que reciben información son la propia División y las unidades responsables de la validación y autorización de fiscalizadores, así como otras entidades públicas cuando corresponda en el marco de sus competencias.

En cuanto al formato de entrega de datos, el intercambio se realiza mediante registro estructurado en base de datos relacional, complementado con documentación adjunta en formato PDF cuando corresponde. El procesamiento se orienta a la verificación de antecedentes, control de cumplimiento y generación de reportes regulatorios, configurando un esquema con mayor nivel de estructuración respecto de otros flujos documentales identificados en el Ministerio.

## Subsecretaría de Prevención del Delito

### División de Desarrollo Territorial

El objetivo de la gestión de información en la División de Desarrollo Territorial es el seguimiento del cumplimiento de obligaciones municipales y el monitoreo territorial de iniciativas preventivas en ejecución, en el marco de las funciones de supervisión institucional. La plataforma utilizada corresponde a sistemas institucionales que concentran información reportada por los municipios bajo mandatos formales de reporte.

Las instituciones que ingresan información son los propios municipios, que registran antecedentes directamente en las plataformas habilitadas para tal efecto. Las instituciones que reciben información son la División y sus unidades de control y gestión, que utilizan estos registros como base para la supervisión, validación y seguimiento de compromisos.

Respecto del formato de entrega de datos, el intercambio se realiza mediante ingreso estructurado en sistema y acceso directo para consulta. Para efectos de análisis interno y consolidación de resultados, la información es posteriormente extraída a planillas Excel, configurando un esquema donde el procesamiento principal se desarrolla sobre extracciones estructuradas fuera del sistema fuente, manteniendo el análisis mayoritariamente externo a la plataforma original.

**División de Estudios y Tecnología**

En la División de Estudios y Tecnología se identifican tres modalidades diferenciadas de gestión informacional, determinadas por el tipo de sistema y el propósito del uso de los datos.

En una primera modalidad, el objetivo de la gestión de información es la producción de análisis estadístico y reportes institucionales a partir de información policial periódica. La plataforma utilizada corresponde a sistemas internos y repositorios de análisis que reciben extractos de datos previamente generados desde los sistemas de origen. Las instituciones que ingresan información son principalmente Carabineros de Chile y la Policía de Investigaciones, que remiten bases en formatos como DBF o Excel mediante correo electrónico y, en algunos casos, a través de soportes físicos. Las instituciones que reciben información son los equipos analíticos de la División, responsables de consolidar y procesar los antecedentes para la elaboración de productos estadísticos.

Respecto del formato de entrega de datos, el intercambio se basa en la transferencia de archivos estructurados en formatos legados y planillas electrónicas. El procesamiento implica integración, estandarización y análisis interno sobre insumos previamente extraídos, sin conexión directa a los sistemas fuente, configurando un esquema donde el valor analítico se construye a partir del tratamiento posterior de datos ya consolidados.

En una segunda modalidad, correspondiente al Observatorio de Homicidios, el objetivo de la gestión de información es consolidar y unificar la cifra oficial de víctimas de homicidios consumados, así como caracterizar sus perfiles sociodemográficos y contextuales, contribuyendo a la producción de estadísticas oficiales y análisis especializados. La plataforma opera actualmente como un entorno colaborativo de gestión de datos basado en repositorios compartidos para intercambio interinstitucional. Las instituciones que ingresan información son principalmente Carabineros de Chile, la Policía de Investigaciones, Gendarmería de Chile y el Servicio Nacional de la Mujer y la Equidad de Género, que remiten antecedentes periódicos sobre casos registrados. Las instituciones que reciben información

son el equipo técnico del Observatorio y las autoridades responsables de la definición de políticas públicas en materia de homicidios y delitos violentos.

En cuanto al formato de entrega de datos, el intercambio se materializa principalmente mediante planillas Excel no estandarizadas remitidas periódicamente, lo que exige procesos internos de depuración, conciliación de registros y normalización de variables para la construcción de la estadística oficial consolidada.

En una tercera modalidad, asociada a los sistemas SITIA, el objetivo de la gestión de información es habilitar la detección y monitoreo operativo en tiempo real mediante integración técnica avanzada de distintas fuentes. La plataforma corresponde a módulos tecnológicos interoperables que operan bajo arquitecturas orientadas a servicios. Las instituciones que ingresan información son sistemas institucionales y dispositivos tecnológicos que exponen información estructurada, incluyendo fuentes policiales y otros organismos que proveen datos operativos. Las instituciones que reciben información son unidades operativas y usuarios habilitados que consumen los datos para fines inmediatos de gestión y control.

En este caso, el formato de entrega de datos se materializa mediante streaming de información, consultas directas a sistemas fuente y uso de formatos estructurados como JSON, eliminando la mediación de archivos enviados por correo. El procesamiento se orienta a la integración continua y al acceso oportuno a la información, privilegiando la interoperabilidad sistémica por sobre la consolidación posterior de extractos documentales.

**Centro Integrado de Coordinación Policial (CICPOL)**

El objetivo de la gestión de información en el Centro Integrado de Coordinación Policial no es producir ni administrar información propia, sino articular el acceso, consulta y uso operativo de antecedentes generados por distintas instituciones del Sistema, con el fin de apoyar procesos de coordinación interinstitucional y toma de decisiones operativas. La plataforma se basa en una arquitectura de acceso distribuido, sin repositorio central propio, estableciendo conexiones y mecanismos de consulta hacia los sistemas institucionales de las entidades colaboradoras.

Las instituciones que ingresan información son las entidades colaboradoras que mantienen la titularidad, custodia y administración de sus sistemas, entre ellas las policías, Gendarmería de Chile, la Dirección General del Territorio Marítimo y de Marina Mercante (Directemar), el Servicio Nacional de Aduanas y otros organismos sectoriales, cuyos registros contienen antecedentes vinculados a personas, vehículos, eventos, control territorial, investigación criminal, sistema penitenciario, control migratorio, ámbito marítimo y fiscalización aduanera.

Las instituciones que reciben información son las Unidades de Coordinación Estratégica (UCEs) en el territorio y el nivel central de CICPOL, conforme a lo establecido en el Decreto Supremo N° 55, las cuales utilizan estos antecedentes para el análisis situacional y la coordinación operativa interinstitucional.

En cuanto al formato de entrega de datos, el intercambio se materializa mediante consultas directas a sistemas institucionales, uso de plataformas operativas especializadas y mecanismos de interoperabilidad como servicios web y APIs, lo que permite acceder a información actualizada sin recurrir a la transferencia masiva de archivos. El procesamiento se basa en el cruce contextual y análisis funcional de la información disponible, sin consolidación permanente en un repositorio central, dependiendo de los niveles de acceso y capacidades técnicas habilitados por cada institución colaboradora, lo que configura un entorno de integración heterogénea.

#### 1.1.2.2. Infraestructura tecnológica

El levantamiento de infraestructura tecnológica del sistema actual permite identificar distintos niveles de desarrollo, madurez y autonomía tecnológica entre la Subsecretaría de Seguridad Pública, la Subsecretaría de Prevención del Delito y CICPOL. Las diferencias observadas no sólo responden a trayectorias institucionales diversas, sino que inciden directamente en la capacidad efectiva de almacenamiento, procesamiento, resguardo y articulación de información dentro del ecosistema de seguridad pública.

**Subsecretaría de Seguridad Pública**

**a) Infraestructura On-Premise**

En materia de infraestructura local, la Subsecretaría de Seguridad Pública no dispone actualmente de servidores productivos destinados al almacenamiento o procesamiento de información delictiva. No obstante, se encuentra en fase de planificación e implementación de una arquitectura hiperconvergente basada en servidores de alto desempeño, equipados con procesadores multinúcleo de última generación, memoria de alta capacidad y almacenamiento NVMe orientado a cargas intensivas de lectura y procesamiento.

El diseño proyectado contempla además equipamiento de red corporativo, incluyendo switches de acceso y distribución con capacidades PoE y enlaces de alta velocidad, junto con contratos de soporte especializado bajo esquemas de alta disponibilidad. Estos componentes se encuentran sujetos a aprobación presupuestaria correspondiente al año 2026 y aún no han sido desplegados.

**b) Servicios Cloud**

En paralelo a la infraestructura física proyectada, la SSP ha definido una estrategia tecnológica de carácter híbrido apoyada en servicios de nube pública. En Microsoft Azure se contempla la contratación de créditos de consumo bajo un esquema plurianual, con el objetivo de habilitar entornos virtuales, almacenamiento y servicios gestionados conforme se consoliden los sistemas institucionales.

En Amazon Web Services se ha planificado una arquitectura que incluye instancias de cómputo diferenciadas para aplicaciones Windows y Linux, balanceadores de carga para distribución de tráfico, firewall de aplicaciones web (WAF) para protección de capa 7, almacenamiento en Amazon S3 para respaldos y bases de datos gestionadas en PostgreSQL bajo modalidad Multi-AZ para asegurar continuidad operacional. Asimismo, se considera

conectividad segura mediante VPN Site-to-Site, direcciones IP públicas controladas y gateways de salida administrados.

Estas capacidades se encuentran actualmente en proceso de contratación y planificación, por lo que aún no constituyen una plataforma productiva en operación.

**c) Software Base**

El modelo tecnológico proyectado incluye la adopción de plataformas de virtualización y gestión de infraestructura tales como Nutanix Cloud Platform y VMware ESXi, junto con soluciones empresariales de respaldo y recuperación ante desastres, y sistemas operativos empresariales como Red Hat Enterprise Linux para entornos virtualizados.

Este componente busca asegurar estandarización tecnológica, portabilidad entre entornos locales y cloud, y continuidad operacional bajo estándares corporativos. Sin embargo, su implementación está supeditada a disponibilidad presupuestaria futura.

**d) Seguridad**

El componente actualmente más consolidado en la SSP corresponde al ámbito de seguridad perimetral. Se encuentra implementada una solución basada en equipamiento Fortinet de alto rendimiento, que incluye firewalls corporativos con capacidades avanzadas de inspección de tráfico, segmentación de red y aceleración por hardware, junto con switches de acceso y distribución para la red interna institucional.

El esquema incorpora licenciamiento de seguridad integral por tres años, incluyendo prevención de intrusiones, control de aplicaciones, filtrado DNS/URL y soporte premium. Este proyecto se encuentra operativo desde agosto de 2025 y constituye la base tecnológica habilitante sobre la cual se desplegará la futura infraestructura institucional.

En síntesis, la SSP presenta actualmente un escenario de infraestructura mayoritariamente en fase de implementación, con capacidades de seguridad ya operativas, pero sin plataformas productivas consolidadas para la gestión estructurada de datos.

**Subsecretaría de Prevención del Delito**

**a) Infraestructura On-Premise**

La Subsecretaría de Prevención del Delito dispone de una infraestructura local compuesta por servidores físicos y virtuales que actualmente soportan sus sistemas institucionales productivos. No obstante, la capacidad instalada se encuentra cercana a su límite operativo, lo que ha motivado un proceso de migración progresiva hacia entornos cloud, particularmente hacia Microsoft Azure bajo esquemas de VMware Cloud.

Este escenario refleja una etapa de transición tecnológica, en la que la infraestructura local continúa operativa mientras se consolida una estrategia de modernización orientada a mayor escalabilidad y elasticidad.

**b) Servicios Cloud**

En Microsoft Azure, la SPD mantiene un número significativo de máquinas virtuales que operan con sistemas Windows Server y distribuciones Red Hat Enterprise Linux, con capacidad de almacenamiento disponible y margen operativo para crecimiento. La infraestructura se encuentra desplegada en la región Este de Estados Unidos y opera bajo contrato institucional con Microsoft.

Adicionalmente, la institución mantiene servicios en Amazon Web Services administrados por un proveedor externo, incluyendo entornos de bases de datos Oracle. Este modelo híbrido permite distribuir cargas y asegurar continuidad operacional, aunque implica mayor complejidad en términos de administración multi-plataforma.

**c) Software Base y Licenciamiento**

La SPD opera con motores de base de datos SQL Server, MySQL y Oracle, y dispone de herramientas de reportería y análisis como Power BI bajo un contrato institucional Microsoft E5 que cubre a la totalidad de la organización. Este contrato no sólo habilita herramientas de productividad, sino también capacidades avanzadas de seguridad, identidad y gestión.

El modelo de licenciamiento vigente constituye una base tecnológica homogénea que facilita la estandarización y la integración futura de servicios.

**d) Seguridad**

La arquitectura de seguridad de la SPD se encuentra consolidada y contempla clusters FortiGate para control de tráfico externo e interno, herramientas especializadas de monitoreo y análisis, así como capacidades avanzadas de protección en la nube mediante Azure Firewall Premium y mecanismos de defensa alineados con estándares internacionales.

Este entorno configura un esquema de defensa en profundidad con monitoreo activo y segmentación de red, otorgando un nivel de madurez tecnológica superior en comparación con otras entidades del sistema.

En términos generales, la SPD presenta una infraestructura tecnológica operativa y consolidada, con procesos de modernización en curso y un portafolio amplio de sistemas productivos.

**Centro Integrado de Coordinación Policial**

En el caso de CICPOL, el levantamiento preliminar confirma que el centro no dispone actualmente de infraestructura tecnológica propia destinada al alojamiento, procesamiento o resguardo de información, ni cuenta con una dotación interna de personal especializado en tecnologías de la información para la administración o soporte de sistemas.

Su funcionamiento depende íntegramente de la infraestructura provista por Carabineros de Chile y la Policía de Investigaciones de Chile. En este marco, CICPOL mantiene accesos operativos a los sistemas institucionales de ambas policías, los cuales utiliza como fuentes

primarias de información para labores de coordinación, consulta y articulación interinstitucional.

No se identifica infraestructura propia de almacenamiento ni plataformas autónomas de gestión de datos. El modelo actual se basa en el principio de consulta sobre sistemas de origen, bajo dependencia tecnológica externa tanto en términos de soporte como de disponibilidad de la información.

## 1.2. Análisis de interoperabilidad y restricciones estructurales

### 1.2.1. Compatibilidad técnica entre sistemas y flujos

El análisis de compatibilidad técnico-normativa entre los sistemas que conforman el ecosistema de seguridad pública revela que el principal desafío no radica en la ausencia de plataformas tecnológicas, sino en la heterogeneidad de arquitecturas, modelos de datos y niveles de madurez digital entre las instituciones participantes. Carabineros de Chile, la Policía de Investigaciones, Gendarmería de Chile, el Ministerio Público y los distintos organismos sectoriales han desarrollado históricamente sus sistemas de información de manera autónoma, optimizándolos para sus propias necesidades operativas. Esta fragmentación evidencia brechas estructurales respecto del principio de interoperabilidad que rige al Sistema de Seguridad Pública, establecido en la Ley N.º 21.730 y desarrollado operativamente en el Decreto Supremo N.º 55 de 2025, el cual obliga a los integrantes del sistema a disponer de mecanismos de intercambio de información coordinados, seguros y trazables.

Desde el punto de vista de la arquitectura tecnológica, coexisten sistemas monolíticos heredados, plataformas cliente servidor y soluciones más recientes basadas en servicios y APIs. Esta coexistencia genera fricciones técnicas al momento de implementar flujos de información oportunos y consistentes, especialmente cuando se requiere integrar datos provenientes de múltiples fuentes con distintos esquemas de actualización, latencias y capacidades de escalamiento. En este contexto, la Norma Técnica de Interoperabilidad del Estado, aprobada por el Ministerio Secretaría General de la Presidencia, junto con la Red de Interoperabilidad, operan como la capa de abstracción oficial destinada a desacoplar los sistemas internos de las instituciones de los mecanismos de intercambio, reduciendo la necesidad de modificaciones estructurales profundas en los sistemas legados y asegurando el cumplimiento de los estándares de seguridad de la información exigidos por la normativa vigente en materia de ciberseguridad.

En términos de flujos de información, se identifican tres tipologías diferenciadas, cada una sujeta a exigencias técnicas y regulatorias específicas. En primer lugar, los flujos operativos críticos, asociados a la coordinación policial y a la gestión de emergencias en el ámbito de la respuesta policial inmediata, particularmente en el entorno del CICPOL. Estos comprenden sistemas de despacho y geolocalización de patrullas, plataformas de monitoreo y teleprotección en tiempo real, así como herramientas de consulta nominada de órdenes vigentes y encargos en terreno. Dada su naturaleza, requieren intercambio de información nominada, de baja latencia y alta disponibilidad, y se encuentran sujetos a estrictos regímenes de reserva, trazabilidad y control de acceso, conforme al marco regulatorio aplicable.

En segundo lugar, los flujos tácticos y estratégicos, orientados al análisis de patrones delictuales, la planificación de recursos y la evaluación de políticas públicas, los cuales operan principalmente sobre datos agregados, históricos y anonimizados, en coherencia con las restricciones establecidas en la Ley N.º 21.730 respecto de la singularización de personas determinadas en los sistemas de análisis ministeriales.

En tercer lugar, los flujos administrativos y documentales, vinculados a la gestión de expedientes, oficios electrónicos y reportes institucionales, cuya compatibilidad técnica debe regirse por los estándares establecidos para los sistemas de gestión documental electrónica, asegurando su trazabilidad, integridad y valor legal.

La compatibilidad técnico-normativa entre estos flujos exige una clara separación de dominios funcionales, tanto a nivel lógico como de infraestructura. En particular, los sistemas analíticos no deben consumir directamente fuentes operativas nominadas, sino versiones transformadas, depuradas y sometidas a controles de anonimización y minimización de datos, conforme a lo dispuesto en la Ley N.º 19.628 sobre protección de la vida privada. Asimismo, los flujos de información deben incorporar mecanismos obligatorios de trazabilidad, control de accesos y registro de uso, en línea con las obligaciones de gobernanza y control establecidas en el Decreto Supremo N.º 55, de modo que todo acceso a la información y toda decisión basada en evidencia puedan ser auditados y reproducidos en el tiempo.

Finalmente, la compatibilidad semántica emerge como un elemento crítico para la interoperabilidad efectiva del sistema. Más allá de la conectividad técnica, el intercambio de información requiere acuerdos formales sobre definiciones comunes, catálogos de datos, taxonomías delictuales y estándares de metadatos. La construcción de un modelo de datos común de seguridad pública no constituye únicamente una necesidad técnica, sino una condición habilitante para formalizar los mecanismos y convenios de intercambio de información entre instituciones, conforme a las exigencias establecidas en el Decreto Supremo N.º 55, los cuales deben especificar con precisión los tipos de datos compartidos, sus finalidades, los estándares de transmisión aplicables y las responsabilidades institucionales asociadas.

### 1.2.2. Identificación de restricciones normativas que condicionan el intercambio de datos

El análisis de los flujos funcionales identificados en el levantamiento evidencia la existencia de restricciones normativas que inciden de manera diferenciada sobre la viabilidad de interoperabilidad del Sistema de Seguridad Pública. Estas restricciones no operan como prohibiciones generales, sino como condicionantes estructurales que delimitan los fines, modalidades y alcances posibles del intercambio de información entre instituciones.

**Restricciones asociadas al tratamiento de datos**

Una primera categoría de restricciones se relaciona con la finalidad y el alcance del tratamiento de datos personales. La normativa vigente establece que los organismos públicos sólo pueden tratar datos dentro del ámbito de sus competencias legales y para fines expresamente autorizados. En consecuencia, el análisis muestra que no todos los flujos

identificados pueden destinarse indistintamente a usos operativos, analíticos o estratégicos, sino que su articulación depende de la finalidad específica que justifica el tratamiento.

Asimismo, la prohibición general de tratar datos personales sensibles sin habilitación legal expresa constituye un límite relevante para determinados flujos, especialmente aquellos vinculados a análisis de políticas públicas o consolidaciones multifuente. En este contexto, el mandato legal que impide la singularización de personas determinadas en los sistemas de análisis ministeriales introduce una diferenciación estructural entre dominios operativos, donde puede existir tratamiento nominativo bajo condiciones específicas, y dominios analíticos, que deben operar sobre datos agregados o anonimizados.

La coexistencia de estos dominios funcionales emerge como una condición normativa que estructura la arquitectura posible del sistema, en la medida en que no todos los flujos pueden integrarse bajo un mismo régimen de tratamiento de datos.

**Restricciones de acceso y uso de la información**

El análisis también evidencia que el acceso a la información se encuentra jurídicamente segmentado por funciones, competencias y principio de necesidad de conocer. Esta segmentación impide concebir el Sistema de Información como un entorno de acceso irrestricto y condiciona el diseño de mecanismos de interoperabilidad a esquemas diferenciados de perfiles y atribuciones.

Adicionalmente, el régimen de secreto y confidencialidad aplicable a información no pública, incluyendo antecedentes vinculados a investigaciones penales o materias de inteligencia, introduce límites específicos para ciertos flujos identificados, particularmente aquellos asociados a coordinación operativa o intercambio en tiempo real.

En el levantamiento realizado se observan prácticas de intercambio mediante soportes documentales y canales no sistémicos que dificultan la implementación de controles granulares de acceso y trazabilidad. Estas prácticas evidencian tensiones entre las exigencias normativas de segmentación y los mecanismos actualmente utilizados para el intercambio de información.

**Restricciones derivadas de la autonomía institucional**

Una tercera categoría de restricciones se vincula con la estructura institucional del sistema. Si bien la interoperabilidad constituye un mandato legal, su implementación depende de la suscripción de convenios o protocolos interinstitucionales que definan fundamentos jurídicos, finalidades, tipos de datos y responsabilidades de custodia.

En el caso de órganos constitucionalmente autónomos, como el Ministerio Público y las municipalidades, el análisis muestra que la interoperabilidad se encuentra condicionada por su autonomía institucional. La participación efectiva de estos organismos en determinados flujos depende de acuerdos formales, lo que configura una variable jurídica externa al diseño técnico del sistema.

En consecuencia, la viabilidad de interoperabilidad no depende exclusivamente de capacidades tecnológicas, sino también de condiciones jurídico-institucionales que deben ser consideradas en la planificación del sistema.

**Restricciones asociadas a seguridad y trazabilidad**

Finalmente, el marco normativo impone exigencias reforzadas en materia de seguridad de la información, incluyendo confidencialidad, integridad, disponibilidad y trazabilidad. Estas exigencias operan como condiciones estructurales para la interoperabilidad, particularmente en flujos que involucran información sensible o nominada.

El levantamiento evidencia que ciertos mecanismos actualmente utilizados para el intercambio y análisis, como el uso de archivos extraídos o canales no sistémicos, presentan limitaciones para cumplir plenamente con estos estándares de control y auditoría. Esta constatación permite identificar ámbitos donde la compatibilidad normativa no se agota en la habilitación legal del intercambio, sino que se vincula también con las condiciones técnicas bajo las cuales éste se materializa.

En conjunto, estas categorías de restricciones muestran que la interoperabilidad del Sistema no enfrenta un único tipo de límite normativo, sino un conjunto diferenciado de condicionantes que varían según finalidad, tipo de dato, régimen institucional y nivel de sensibilidad de la información. Con el objeto de sistematizar esta heterogeneidad y evaluar la viabilidad técnica y jurídica de cada intercambio identificado, se procedió a la construcción de una Matriz de Interoperabilidad Técnico-Normativa, cuyos resultados se presentan a continuación.

### 1.2.3. Construcción y validación de la matriz técnico-normativa

La aplicación de la Matriz de Interoperabilidad Técnico-Normativa sobre el inventario institucional permitió identificar y caracterizar trece flujos funcionales críticos que estructuran actualmente el intercambio de información en el Sistema. El análisis de estos flujos evidencia que la interoperabilidad del sistema no es homogénea, sino que presenta grados diferenciados de viabilidad técnica y normativa, determinados por la finalidad del tratamiento, el tipo de datos involucrados y el marco institucional en el que se producen los intercambios.

En primer lugar, se constata una alta diversidad de flujos distribuidos en dominios analíticos, operativos, documentales y regulatorios. Esta diversidad implica que las exigencias normativas aplicables no son uniformes, sino que varían según la finalidad del uso de la información y el rol institucional de las unidades que participan en cada flujo. En este sentido, el análisis muestra que coexisten flujos orientados a funciones regulatorias y de fiscalización, que requieren resguardos reforzados de custodia administrativa, con flujos operativos que demandan disponibilidad continua y controles estrictos de acceso para su uso en tiempo real.

En segundo término, el análisis evidencia que un conjunto relevante de flujos no enfrenta impedimentos normativos estructurales para su articulación, siempre que se respeten las exigencias legales relativas a finalidad, deber de secreto, trazabilidad y control de accesos. En estos casos, las principales tensiones identificadas no derivan del marco normativo vigente, sino de prácticas operativas asociadas al tratamiento posterior de la información, particularmente cuando el análisis se realiza a partir de extracciones fuera de los sistemas

fuente. Estos flujos presentan condiciones favorables para avanzar en interoperabilidad mediante la formalización de estándares técnicos y mecanismos de gobernanza, sin requerir modificaciones legales.

No obstante lo anterior, la matriz identifica un conjunto significativo de flujos cuya interoperabilidad se encuentra condicionada por restricciones normativas específicas o por dependencias institucionales externas. En estos casos, aun existiendo capacidades técnicas para el intercambio de información, la articulación efectiva se encuentra subordinada a la autonomía de órganos externos al Ministerio de Seguridad Pública. El análisis muestra que, para estos flujos, el principal habilitador de interoperabilidad no es tecnológico, sino jurídico-institucional, requiriéndose la formalización de convenios, protocolos y reglas claras de custodia y uso de la información.

Asimismo, se identifican flujos cuya integración se ve limitada por barreras estructurales asociadas al uso de canales no sistémicos, soportes físicos o formatos legados para la transferencia de información sensible. Estas prácticas restringen de manera significativa las posibilidades de interoperabilidad bajo estándares adecuados de seguridad, trazabilidad y control, configurando situaciones en las que resulta necesario abordar previamente transformaciones en los procesos de intercambio antes de considerar su integración al Sistema Integrado de Información.

Un resultado transversal del análisis es la identificación de tensiones recurrentes entre eficiencia operativa y resguardo normativo, particularmente en flujos que requieren información oportuna y, en algunos casos, nominada. El análisis muestra que estas tensiones evidencian la necesidad de decisiones de diseño institucional, tales como la segregación de entornos funcionales, la diferenciación de flujos según finalidad y la implementación de mecanismos reforzados de trazabilidad, control y auditoría.

En su conjunto, estos resultados permiten establecer una línea base clara sobre el estado actual de la interoperabilidad en el Sistema, identificando ámbitos con condiciones favorables para avances inmediatos, áreas que requieren definiciones adicionales de gobernanza y situaciones que demandan transformaciones estructurales de mayor alcance. Estos hallazgos constituyen un insumo directo para orientar las decisiones de diseño, priorización y evolución del Sistema Integrado de Información, en coherencia con el marco normativo vigente, la protección de los datos y la autonomía de las instituciones que integran el sistema.

## 1.3. Definición de estándares de interoperabilidad, seguridad y calidad de datos aplicables al Sistema Integrado de Información

**Propósito del apartado y alcance de los estándares**

La puesta en marcha del Sistema Integrado de Información del Ministerio de Seguridad Pública exige la definición explícita de estándares técnicos, operacionales y de gobernanza que aseguren la coherencia, la seguridad y la confiabilidad del ecosistema de información que el Ministerio articula. Estos estándares constituyen el marco estructural que deberá orientar el diseño e implementación del sistema, permitiendo que sistemas, plataformas y

bases de datos heterogéneas, desarrolladas bajo lógicas institucionales diversas y marcos normativos diferenciados, puedan operar de manera coordinada como parte de un esquema integrado.

A partir del marco normativo vigente y del diagnóstico del ecosistema informacional desarrollado en los apartados precedentes, se hace necesario delimitar ámbitos concretos de estandarización que permitan abordar de manera sistemática las brechas identificadas y viabilizar una interoperabilidad efectiva, segura y sostenible. En este contexto, el propósito del presente apartado es identificar los dominios críticos en los que el Ministerio deberá establecer definiciones comunes, con el objeto de asegurar coherencia técnica, protección adecuada de la información, trazabilidad operativa y articulación interinstitucional.

En coherencia con este enfoque, el presente apartado no define tecnologías cerradas ni soluciones de implementación específicas, ni anticipa una configuración arquitectónica determinada. Su objetivo es fijar criterios y condiciones que orienten el diseño del sistema, asegurando consistencia con el marco normativo, con las restricciones estructurales identificadas y con las capacidades institucionales efectivamente existentes.

**Síntesis del estado actual que fundamenta la estandarización**

El diagnóstico realizado evidencia que la interoperabilidad en el Ministerio de Seguridad Pública y en CICPOL se desarrolla actualmente en un entorno fragmentado, caracterizado por integraciones parciales, mecanismos heterogéneos de intercambio y distintos niveles de madurez tecnológica entre instituciones. Persisten limitaciones asociadas a la ausencia de estándares comunes a nivel ministerial, a la dependencia de procesos manuales o semiautomatizados y a brechas en gobernanza transversal que dificultan la articulación sistemática de flujos de información y la consolidación de capacidades integradas de análisis y apoyo a la toma de decisiones.

Adicionalmente, la materialización del mandato de interoperabilidad debe compatibilizar exigencias estrictas de protección de datos personales y de seguridad de la información con la autonomía institucional de los actores participantes, en particular tratándose de órganos con estatutos jurídicos propios cuya participación en esquemas de intercambio requiere resguardar competencias, responsabilidades y custodias en origen.

Sobre la base de este escenario, los lineamientos que se presentan a continuación establecen condiciones estructurales que deberá cumplir el Sistema Integrado de Información en materia de interoperabilidad, seguridad y calidad de datos. Estos estándares no constituyen una solución en sí mismos, sino un marco de referencia que delimita y ordena las decisiones de diseño posteriores, asegurando coherencia con el diagnóstico realizado y con las exigencias normativas aplicables al Sistema de Seguridad Pública.

### 1.3.1. Estándares de interoperabilidad

La interoperabilidad constituye una condición estructural para la integración de los sistemas de información que conforman el ecosistema del Ministerio de Seguridad Pública, en la medida en que determina la capacidad de plataformas heterogéneas de intercambiar información de manera segura, trazable y sostenible en el tiempo. No se trata únicamente de

un atributo técnico, sino de un requisito organizacional y normativo que habilita la coordinación efectiva entre instituciones con competencias diferenciadas.

En el marco del Estado, esta interoperabilidad debe alinearse con la Norma Técnica de Interoperabilidad, aprobada mediante el Decreto N° 12 de 2023 del Ministerio Secretaría General de la Presidencia, la cual establece estándares y herramientas para el intercambio de datos y documentos electrónicos entre órganos de la Administración del Estado. Esta normativa define principios, obligaciones y mecanismos que orientan la exposición y el consumo de servicios de información bajo criterios de seguridad, trazabilidad y control.

Un componente central de esta normativa es la Red de Interoperabilidad, concebida como el estándar de intercambio de información entre organismos del Estado y llamada a sustituir progresivamente los mecanismos de integración basados en la PISEE en su versión original, consolidando su operación bajo el modelo actualizado de Red de Interoperabilidad (PISEE 2.0), conforme al régimen transitorio establecido. La Red opera sobre la base de Nodos de Interoperabilidad alojados en cada institución, que actúan como puntos seguros de intercambio y deben garantizar la encriptación de mensajes, la autenticación mutua mediante certificados digitales y el registro de trazabilidad en tiempo real. Complementariamente, la Guía Técnica de Interoperabilidad profundiza en los aspectos operativos y en los procedimientos para la inscripción de servicios en el Catálogo de Interoperabilidad, instrumento que permite a las instituciones publicar los datos que exponen y las condiciones técnicas bajo las cuales estos pueden ser consumidos.

Sobre esta base normativa y técnica, el Sistema Integrado de Información deberá estructurar sus mecanismos de intercambio de información conforme a estándares que aseguren consistencia en las integraciones, reduzcan dependencias específicas entre plataformas y permitan una evolución ordenada del ecosistema institucional. Estos lineamientos establecen criterios comunes para el diseño y operación de las integraciones, en coherencia con el marco regulatorio vigente y con las restricciones estructurales previamente identificadas. A continuación, se describen los principales aspectos técnicos que deberán considerarse en esta materia.

**a) Protocolos de Conectividad para Consultas**

El Sistema Integrado de Información deberá contemplar mecanismos estandarizados de conexión entre el componente encargado de realizar consultas y los sistemas de información de las instituciones participantes, permitiendo ejecutar consultas y obtener resultados susceptibles de integrarse en respuestas consolidadas. Considerando la diversidad de tecnologías de bases de datos empleadas por los órganos del Estado, resulta necesario definir protocolos comunes que orienten la exposición y consumo de fuentes de datos.

Como referencia técnica, el protocolo JDBC constituye un estándar ampliamente adoptado para la conectividad con bases de datos relacionales y presenta altos niveles de compatibilidad con tecnologías actualmente en uso en el sector público. En este contexto, cuando la infraestructura institucional lo permita, se deberá favorecer la exposición de fuentes de datos mediante conectores compatibles con este tipo de estándar, de manera que el componente de consulta pueda establecer conexiones bajo criterios homogéneos, independientemente de la tecnología subyacente.

En aquellos casos en que el acceso directo a la base de datos no resulte factible por restricciones técnicas, de seguridad o de arquitectura institucional, podrán utilizarse interfaces de servicios REST como mecanismo alternativo de consulta. Dichas interfaces deberán ajustarse a especificaciones técnicas comunes definidas a nivel ministerial, incluyendo formatos de solicitud y respuesta, esquemas de autenticación y criterios de manejo de errores. Este enfoque permite mantener flexibilidad tecnológica en las instituciones participantes, resguardando al mismo tiempo coherencia y control en los mecanismos de intercambio de información.

**b) Esquemas de Datos y Versionamiento**

Los sistemas de información de las instituciones del Estado evolucionan de manera permanente en respuesta a nuevos requerimientos operativos, modificaciones normativas o mejoras tecnológicas. Esta evolución suele traducirse en cambios en las estructuras de datos, incorporación de nuevos campos, modificación de tipos de datos, renombrado de columnas o reestructuración de tablas completas. En un entorno de integración interinstitucional, donde un componente central interactúa con múltiples sistemas institucionales, cualquier modificación no coordinada en los esquemas de datos puede provocar fallas en las consultas, interrumpir procesos críticos y afectar la continuidad del servicio.

En este contexto, la gestión ordenada de los esquemas de datos debe constituir un requisito estructural del Sistema Integrado. La ausencia de mecanismos formales de registro, notificación y transición expone al sistema a fallas imprevistas cada vez que una institución modifica la estructura de sus datos, generando una fragilidad operativa incompatible con las exigencias de un sistema de información en materia de seguridad pública.

El Sistema Integrado deberá contemplar la existencia de un catálogo de datos que consolide la información estructural de las fuentes expuestas para fines de integración. Las instituciones participantes deberán registrar en dicho catálogo las estructuras de las tablas y campos que pongan a disposición, documentando al menos el nombre del elemento, su tipo de dato, su descripción funcional y las restricciones aplicables. Esta documentación deberá mantenerse actualizada y sincronizada con el estado real de los sistemas, incorporando oportunamente cualquier modificación planificada.

Asimismo, la evolución de los esquemas deberá orientarse hacia la compatibilidad hacia atrás, privilegiando modificaciones que no interrumpan las integraciones existentes. La incorporación de nuevas columnas o tablas, en la medida en que no altere estructuras previamente consumidas, no debería afectar la operación de las consultas vigentes. En cambio, las modificaciones que alteren la compatibilidad, tales como el cambio de tipo de dato en una columna, el renombrado de campos o la eliminación de estructuras existentes, deberán considerar períodos de transición, previamente definidos al momento de planificar el cambio incompatible. Como referencia operativa, podría establecerse un plazo mínimo de noventa días durante el cual se mantengan disponibles tanto el esquema anterior como el nuevo, permitiendo la adaptación progresiva de los procesos asociados.

Este enfoque de gestión de esquemas contribuye a reducir fallas inesperadas en los sistemas consumidores, evita dependencias rígidas entre instituciones y favorece una evolución ordenada del ecosistema informacional. Asimismo, fortalece las bases de un gobierno de

datos consistente con las exigencias técnicas, normativas y operativas propias del Sistema de Seguridad Pública.

**c) Acuerdos de Nivel de Servicio (*Service Level Agreement*, SLA)**

En un entorno de integración interinstitucional, los resultados consolidados dependen del funcionamiento coordinado de múltiples sistemas pertenecientes a distintas instituciones. En consecuencia, la disponibilidad, el rendimiento y la estabilidad de cada fuente de datos inciden directamente en la confiabilidad del servicio integrado. Bajo esta lógica, el Sistema Integrado deberá contemplar la formalización de Acuerdos de Nivel de Servicio entre el Ministerio y cada institución participante, con el objeto de definir condiciones mínimas de operación para los sistemas cuyos datos sean expuestos para fines de integración.

Estos acuerdos deberán establecer compromisos explícitos en dimensiones tales como disponibilidad, rendimiento y capacidad operativa. En materia de disponibilidad, como referencia técnica, podría considerarse que las fuentes de datos apunten a niveles cercanos al 99% mensual, equivalente a un tiempo máximo de indisponibilidad no programada aproximado de siete horas en dicho período. En cuanto a rendimiento, los tiempos máximos de respuesta deberán definirse de manera diferenciada según la naturaleza y complejidad de las consultas, considerando las características técnicas de cada sistema. En relación con la capacidad, cada institución deberá declarar el volumen estimado de consultas concurrentes que su infraestructura puede soportar, permitiendo dimensionar adecuadamente la demanda y gestionar la carga de forma coherente.

Asimismo, deberán establecerse reglas claras para la gestión de mantenimientos programados e indisponibilidades no planificadas. A modo orientativo, podría requerirse la comunicación previa de ventanas de mantenimiento con una antelación mínima, por ejemplo, de setenta y dos horas, indicando la duración estimada y los servicios afectados. Los eventos de indisponibilidad no programada deberán ser informados oportunamente, activando mecanismos de gestión de incidentes previamente definidos.

El Sistema Integrado deberá contar además con mecanismos de monitoreo que permitan observar la disponibilidad y el rendimiento de las fuentes de información. Las métricas obtenidas podrán compartirse periódicamente con las instituciones participantes, no sólo con fines de control, sino también como insumo para procesos de mejora continua y ajuste progresivo de los niveles de servicio.

En este marco, los Acuerdos de Nivel de Servicio se configuran como un instrumento de gobernanza operativa que permite alinear expectativas, reducir incertidumbre y asegurar condiciones mínimas de confiabilidad en un entorno interinstitucional caracterizado por altos niveles de interdependencia.

**d) Capacidades de Consulta SQL**

En un entorno de integración de datos entre múltiples instituciones, el componente encargado de ejecutar consultas deberá interactuar con sistemas de bases de datos que operan sobre tecnologías heterogéneas y que presentan variaciones en los dialectos SQL soportados. Esta diversidad introduce riesgos de incompatibilidad sintáctica o funcional que pueden afectar la estabilidad y previsibilidad de las integraciones. En consecuencia, resulta necesario definir un

marco común de capacidades de consulta que establezca un nivel mínimo de compatibilidad entre sistemas.

Como referencia técnica, podría adoptarse como línea base un subconjunto de funcionalidades alineado con el estándar SQL:2016 que presente alto nivel de compatibilidad entre los sistemas de bases de datos más utilizados en el ecosistema institucional. Este subconjunto debería incluir, al menos:

- Operaciones de Consulta: Sentencias básicas de selección, filtrado y ordenamiento.
- Agregación de Datos: Funciones estándar como COUNT, SUM, AVG, MIN y MAX.
- Lógica y Comparación: Operadores aritméticos, lógicos (AND, OR, NOT) y de comparación (=, <>, <, >).
- Relaciones: Capacidad de ejecutar uniones básicas, específicamente INNER JOIN y LEFT JOIN.
- Subconsultas: Soporte para subconsultas simples
- Manipulación de Tipos: Funciones comunes para el manejo de cadenas de texto y fechas.

En coherencia con lo anterior, el Sistema Integrado deberá disponer de un catálogo que registre, para cada fuente de datos expuesta, el sistema de base de datos empleado, su nivel de alineación con el subconjunto SQL definido y las eventuales limitaciones técnicas que puedan afectar la ejecución de determinadas consultas. Este registro permitirá diseñar consultas de manera predecible, transparentar restricciones técnicas y reducir dependencias específicas entre los sistemas proveedores de datos y el componente de integración.

El componente de consulta deberá generar sintaxis compatible con el subconjunto común definido, evitando desarrollos específicos por tecnología y facilitando la incorporación progresiva de nuevas fuentes de información. La estandarización de capacidades mínimas de consulta constituye, en este sentido, una condición relevante para la escalabilidad, mantenibilidad y sostenibilidad del sistema en el tiempo.

### 1.3.2. Estándares de seguridad

La naturaleza crítica y sensible de la información gestionada en el ámbito de la seguridad pública exige la adopción de estándares de seguridad rigurosos que garanticen la confidencialidad, integridad, disponibilidad y trazabilidad de los datos, tanto en su almacenamiento como durante su transmisión entre instituciones. Estos estándares constituyen una condición estructural del Sistema Integrado de Información y deben incorporarse de manera transversal en su diseño y operación.

En el marco del Estado, tales exigencias deben alinearse con la Norma Técnica de Seguridad de la Información y Ciberseguridad, aprobada mediante el Decreto N° 7 de 2023, que establece las obligaciones aplicables a los órganos de la Administración en materia de protección de activos de información. Esta normativa dispone la adopción de una Política de Seguridad de la Información institucional y organiza la gestión de ciberseguridad en cinco funciones fundamentales: identificación de activos, protección de accesos y perímetros, detección de incidentes mediante monitoreo continuo, respuesta ante eventos de seguridad y recuperación de capacidades.

En un entorno de integración interinstitucional, estas exigencias no pueden limitarse a la infraestructura de un solo organismo, sino que deben extenderse a toda la cadena de intercambio de información, abarcando los mecanismos de conectividad, los sistemas que exponen datos y los componentes que los consumen. Ello implica asegurar controles robustos de autenticación, esquemas de gestión de accesos basados en riesgo, mecanismos de auditoría y trazabilidad, y procedimientos formales de gestión de incidentes que permitan verificar y resguardar el uso adecuado de la información intercambiada.

Sobre esta base normativa y funcional, el Sistema Integrado deberá contemplar estándares específicos de seguridad aplicables a sus distintos componentes, incluyendo conectividad segura, clasificación y protección de datos, gestión de identidades y administración de credenciales. Estos elementos se desarrollan en los apartados siguientes.

**a) Conectividad y Cifrado en Tránsito**

Las consultas y mecanismos de intercambio de información suponen la transmisión de datos entre el Ministerio y las instituciones participantes a través de redes de comunicación. La protección de esta información durante su tránsito constituye una exigencia estructural del Sistema Integrado, dado que la interceptación, alteración o suplantación de comunicaciones podría comprometer antecedentes sensibles vinculados a la seguridad pública.

En este contexto, el Sistema Integrado deberá establecer mecanismos de conectividad que aseguren enlaces cifrados y autenticados entre el Ministerio y cada institución participante, considerando la heterogeneidad de arquitecturas tecnológicas existentes y las restricciones operativas propias de cada organismo. La definición de estos mecanismos deberá orientarse a minimizar la superficie de exposición, garantizar la integridad de las comunicaciones y asegurar la trazabilidad de las interacciones entre sistemas.

**Túneles Zero Trust**

Como criterio de diseño, los mecanismos de conectividad deberán alinearse con el paradigma de confianza cero (Zero Trust) (Yeoh et al., 2023), conforme al cual ningún actor, sistema o red es considerado confiable por defecto, independientemente de su ubicación dentro o fuera del perímetro institucional. Este enfoque desplaza la confianza implícita en la red hacia la verificación explícita y continua de cada interacción.

Bajo este principio, cada conexión entre el Ministerio y las instituciones participantes deberá establecerse mediante autenticación robusta, cifrado extremo a extremo y registro de trazabilidad, aplicando el criterio de mínimo privilegio en la asignación de accesos. Toda interacción entre sistemas deberá ser auditada y atribuible, permitiendo identificar de manera precisa el origen, el destino y las condiciones de cada intercambio.

La implementación de túneles seguros bajo este paradigma permite exponer fuentes de información sin requerir su publicación directa en redes públicas, estableciendo canales cifrados y autenticados entre los componentes encargados de realizar consultas y los sistemas institucionales que proveen datos. Este diseño reduce la superficie de exposición, desacopla las integraciones de configuraciones perimetrales específicas y facilita una

integración coherente en un ecosistema interinstitucional con niveles heterogéneos de madurez tecnológica.

En este marco, cada institución deberá mantener el control sobre sus sistemas y desplegar los componentes necesarios dentro de su propia infraestructura, ajustándose a los protocolos comunes definidos para la interoperabilidad segura y resguardando la custodia institucional de la información.

**Mecanismo Alternativo: Redes Privadas Virtuales (VPN)**

Las redes privadas virtuales de tipo site-to-site constituyen una alternativa técnicamente válida para establecer conectividad segura entre instituciones. Una VPN permite configurar un túnel cifrado entre las redes del Ministerio y de la institución participante, habilitando la comunicación entre sistemas como si formaran parte de un mismo entorno de red local.

No obstante, la experiencia acumulada en el ecosistema institucional del Estado indica que las VPN presentan limitaciones relevantes para un despliegue a escala. Su configuración e integración suelen requerir coordinación estrecha entre equipos de redes de ambas instituciones, definición de rangos de direcciones IP, ajustes en reglas de firewall y resolución de eventuales conflictos de direccionamiento. Además, la adopción de infraestructura VPN es heterogénea entre los órganos del Estado, y no todas las instituciones disponen de capacidades técnicas o recursos suficientes para su administración sostenida.

En este contexto, las VPN pueden considerarse un mecanismo aceptable en aquellos casos en que la institución ya cuente con infraestructura consolidada y capacidades operativas para su gestión. Sin embargo, no deberían constituir el mecanismo ordinario de conectividad del Sistema Integrado. Su utilización deberá evaluarse caso a caso, particularmente en escenarios donde no resulte viable implementar los mecanismos de conectividad definidos como referencia principal.

**Mecanismo Alternativo: Exposición Directa**

Desde una perspectiva técnica, los motores de bases de datos actuales permiten establecer conexiones cifradas mediante protocolos como TLS y mecanismos de autenticación basados en certificados digitales. Ello hace posible, en términos estrictamente tecnológicos, habilitar conexiones directas entre sistemas sin recurrir a túneles dedicados o redes privadas virtuales.

Sin embargo, la exposición directa de servicios en redes públicas incrementa la superficie de ataque y puede generar riesgos asociados a intentos de denegación de servicio (DDoS), exploración automatizada de vulnerabilidades u otros incidentes de seguridad. Tratándose de información vinculada a la seguridad pública, este tipo de configuración debe evaluarse bajo criterios especialmente restrictivos y en el marco de una gestión formal de riesgos.

En consecuencia, la exposición directa no debería constituir el mecanismo ordinario de interoperabilidad. En aquellos casos en que se estime técnicamente viable y necesario, su implementación deberá complementarse con capas adicionales de protección, tales como controles de acceso reforzados, monitoreo continuo, mecanismos de detección y mitigación de ataques, y procedimientos formales de validación técnica e institucional previos a su habilitación.

**Mecanismo Alternativo: Desarrollo de Adaptadores Ad-Hoc**

Desde una perspectiva técnica, es posible desarrollar integraciones específicas para aquellas instituciones que no cumplan plenamente con los protocolos definidos para el Sistema Integrado. Sin embargo, este tipo de desarrollos debe considerarse excepcional y no como una práctica ordinaria de integración.

La estandarización constituye un principio estructural del diseño del sistema, en la medida en que favorece la escalabilidad, la seguridad, la mantenibilidad y el control de la complejidad a lo largo del tiempo. La implementación de adaptadores particulares para cada institución tiende a fragmentar el ecosistema, incrementar la deuda técnica, generar dependencias rígidas y elevar los costos asociados al soporte y a la evolución futura del sistema.

En consecuencia, la regla general debe orientarse a la alineación progresiva de las instituciones participantes con los estándares de interoperabilidad definidos. El desarrollo de soluciones a la medida sólo debiera evaluarse en situaciones debidamente justificadas, cuando no exista una alternativa técnica viable dentro del marco común establecido.

Con independencia del mecanismo de conectividad adoptado, todas las conexiones del Sistema Integrado deberán operar bajo esquemas de autenticación mutua mediante certificados digitales (mTLS), asegurando la verificación recíproca de identidad entre las partes, la integridad de la comunicación y la trazabilidad completa de cada interacción.

**b) Clasificación y Protección de Datos**

El diseño de seguridad del Sistema Integrado deberá establecer una distinción estructural entre la clasificación de la información y la autorización de acceso. Mientras la autorización constituye el permiso técnico que habilita a un usuario para consultar un recurso determinado, la clasificación corresponde a un atributo propio del dato que define su nivel de sensibilidad y, en consecuencia, determina las exigencias de protección y el deber de resguardo asociado a su tratamiento.

La clasificación no sustituye los mecanismos de control de acceso, sino que los complementa. Su función es explicitar la criticidad de la información y establecer el marco de restricciones que rige su almacenamiento, circulación, uso y eventual divulgación, una vez que el acceso ha sido otorgado conforme a las competencias legales del usuario.

Con este propósito, el Sistema Integrado deberá contemplar un esquema de clasificación estructurado en cuatro niveles:

- **Nivel Público:** Corresponde a información cuya divulgación no genera riesgos jurídicos ni operativos, y que puede ser difundida sin restricciones adicionales. Incluye, por ejemplo, estadísticas agregadas o antecedentes publicados en cumplimiento de obligaciones de transparencia activa.

- **Nivel Uso Interno:** Corresponde a información destinada al funcionamiento ordinario de las instituciones, cuya difusión externa no se encuentra autorizada por su naturaleza administrativa u operativa. Su circulación deberá limitarse a funcionarios y

equipos que requieran acceder a ella en el ejercicio de sus funciones.

- **Nivel Reservado:** Corresponde a información protegida por disposiciones legales específicas, incluyendo datos personales, antecedentes de investigaciones u otra información sujeta a deber de confidencialidad. El acceso a este nivel implica obligaciones legales explícitas de resguardo y restricciones estrictas de divulgación.

- **Nivel Secreto:** Corresponde a información cuya divulgación no autorizada puede comprometer gravemente la seguridad pública, la integridad de personas o el éxito de operaciones institucionales. Su tratamiento deberá sujetarse a los más altos estándares de protección, con restricciones reforzadas de acceso, almacenamiento y transmisión.

La adopción de un esquema de clasificación como el descrito permite aplicar medidas de seguridad proporcionales al nivel de riesgo, asegurar coherencia entre sensibilidad del dato y condiciones de acceso, y alinear la gestión de la información con el marco normativo vigente en materia de seguridad y protección de datos.

**c) Gestión de Identidad y Autorización de Acceso**

Complementariamente al esquema de clasificación de la información, el Sistema Integrado deberá estructurar su modelo de autorización sobre la base del principio de mínimo privilegio. La validación de una credencial no deberá habilitar acceso general al conjunto de datos disponibles, sino únicamente a aquellos recursos que resulten estrictamente necesarios para el cumplimiento de la función específica asignada al usuario.

El esquema de acceso deberá operar bajo la lógica de la necesidad de conocer, definiendo perfiles de acceso en función de roles institucionales, competencias legales y responsabilidades efectivas. En consecuencia, el sistema deberá discriminar técnicamente el tipo y nivel de información accesible según la labor que desempeñe el funcionario, asegurando coherencia entre atribuciones normativas y permisos operativos.

En aquellos casos en que un usuario requiera realizar análisis estadísticos, seguimiento de gestión u otras funciones de carácter analítico, el sistema deberá privilegiar la provisión de información agregada, anonimizada o seudonimizada, limitando el acceso a datos nominados o altamente sensibles cuando estos no resulten indispensables para la finalidad declarada. Este enfoque reduce la exposición innecesaria de información crítica y refuerza la consistencia entre sensibilidad del dato, rol del usuario y condiciones de acceso autorizadas.

**d) Gestión de Credenciales y Confidencialidad**

El Sistema Integrado deberá contemplar un mecanismo formal para el almacenamiento y administración segura de credenciales de acceso a bases de datos, claves de cifrado, certificados digitales y otros elementos sensibles cuya exposición pudiera comprometer la seguridad del ecosistema informacional en su conjunto.

Como principio de diseño, deberá implementarse un sistema de gestión de secretos que almacene estas credenciales de manera cifrada y que proporcione acceso controlado y auditado exclusivamente a los componentes que requieran utilizarlas para fines operativos.

En ningún caso las credenciales deberán mantenerse en texto plano ni estar accesibles directamente por usuarios finales o incorporadas en código fuente, archivos de configuración u otros repositorios sin protección.

Asimismo, deberá definirse una política de rotación periódica de credenciales, diferenciando entre accesos administrativos y cuentas de servicio automatizadas. A modo referencial, podrán considerarse ciclos de rotación del orden de noventa días para accesos administrativos y de ciento ochenta días para credenciales asociadas a servicios, ajustables en función de la evaluación de riesgos y de las exigencias normativas aplicables.

Todo acceso al sistema de gestión de secretos deberá quedar registrado en mecanismos de auditoría trazables. Además, deberán establecerse procedimientos formales de revocación inmediata ante sospecha de compromiso, pérdida o uso indebido de credenciales, con el fin de reducir la ventana de exposición y resguardar la continuidad operativa del Sistema Integrado.

### 1.3.3. Estándares de calidad de datos

La utilidad del Sistema Integrado depende de manera directa de la calidad de los datos que lo alimentan. Información incompleta, desactualizada, inconsistente o incorrecta compromete la validez de los análisis y puede derivar en decisiones deficientes en un ámbito particularmente sensible como la seguridad pública. En consecuencia, el Sistema Integrado deberá establecer estándares mínimos de calidad que las fuentes de información deberán cumplir para asegurar confiabilidad, trazabilidad y coherencia en la información integrada.

**a) Documentación y Metadatos**

Los datos que carecen de documentación adecuada resultan difíciles de interpretar correctamente, generando ambigüedad respecto de su significado, unidades de medida, códigos utilizados o metodologías de cálculo. Esta ambigüedad puede conducir a interpretaciones erróneas y a la elaboración de análisis no comparables entre instituciones.

Por ello, cada institución debería documentar formalmente las fuentes de datos que exponga al sistema, incluyendo al menos:

- Descripción general de la base de datos y su propósito
- Descripción de las tablas, incluyendo su contenido
- Descripción de las columnas incluyendo su definición de negocio y tipo de dato y unidad de medida cuando corresponda
- Documentación de los códigos utilizados, incluyendo su significado
- Identificación del área responsable de la fuente de datos y del contacto técnico para consultas

Esta información deberá registrarse en el catálogo de datos que sirva de soporte al sistema, el cual deberá permitir la búsqueda, consulta y comprensión previa de las fuentes disponibles antes de su utilización.

Asimismo, cada institución deberá designar formalmente uno o más responsables de datos (data stewards), encargados de mantener actualizada la documentación, validar cambios estructurales y actuar como contraparte técnica frente a consultas relativas al significado, calidad o disponibilidad de la información.

# 2. Diseño técnico detallado del sistema federado

Este capítulo desarrolla la propuesta arquitectónica que surge del diagnóstico normativo, técnico y de interoperabilidad presentado en el Capítulo 1. A partir de las restricciones identificadas, en particular la autonomía institucional, los límites legales al tratamiento de datos personales y la necesidad de integración multifuente con trazabilidad, se adopta una arquitectura de carácter federado como solución estructural para el Sistema Integrado de Información.

El objetivo es traducir esta definición arquitectónica en una especificación técnica operativa, describiendo la estructura del nodo articulador del Ministerio, la delimitación de los dominios de datos y la implementación de los flujos de consulta, seguridad, auditoría y operación continua. Se detallan componentes, procesos y requerimientos verificables, manteniendo neutralidad tecnológica y coherencia con el marco normativo vigente.

En el Capítulo 2.1 se presenta el modelo conceptual del Ministerio de Seguridad Pública como nodo articulador central, incluyendo la definición de los dominios de datos y el principio de custodia de la información en su institución de origen.

El Capítulo 2.2 describe la modelación operativa del sistema, detallando los flujos de consulta, las reglas de visibilidad y control de acceso, y la arquitectura conceptual que soporta la integración multifuente, la trazabilidad y la entrega unificada de resultados a usuarios autorizados.

El Capítulo 2.3 establece los requerimientos técnicos del sistema, abarcando componentes funcionales y no funcionales, criterios de seguridad, continuidad operativa y desempeño, así como la lógica de expansión modular para integrar progresivamente nuevas instituciones al ecosistema.

## 2.1. Modelo conceptual de federación del MSP

El modelo conceptual define al Ministerio de Seguridad Pública como nodo articulador central del ecosistema de información del Sistema de Seguridad Pública. Esta configuración establece un punto único de coordinación para garantizar interoperabilidad, seguridad de la información sensible y disponibilidad continua para la toma de decisiones estratégicas, en un entorno caracterizado por la coexistencia de múltiples sistemas institucionales.

El modelo se estructura en torno a tres capacidades esenciales para superar las limitaciones de una arquitectura descentralizada. En primer lugar, consolida la gestión de los datos bajo custodia directa del Ministerio mediante un Data Lake y un Data Warehouse unificados, orientados a la integración, almacenamiento y explotación analítica de información institucional. En segundo lugar, habilita mecanismos de interoperabilidad que permiten

consultar fuentes externas respetando la soberanía y custodia de los datos en sus instituciones de origen, evitando la duplicación innecesaria de información. Finalmente, incorpora un marco de gobernanza transversal, apoyado en un catálogo de datos institucional, que asegura el control, la trazabilidad y el uso legítimo de la información en todo el ecosistema.

Un aspecto fundamental es la neutralidad tecnológica de la arquitectura, descrita en términos de capacidades estándar implementables en cualquier plataforma de nube pública, ya sea Amazon Web Services, Microsoft Azure o Google Cloud Platform, así como en configuraciones híbridas o multi-nube. Esta neutralidad reduce la dependencia de proveedores específicos, facilita la gestión contractual y mantiene la flexibilidad necesaria para adaptar el motor de consultas y los componentes de almacenamiento ante cambios en las políticas de contratación pública.

Desde el punto de vista operativo, el modelo se articula en torno a un motor de consultas integrado capaz de gestionar los dos grandes dominios de datos identificados: los centralizados y aquellos mantenidos por otras instituciones del Sistema. Este componente actúa como punto único de acceso para los usuarios autorizados, consolidando información proveniente de múltiples fuentes bajo reglas uniformes de visibilidad, control de acceso y auditoría. De este modo, se habilitan análisis transversales y la generación de inteligencia operativa, asegurando que todo acceso a la información del ecosistema se realice de manera consistente y trazable a través de este punto de coordinación.

### 2.1.1. Definición de los dominios de datos relevantes del sistema federado del Sistema de Seguridad Pública

El ecosistema de información del Sistema de Seguridad Pública se compone de activos de datos con orígenes, naturalezas y regímenes de custodia fundamentalmente diferentes. La correcta caracterización de estos dominios constituye el fundamento para el diseño del modelo de federación, ya que determina las estrategias de procesamiento, almacenamiento y acceso aplicables a cada tipo de información. A partir del diagnóstico realizado y del análisis de las capacidades institucionales, se han identificado dos grandes dominios que estructuran el modelo propuesto.

**Dominio de Datos Centralizados**

El primer dominio comprende la información que el Ministerio de Seguridad Pública genera directamente en el ejercicio de sus funciones, o que recibe formalmente de otras instituciones mediante convenios, transferencias autorizadas o mandatos legales que le confieren custodia permanente. Esta información se procesa y disponibiliza en la infraestructura de datos del Ministerio, conformada por un Data Lake para el almacenamiento de datos en crudo y en diversos formatos durante su procesamiento fase de procesamiento, y un Data Warehouse optimizado para consultas analíticas y reportería.

Respecto de esta información, el Ministerio ejerce control pleno sobre su ciclo de vida completo, asumiendo la responsabilidad institucional de garantizar su calidad, integridad, seguridad y uso conforme a la normativa aplicable. Los datos atraviesan procesos sistemáticos de ingesta, validación, transformación y estructuración que los preparan para el

consumo analítico. Esta información puede ser modelada según las necesidades del Ministerio, habilitando la realización de análisis históricos, la construcción de series temporales y la aplicación de técnicas avanzadas de análisis.

**Dominio de Datos Federados**

El segundo dominio abarca la información que es generada, custodiada y gestionada por otras instituciones del Estado en el ejercicio de sus competencias legales. Esta información resulta imprescindible para los análisis integrados y la coordinación operativa que el Sistema requiere, pero su custodia, actualización y responsabilidad sobre su integridad permanece en la institución de origen.

A diferencia del dominio centralizado, esta información no se replica permanentemente en la infraestructura del Ministerio. El acceso se realiza mediante conexiones federadas que el sistema información del Ministerio establece hacia las fuentes externas, permitiendo obtener los datos necesarios para responder a consultas específicas sin duplicar las bases de datos completas. Este enfoque garantiza que las instituciones propietarias mantengan soberanía sobre su información, siendo ellas quienes definen qué datos exponen hacia el sistema federado y bajo qué condiciones técnicas y normativas. La incorporación de cada fuente al sistema federado se realiza de manera progresiva, mediante acuerdos específicos que definen el alcance de los datos accesibles

**Soberanía de Datos en Origen**

El modelo de federación se fundamenta en el principio de soberanía de datos, que establece que cada institución del Estado mantiene autoridad sobre la información que genera en el ejercicio de sus funciones legales. Este principio reconoce que la información institucional está intrínsecamente vinculada a las competencias, responsabilidades y marcos normativos de la institución que la genera, y que dicha institución es la responsable última de su calidad, integridad y actualización.

La soberanía de datos se materializa en el modelo propuesto a través del diseño de las conexiones federadas. Cada institución define qué información expone hacia el sistema del Ministerio, estableciendo los campos accesibles, las restricciones aplicables y las condiciones de uso. Los datos no se duplican permanentemente, sino que se consultan en tiempo real desde su ubicación de origen. La responsabilidad sobre la calidad e integridad del dato recae en la institución origen, mientras que el Ministerio asume responsabilidad sobre el uso apropiado de la información obtenida, la seguridad del sistema de consultas y la trazabilidad de los accesos realizados.

### 2.1.2. Diseño del modelo de federación y rol articulador del MSP

El modelo de federación establece el marco conceptual que define cómo se estructura el ecosistema de información del Sistema de Seguridad Pública y cómo las instituciones participantes acceden a los datos que requieren para el cumplimiento de sus funciones. Este modelo posiciona al Ministerio como el coordinador central del sistema, estableciendo las reglas de acceso y los principios que rigen toda interacción con la información.

### Lógica de Distribución y Flujo de Información

El modelo de federación configura un ecosistema donde el Ministerio de Seguridad Pública opera como el nodo central a través del cual fluye todo el acceso a información integrada. Esta configuración responde a la necesidad de contar con un punto único de coordinación que garantice la coherencia, trazabilidad y seguridad del sistema en su conjunto.

La arquitectura distingue entre las instituciones que actúan como fuentes de datos y las instituciones que actúan como consumidoras de información. Las instituciones fuente son aquellas que generan datos relevantes para la seguridad pública y que, mediante acuerdos con el Ministerio, exponen parte de su información hacia el sistema federado. Estas instituciones mantienen sus propias bases de datos y sistemas, definiendo soberanamente qué información comparten bajo las condiciones técnicas definidas por el Ministerio de Seguridad Pública. Las instituciones consumidoras son todas aquellas entidades del Sistema que requieren acceder a información para el ejercicio de sus funciones, ya sea información centralizada en el Ministerio o información federada desde otras fuentes.

El flujo de información opera siempre a través del sistema integrado del Ministerio. Cuando una institución consumidora requiere datos, formula su solicitud al sistema del Ministerio, que verifica las autorizaciones correspondientes y ejecuta la consulta. Si los datos solicitados residen en el sistema centralizado del Ministerio, la consulta se resuelve localmente. Si los datos residen en una fuente federada, el sistema del Ministerio ejecuta la conexión hacia esa fuente, obtiene los resultados y los entrega al solicitante. En ningún caso las instituciones consumidoras establecen conexiones directas con otras instituciones sin pasar por el sistema del Ministerio.

Este diseño centralizado presenta ventajas significativas para la gobernanza del sistema. El Ministerio mantiene visibilidad completa sobre todos los accesos a información, habilitando la auditoría y el control. Las políticas de seguridad y acceso se aplican de manera uniforme en un único punto. El catálogo de datos disponibles se gestiona centralizadamente, facilitando el descubrimiento de información por parte de los usuarios. Las conexiones técnicas con las fuentes se integran una sola vez, sin requerir que cada institución consumidora establezca y mantenga sus propias integraciones.

### Rol del Ministerio de Seguridad Pública como Coordinador Central

El modelo de federación posiciona al Ministerio de Seguridad Pública como el coordinador central del ecosistema de información del Sistema de Seguridad Pública. Este rol cumple el papel de aprovisionar la infraestructura para abarcar responsabilidades de gobernanza, normalización y articulación institucional.

En el apartado de coordinación, el Ministerio establece y mantiene las relaciones con las instituciones fuente, negociando los acuerdos de intercambio de información. El Ministerio actúa como interlocutor único frente a las instituciones que aportan datos al sistema federado, simplificando la gestión para estas instituciones que solo deben establecer una relación con el Ministerio en lugar de múltiples relaciones bilaterales con cada potencial consumidor.

En el apartado normativo, el Ministerio define los estándares técnicos que rigen la interoperabilidad del sistema, los protocolos de seguridad que deben cumplirse, las políticas de acceso que determinan quién puede consultar qué información, y los procedimientos de auditoría que garantizan la trazabilidad. Estas definiciones se aplican de manera uniforme a todo el ecosistema, garantizando coherencia y facilitando el cumplimiento normativo.

En el apartado operativo, el Ministerio administra la infraestructura del sistema integrado, que comprende el Data Lake y Data Warehouse para datos centralizados, las conexiones federadas hacia fuentes externas, el motor de consultas que integra ambos dominios, el catálogo de datos que documenta los activos disponibles, y los servicios de seguridad y auditoría que protegen el sistema. El Ministerio es responsable de la disponibilidad, rendimiento y seguridad de esta infraestructura.

**Principios Generales de Acceso a la Información**

El acceso a la información en el sistema integrado se rige por principios fundamentales que buscan equilibrar la necesidad operativa de contar con información para el cumplimiento de las funciones de seguridad pública, con la protección de los datos, los derechos de las personas y las restricciones normativas aplicables. Estos principios se implementan centralizadamente en el sistema del Ministerio, garantizando su aplicación uniforme a todas las consultas.

El **principio de necesidad operativa** establece que el acceso a información se otorga únicamente cuando existe una justificación demostrada para el cumplimiento de funciones legítimas de seguridad pública. Las autorizaciones se vinculan a roles funcionales específicos y finalidades determinadas.

El **principio de mínimo privilegio** establece que cada usuario recibe únicamente los permisos estrictamente necesarios para realizar su trabajo. Este principio se implementa mediante perfiles de acceso granulares que definen qué conjuntos de datos, qué campos específicos y qué operaciones puede realizar cada rol. El sistema administra estos perfiles centralizadamente, asegurando que no se otorguen capacidades excesivas.

El **principio de trazabilidad** exige que toda interacción con la información del sistema quede documentada de forma exhaustiva. El sistema registra la identidad del solicitante, la consulta realizada, los datos accedidos y el momento del acceso. Estos registros se almacenan de manera inmutable y están disponibles para auditoría, permitiendo detectar usos indebidos.

El **principio de cumplimiento normativo** exige que todo acceso se realice en estricto apego a la legislación vigente. El sistema implementa las restricciones derivadas de la normativa de protección de datos personales, las disposiciones sobre información reservada, las regulaciones específicas de cada tipo de dato y las obligaciones internacionales. Estas restricciones se configuran centralizadamente y se aplican automáticamente a las consultas correspondientes.

### 2.1.3. Modelación de flujos de consulta, reglas de visibilidad y arquitectura conceptual

Este apartado describe cómo el modelo conceptual desarrollado en las secciones anteriores se traduce en mecanismos operativos y tecnológicos concretos. Se abordan los flujos mediante los cuales se procesan las consultas de información, las reglas que determinan la visibilidad de los datos, y la arquitectura técnica que soporta los componentes del sistema integrado.

**Flujos de Consulta de Información**

El sistema integrado del Ministerio permite a los usuarios autorizados consultar información residente tanto en el repositorio centralizado como en fuentes federadas, ofreciendo una experiencia unificada que abstrae la complejidad de la distribución física de los datos. Este proceso ocurre sobre una infraestructura de red segura, aislada lógicamente, donde cada transacción es validada y auditada.

El flujo de una consulta se inicia cuando un usuario autorizado formula una solicitud a través de la Capa de Presentación. Esta solicitud expresa qué información se requiere y los criterios de selección. El sistema recibe la petición y verifica la identidad del usuario y su pertenencia institucional, confirmando que se trata de un acceso legítimo proveniente de una institución autorizada.

Cuando la solicitud está autorizada, el Motor de Consultas determina la ubicación de los datos consultando su propio catálogo de datos.

- Si los datos residen en el Sistema Centralizado, la consulta se ejecuta sobre el Data Warehouse (para respuestas de baja latencia) o el Data Lake (para análisis profundos).

- Si los datos residen en una Fuente Federada, el motor descompone la consulta en subconsultas y establece una conexión segura mediante hacia la institución origen.

En el caso de las conexiones federadas, la institución origen procesa la subconsulta en su propia infraestructura y retorna únicamente los resultados solicitados. Una vez obtenidos todos los datos, el motor coordina la ejecución paralela, consolida los resultados parciales aplicando operaciones de unión y limpieza, y entrega la respuesta transparente al usuario.

Finalmente, el Sistema de Auditoría captura un registro inmutable de la operación. Este registro documenta quién ejecutó la acción, las credenciales verificadas, el momento exacto, la ubicación de origen y los datos específicos accedidos, garantizando la trazabilidad completa.

**Reglas de Visibilidad de la Información**

Las reglas de visibilidad determinan qué información puede ver cada usuario, materializando los principios de seguridad en configuraciones técnicas. Estas reglas se administran

centralizadamente y se apoyan en un catálogo de datos robusto que actúa como el inventario maestro del sistema.

La estructura de visibilidad se gestiona mediante perfiles de acceso que otorgan permisos granulares basados en la institución y el rol funcional del usuario. Los perfiles se pueden definir en diferentes niveles de detalle de acceso para los distintos conjuntos de datos. Un usuario puede tener acceso completo a ciertos datos, acceso parcial a otros, y ningún acceso a los restantes.

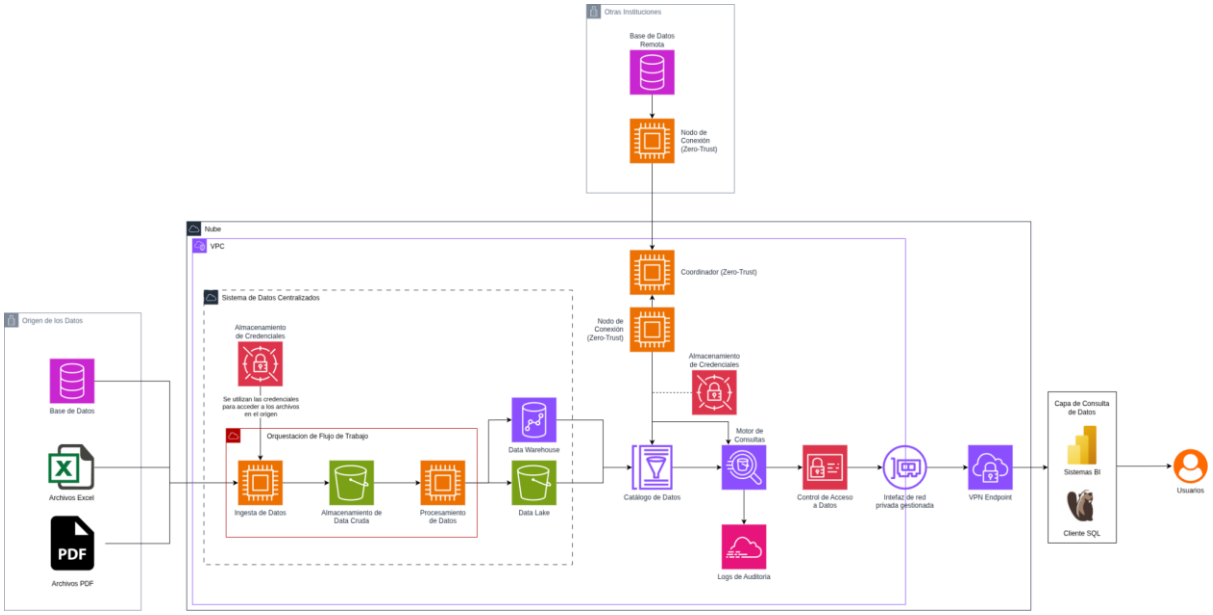
Las reglas de visibilidad también pueden incorporar restricciones contextuales que condicionan el acceso según circunstancias específicas. La jurisdicción geográfica puede limitar la visibilidad a datos de determinadas regiones o comunas correspondientes al ámbito de competencia del usuario. La temporalidad puede restringir el acceso a ciertos períodos o establecer ventanas de consulta limitadas. Estas restricciones se evalúan dinámicamente en cada consulta.

El catálogo de datos tiene un rol crucial en la visibilidad, registrando no solo la ubicación técnica de los activos (nombres de tablas, tipos de columnas), sino también metadatos de negocio y de gobernanza (propietarios, clasificaciones de seguridad). Además, implementa capacidades de rastreo de linaje, documentando el recorrido completo del dato desde su sistema origen, pasando por las transformaciones aplicadas, hasta su consumo final. Esto permite realizar análisis de impacto y validar la calidad de la fuente antes de autorizar su visualización. El catálogo puede incluso indexar fuentes "oscuras" (declaradas pero no conectadas técnicamente), proporcionando visibilidad sobre la existencia de información que, por restricciones legales, debe solicitarse por vías administrativas tradicionales.

**Arquitectura Conceptual y Tecnológica del Sistema Integrado**

Para tangibilizar el modelo operativo descrito, se ha definido una arquitectura tecnológica basada en estándares de industria que asegura la escalabilidad, la alta disponibilidad y la neutralidad respecto a proveedores de nube. La siguiente figura ilustra la topología de la solución, presentando los componentes funcionales requeridos para el sistema de información integrado del Ministerio.

**Figura 2**: Vista general de la arquitectura tecnológica y componentes del sistema.




**Fuente**: Elaboración propia

El esquema anterior ofrece una visión panorámica de cómo interactúan las distintas tecnologías para habilitar el flujo seguro de información. Para comprender en profundidad el funcionamiento de esta arquitectura, a continuación se desglosan las características y funciones específicas de cada uno de los componentes tecnológicos ilustrados, incluyendo ejemplos de servicios equivalentes ofrecidos por los principales proveedores de nube.

**Infraestructura de Red y Seguridad Perimetral:** La arquitectura base se despliega sobre una red privada virtual aislada lógicamente. Ningún componente crítico posee dirección IP pública accesible directamente desde internet; el tráfico permanece dentro de un perímetro seguro gestionado con controles granulares de *firewall*. La conectividad externa se administra mediante puntos de control monitoreados y *endpoints* de VPN que establecen túneles cifrados hacia las capas de presentación e interfaces.

- **Capa de Origen y Captura:** Para el dominio de datos centralizados, existen procesos automatizados de extracción que se ejecutan periódicamente. Estos procesos depositan los datos en un almacenamiento "crudo", preservando los formatos originales. Esto asegura que siempre exista una copia fiel de la fuente original para fines de respaldo o reprocesamiento.

- **Plataforma de Procesamiento y Transformación:** El sistema utiliza tecnologías de contenedores para empaquetar las aplicaciones de procesamiento, garantizando un comportamiento consistente entre entornos de desarrollo y producción. Un sistema de orquestación coordina la ejecución de flujos de trabajo, gestionando dependencias y reintentos. Esta capa implementa la lógica de negocio que corrige errores, estandariza formatos, homóloga códigos y detecta anomalías, contando con capacidad de escalamiento automático para ajustar los recursos computacionales según la carga de trabajo.

A modo de referencia tecnológica, las soluciones comunes para la orquestación incluyen Apache Airflow (Open Source), Azure Data Factory y AWS Step Functions. Por su parte, para la ejecución y procesamiento mediante contenedores o notebooks, destacan servicios como Azure Container Apps y Synapse, o sus equivalentes en AWS como AWS Fargate y AWS Glue. Es importante notar que los modelos Open Source ejecutados en arquitectura local tienen la ventaja de mantener el control y gobernanza sobre los datos.

- **Almacenamiento de Datos (Data Lake y Data Warehouse):** La estrategia de almacenamiento es híbrida. El *Data Lake* almacena la información procesada en formatos columnares optimizados, organizados por dominios de negocio y particionados estratégicamente para mejorar el rendimiento de lectura. Complementariamente, el *Data Warehouse* contiene tablas normalizadas y vistas materializadas, diseñadas para responder consultas analíticas, actuando como la capa de servicio principal para la reportería.

  Para la implementación de esta arquitectura, en Azure se utilizan Azure Data Lake Storage Gen2 y Azure Synapse Analytics. Sus equivalentes directos en AWS corresponden a Amazon S3 (su oferta de Data Lake) y Amazon Redshift (como solución de Data Warehouse).

- **Motor de Consultas Federadas:** Este componente central permite ejecutar consultas SQL estándar sobre múltiples fuentes heterogéneas como si constituyeran una única base de datos lógica. El motor es capaz de analizar la consulta, determinar qué datos residen en el almacenamiento local y cuáles en instituciones externas, y descomponer la solicitud en subconsultas ejecutables independientemente. Su función principal es abstraer la complejidad técnica de la federación, consolidando resultados dispersos de manera transparente para el usuario final.

  En el ámbito Open Source, la tecnología líder para esta función es Trino. Sus equivalentes directos en servicios gestionados de nube son Amazon Athena en AWS y los pools SQL serverless de Azure Synapse Analytics en Azure.

- **Catálogo de Datos:** Centraliza los metadatos técnicos, de negocio y de gobernanza, permitiendo búsquedas con términos naturales sin necesidad de conocer las estructuras subyacentes. Su capacidad de rastreo de linaje es fundamental para la auditoría, permitiendo reconstruir la historia de cualquier dato presentado por el sistema y garantizando la confianza en la información.

  En el ecosistema Open Source, la solución destacada para esta función es OpenMetadata. En cuanto a servicios gestionados de nube, Azure ofrece Microsoft Purview como su suite de gobernanza unificada.

- **Sistema de Auditoría:** Componente transversal que captura registros de todas las operaciones. Estos *logs* se almacenan en una infraestructura separada con inmutabilidad técnica, lo que impide su modificación o eliminación. Esto asegura que los registros de acceso tengan valor probatorio ante auditorías internas, investigaciones administrativas o procesos judiciales.

- **Capa de Presentación e Interfaces:** Proporciona los puntos de acceso para usuarios y sistemas. Expone repositorios mediante *endpoints* SQL para herramientas de *Business Intelligence* (BI) y clientes de análisis avanzado, así como APIs REST para la integración con aplicaciones y portales web. Las herramientas de BI conectadas a esta capa democratizan el acceso, permitiendo la construcción de *dashboards* y reportes interactivos sin requerir conocimientos profundos de programación, mientras que los accesos directos SQL facilitan la labor de los analistas de datos especializados.

En síntesis, el modelo conceptual de federación propuesto proporciona al Ministerio de Seguridad Pública una arquitectura tecnológica que equilibra la necesidad de acceso integrado a información distribuida con los principios de soberanía institucional, protección de datos sensibles y gobernanza apropiada. La separación clara entre datos centralizados y federados, combinada con una infraestructura de seguridad en profundidad y mecanismos exhaustivos de auditoría, establece las bases técnicas para un sistema de información que responde a los desafíos operacionales del Sistema de Seguridad Pública mientras mantiene los más altos estándares de protección de información y cumplimiento normativo. La arquitectura agnóstica a proveedores y su diseño modular garantiza que el sistema pueda evolucionar conforme cambien las necesidades institucionales, las capacidades tecnológicas disponibles y el marco regulatorio aplicable, asegurando la sostenibilidad de largo plazo de la inversión realizada.

## 2.2. Procesos operativos y flujos de gestión en la federación

Para que la arquitectura federada sea funcional, no basta con la conectividad técnica; se requiere una coreografía de procesos que definan el ciclo de vida de una consulta y la gestión de la plataforma. Estos procesos garantizan que el flujo de información sea predecible, seguro y auditable.

### 2.2.1. Diseño de procesos de consulta federada y aplicación de reglas de acceso

El proceso de consulta no es una conexión directa "punto a punto", sino un flujo mediado por la gobernanza del Ministerio. El flujo operativo se descompone en las siguientes etapas:

- Originación y Autenticación: El usuario (ej. un analista de la Subsecretaría de Prevención del Delito) accede al portal o herramienta de análisis. El sistema valida su identidad mediante el Servicio de Identidad Centralizado, verificando que su cuenta esté activa y que su dispositivo cumpla con las políticas de seguridad.
- Validación de Atribuciones (Reglas de Acceso): Antes de ejecutar cualquier búsqueda, el motor de consultas contrasta la solicitud con la Matriz de Permisos. *Ejemplo:* Si el usuario solicita datos de "Procedimientos Policiales", el sistema verifica si su rol tiene permiso para ver datos *nominados* (con nombres) o solo *agregados* (estadísticos), aplicando filtros automáticos en la sentencia SQL resultante.
- Ejecución Multifuente: El motor de consultas descompone la petición. Si la respuesta requiere datos de Carabineros de Chile y de la PDI simultáneamente, el motor envía subconsultas paralelas a ambos nodos institucionales.

- Consolidación y Entrega: Los resultados regresan al Ministerio, donde se anonimizan si la regla de visibilidad así lo exige, se integran en un único reporte y se presentan al usuario.

### 2.2.2. Mecanismos de auditoría, gestión de incidentes y control operativo

La operación del sistema integrado requiere un monitoreo constante que va más allá de "si el sistema está prendido o apagado". Se establecen tres líneas de control:

- Monitoreo de Salud de la Federación: El Ministerio dispone de un tablero de control que mide la latencia de respuesta de cada institución federada. Si un nodo (ej. una base de datos de una subsecretaría) presenta lentitud, el sistema genera una alerta técnica automática para el Custodio Técnico de esa institución.
- Gestión de Incidentes de Acceso: Cualquier intento de acceso fallido por falta de permisos o desde una ubicación no autorizada activa un protocolo de seguridad. El incidente se registra y se notifica al Oficial de Seguridad de la Información (OSI) para descartar intentos de intrusión.
- Mesa de Ayuda Interinstitucional: Se establece un flujo de escalamiento donde los problemas de *calidad de datos* (ej. un dato que parece erróneo) se derivan al Data Steward de la institución fuente, mientras que problemas de *conectividad* se resuelven entre los equipos de infraestructura del MSP y la institución afectada.

### 2.2.3. Diseño del registro de actividad para trazabilidad e integridad de la información

Como se ha mencionado, la trazabilidad es el "seguro de vida" de la federación. El registro de actividad (log) se diseña bajo los siguientes estándares:

- Inmutabilidad: Los registros de auditoría se almacenan en un repositorio con tecnología de "escritura única, lectura múltiple" (WORM). Ni siquiera un administrador de sistemas del Ministerio puede borrar quién consultó qué dato.
    - Granularidad del Log: Cada registro debe contener obligatoriamente:
    - Sujeto: Quién realizó la consulta.
    - Objeto: Qué tablas o campos fueron accedidos.
    - Acción: Qué tipo de operación realizó (lectura, exportación, etc.).
- Contexto: Dirección IP, hora UTC (sincronizada con el SHOA) y justificación de la consulta si el dato es de nivel "Reservado".
- Soberanía de Auditoría: Las instituciones federadas tienen derecho a solicitar reportes de quién del Ministerio ha consultado sus datos, asegurando una transparencia bidireccional que fortalece la confianza en el ecosistema.

## 2.3. Requerimientos tecnológicos para habilitar la federación

Este apartado traduce el modelo conceptual y los procesos operativos descritos en los capítulos anteriores en un conjunto concreto de requerimientos tecnológicos de infraestructura y software que el Ministerio de Seguridad Pública deberá licitar, adquirir o implementar para materializar el Sistema Integrado de Información del Sistema de Seguridad Pública. Mientras que las secciones precedentes establecieron la lógica de federación, las reglas de gobernanza y los flujos de consulta en términos conceptuales, el presente capítulo aterriza esas definiciones en tecnologías específicas, configuraciones de infraestructura y criterios de selección que orientarán las decisiones de implementación.

La selección tecnológica que aquí se presenta responde a una decisión estratégica fundamental: priorizar el uso de tecnologías de código abierto (Open Source) como eje central de la arquitectura. Esta priorización no obedece únicamente a consideraciones económicas, sino que constituye una decisión de soberanía tecnológica que busca evitar la dependencia cautiva de un proveedor específico (vendor lock-in), asegurar la portabilidad de la solución entre distintas infraestructuras de nube y habilitar, en el mediano plazo, un escenario multi-cloud donde el sistema pueda operar de forma distribuida o migrar entre proveedores con un costo de fricción reducido.

El diseño técnico toma como referencia dos plataformas de nube pública: Microsoft Azure, que constituye la plataforma predilecta del Ministerio, y Amazon Web Services (AWS), que representa una alternativa consolidada con amplia cobertura de servicios gestionados. Para cada componente tecnológico se presenta la solución Open Source acompañada de los servicios equivalentes disponibles en ambas nubes, de modo que la arquitectura pueda desplegarse en cualquiera de las dos plataformas o, eventualmente, en un esquema híbrido que combine ambas.

### 2.3.1. Requerimientos funcionales del sistema federado

Los requerimientos funcionales definen las capacidades operativas que el sistema debe ofrecer para cumplir con los objetivos de integración de información establecidos en el modelo de federación. Estos requerimientos se derivan directamente de los flujos de consulta, los dominios de datos y las reglas de gobernanza descritas en los capítulos anteriores, y se traducen en componentes tecnológicos específicos que conforman la arquitectura de referencia del SIISSEP.

**Orquestación de flujos de trabajo para ingesta y procesamiento de datos**

El sistema requiere una plataforma robusta de orquestación que permita coordinar, programar y supervisar todos los procesos de extracción, transformación y carga de datos (ETL) que alimentan el dominio centralizado.

Es importante precisar que el modelo de ingesta opera exclusivamente bajo la modalidad de extracción ("pull"). En el dominio centralizado, los procesos de ingesta son activados por el propio Ministerio mediante extracciones programadas que obtienen los datos desde las fuentes de origen en intervalos definidos. No se contempla la modalidad de recepción pasiva

("push") mediante la cual las instituciones envíen datos directamente hacia la infraestructura del Ministerio, dado que esto requeriría disponibilizar interfaces de recepción (APIs) que incrementarían la superficie de ataque y la complejidad operativa del sistema. En el dominio federado, por definición, todas las consultas operan bajo la lógica "pull", donde el motor de consultas del Ministerio establece conexiones hacia las fuentes externas al momento de resolver una solicitud de información.

La tecnología recomendada para la orquestación es Apache Airflow, una plataforma de código abierto ampliamente adoptada en entornos de datos empresariales y gubernamentales. Apache Airflow permite definir flujos de trabajo como código utilizando el lenguaje Python, lo que facilita el versionamiento, la revisión por pares y la integración con sistemas de control de versiones. Su arquitectura basada en grafos acíclicos dirigidos (DAGs) permite modelar dependencias complejas entre tareas, gestionar reintentos automáticos ante fallos y escalar horizontalmente según la demanda de procesamiento. Adicionalmente, su naturaleza Open Source permite su despliegue en infraestructuras institucionales propias, contribuyendo a mantener el control y la gobernanza sobre los datos y los procesos de tratamiento, al tiempo que garantiza independencia respecto de proveedores y la posibilidad de personalizar la herramienta según las necesidades específicas del Ministerio.

En caso de que el Ministerio opte por utilizar servicios gestionados de nube para la orquestación, las alternativas equivalentes son AWS Step Functions en la plataforma de Amazon, que ofrece un modelo de orquestación serverless basado en máquinas de estado, y Azure Data Factory en la plataforma de Microsoft, que proporciona capacidades de integración de datos y orquestación visual de flujos de trabajo.

**Computación y procesamiento mediante contenedores**

Un pilar fundamental de la arquitectura propuesta es la contenerización de todos los procesos de ingesta, transformación y procesamiento de datos. Cada proceso, ya sea de limpieza, estandarización, homologación de códigos, anonimización o validación de calidad, debe estar empaquetado como un contenedor Docker independiente. Esta decisión de diseño responde a múltiples objetivos técnicos y estratégicos.

En primer lugar, la contenerización garantiza la consistencia entre entornos. Un proceso que fue desarrollado y probado en un ambiente de desarrollo se ejecutará de manera idéntica en el entorno de certificación y en producción, eliminando las discrepancias que históricamente han generado incidentes por diferencias de configuración entre ambientes. En segundo lugar, los contenedores facilitan la portabilidad entre nubes, dado que un contenedor Docker puede ejecutarse en cualquier plataforma que soporte este estándar, lo que refuerza la estrategia de neutralidad tecnológica del proyecto. En tercer lugar, la contenerización habilita el escalamiento horizontal, permitiendo que el sistema lance múltiples instancias de un mismo proceso cuando la carga de trabajo lo requiera.

Los procesos de transformación consistirán típicamente en aplicaciones escritas en Python, empaquetadas como contenedores Docker, que son orquestadas por Apache Airflow según las dependencias y periodicidades definidas para cada flujo de datos. Para procesamientos de menor complejidad u orientados a eventos puntuales, se contemplan también capacidades

de computación serverless que permitan ejecutar funciones ligeras sin necesidad de mantener infraestructura permanente.

En el contexto de AWS, la ejecución de contenedores se realizaría mediante Amazon Elastic Container Service (ECS) o AWS Fargate, que ofrece un modelo serverless donde el Ministerio no necesita gestionar servidores subyacentes. Para procesos ligeros y orientados a eventos, AWS Lambda proporciona capacidades de ejecución de funciones sin servidor con facturación por uso efectivo. En la plataforma de Azure, los equivalentes corresponden a Azure Container Apps para la ejecución de contenedores, y Azure Functions para la computación serverless de procesos ligeros.

**Almacenamiento de objetos para la capa de persistencia**

La infraestructura de almacenamiento del sistema se estructura sobre servicios de almacenamiento de objetos en la nube, que conforman la capa de persistencia fundamental del Data Lake. Este componente almacena los datos en su zona "cruda" (raw), preservando los formatos originales provenientes de las fuentes de ingesta, así como las versiones procesadas y estructuradas que resultan de las transformaciones aplicadas por los procesos de ETL.

El almacenamiento de objetos se selecciona como tecnología base por sus características de alta durabilidad, su modelo de costos proporcional al volumen almacenado, su capacidad de escalamiento prácticamente ilimitada y su compatibilidad nativa con las herramientas de procesamiento y consulta del ecosistema. Los datos se organizan en zonas diferenciadas dentro del Data Lake, particionados estratégicamente por dominio de negocio, institución de origen y temporalidad, lo que optimiza el rendimiento de lectura y facilita la aplicación de políticas de retención y ciclo de vida.

En AWS, el servicio correspondiente es Amazon Simple Storage Service (Amazon S3), que constituye el estándar de facto para almacenamiento de objetos en la nube. En Azure, el equivalente es Azure Blob Storage, específicamente en su variante Azure Data Lake Storage Gen2, que extiende las capacidades de Blob Storage con un espacio de nombres jerárquico optimizado para cargas de trabajo analíticas.

**Motor de consultas federadas**

El motor de consultas federadas constituye el componente más crítico de la arquitectura, dado que materializa la capacidad central del sistema: permitir que los usuarios autorizados ejecuten consultas SQL estándar sobre múltiples fuentes de datos heterogéneas como si conformaran una única base de datos lógica. Este componente es el que hace posible la federación en la práctica, abstrayendo completamente la complejidad de la distribución física de los datos frente al usuario final.

El motor de consultas recibe las solicitudes de los usuarios, analiza la consulta para determinar qué datos residen en el almacenamiento centralizado del Ministerio (Data Lake y Data Warehouse) y cuáles deben obtenerse de fuentes federadas externas, descompone la solicitud en subconsultas ejecutables de forma independiente y paralela, coordina la ejecución distribuida, y consolida los resultados parciales en una respuesta unificada que se entrega de

forma transparente al solicitante. Todo este proceso ocurre de manera automática, sin que el usuario necesite conocer la ubicación física de los datos ni los detalles técnicos de la conexión con cada fuente.

La tecnología recomendada para este componente es Trino, un motor de consultas SQL distribuido de código abierto, diseñado específicamente para consultas analíticas de alto rendimiento sobre fuentes de datos federadas. Trino es el sucesor del proyecto PrestoSQL y ha sido adoptado por organizaciones de gran escala a nivel mundial por su capacidad de conectarse simultáneamente a bases de datos relacionales (PostgreSQL, MySQL, SQL Server, Oracle), sistemas de archivos distribuidos (S3, HDFS), bases de datos NoSQL y servicios de almacenamiento en la nube, procesando consultas de forma paralela con tiempos de respuesta interactivos.

Una capacidad especialmente relevante de Trino para el contexto del SIISSEP es su sistema nativo de control de acceso granular. Trino permite definir permisos de acceso con granularidad fina, alcanzando niveles de restricción por esquema, por tabla, por columna e incluso por fila. Esto significa que es posible configurar que un determinado perfil de usuario tenga acceso completo a ciertos conjuntos de datos, acceso parcial a otros (visualizando solo algunas columnas o registros que cumplan condiciones específicas) y ningún acceso a los restantes, todo gestionado desde un único punto de control. Esta capacidad permite implementar directamente en el motor de consultas las reglas de visibilidad y los perfiles de acceso definidos en el modelo de gobernanza.

En caso de que el Ministerio opte por servicios gestionados de nube, AWS y Azure ofrecen alternativas sin embargo será necesario hacer integraciones adicionales que cumplan la función de conectores. Esto se logra mediante códigos desplegados en servicios como AWS Lambda, donde se define la lógica de conexión hacia la fuente federada. Las alternativas equivalentes son Amazon Athena en AWS, que proporciona un motor de consultas SQL serverless basado en Trino y compatible con datos almacenados en S3, y los pools SQL serverless de Azure Synapse Analytics en la plataforma de Microsoft, que ofrecen capacidades similares de consulta distribuida sobre el almacenamiento de Azure.

**Catálogo de datos y gobernanza**

El catálogo de datos constituye el inventario maestro de todos los activos de información del sistema, desempeñando un rol fundamental para la gobernanza, el descubrimiento y la trazabilidad de los datos. Este componente centraliza los metadatos técnicos (nombres de tablas, tipos de columnas, esquemas de bases de datos), los metadatos de negocio (descripciones funcionales, propietarios de datos, clasificaciones de seguridad) y los metadatos de gobernanza (políticas de acceso, restricciones normativas, acuerdos de intercambio aplicables).

La tecnología recomendada para este componente es OpenMetadata, una plataforma de código abierto que ofrece una solución completa y moderna para el descubrimiento de datos, la gestión de metadatos, el rastreo de linaje y la colaboración entre equipos. OpenMetadata se integra nativamente con las tecnologías del ecosistema propuesto, incluyendo Trino,

Apache Airflow y los servicios de almacenamiento en la nube, proporcionando una visión unificada de todos los activos de información del sistema.

En el contexto de servicios gestionados de nube, las alternativas equivalentes son AWS Glue Data Catalog en la plataforma de Amazon, que proporciona un repositorio centralizado de metadatos integrado con los servicios de datos de AWS, y Microsoft Purview en la plataforma de Azure, que ofrece una suite unificada de gobernanza de datos con capacidades avanzadas de clasificación, linaje y cumplimiento normativo.

**Data Warehouse para almacenamiento analítico centralizado**

Complementariamente al Data Lake, el sistema requiere un Data Warehouse optimizado para responder consultas analíticas de alta velocidad y baja latencia. Mientras que el Data Lake almacena los datos en formatos abiertos y flexibles, adecuados para el procesamiento masivo y la exploración de datos, el Data Warehouse contiene tablas normalizadas, vistas materializadas y modelos de datos dimensionales diseñados específicamente para alimentar la reportería, los tableros de control (dashboards) y los análisis estadísticos que requieren los usuarios del sistema.

El Data Warehouse actúa como la capa de servicio principal para los consumidores de información que necesitan respuestas rápidas y predecibles, tales como los analistas de las subsecretarías que generan reportes periódicos o los equipos de inteligencia operativa que requieren indicadores actualizados para la toma de decisiones.

A diferencia de otros componentes donde se recomienda una solución Open Source como opción preferente, el Data Warehouse es un caso donde las soluciones de nube gestionada presentan ventajas significativas en términos de rendimiento, escalabilidad y administración. En AWS, el servicio correspondiente es Amazon Redshift, un Data Warehouse columnar completamente gestionado que ofrece escalamiento automático y capacidades de consulta sobre petabytes de datos. En Azure, el equivalente es Azure Synapse Analytics en su modalidad Dedicated SQL Pool, que proporciona un motor de procesamiento masivamente paralelo diseñado para cargas de trabajo analíticas empresariales.

**Conectividad segura mediante modelo Zero Trust**

La interconexión entre el nodo central del Ministerio y las instituciones federadas constituye uno de los aspectos más sensibles de la arquitectura, dado que involucra el tránsito de información de alta criticidad para la seguridad pública a través de redes que deben ser protegidas con los más altos estándares de seguridad.

El modelo de conectividad propuesto se basa en el paradigma de confianza cero (Zero Trust), que parte del principio de que ningún actor, dispositivo o red es inherentemente confiable, y que toda comunicación debe ser autenticada, autorizada y cifrada de extremo a extremo, independientemente de su origen.

La tecnología recomendada para implementar los túneles de conectividad segura es Tailscale con Headscale como servidor de coordinación autogestionado. Headscale es una

implementación de código abierto del plano de control de Tailscale que permite operar la infraestructura de red privada virtual de forma completamente soberana, sin depender de servicios externos. Sobre esta base, Tailscale provee el protocolo subyacente de red, combinando la solidez criptográfica moderna de WireGuard con una capa de gestión de identidades y dispositivos que simplifica significativamente la administración operacional de los túneles seguros.

La elección de Tailscale con Headscale responde a la misma lógica de soberanía tecnológica que guía toda la arquitectura: al utilizar componentes de código abierto, el Ministerio mantiene control total sobre su infraestructura de conectividad, sin depender de hardware propietario, licencias de proveedores específicos ni servicios de terceros para la gestión de los túneles seguros. Como alternativa, el servicio gestionado de Tailscale puede considerarse para entornos donde la simplicidad operacional sea prioritaria; sin embargo, esta opción introduce una dependencia externa sobre un proveedor privado, lo que debe evaluarse cuidadosamente en función de los requisitos de soberanía digital del Ministerio. Esta independencia resulta especialmente relevante en el contexto de un sistema que conecta instituciones del Estado que manejan información sensible de seguridad pública.

**Gestión centralizada de la confidencialidad de datos**

Un aspecto frecuentemente subestimado en arquitecturas de datos distribuidas es la gestión segura de las credenciales que los procesos del sistema utilizan para conectarse a las distintas fuentes de información. En el SIISSEP, esto abarca tanto las credenciales de acceso a las bases de datos de las instituciones federadas, que el motor de consultas Trino requiere para establecer sus conexiones, como las credenciales utilizadas por los procesos de orquestación (Apache Airflow) para autenticarse ante las fuentes del dominio centralizado durante los ciclos de ingesta.

Almacenar estas credenciales en archivos de configuración, variables de entorno de los contenedores o repositorios de código constituye una práctica que introduce riesgos graves de seguridad: cualquier acceso no autorizado al entorno de ejecución podría comprometer la totalidad de las conexiones federadas del sistema. Para eliminar esta vulnerabilidad, la arquitectura incorpora un gestor centralizado de secretos, cuya función es almacenar, encriptar y distribuir credenciales de forma dinámica a los procesos que las requieren, garantizando que ningún secreto quede expuesto en texto plano en ninguna capa del sistema.

Este componente se implementa mediante el servicio de gestión de secretos nativo de la plataforma de nube donde resida la infraestructura del SIISSEP. En AWS, el servicio correspondiente es AWS Secrets Manager, que permite almacenar las credenciales de las conexiones federadas y de los procesos de ingesta de forma encriptada, emitir credenciales de vida corta que expiran automáticamente tras un período definido y rotar las credenciales de forma automática y programada. Cada proceso del sistema, identificado por su rol de ejecución, recibe únicamente los secretos que necesita para operar, sin acceso al resto. Todos los accesos quedan registrados en AWS CloudTrail, proporcionando trazabilidad completa sobre qué proceso obtuvo qué credencial y en qué momento.

En Azure, el servicio equivalente es Azure Key Vault, que proporciona almacenamiento seguro de secretos, claves criptográficas y certificados con integración nativa en los servicios de identidad de la plataforma. Azure Key Vault ofrece las mismas capacidades de acceso granular por identidad de proceso, rotación de credenciales y registro de auditoría de accesos, alineándose con el modelo de gobernanza y trazabilidad del sistema.

**Sistema de auditoría e inmutabilidad de registros**

La trazabilidad de todas las operaciones realizadas sobre el sistema constituye un requisito transversal de primer orden, tanto desde la perspectiva de la gobernanza de datos como desde los estándares de ciberseguridad aplicables al sector público. El sistema de auditoría del SIISSEP tiene como objetivo registrar de forma exhaustiva, verificable e inalterable cada interacción relevante: qué usuario accedió al sistema, qué consulta ejecutó, qué datos fueron accedidos y en qué momento preciso. Estos registros constituyen el mecanismo de rendición de cuentas del sistema y son la base para cualquier investigación administrativa o proceso de auditoría interna o externa.

Para garantizar la integridad de estos registros, el sistema adopta una arquitectura de logs de escritura única. Una vez que un evento es registrado, no puede ser modificado ni eliminado por ningún operador del sistema, ni siquiera por administradores con privilegios elevados. Esta propiedad de inmutabilidad es lo que otorga valor probatorio a los registros y diferencia un sistema de auditoría robusto de un simple archivo de eventos.

La arquitectura de observabilidad propuesta se basa en dos componentes Open Source del ecosistema de la Cloud Native Computing Foundation (CNCF). En primer lugar, OpenTelemetry actúa como el estándar de instrumentación, recolectando eventos de auditoría desde todos los componentes del sistema (Trino, Airflow, los procesos dockerizados y el gestor de secretos) bajo un formato unificado y neutral respecto de proveedores. En segundo lugar, Grafana Loki actúa como el repositorio centralizado de logs, almacenando los eventos de auditoría de forma indexada y eficiente. La inmutabilidad técnica se garantiza configurando Loki sobre el almacenamiento de objetos (S3 o Azure Blob Storage) con políticas de retención bloqueadas, lo que impide la eliminación de objetos durante el período de resguardo definido.

A través de Grafana, la herramienta de visualización del mismo ecosistema, el equipo de seguridad y los auditores del Ministerio acceden a tableros de monitoreo en tiempo real que permiten detectar patrones de acceso inusuales, alertas de seguridad y el historial completo de operaciones. Las instituciones federadas tienen la posibilidad de solicitar reportes de auditoría sobre los accesos realizados a sus datos, garantizando la transparencia bidireccional que fortalece la confianza institucional en el modelo federado.

**Interfaz de usuario, visualización y acceso a datos**

El acceso de los usuarios al sistema se realiza a través de una única capa de consulta unificada: el motor Trino. Todas las herramientas de consumo de datos, ya sean plataformas de Business Intelligence o clientes SQL especializados, se conectan a Trino mediante protocolos estándar (JDBC/ODBC), lo que garantiza que las reglas de acceso, la trazabilidad

y los controles de seguridad se apliquen de forma consistente sobre un único punto de entrada, independientemente de la herramienta que utilice el usuario.

En el plano de la visualización y reportería, Power BI de Microsoft constituye la herramienta principal de consumo de información, dada su adopción en el sector público chileno y su integración con el ecosistema de productividad del Ministerio. Power BI se conecta directamente a Trino mediante su conector ODBC nativo, permitiendo la construcción de tableros de control interactivos, reportes automatizados y análisis exploratorios. Para los analistas de datos y equipos técnicos que requieren acceso directo al motor de consultas, herramientas como DBeaver, un cliente de bases de datos universal y de código abierto, permiten ejecutar consultas SQL avanzadas, explorar esquemas de datos y realizar análisis ad hoc sobre el conjunto completo de información disponible en el sistema federado, conectándose igualmente a Trino mediante protocolos estándar.

**Acceso remoto de usuarios mediante túnel seguro**

La misma lógica de conectividad que rige la interconexión entre el nodo central del Ministerio y las instituciones federadas se extiende al acceso de los usuarios finales al motor de consultas.

El acceso de los usuarios se implementa mediante Tailscale con Headscale como servidor de coordinación autogestionado, el mismo protocolo de red privada virtual de código abierto utilizado para los túneles institucionales. Headscale es una implementación de servidor de control de Tailscale completamente de código abierto que permite operar la infraestructura sin dependencia de servicios externos. Cada funcionario autorizado instala el cliente Tailscale en su dispositivo de trabajo y recibe una identidad criptográfica que lo identifica de forma única dentro del ecosistema. Al activar la conexión, el dispositivo establece un túnel cifrado hacia la VPC del Ministerio, autenticándose mediante su clave privada sin necesidad de exponer ningún componente del sistema a internet. Una vez establecido el túnel, el usuario accede al motor de consultas Trino y a las herramientas de visualización como si estuviera operando dentro de la red interna del Ministerio, independientemente de su ubicación física.

Para entornos donde no se requiera soberanía total sobre la infraestructura de coordinación, el servicio gestionado de Tailscale constituye una alternativa funcional equivalente que simplifica la administración de claves y dispositivos; sin embargo, esta opción introduce una dependencia externa sobre un proveedor privado, lo que debe evaluarse en función de los requisitos de soberanía digital del Ministerio.

Esta arquitectura garantiza que ningún componente del SIISSEP sea accesible desde internet de forma directa. Todo el tráfico de usuarios pasa obligatoriamente por el túnel Tailscale, donde la identidad del dispositivo y del usuario es verificada criptográficamente antes de permitir cualquier acceso a la red interna, reforzando de manera consistente el modelo de confianza cero que rige la arquitectura de seguridad del sistema en su conjunto.

### 2.3.2. Requerimientos no funcionales: seguridad, continuidad operativa y desempeño

Los requerimientos no funcionales definen los atributos de calidad que el sistema debe garantizar de manera transversal, independientemente de la funcionalidad específica que se esté ejecutando. En el contexto de un sistema que integra información sensible de seguridad pública proveniente de hasta 43 instituciones del Estado, estos atributos adquieren una relevancia crítica, dado que una falla en cualquiera de ellos puede comprometer la confianza institucional, la integridad de la información o la continuidad de las operaciones.

**Seguridad de la información y control de acceso granular**

La seguridad constituye el atributo no funcional más crítico del sistema, dado el carácter sensible de la información que procesa y la multiplicidad de actores institucionales involucrados. El modelo de seguridad del SIISSEP se estructura en varias capas de protección que operan de forma complementaria.

En materia de cifrado, toda la información debe estar protegida tanto en reposo como en tránsito. Los datos almacenados en el Data Lake y el Data Warehouse utilizan cifrado AES-256 (Advanced Encryption Standard con clave de 256 bits), que constituye el estándar de referencia para la protección de datos clasificados. Las comunicaciones entre componentes del sistema, entre el nodo central y las instituciones federadas, y entre los usuarios y la capa de presentación deben estar protegidas mediante TLS 1.2 o superior, con los túneles de conectividad institucional implementados sobre Tailscale como se describió en la sección anterior.

En materia de autenticación de usuarios, el sistema debe implementar autenticación multifactor (MFA) para todos los accesos, combinando al menos dos factores de verificación (por ejemplo, credenciales de usuario más un token temporal generado por una aplicación autenticadora). Este requisito se alinea con las disposiciones del Decreto N° 7 de Ciberseguridad y con las mejores prácticas internacionales para sistemas que procesan información sensible.

En materia de control de acceso, el motor de consultas Trino implementa un sistema de control de acceso basado en roles (RBAC) con una granularidad que permite definir permisos en múltiples niveles de detalle. A nivel de catálogo, se puede restringir qué fuentes de datos son visibles para cada perfil de usuario. A nivel de esquema y tabla, se puede controlar qué conjuntos de datos específicos puede consultar cada rol. A nivel de columna, se puede ocultar campos sensibles (como nombres, RUT o direcciones) para perfiles que solo requieren datos agregados o estadísticos. A nivel de fila, se pueden aplicar filtros automáticos que limiten los registros visibles según criterios contextuales como la jurisdicción geográfica del usuario o el período temporal autorizado.

Esta granularidad permite materializar directamente en la plataforma tecnológica las reglas de visibilidad y los perfiles de acceso definidos en el modelo de gobernanza (Capítulo 2), asegurando que las políticas normativas se traduzcan en restricciones técnicas efectivamente implementadas y automáticamente aplicadas.

### Escalabilidad y desempeño

El sistema está diseñado para soportar la incorporación progresiva de hasta 43 instituciones del Sistema de Seguridad Pública sin experimentar degradación en los tiempos de respuesta ni en la calidad del servicio. Esta capacidad de escalamiento se logra mediante la combinación de una arquitectura basada en contenedores que permite escalar horizontalmente, servicios de almacenamiento en la nube que escalan de forma prácticamente ilimitada y un motor de consultas distribuido como Trino que puede agregar nodos de procesamiento según la demanda.

Los tiempos de respuesta del sistema deben ajustarse al tipo de consulta. Las consultas operativas sobre el Data Warehouse (reportes estándar, indicadores de gestión) deben resolverse en segundos. Las consultas federadas que involucren múltiples instituciones pueden requerir tiempos mayores dependiendo de la latencia de las fuentes externas, pero mediante el motor de consultas el sistema optimiza la ejecución paralela de subconsultas para minimizar los tiempos de consolidación.

### Continuidad operativa y disponibilidad

El SIISSEP debe operar con un estándar de disponibilidad de al menos 99,9% de tiempo de actividad, lo que equivale a un tiempo máximo de inactividad no planificada de aproximadamente 8,7 horas al año. Este nivel de disponibilidad es necesario para soportar las decisiones operativas críticas del Sistema de Seguridad Pública, que requieren acceso continuo a la información.

La arquitectura distribuida y basada en contenedores facilita la implementación de redundancia a nivel de componentes. Los servicios de almacenamiento en la nube (S3 y Azure Blob Storage) ofrecen redundancia geográfica nativa, replicando los datos automáticamente en múltiples ubicaciones. El motor de consultas Trino puede desplegarse en configuraciones de alta disponibilidad con múltiples nodos coordinadores. Los procesos orquestados por Apache Airflow incorporan mecanismos nativos de reintento y recuperación ante fallos.

Al utilizar servicios gestionados de nube para el almacenamiento y la computación, el Ministerio traslada la carga del mantenimiento de hardware, la gestión de parches de seguridad a nivel de infraestructura y la administración de centros de datos al proveedor de nube, permitiendo que los equipos técnicos del Ministerio concentren sus esfuerzos en la lógica de negocio, la calidad de los datos y la evolución funcional del sistema.

### Neutralidad tecnológica y portabilidad

Como se ha señalado a lo largo de este capítulo, la arquitectura recomienda tecnologías de código abierto y estándares abiertos para los componentes críticos del sistema. Apache Airflow para la orquestación, Trino para el motor de consultas, OpenMetadata para el catálogo de datos, Docker para la contenerización y Headscale para la conectividad segura son todos proyectos Open Source con comunidades activas, gobernanza transparente y amplia adopción en la industria.

Esta decisión garantiza que la propiedad intelectual del sistema, incluyendo toda la lógica de procesamiento, las reglas de gobernanza implementadas y las configuraciones de seguridad, pertenezca íntegramente al Ministerio de Seguridad Pública. No existe dependencia de licencias propietarias, formatos cerrados ni APIs exclusivas de un proveedor para los componentes centrales de la arquitectura. Si en el futuro el Ministerio decide cambiar de proveedor de nube, migrar a una infraestructura híbrida o adoptar un modelo multi-cloud, los componentes Open Source del sistema podrán desplegarse en la nueva plataforma sin necesidad de reescribir la lógica de negocio ni adquirir nuevas licencias.

### 2.3.3. Componentes tecnológicos críticos y criterios de expansión modular

La incorporación de nuevas instituciones al sistema federado se realizará de manera progresiva, siguiendo un modelo de expansión por oleadas que permita validar cada integración antes de avanzar a la siguiente. Este enfoque reconoce que las instituciones del Sistema de Seguridad Pública presentan niveles de madurez digital heterogéneos y que la integración de cada nueva fuente requiere procesos de negociación, configuración técnica y validación que deben ejecutarse de forma ordenada.

Desde el punto de vista tecnológico, cada nueva integración implica la satisfacción de tres condiciones técnicas fundamentales que constituyen los prerrequisitos de incorporación al sistema federado. La ausencia de cualquiera de ellas determina que la institución no puede ser integrada hasta que dicha condición sea resuelta.

El primer requisito corresponde a la configuración de un conector compatible con el motor de consultas federadas. En el caso de Trino, este opera bajo una arquitectura de conectores extensibles, donde cada tipo de fuente de datos (PostgreSQL, MySQL, SQL Server, Oracle, entre otras) dispone de un conector específico que traduce las consultas SQL de Trino al protocolo nativo de esa base de datos. Para integrar una nueva institución, el equipo técnico del Ministerio debe configurar el conector correspondiente al sistema de base de datos que la institución utiliza, registrar la fuente en el catálogo de datos (OpenMetadata) y definir las reglas de acceso granular aplicables a esa fuente. Este proceso es incremental y no requiere modificaciones en los conectores ya configurados, preservando la estabilidad de las integraciones existentes.

El segundo requisito es la implementación de un nodo de conectividad Zero Trust en la infraestructura de la institución que se incorpora. El modelo de seguridad del SIISSEP sugiere que la comunicación entre el Ministerio y las fuentes federadas se lleve a cabo mediante un túnel cifrado bajo el paradigma de confianza cero. Para materializar esto, la institución federada debe instalar y configurar un nodo del cliente Tailscale en su infraestructura, el cual se registra en el servidor de coordinación centralizado del Ministerio. Una vez establecido el nodo, el túnel cifrado entre el Ministerio y la institución queda operativo y el motor de consultas puede alcanzar la base de datos federada de forma segura.

El tercer requisito, y el que representa el mayor desafío en el contexto de instituciones con baja madurez tecnológica, es la existencia de una base de datos estructurada y accesible en la infraestructura de la institución. El motor de consultas federadas opera sobre fuentes de

datos relacionales o compatibles con conectores SQL. Se requiere una base de datos con un esquema definido, credenciales de acceso y capacidad de responder consultas de forma programática. Un sistema que almacena su información en hojas de cálculo, documentos ofimáticos o sistemas propietarios sin interfaz de consulta estructurada no es directamente integrable en el modelo federado. En estos casos, la institución enfrenta dos caminos posibles.

1. Implementar una base de datos relacional que refleje su información (migrando desde los formatos actuales)
2. Desarrollar una capa de acceso intermedia que exponga la información mediante un protocolo compatible.

Ambas opciones implican inversión técnica previa, lo que refuerza la importancia de evaluar la madurez digital como criterio de priorización en las oleadas de expansión.

Los criterios para la priorización de instituciones en cada oleada deben, por tanto, considerar de forma integrada la relevancia operativa de los datos que la institución aporta, su nivel de madurez tecnológica –que determina si los tres prerrequisitos anteriores pueden satisfacerse en el corto plazo o requieren un proceso previo de modernización–, la existencia de marcos normativos habilitantes para el intercambio de información y la disposición institucional para formalizar los acuerdos de intercambio y designar los roles de gobernanza requeridos, tales como propietarios de datos, custodios técnicos y enlaces de coordinación.

Sobre la base del diseño arquitectónico y los requerimientos tecnológicos definidos en este capítulo, el informe final presentará un análisis detallado y comparativo de un mínimo de dos y un máximo de tres alternativas técnicas concretas para la implementación del sistema en entornos de nube pública. Estas alternativas se fundamentarán en infraestructuras de nube, aprovechando su flexibilidad, escalabilidad y eficiencia operativa, y serán plenamente coherentes con los principios, componentes y criterios establecidos previamente. La comparación permitirá evaluar distintos escenarios de despliegue posibles, proporcionando una base objetiva para la toma de decisiones tecnológicas.

# 3. Diseño organizacional y normativo acorde a las obligaciones del MSP

La implementación del Sistema Integrado de Información requiere un diseño organizacional y normativo coherente con las obligaciones legales del Ministerio de Seguridad Pública, con su rol rector en materia de seguridad pública y con la autonomía funcional de las instituciones que conforman el ecosistema federado. Este diseño debe permitir al Ministerio ejercer funciones de coordinación, estandarización y supervisión, sin asumir la propiedad ni la administración directa de los sistemas y datos que permanecen bajo la responsabilidad de las instituciones de origen.

En este contexto, el diseño organizacional se estructura sobre un modelo de gobernanza federada, en el cual el Ministerio define marcos, estándares y mecanismos de articulación comunes, mientras que las instituciones participantes conservan la titularidad, operación y

responsabilidad primaria sobre sus datos y sistemas. Este enfoque resulta consistente con el mandato legal vigente, en particular con la Ley N.º 21.730, y permite compatibilizar la integración de información para fines estratégicos con el respeto a las competencias, autonomías y regímenes jurídicos específicos de cada organismo.

Desde el punto de vista normativo, este diseño exige la formalización explícita de roles, responsabilidades y procedimientos mediante instrumentos administrativos y convenios interinstitucionales que otorguen certeza jurídica a las prácticas de intercambio, uso y resguardo de la información. Tales instrumentos deben definir con precisión los alcances de la interoperabilidad, los tipos de datos compartidos, las condiciones de acceso, los mecanismos de trazabilidad y las obligaciones recíprocas de las partes, evitando ambigüedades que puedan afectar la continuidad operativa o la protección de los derechos de las personas.

Sobre esta base, la sección siguiente desarrolla la estructura de roles técnicos y de gobernanza de datos que materializa el modelo federado, así como los mecanismos de coordinación y control necesarios para su operación sostenida.

## 3.1. Roles y responsabilidades en la gobernanza federada

La gobernanza del Sistema Integrado de Información se estructura sobre la base de una distribución clara de roles y responsabilidades entre el Ministerio de Seguridad Pública y las instituciones federadas. Esta gobernanza no se concibe como un esquema jerárquico de control centralizado, sino como un modelo coordinado de responsabilidades compartidas, orientado a asegurar la interoperabilidad, la seguridad y la calidad de la información.

Al Ministerio le corresponde ejercer el rol de autoridad de gobernanza del sistema, definiendo los estándares técnicos, de seguridad y de calidad de datos, administrando el motor de consultas federadas, el catálogo de datos y los mecanismos de monitoreo, y velando por el cumplimiento de los acuerdos establecidos. Asimismo, el Ministerio actúa como articulador institucional, promoviendo la incorporación progresiva de nuevas fuentes de información y facilitando la resolución de conflictos técnicos u operativos que puedan surgir en el funcionamiento del ecosistema.

Las instituciones federadas, por su parte, mantienen la responsabilidad sobre la generación, actualización, exactitud y resguardo de los datos que exponen al sistema. Les corresponde asegurar que sus sistemas cumplan con los estándares definidos, mantener la disponibilidad de las fuentes federadas conforme a los acuerdos de nivel de servicio y colaborar activamente en los procesos de validación, actualización y mejora continua del sistema integrado.

Este reparto de responsabilidades permite preservar la autonomía institucional, al mismo tiempo que establece un marco claro de obligaciones recíprocas que hace viable la operación sostenida del modelo federado. A continuación, se presentan los roles técnicos y de gobernanza.

**Roles técnicos**

**a) Ingeniero de Infraestructura Cloud.** Responsable del diseño, aprovisionamiento, configuración y operación de los recursos de nube pública que sustentan la plataforma. Sus funciones abarcan la gestión de los entornos de cómputo y contenedores, las redes virtuales privadas, el almacenamiento de objetos y las configuraciones de alta disponibilidad y recuperación ante desastres. Diseña y mantiene la infraestructura como código (IaC) para los entornos de producción, certificación y desarrollo, y administra los recursos cloud optimizando el uso y el control de costos. Conforme a las recomendaciones de la Secretaría de Gobierno Digital, este perfil requiere conocimientos específicos en la administración de servicios cloud, la gestión del modelo comercial de créditos y consumo, y la coordinación con los partners o socios de negocios del proveedor. Este rol es crítico desde la Fase 1 y su presencia es permanente durante todo el ciclo de vida del sistema.

**b) Ingeniero de Datos.** Responsable del diseño, construcción y operación de los flujos de datos que alimentan el dominio centralizado del SIISSEP. Le corresponde implementar los flujos ETL que transportan datos desde las fuentes de origen hacia el Data Lake y el Data Warehouse, desarrollar los procesos de limpieza, estandarización y validación de calidad, diseñar y mantener los modelos de datos analíticos, y colaborar en la configuración de los conectores del motor de consultas federadas. Se activa en la Fase 1 y su relevancia se incrementa conforme se incorporan nuevas fuentes de datos.

**c) Especialista en Ciberseguridad.** Responsable de la protección integral de los activos de información del SIISSEP frente a amenazas internas y externas, conforme a las obligaciones del Decreto N.° 7 y a la normativa de Organismos de Importancia Vital. Le corresponde implementar y mantener los controles de seguridad perimetral y de red, administrar la infraestructura de conectividad segura basada en el paradigma Zero Trust, gestionar el sistema centralizado de secretos y credenciales, operar el control de acceso basado en roles, supervisar la auditoría e inmutabilidad de registros, y liderar los procesos de respuesta ante incidentes y notificación ante la Agencia Nacional de Ciberseguridad (ANCI). Este rol debe estar presente desde la Fase 1 y su relevancia se intensifica significativamente a partir de la Fase 3, cuando la plataforma comienza a recibir conexiones externas. La Secretaría de Gobierno Digital establece como condición habilitante para la operación en entornos cloud que las instituciones cuenten con un CISO, ya sea con recursos propios o externalizados.

**d) Administrador de Plataforma de Datos.** Responsable de la operación y mantención de los componentes de software del ecosistema de datos, tales como el motor de consultas federadas, la plataforma de orquestación y el catálogo de datos, resolviendo incidentes operativos de dichos sistemas. Mantiene la plataforma de orquestación asegurando la correcta ejecución de los procesos ETL programados y la gestión de fallos y reintentos. Coordina con los gestores de metadatos de las instituciones federadas la actualización del catálogo de datos, gestiona las actualizaciones de los componentes aplicando parches de seguridad y verificando la compatibilidad entre versiones, y administra los usuarios, roles y permisos de acceso en los distintos componentes de la plataforma, en coordinación con el equipo de ciberseguridad y conforme a las políticas de acceso definidas. Se activa a partir de la Fase 1 y se mantiene como función permanente. Requiere experiencia específica en las tecnologías adoptadas por la arquitectura del SIISSEP.

**Roles para la gobernanza de datos**

**a) Coordinación de Gobernanza.** Responsable de conducir la gestión de datos a nivel del ecosistema completo. Define las políticas, lineamientos y estándares que rigen el intercambio de datos en la federación, gestiona el ciclo de vida de los acuerdos de intercambio de información, arbitra los conflictos entre instituciones respecto de la interpretación o aplicación de las políticas de datos, y supervisa la incorporación progresiva de nuevas instituciones evaluando su nivel de preparación.

**b) Propietario de Datos (Centralizado y Federado).** Tanto el Ministerio como las instituciones federadas deben designar la autoridad funcional que defina las reglas de uso, calidad y confidencialidad de la información bajo su responsabilidad directa, y que apruebe la habilitación de fuentes propias para su consulta.

**c) Custodio de Datos (Centralizado y Federado).** Responsable operativo de la integridad y disponibilidad de los activos de información. El centralizado asegurar la calidad y el gobierno de los datos propios del Ministerio, y el federado como el interlocutor técnico ante las instituciones externas, encargado de garantizar que las fuentes expuestas cumplan con los estándares de interoperabilidad y disponibilidad requeridos.

**d) Oficial de Privacidad y Protección de Datos.** Responsable de asegurar que el tratamiento de datos personales en el SIISSEP se realice en conformidad con la Ley N.° 19.628 y la Ley N.° 21.719. Supervisa los aspectos legales y técnicos de la protección de datos, asesora en la aplicación de técnicas de anonimización o seudonimización, evalúa el impacto en privacidad de la incorporación de nuevas fuentes o flujos de consulta, y revisa las condiciones de tratamiento de datos personales y sensibles en los acuerdos de intercambio.

**e) Gestor de Calidad de Datos.** Responsable de asegurar que la información proveniente de las distintas instituciones cumpla estándares mínimos de completitud, consistencia, exactitud y oportunidad. Define los criterios de calidad que deben satisfacer las fuentes federadas, diseña y opera las validaciones automáticas en los flujos de ingesta, y monitorea indicadores transversales que permitan detectar degradaciones. Cuando se identifican incidentes de calidad, coordina directamente con el Custodio de Datos de la institución de origen para acordar acciones correctivas.

**f) Gestor de Metadatos y Catálogo.** Responsable de mantener el inventario maestro de activos de información del ecosistema, asegurando que todos los datos disponibles estén documentados, clasificados y se facilite su identificación. Mantiene actualizados los diccionarios de datos, el linaje y las definiciones estándar en el catálogo, registra la clasificación de seguridad de cada activo conforme al esquema de cuatro niveles (Público, Uso Interno, Reservado, Secreto), y gestiona el versionamiento de esquemas de datos. En un sistema que integra fuentes de decenas de instituciones, un catálogo centralizado y actualizado es condición esencial para que los usuarios comprendan qué información existe y bajo qué condiciones puede ser utilizada.

**g) Analistas y Científicos de Datos:** Usuarios finales de la arquitectura federada responsables de transformar los datos integrados en insumos para la toma de decisiones estratégicas y el diseño de políticas públicas basadas en evidencia. Su función se centra en la explotación técnica del ecosistema mediante la construcción de tableros de control y cuentan con permisos de lectura únicamente a los recursos acorde a sus responsabilidades.

### 3.1.1. Gestión de incidentes de seguridad y responsabilidades como Operador de Importancia Vital (OIV)

La gestión de incidentes de seguridad de la información constituye un componente esencial del modelo de gobernanza federada, especialmente en un entorno de interoperabilidad donde múltiples instituciones exponen datos a través de mecanismos tecnológicos comunes.

En este contexto, cada institución federada mantiene la responsabilidad primaria sobre la detección, contención, análisis y remediación de incidentes que afecten sus propios sistemas, plataformas e infraestructuras tecnológicas. En su calidad de Operador de Importancia Vital respecto de dichos activos, cada entidad deberá cumplir con las obligaciones de notificación y reporte establecidas por la normativa vigente ante la Agencia Nacional de Ciberseguridad (ANCI) o la autoridad competente que corresponda.

El MSP, por su parte, actuará como OIV respecto de los componentes centrales bajo su administración directa, tales como el motor de consultas federadas, el catálogo de datos, la infraestructura común y los servicios tecnológicos asociados al SIISSEP. En caso de incidentes que afecten estos activos, corresponderá al Ministerio realizar las notificaciones y reportes exigidos por la normativa aplicable, así como activar los protocolos internos de respuesta y recuperación.

Adicionalmente, cuando un incidente originado en una institución federada pueda generar impactos sistémicos en la operación del ecosistema integrado (por ejemplo, comprometiendo la integridad de los flujos federados o la disponibilidad del servicio), deberá establecerse un mecanismo formal de comunicación y coordinación con el Ministerio, a efectos de evaluar medidas de mitigación, suspensión temporal de conexiones o ajustes en los perfiles de acceso, resguardando la continuidad operativa y la seguridad global del sistema.

Este esquema permite compatibilizar la autonomía institucional en materia de gestión de incidentes con la necesidad de coordinación central en aquellos casos donde el riesgo trasciende a un solo organismo y afecta el funcionamiento del modelo federado en su conjunto.

### 3.1.2. Identificación de propietarios de datos y custodios técnicos

Un elemento central del modelo de gobernanza es la identificación explícita de los propietarios de los datos y de los custodios técnicos asociados a cada fuente de información integrada al sistema. La ausencia de esta definición genera vacíos de responsabilidad que dificultan la gestión de incidentes, la corrección de errores y la evolución ordenada de los sistemas.

El propietario del dato corresponde a la unidad o institución responsable del contenido, significado, calidad y legitimidad del dato, así como de las decisiones sobre su uso, compartición y restricciones de acceso. Esta responsabilidad es de naturaleza funcional y normativa, y no se transfiere al Ministerio por el solo hecho de exponer los datos a través del Sistema Integrado.

El custodio técnico del dato, en cambio, es responsable de la operación técnica del sistema que almacena y expone la información, incluyendo la disponibilidad del servicio, la implementación de controles de seguridad, la ejecución de respaldos y la aplicación de

cambios técnicos en los esquemas de datos. En muchos casos, el propietario del dato y el custodio técnico pueden coincidir dentro de una misma institución; en otros, estas funciones pueden recaer en unidades distintas, lo que hace aún más relevante su identificación formal.

Ambos roles deberán quedar registrados en el inventario institucional y en el catálogo de datos del Ministerio, incluyendo información de contacto y responsabilidades específicas, de modo de facilitar la coordinación operativa y la gestión del sistema federado.

### 3.1.3. Definición de roles y responsabilidades para la gestión, uso y resguardo del dato

La gestión del dato en el Sistema Integrado abarca su ciclo de vida completo, desde su generación y almacenamiento en los sistemas de origen, hasta su consulta, uso y eventual eliminación. Para cada una de estas etapas, la Coordinación de Gobernanza de Datos debe asegurar la correcta implementación de la política, definiendo responsabilidades claras que permitan asegurar un tratamiento adecuado y coherente de la información en todo el ecosistema.

Las instituciones de origen, a través de sus Propietarios de Datos y Gestores de la Calidad de Datos, son responsables de garantizar que los datos que generan y exponen sean correctos, actualizados y coherentes con su propósito institucional. Por su parte, corresponde al Administrador de Datos, apoyado en la infraestructura del Custodio de Datos, aplicar las clasificaciones de seguridad correspondientes y los controles de acceso definidos. Asimismo, con la supervisión del Oficial de Privacidad, deben asegurar que el uso de los datos se ajuste a las finalidades declaradas, aplicando técnicas de anonimización si es necesario, y garantizando el cumplimiento de las restricciones legales aplicables.

El Ministerio, en su rol de articulador, es responsable de asegurar que el acceso a los datos se realice de acuerdo con los perfiles autorizados. Los datos se han estandarizado y declarados apropiadamente por el Gestor de Metadatos y Catálogo. Además, en conjunto con los roles de ciberseguridad y los Custodios de Datos centrales, debe garantizar que las consultas queden debidamente registradas para efectos de trazabilidad y auditoría, y que se implementen mecanismos técnicos integrados que prevengan usos indebidos o no autorizados de la información.

El Gestor de la Calidad de Datos garantiza que la información cumpla con los estándares de integridad y precisión necesarios para su explotación. Por su parte, los Usuarios de Datos asumen la responsabilidad de utilizar dicha información exclusivamente para los fines institucionales autorizados y bajo los permisos asignados, respetando estrictamente las clasificaciones de seguridad y las obligaciones de confidencialidad vigentes.

### 3.1.4. Formalización del modelo de roles y validación institucional

Para asegurar la efectividad del modelo de gobernanza propuesto, resulta indispensable su formalización mediante actos administrativos, lineamientos internos y convenios interinstitucionales. Esta formalización permite transformar el diseño conceptual en un marco operativo vinculante, otorgando claridad y respaldo jurídico a los roles y responsabilidades definidos.

Cada institución participante deberá validar internamente los roles asignados, designando formalmente a los propietarios de datos, custodios técnicos y responsables de coordinación con el Ministerio. Estas designaciones deberán comunicarse al Ministerio y mantenerse actualizadas, de modo de asegurar la continuidad del sistema frente a cambios organizacionales o de personal.

El Ministerio, por su parte, deberá consolidar esta información en un registro institucional de gobernanza del Sistema Integrado, que permita visualizar la distribución de responsabilidades, facilitar la coordinación interinstitucional y apoyar los procesos de auditoría y mejora continua. La validación institucional del modelo no debe entenderse como un hito único, sino como un proceso periódico de revisión y ajuste, que permita adaptar la gobernanza del sistema a la evolución normativa, tecnológica y organizacional del ecosistema de seguridad pública.

## 3.2. Políticas y estándares normativos aplicados a la federación de datos sensibles

La federación de datos sensibles en el marco del Sistema Integrado de Información del Ministerio de Seguridad Pública requiere la definición y adopción de un conjunto coherente de políticas y estándares normativos que aseguren un uso legítimo, proporcional y seguro de la información. Estas políticas deben constituir un marco común aplicable a todas las instituciones federadas, respetando sus competencias legales y niveles de autonomía, pero garantizando condiciones mínimas homogéneas para el intercambio, acceso y tratamiento de los datos. El objetivo central es habilitar la interoperabilidad efectiva sin debilitar los resguardos jurídicos, éticos y técnicos asociados a información de alta criticidad para la seguridad pública y los derechos fundamentales de las personas.

Este marco normativo debe alinearse con la legislación vigente en materia de protección de datos personales, seguridad de la información y transparencia, así como con los principios de legalidad, finalidad, necesidad, proporcionalidad y responsabilidad institucional. Asimismo, debe contemplar mecanismos de actualización periódica que permitan su adaptación a cambios normativos, tecnológicos y operacionales, particularmente en un contexto de rápida evolución de las capacidades analíticas y de procesamiento de información.

### 3.2.1. Definición de políticas de acceso, uso, clasificación y seguridad de la información

Las políticas de acceso y uso de la información deben establecer de manera explícita quiénes pueden acceder a los datos, bajo qué condiciones, con qué finalidades y a través de qué mecanismos de autorización y autenticación. Estas políticas deben basarse en un enfoque de acceso por roles y atributos, garantizando que cada usuario o sistema acceda únicamente a la información estrictamente necesaria para el cumplimiento de sus funciones, conforme al principio de mínimo privilegio. El uso de la información debe quedar claramente delimitado por finalidades institucionales previamente definidas, prohibiendo usos secundarios no autorizados o incompatibles con el propósito original de la recolección del dato.

En paralelo, resulta fundamental contar con un esquema común de clasificación de la información que distinga niveles de sensibilidad, criticidad y restricciones de uso, permitiendo aplicar controles diferenciados según el tipo de dato involucrado. Esta clasificación debe ser consistente entre las instituciones federadas y servir como base para la definición de medidas de seguridad técnicas y organizacionales, tales como cifrado, segmentación de accesos, resguardos físicos y lógicos, y procedimientos de respaldo y recuperación ante incidentes. La política de seguridad de la información debe contemplar, además, la gestión de incidentes, la notificación de brechas y la asignación clara de responsabilidades ante eventuales vulneraciones.

### 3.2.2. Criterios para el tratamiento de datos sensibles, videovigilancia, inteligencia artificial y biometría

El tratamiento de datos sensibles requiere criterios normativos reforzados, dada su especial capacidad de afectar derechos fundamentales como la privacidad, la honra y la no discriminación. En este contexto, deben establecerse reglas específicas para la recolección, almacenamiento, análisis y conservación de este tipo de información, asegurando que su uso esté estrictamente habilitado por la normativa vigente y debidamente justificado desde el punto de vista de la necesidad operativa y el interés público. La federación de datos sensibles debe contemplar, cuando corresponda, mecanismos de anonimización, seudonimización o minimización de datos, especialmente en contextos analíticos o estadísticos.

En el caso de sistemas de videovigilancia, inteligencia artificial y tecnologías biométricas, se requiere una regulación aún más precisa, que aborde tanto los aspectos técnicos como los riesgos éticos y legales asociados. Las políticas deben definir claramente los escenarios de uso permitidos, los límites de automatización en la toma de decisiones, los requisitos de supervisión humana y los mecanismos de evaluación de impacto en derechos fundamentales. Asimismo, deben establecerse criterios de transparencia, explicabilidad y control, particularmente cuando estas tecnologías se utilicen para apoyo a labores de prevención, investigación o análisis estratégico en seguridad pública.

Un ejemplo de estas dinámicas se observa en plataformas como SITIA, que integran videovigilancia, análisis automatizado de patentes mediante inteligencia artificial y gestión de evidencia digital. En estos casos, la plataforma puede operar como nodo de articulación y custodia de información que posteriormente es utilizada por Carabineros de Chile o el Ministerio Público. Aun cuando el sistema no adopte decisiones operativas directas, su rol en la centralización y procesamiento de datos sensibles exige reglas explícitas de uso, trazabilidad, supervisión humana y protección de derechos fundamentales.

### 3.2.3. Estándares mínimos de interoperabilidad, trazabilidad y auditoría

Para asegurar un funcionamiento confiable del sistema federado, es indispensable definir estándares mínimos de interoperabilidad que regulen los formatos de intercambio, los protocolos de comunicación, los mecanismos de identificación y autenticación, y las condiciones técnicas bajo las cuales se produce el acceso a la información entre instituciones. Estos estándares deben ser suficientemente flexibles para integrarse con sistemas

heterogéneos, pero lo bastante precisos para garantizar consistencia, calidad y seguridad en los flujos de datos.

De igual forma, la trazabilidad debe ser un componente obligatorio del modelo, permitiendo registrar de manera íntegra y verificable quién accede a la información, cuándo, desde qué sistema y con qué finalidad. Estos registros deben ser protegidos contra alteraciones y mantenerse disponibles para fines de control interno, auditoría y rendición de cuentas. La auditoría, tanto técnica como organizacional, debe contemplar revisiones periódicas del cumplimiento de las políticas y estándares definidos, así como evaluaciones de riesgos y controles asociados al tratamiento de datos sensibles. Este enfoque busca no solo detectar y corregir desviaciones, sino también fortalecer la confianza institucional y ciudadana en el uso del Sistema Integrado de Información del MSP.

## 3.3. Modelo de gobernanza federada interinstitucional del MSP

El modelo de gobernanza federada interinstitucional del Ministerio de Seguridad Pública se concibe como el marco organizacional, normativo y operativo que permite articular a un conjunto diverso de instituciones con competencias, mandatos legales y niveles de autonomía diferenciados, en torno al Sistema Integrado de Información. Este modelo busca equilibrar la necesidad de coordinación efectiva y uso integrado de la información para fines de seguridad pública, con el respeto irrestricto a la autonomía institucional, las atribuciones legales específicas y los regímenes propios de administración de datos de cada organismo participante.

La gobernanza federada no implica una centralización de la propiedad ni del control de los datos, sino la definición de reglas comunes para su intercambio, uso y resguardo, bajo un esquema de responsabilidades compartidas y claramente delimitadas. En este contexto, el MSP actúa como entidad articuladora y garante del marco común, promoviendo la coherencia del ecosistema, la interoperabilidad técnica y semántica, y el cumplimiento de los principios normativos y de seguridad definidos, sin sustituir las funciones ni decisiones propias de las instituciones federadas.

### 3.3.1. Diseño de instancias de coordinación interinstitucional

El modelo de gobernanza requiere la creación de instancias formales de coordinación interinstitucional que permitan la toma de decisiones estratégicas, la resolución de conflictos y la supervisión del funcionamiento del sistema federado. Estas instancias deben estructurarse en distintos niveles, considerando tanto la dimensión estratégica como la operativa, e incorporar representación de las instituciones participantes conforme a sus roles y responsabilidades en el ecosistema de información.

A nivel estratégico, se debe contemplar una instancia de alto nivel orientada a definir lineamientos generales, prioridades de integración, criterios de incorporación de nuevas instituciones o fuentes de datos, y directrices para la evolución del sistema. En el plano operativo y técnico, se requieren espacios de coordinación permanente que permitan abordar aspectos relacionados con interoperabilidad, seguridad, calidad de datos, gestión de

incidentes y cumplimiento normativo. Estas instancias deben operar bajo reglas claras de funcionamiento, con mecanismos formales de convocatoria, registro de acuerdos y seguimiento de compromisos, asegurando continuidad y trazabilidad en la gestión interinstitucional.

### 3.3.2. Definición de acuerdos de intercambio de información y límites del rol articulador del MSP

La interoperabilidad en un contexto federado exige la formalización de acuerdos de intercambio de información que establezcan de manera explícita las condiciones bajo las cuales los datos pueden ser compartidos entre instituciones. Estos acuerdos deben definir el tipo de información involucrada, las finalidades habilitadas, los mecanismos de acceso, las medidas de seguridad aplicables, los plazos de conservación y las responsabilidades asociadas al uso indebido o a eventuales incidentes. Asimismo, deben contemplar procedimientos de suspensión o modificación del intercambio ante cambios normativos, tecnológicos o institucionales.

En este marco, resulta esencial delimitar con precisión el rol articulador del MSP, evitando interpretaciones que puedan derivar en una centralización de facto del control de los datos. El MSP no actúa como propietario de la información ni como autoridad jerárquica sobre las instituciones federadas, sino como coordinador del sistema, facilitador de la interoperabilidad y garante del cumplimiento de los estándares comunes. Sus atribuciones deben circunscribirse a la definición del marco normativo, la coordinación de instancias interinstitucionales y la supervisión del correcto funcionamiento del sistema, respetando en todo momento la autonomía decisional y la responsabilidad legal de cada organismo respecto de sus datos.

### 3.3.3. Síntesis del modelo de gobernanza en documento estructural

El modelo de gobernanza federada debe consolidarse en un documento estructural que sirva como referencia oficial para todas las instituciones participantes y para los equipos responsables de la implementación y operación del Sistema Integrado de Información. Esta Política de Gobernanza de Datos debe integrar de manera coherente los principios rectores, la estructura de gobernanza, los roles y responsabilidades, las instancias de coordinación, y los mecanismos de toma de decisiones y resolución de controversias.

Asimismo, debe establecer un marco claro para la incorporación progresiva de nuevas instituciones, la actualización de estándares y políticas, y la evaluación periódica del modelo de gobernanza. La formalización de este documento no solo contribuye a la claridad institucional y a la reducción de ambigüedades operativas, sino que constituye un elemento clave para la sostenibilidad del sistema federado, la rendición de cuentas y la construcción de confianza entre las instituciones del Estado y con la ciudadanía.

# 4. Plan de implementación

La materialización del SIISSEP requiere un plan de implementación que traduzca el diseño conceptual, normativo y arquitectónico desarrollado en los capítulos precedentes en una

secuencia ordenada de actividades, hitos y decisiones concretas. Este plan debe contemplar no sólo la dimensión tecnológica del despliegue, sino también la construcción progresiva de las capacidades humanas, organizacionales e institucionales que hacen posible la operación sostenida del sistema en el tiempo.

La complejidad del proyecto no radica únicamente en la sofisticación de los componentes técnicos involucrados, sino en la naturaleza interinstitucional del ecosistema que se busca articular. El SIISSEP proyecta la participación de hasta cuarenta y tres instituciones del Estado, cada una con niveles de madurez tecnológica, capacidades profesionales y marcos normativos diferentes.

El presente capítulo se organiza en dos secciones. La primera desarrolla la ruta de implementación, describiendo en detalle los objetivos, actividades principales, entregables y condiciones de éxito. La segunda sección presenta el plan de desarrollo de capacidades y roles, abordando los perfiles técnicos requeridos para construir y operar la plataforma, el desarrollo de capacidades institucionales tanto en el Ministerio como en las instituciones federadas, y las consideraciones para la gestión del cambio organizacional que un proyecto de esta envergadura demanda; ver (Piercy et al. 2013).

## 4.1. Ruta de Implementación

El plan de implementación del SIISSEP se estructura bajo un modelo de despliegue progresivo organizado en cuatro fases secuenciales que se detallarán en los siguientes subcapítulos. La primera fase establece la plataforma centralizada de datos como fundamento operativo del sistema. La segunda fase habilita el motor de consultas federadas sobre la base centralizada, consolidando la interfaz unificada de acceso a la información. La tercera fase incorpora las primeras instituciones federadas al ecosistema, validando en condiciones reales el modelo completo de interoperabilidad. La cuarta fase corresponde a la operación continua del sistema, que incluye simultáneamente la mantención de la plataforma y la incorporación progresiva de nuevas instituciones federadas, constituyendo una etapa de duración indefinida en la medida en que el ecosistema es, por su propia naturaleza, un sistema en permanente evolución. Este enfoque garantiza que el SIISSEP no sea solo una herramienta ministerial, sino el motor de información que sustenta de manera integrada los compromisos del Estado en seguridad pública.

En esta etapa, resulta crítico integrar de manera prioritaria a las Municipalidades, dado que su gestión local aporta información territorial fundamental sobre incivilidades, patrullaje preventivo y realidad barrial, elementos clave para los objetivos de la política nacional.

Para garantizar el éxito de la interoperabilidad, el Ministerio de Seguridad Pública (MSP) debe liderar un proceso de acompañamiento técnico y estratégico con las instituciones externas. Este acompañamiento no solo busca generar confianzas institucionales respecto a la soberanía de los datos, sino también asesorar en la creación de la infraestructura adecuada en aquellas entidades con menor madurez digital.

La expansión se organizará en torno a los seis ámbitos de acción de la PNSP, integrando a sus instituciones asociadas:

- Prevención en Niñez, Adolescencia y Juventud: Incorporación de datos de los sectores de Educación, Salud, Subsecretaría de la Niñez, Servicio Nacional de Protección Especializada (Mejor Niñez), y programas municipales de intervención temprana, entre otros.
- Prevención Territorial: Integración sistémica con Municipalidades, Gobiernos Regionales, Carabineros y organizaciones comunitarias para el monitoreo de espacios públicos.
- Control del Delito: Conexión con Aduanas, Directemar, DGMN y empresas de seguridad privada para la vigilancia fronteriza y de armas.
- Persecución Penal: Fortalecimiento de la interoperabilidad con el Ministerio Público y las policías (Carabineros, PDI, Directemar).
- Sanción, Cárceles y Reinserción: Integración de los sistemas de inteligencia penitenciaria de Gendarmería de Chile y el Ministerio de Justicia.
- Atención y Protección a Víctimas: Articulación de la red de asistencia judicial y centros de apoyo especializados.

Cada fase se concibe como un bloque autónomo con objetivos, entregables y criterios de aceptación propios, de modo que al término de cada una el sistema se encuentre en un estado operativo estable que genere valor inmediato para sus usuarios, independientemente de si las fases posteriores se ejecutan según los plazos originalmente previstos. Esta autonomía relativa entre fases constituye un resguardo fundamental frente a la incertidumbre inherente a proyectos de esta naturaleza, donde factores presupuestarios, normativos o institucionales pueden alterar los plazos pero no deberían comprometer la funcionalidad ya alcanzada.

La secuencia propuesta responde a una lógica de complejidad creciente y dependencia técnica. No es posible habilitar consultas federadas sin una plataforma base operativa, no es prudente conectar instituciones externas a un motor de consultas que no ha sido validado con fuentes controladas y no resulta viable escalar la incorporación de decenas de instituciones sin haber consolidado previamente los procedimientos, estándares y mecanismos de soporte que la operación federada exige. Cada fase, por tanto, genera las condiciones habilitantes para la siguiente, al mismo tiempo que produce resultados concretos para el Ministerio.

Este enfoque incremental no sólo mitiga riesgos técnicos y organizacionales, sino que permite generar resultados tangibles desde etapas tempranas del proyecto. Al finalizar la primera fase, el Ministerio dispondrá de una plataforma funcional de datos con información centralizada y consultable. Al concluir la segunda fase, se habrá establecido la capa de abstracción que permitirá a los usuarios acceder a la información sin necesidad de conocer la ubicación física ni la estructura de las fuentes subyacentes. Cada fase subsiguiente amplía el alcance y el valor del sistema, generando un ciclo virtuoso de adopción, validación y mejora continua.

**Fase 1: Fundación de la plataforma centralizada de datos**

La primera fase tiene como objetivo construir y poner en operación la infraestructura tecnológica base del SIISSEP. Al término de esta fase, el Ministerio contará con un Data Lake y un Data Warehouse operativos, alimentados con datos provenientes hacia su sistema centralizado. Esta fase constituye el cimiento sobre el cual se construirán todas las capacidades posteriores del sistema.

El alcance de esta fase comprende el aprovisionamiento de los servicios de nube pública conforme a las recomendaciones de la Secretaría de Gobierno Digital, incluyendo la selección del proveedor, la coordinación con sus socios comerciales y la configuración de los entornos de red, cómputo y almacenamiento, el despliegue de los almacenes de datos centralizados (Data Lake como repositorio de datos en bruto y Data Warehouse como sistema optimizado para consultas analíticas), y la construcción de los flujos automatizados de ingesta y transformación (ETL) que extraen datos desde las fuentes de origen, los estandarizan conforme a los diccionarios de datos definidos y los cargan en los almacenes correspondientes. Toda la infraestructura se gestiona mediante prácticas de infraestructura como código para asegurar su reproducibilidad, versionamiento y auditabilidad.

Desde el primer día de implementación se incorporan los controles de gestión centralizada de secretos y credenciales, cifrado en reposo y en tránsito, y un sistema de registro de actividad inmutable que garantiza la trazabilidad de todas las operaciones. La seguridad no es un componente que se agrega al final del despliegue, sino una condición transversal que debe estar presente desde la primera línea de configuración, conforme a las obligaciones del Decreto N.° 7 sobre Seguridad de la Información y Ciberseguridad. Se despliegan también los componentes iniciales de monitoreo y observabilidad, preparando la plataforma para recibir en la fase siguiente el motor de consultas que habilitará el acceso real de los usuarios.

La condición para avanzar a la Fase 2 es que la plataforma centralizada opere de manera estable, con datos verificados y con los procesos de seguridad y monitoreo debidamente validados.

**Fase 2: Habilitación del motor de consultas federadas**

La segunda fase tiene como objetivo desplegar y poner en operación el motor de consultas federadas, como por ejemplo Trino, que constituye la pieza central de la arquitectura del SIISSEP y el mecanismo único a través del cual los usuarios ejecutarán todas sus consultas sobre el sistema. Es a partir de esta fase que el SIISSEP se convierte en un sistema verdaderamente utilizable. Se incorporan usuarios con identidades formales, se activan los perfiles de control de acceso por roles y se pone en marcha el sistema de auditoría y trazabilidad que registra de manera exhaustiva toda la actividad del sistema de información. Dado que este motor es el canal exclusivo de consulta tanto en esta fase como en todas las posteriores, su correcta configuración y seguridad es condición indispensable para la operación del ecosistema.

Durante esta fase, el motor se configura inicialmente para operar sobre las fuentes centralizadas del Ministerio desplegadas en la Fase 1, lo que permite validar su funcionamiento, rendimiento y mecanismos de control de acceso en un entorno controlado antes de incorporar fuentes externas. La decisión de desplegar el motor sobre fuentes propias antes de conectar instituciones externas responde a un criterio de prudencia operativa: un motor de consultas federadas es un componente de alta complejidad técnica cuya correcta configuración exige ajustes de rendimiento, gestión de memoria, optimización de consultas y validación rigurosa de los mecanismos de seguridad. Realizar estos ajustes sobre fuentes controladas y bien conocidas reduce significativamente el riesgo y permite al equipo técnico adquirir la experiencia operativa necesaria antes de exponerlo a la variabilidad inherente de las fuentes institucionales externas.

En paralelo con el motor de consultas se despliega el catálogo de datos del ecosistema, cuyo propósito es documentar, clasificar y facilitar la identificación de los activos de información disponibles, incluyendo metadatos descriptivos, linaje, clasificación de seguridad e información de contacto de los responsables. El catálogo constituye una condición esencial para que los usuarios comprendan qué información existe, de dónde proviene y bajo qué condiciones puede ser utilizada, especialmente conforme el ecosistema incorpore decenas de fuentes en fases posteriores. El sistema de auditoría y trazabilidad captura de manera exhaustiva todas las consultas ejecutadas conforme a los requisitos normativos de la Ley N.° 21.730 y del Decreto N.° 7, y se realizan pruebas de rendimiento que validan los tiempos de respuesta definidos en los requerimientos no funcionales del sistema.

La condición para avanzar a la Fase 3 es que el motor de consultas opere de manera estable y segura, que los usuarios reales hayan validado la funcionalidad y los tiempos de respuesta, y que los mecanismos de control de acceso y auditoría hayan sido verificados satisfactoriamente.

**Fase 3: Integración de los primeros nodos federados**

La tercera fase tiene como objetivo transicionar el SIISSEP desde una plataforma centralizada hacia un ecosistema federado propiamente tal, mediante la incorporación de las primeras instituciones federadas. Esta fase constituye la validación integral del modelo de interoperabilidad diseñado. No solo se prueban los componentes técnicos de conectividad, sino también los procedimientos institucionales de negociación de acuerdos, los mecanismos de gobernanza, los estándares de calidad y las capacidades de soporte que el Ministerio debe ejercer en su rol de articulador del ecosistema.

La selección de las primeras instituciones a integrar debe obedecer a criterios de valor operativo, viabilidad técnica y disposición institucional. Se recomienda priorizar aquellas instituciones cuyos datos sean de alta relevancia para las funciones del Ministerio y que dispongan de sistemas con un nivel mínimo de madurez tecnológica que permita la conectividad remota.

El proceso de integración de cada institución comprende, en primer lugar, la formalización de los acuerdos de intercambio de información que establecen con precisión qué datos se exponen, bajo qué condiciones de acceso, para qué finalidades y con qué Acuerdos de Nivel de Servicio (SLA). En segundo lugar, el establecimiento de túneles de conectividad segura conforme al paradigma Zero Trust adoptado por la arquitectura, operando bajo estándares de autenticación mutua y cifrado de extremo a extremo. En tercer lugar, la configuración de los conectores federados en el motor de consultas y el registro de las nuevas fuentes en el catálogo de datos. Finalmente, la ejecución de un período formal de validación que permite evaluar el funcionamiento del ecosistema en condiciones reales, documentar aprendizajes y recopilar retroalimentación de los usuarios finales.

Esta fase debe ir acompañada de un proceso deliberado de sustitución de los canales informales de intercambio de información que actualmente operan entre el Ministerio y las instituciones integradas. Los flujos basados en correo electrónico, soportes físicos, archivos PDF o planillas Excel deben migrar progresivamente hacia el intercambio sistémico y trazable del SIISSEP, resolviendo así una de las debilidades estructurales más significativas identificadas en el diagnóstico.

La condición para avanzar a la Fase 4 es que el modelo federado haya sido validado satisfactoriamente y que se disponga de un protocolo estandarizado y repetible para la incorporación de nuevas instituciones.

Es importante destacar que la implementación de las fases 2 y 3 debe desarrollarse de manera gradual y con un acompañamiento técnico continuo por parte del Ministerio de Seguridad Pública, especialmente en el caso de aquellas instituciones (o unidades dentro de ellas) que no dispongan aún de la infraestructura tecnológica, capacidades técnicas o madurez digital necesarias para integrarse plenamente al ecosistema federado. En aquellos casos en que una institución no logre cumplir oportunamente con los requisitos técnicos y operativos establecidos para la Fase 3, su incorporación al sistema quedará temporalmente suspendida, sin impedir la continuidad del proceso de implementación con aquellas entidades que sí hayan completado satisfactoriamente dicha fase. El sistema podrá, por tanto, avanzar hacia la Fase 4 con los nodos federados plenamente operativos, mientras que las instituciones rezagadas continuarán su proceso de preparación con el apoyo del Ministerio hasta alcanzar las condiciones necesarias para su integración. En función de su nivel de madurez tecnológica, podrán establecerse mecanismos alternativos o transitorios de intercambio de información, conforme a las modalidades técnicas descritas en el Apartado 1.3.2 (Estándares de seguridad) y en el Apartado 2.3.3 (Criterios de expansión modular). Durante este período, dichas instituciones seguirán operando mediante los mecanismos de intercambio de información actualmente vigentes, hasta que puedan integrarse plenamente al SIISSEP y participar del intercambio automatizado de datos dentro del ecosistema.

**Fase 4: Operación continua y expansión progresiva del ecosistema**

La cuarta fase difiere estructuralmente de las anteriores. Se trata de la transición del SIISSEP hacia un régimen de operación permanente en el que conviven simultáneamente dos procesos continuos. La mantención y mejora de la plataforma existente, y la incorporación progresiva de nuevas instituciones al ecosistema federado. Esta fase es, por definición, de duración indefinida.

La operación continua del SIISSEP comprende la supervisión permanente de la infraestructura, la gestión de incidentes técnicos, la aplicación de parches de seguridad y actualizaciones, la optimización de consultas y flujos de datos, la revisión periódica de perfiles de acceso, y la gestión de la relación contractual con los proveedores de servicios cloud. Es fundamental no subestimar la envergadura de estas actividades. En plataformas de datos distribuidas, la mantención constituye el componente dominante del ciclo de vida del sistema. Un motor de consultas federadas que integra decenas de fuentes institucionales requiere atención continua para gestionar los cambios en los esquemas de datos de las instituciones de origen, los incidentes de conectividad, las degradaciones de rendimiento y la evolución de los requerimientos funcionales de los usuarios.

La expansión del ecosistema se ejecuta mediante un proceso estandarizado que replica, para cada nueva institución, el ciclo validado durante la Fase 3. La priorización de las instituciones a incorporar debe considerar el valor de la información que aportan, su nivel de preparación tecnológica e institucional, y la demanda de sus datos por parte de los usuarios del sistema. No todas las instituciones se incorporarán al mismo ritmo, algunas podrán integrarse rápidamente exponiendo bases de datos con interfaces estándar, mientras que otras

requerirán procesos previos de preparación tecnológica o formalización institucional. El plan de expansión debe contemplar esta heterogeneidad, incorporando progresivamente organismos sectoriales y gobiernos locales conforme alcanzan las condiciones habilitantes mínimas, y sustituyendo los canales informales que aún persistan por intercambios sistémicos y trazables.

Conforme el ecosistema alcanza una masa crítica de instituciones integradas, el foco se desplaza además hacia la generación de inteligencia avanzada, combinando las fuentes de información disponibles. Las instancias de gobernanza del capítulo 3 adquieren plena operatividad, incluyendo la revisión periódica de los Acuerdos de Nivel de Servicio (SLA), el ajuste de las políticas de seguridad según la evolución normativa y tecnológica, y la consolidación del diccionario de datos interinstitucional que asegura la interoperabilidad semántica completa entre todas las fuentes del sistema.

## 4.2. Plan de desarrollo de capacidades y roles

La incorporación de los roles técnicos y de gobernanza al ecosistema del SIISSEP no ocurre en un solo momento, sino que sigue una secuencia estratégica alineada con la evolución técnica e institucional de cada fase del proyecto. Esta transición gradual asegura que las capacidades humanas se desarrollen al mismo ritmo que la infraestructura tecnológica.

Durante la Fase 1, enfocada en la fundación de la plataforma centralizada, asume sus funciones el Coordinador de Gobernanza, estableciendo desde el inicio las directrices estratégicas e institucionales del proyecto. A la par, se activa el núcleo puramente técnico e infraestructural. El Ingeniero de Infraestructura Cloud y el Ingeniero de Datos construyen los cimientos del sistema (Data Lake, Data Warehouse y flujos ETL). Simultáneamente, el Especialista en Ciberseguridad implementa los controles y el cifrado desde el primer día de configuración, mientras que el Administrador de Plataforma de Datos asume la operación técnica del entorno base.

Al avanzar a la Fase 2, con la habilitación del motor de consultas federadas, el sistema comienza a procesar accesos reales, lo que exige estructurar el control sobre la información. En este punto se integran el Propietario de Datos y el Custodio de Datos centralizados para gobernar los activos propios del Ministerio. A la par, el Gestor de Metadatos y Catálogo documenta los activos disponibles, el Oficial de Privacidad y Protección de Datos supervisa el cumplimiento normativo, y los Analistas y Científicos de Datos ingresan como los primeros usuarios finales explotando la plataforma.

En la Fase 3, el ecosistema se abre para integrar a las primeras instituciones externas. Ante esta nueva complejidad interinstitucional, el Coordinador de Gobernanza articula su gestión para arbitrar y administrar el ecosistema completo. En las instituciones externas asumen sus funciones el Propietario de Datos y el Custodio de Datos federados, apoyados por el Gestor de Calidad de Datos, quien asegura que la información entrante cumpla con los estándares exigidos antes de integrarse al motor de consultas.

Finalmente, la Fase 4 se define como una etapa de expansión y continuidad operacional. En este punto, no se contempla la creación de nuevos roles adicionales, sino la consolidación de la estructura existente. El foco se desplaza hacia el escalamiento del sistema a nuevas

instituciones y el mantenimiento de los niveles de servicio. Todos los roles previamente activados entran en un régimen de operación continua, adaptando sus responsabilidades para absorber el crecimiento del ecosistema conforme se suman nuevos organismos.

A continuación, se resume la integración de los perfiles según la etapa de despliegue:

**Tabla 1:** Roles del Sistema y fase de incorporación.

| Rol | Fase de Incorporación | Ámbito de Responsabilidad |
|---|---|---|
| **Ingeniero de Infraestructura Cloud** | **Fase 1** | Aprovisionamiento de nube, redes y configuración de alta disponibilidad. |
| **Ingeniero de Datos** | **Fase 1** | Construcción de flujos ETL, limpieza y modelado de datos en el Data Lake/Warehouse. |
| **Especialista en Ciberseguridad** | **Fase 1** | Implementación de Zero Trust, gestión de secretos y seguridad perimetral. |
| **Administrador de Plataforma de Datos** | **Fase 1** | Operación técnica del motor de consultas y orquestación de procesos. |
| **Coordinador de Gobernanza** | **Fase 1** | Conducción del ecosistema, arbitraje y gestión de acuerdos de intercambio. |
| **Propietario de Datos (Centralizado)** | **Fase 2** | Definición de reglas de uso y calidad para los datos propios del Ministerio. |
| **Custodio de Datos (Centralizado)** | **Fase 2** | Aseguramiento operativo de la integridad y disponibilidad de los activos centrales. |
| **Oficial de Privacidad y Protección de Datos** | **Fase 2** | Supervisión legal del tratamiento de datos y procesos de anonimización. |
| **Gestor de Metadatos y Catálogo** | **Fase 2** | Mantenimiento del inventario maestro, diccionarios y clasificación de seguridad. |
| **Analistas y Científicos de Datos** | **Fase 2** | Explotación técnica y generación de tableros de control para la toma de decisiones. |
| **Propietario de Datos (Federado)** | **Fase 3** | Autoridad funcional de la institución externa sobre su propia información. |
| **Custodio de Datos (Federado)** | **Fase 3** | Interlocutor técnico externo encargado de la interoperabilidad de su fuente. |
| **Gestor de Calidad de Datos** | **Fase 3** | Validación de estándares de precisión y consistencia en datos. |

**Fuente:** Elaboración propia.

**Estrategia de Gestión del Cambio Organizacional**

La transición desde un ecosistema de información fragmentado y basado en prácticas informales hacia una arquitectura federada constituye un proceso de transformación organizacional y cultural, además de tecnológico. El diagnóstico evidenció que la persistencia de “silos” y el uso de canales no sistémicos responden a dinámicas institucionales arraigadas que no se corrigen únicamente mediante la incorporación de nuevas herramientas. En este contexto, la gestión del cambio se concibe como un componente estructural de la implementación del SIISSEP.

No se explicita un plan detallado de ejecución ni un “cómo” operativo cerrado, sino que se proponen líneas de acción y ámbitos a considerar que deberán ser desarrollados por la instancia responsable de la conducción estratégica. Entre ellos:

- Conformación de Equipos Transversales: Siguiendo a Piercy et al. (2013), la gestión del cambio en el sector público puede apoyarse en equipos cross-funcionales que contribuyan a superar jerarquías tradicionales y facilitar la interoperabilidad. Estos equipos podrían actuar como facilitadores entre el MSP y las instituciones integrantes, promoviendo coordinación y resolución temprana de fricciones operativas.
- Talleres de Sensibilización y Gobernanza: Se sugiere incorporar instancias dirigidas a autoridades y equipos directivos orientadas a reforzar el principio de soberanía del dato en origen y a clarificar el alcance del modelo federado. Resulta relevante enfatizar que la federación no implica transferencia de titularidad ni pérdida de control institucional, sino interoperabilidad bajo estándares comunes de seguridad y trazabilidad. Asimismo, es fundamental integrar la colaboración entre la Unidad de TI y Gestión de Personas para consolidar una cultura de seguridad institucional. Esta alianza permitirá ejecutar programas de sensibilización y capacitación continua que alineen las competencias del personal con las exigencias de gobernanza, asegurando que cada funcionario comprenda su rol y responsabilidad dentro del modelo federado.
- Instalación de Capacidades Técnicas y Operativas: Alineado con la ruta de implementación, se sugieren programas de capacitación diferenciados por perfiles:
    - Para Custodios y Administradores: Formación técnica en la configuración de nodos de conectividad Zero Trust y mantenimiento de conectores SQL.
    - Para Analistas y Científicos de Datos: Talleres de explotación de datos mediante un motor de consultas (por ejemplo Trino) y visualización avanzada en Power BI, enfocados en la toma de decisiones basada en evidencia.
- Protocolo de Sustitución de Canales Informales: Con el fin de reducir la “heterogeneidad crónica” identificada en el diagnóstico, se sugiere establecer un plan de migración progresiva de flujos críticos actualmente gestionados por medios no trazables. Esto puede incluir la desactivación gradual del intercambio de archivos sensibles por correo o soportes físicos, sustituyéndolos por el acceso trazable y auditado provisto por el SIISSEP.

Esta estrategia adopta el marco de *The Teal Book* (2024), el cual enfatiza que la gestión del cambio organizacional y social constituye un componente crítico en la entrega de soluciones de infraestructura pública, asegurando que la tecnología se traduzca en beneficios operativos reales y sostenibles en el tiempo. En consecuencia, la gestión del cambio debiera acompañar la implementación del SIISSEP desde sus etapas iniciales, procurando que la evolución técnica avance en sintonía con la disposición institucional. Para ello, resulta altamente recomendable contar con el apoyo explícito de las máximas autoridades del Ministerio y de

las instituciones participantes, cuya señal política es un factor determinante para la sostenibilidad del modelo y el cumplimiento del mandato de interoperabilidad. Esta conducción estratégica puede complementarse con una política de comunicaciones oportuna que transparente los beneficios del sistema, reduzca la incertidumbre y fomente la confianza bidireccional entre los nodos del ecosistema. Asimismo, se sugiere considerar la generación de victorias tempranas (quick wins) mediante la entrega de valor tangible en fases iniciales, con el objeto de evidenciar utilidad práctica y facilitar la adhesión institucional a etapas de mayor complejidad técnica.

# 5. Conclusiones y recomendaciones

El Sistema Integrado de Información del Sistema de Seguridad Pública se concibe como un componente estructural del Modelo de Gestión y de la Estrategia Bienal[1], en la medida en que proporciona las condiciones informacionales necesarias para que los mecanismos de dirección, toma de decisiones, monitoreo y control definidos en dicho modelo puedan operar de manera efectiva. No se trata únicamente de un desarrollo tecnológico, sino de la base estructural que permite transformar principios de coordinación en capacidades operativas sustentadas en datos verificables.

El levantamiento técnico, normativo y organizacional mostró que el ecosistema actual presenta niveles heterogéneos de madurez digital, coexistiendo plataformas avanzadas con procesos manuales e intercambios informales. Esta fragmentación limita la posibilidad de contar con información oportuna y trazable para el seguimiento de compromisos, el análisis estratégico y la evaluación de resultados, elementos centrales del Modelo de Gestión. Asimismo, las dinámicas institucionales de resguardo sobre los datos dificultan esquemas de centralización tradicional, mientras que la ausencia de trazabilidad sistemática introduce riesgos en materia de seguridad y control.

Frente a este escenario, la arquitectura propuesta articula capacidades centralizadas de orquestación, definición de estándares y monitoreo, con un esquema federado de soberanía de datos en origen. Esta configuración permite al Ministerio ejercer su rol rector en términos de coordinación y estandarización, sin asumir la custodia directa de las bases sectoriales. La federación no supone ausencia de gobernanza, sino una distribución explícita de responsabilidades que facilita la integración progresiva del sistema y resguarda la coherencia operativa necesaria para sostener el Modelo de Gestión.

Desde la perspectiva normativa, el diseño se estructura en coherencia con los mandatos legales sobre interoperabilidad, rectoría ministerial y tratamiento de información en el ámbito de la seguridad pública. Los mecanismos de estandarización, control de accesos y anonimización contribuyen a que los procesos analíticos y operativos se desarrollen dentro de los márgenes definidos por el marco jurídico vigente. En este sentido, el sistema se plantea como un instrumento que facilita el ejercicio de las atribuciones institucionales, más que como un elemento que las altera.

[1] Ver el Informe Final “Diseño del Sistema de Seguridad Pública: Modelo de Gestión y Estrategia Bienal”

En términos de factibilidad, el modelo considera la capacidad institucional actual y propone un esquema escalable que permite avanzar gradualmente, comenzando por núcleos de integración acotados y ampliándose conforme se consoliden estándares y capacidades. La adopción de componentes tecnológicos abiertos y una arquitectura flexible reduce riesgos de dependencia tecnológica y favorece la sostenibilidad en el tiempo. No obstante, su implementación exige fortalecer competencias técnicas especializadas y asegurar recursos adecuados para su operación y evolución.

En consecuencia, el Sistema Integrado de Información no solo habilita el Modelo de Gestión, sino que lo apalanca al dotarlo de un soporte empírico consistente. Permite que los procesos de planificación, seguimiento y ajuste definidos en el modelo se sustenten en información integrada y auditada, reduciendo la dependencia de reportes fragmentados o intercambios informales. Con ello, se amplían las condiciones para una gestión de la seguridad pública más coordinada y basada en evidencia.

**Recomendaciones**

A partir de las conclusiones precedentes, y considerando el carácter estructural del Sistema Integrado de Información como habilitante y apalancador del Modelo de Gestión, las siguientes recomendaciones buscan orientar su implementación de manera gradual, sostenible y coherente con las capacidades institucionales existentes.

1. Implementación modular y validación por fases: Adoptar rigurosamente un despliegue progresivo estructurado en oleadas. La primera fase debe consolidar la plataforma central del Ministerio y desarrollar un Mínimo Producto Viable que integre un número acotado de instituciones con alta madurez tecnológica y alto valor estratégico. Este enfoque permite validar el motor de consultas federadas, ajustar políticas de seguridad en entornos controlados y establecer un estándar técnico replicable antes de ampliar la integración.
2. Instalación temprana de capacidades críticas: Iniciar de manera prioritaria el reclutamiento y formación de perfiles especializados en arquitectura de datos, interoperabilidad, ciberseguridad, gestión de calidad de datos y analítica avanzada. El Ministerio requiere un equipo técnico de alto nivel capaz de ejercer rectoría efectiva sobre estándares y acuerdos de nivel de servicio, evitando una dependencia excesiva de proveedores externos.
3. Formalización normativa y acuerdos de interoperabilidad: Desarrollar instrumentos administrativos y convenios interinstitucionales que definan responsabilidades, estándares técnicos obligatorios, mecanismos de auditoría y protocolos de acceso. La gobernanza federada debe quedar respaldada en actos formales que aseguren sostenibilidad jurídica y operativa.
4. Plan integral de gestión del cambio: Acompañar la implementación desde el primer día con una estrategia explícita de cambio organizacional. Esto incluye comunicación temprana, patrocinio visible de las máximas autoridades, identificación de “quick wins” que demuestren valor tangible y sustitución progresiva de canales informales de intercambio por el sistema oficial.
5. Plan plurianual de inversión y mantenimiento evolutivo: Establecer un marco presupuestario que contemple no solo el desarrollo inicial, sino también la operación, soporte, actualización tecnológica y ampliación progresiva del sistema. La

sostenibilidad del SIISSEP depende de su capacidad de evolucionar junto con las necesidades del Sistema de Seguridad Pública.

6. Consolidación del modelo híbrido como política institucional: Reconocer formalmente que la arquitectura híbrida, entendida como un esquema de orquestación central con soberanía de datos en origen, constituye el estándar estructural para la integración de información en el sector. Toda iniciativa futura en esta materia debería alinearse con este principio, con el fin de evitar la proliferación de soluciones fragmentadas o desarrollos aislados que debiliten la coherencia del sistema.

En síntesis, el éxito del SIISSEP no depende exclusivamente de su robustez tecnológica, sino de su integración efectiva al Modelo de Gestión como plataforma estructural de coordinación basada en datos. Su implementación representa una transformación institucional de carácter sistémico, cuyo impacto se proyecta más allá del ámbito tecnológico y redefine la forma en que el Estado gestiona la seguridad pública.

# Referencias


- Comisión Europea. (2017). *European Interoperability Framework – Implementation Strategy*. Publications Office of the European Union. Luxemburgo. https://op.europa.eu/en/publication-detail/-/publication/bca40dde-deee-11e7-9749-01aa75ed71a1/language-en
- Congreso Nacional de Chile. (1999). *Ley N° 19.628 sobre protección de la vida privada*.https://www.bcn.cl/leychile/navegar?idNorma=141599
- Congreso Nacional de Chile. (2024). *Ley N° 21.719 que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales*.https://www.bcn.cl/leychile/navegar?idNorma=1209272
- Congreso Nacional de Chile. (2025). *Ley N° 21.730 que crea el Ministerio de Seguridad Pública y regula el Sistema de Seguridad Pública*.https://www.bcn.cl/leychile/navegar?idNorma=1210815
- Gobierno Digital, Gobierno de Chile. (s. f.). *Recomendaciones cloud*. https://wikiguias.digital.gob.cl/guias/guias/recomendaciones_cloudMinisterio de Seguridad Pública. (2025). *Decreto Supremo N° 55, que aprueba el Reglamento del Sistema de Seguridad Pública*. Gobierno de Chile. https://www.bcn.cl/leychile/navegar?idNorma=1217094
- Ministerio del Interior y Seguridad Pública. (2023). *Decreto N° 7 que aprueba la Norma Técnica sobre Seguridad de la Información y Ciberseguridad*. Gobierno de Chile. https://www.bcn.cl/leychile/navegar?idNorma=1195120&idVersion=2023-08-17
- Ministerio del Interior y Seguridad Pública. (2024). *Política Nacional de Seguridad Pública 2025–2031*. Gobierno de Chile.
- Ministerio Secretaría General de la Presidencia. (2023a). *Decreto N° 10 que aprueba la Norma Técnica sobre Sistemas de Gestión de Documentos y Expedientes Electrónicos*. Gobierno de Chile. https://www.bcn.cl/leychile/navegar?idNorma=1195123
- Ministerio Secretaría General de la Presidencia. (2023b). *Decreto N° 12 que aprueba la Norma Técnica de Interoperabilidad para los órganos de la Administración del Estado*.https://www.bcn.cl/leychile/navegar?idNorma=1195125
- Office for National Statistics. (s. f.). *The Five Safes framework*. UK Government. https://www.gov.uk/data-ethics-guidance/the-five-safes-framework
- Organisation for Economic Co-operation and Development. (2019). *The path to becoming a data-driven public sector*. OECD Publishing.

- Organisation for Economic Co-operation and Development. (2020). *OECD digital government index 2019: Results and key findings*. OECD Publishing. https://www.oecd.org/en/publications/the-path-to-becoming-a-data-driven-public-sector_059814a7-en.html
- Piercy, N., Phillips, W., & Lewis, M. (2013). Change management in the public sector: The use of cross-functional teams. *Production Planning & Control 24* (10–11), 976–987. https://doi.org/10.1080/09537287.2012.666913
- Sunstein, C. R. (2024). The use of algorithms in society. *The Review of Austrian Economics, 37*, 399–420. https://doi.org/10.1007/s11138-023-00625-z
- The Teal Book. (2024). *Part F, Chapter 35: Management of organisational and societal change*. https://projectdelivery.gov.uk/teal-book/home/part-f-solution-delivery/chapter-35-management-of-organisational-and-societal-change/
- Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and a maturity assessment framework. *Computers & Security, 133*, Article 103412. https://doi.org/10.1016/j.cose.2023.103412

# A. Anexos

## A.1. Inventario técnico y funcional consolidado

La matriz de información asociada se entrega como documento complementario adjunto a este informe.

## A.2. Matriz de interoperabilidad técnico–normativa

| ID / Flujo | Dominio funcional | Descripción sintética del flujo | Exigencia normativa crítica | Tensión normativo-operativa | Condición habilitante y control |
|---|---|---|---|---|---|
| **F-01 GSTOP (SSP/DSOP)** | Analítico | Plataforma centralizada con carga regional/comunal y extracción a Excel para análisis y reportes mensuales. | Mandato de interoperabilidad, trazabilidad y control de acceso (Ley 21.730; DS 55). | El análisis realizado a partir de extracciones requiere mecanismos complementarios de control para resguardar la trazabilidad del uso de la información. | Estándares ministeriales, catálogo de datos, perfiles de acceso y control de cambios. |
| **F-02 PGOA – Reportes policiales (PDF)** | Documental | Envío formal de planes, metas e informes policiales mediante oficios en formato PDF, asociados a reportes estructurados del PGOA. | Formalización del intercambio, deber de secreto y trazabilidad. | La utilización del PDF como canal formal de reporte introduce una dependencia documental para la reutilización sistémica de información que es originalmente estructurada. | Protocolo formal MSP–policías y consolidación del ingreso estructurado en la plataforma institucional. |
| **F-03 PGOA – Plataforma** | Analítico | Ingreso estructurado en plataforma institucional con exportación a Excel para evaluación interna. | Prohibición de singularización en sistemas analíticos ministeriales (Ley 21.730). | El análisis a partir de extracciones requiere mecanismos organizacionales que aseguren la trazabilidad del uso de la información y la coherencia con la finalidad declarada. | Segregación de dominio analítico, catálogo de datos y control de accesos. |

| ID / Flujo | Dominio funcional | Descripción sintética del flujo | Exigencia normativa crítica | Tensión normativo-operativa | Condición habilitante y control |
|---|---|---|---|---|---|
| **F-04 CECIPU (DICOPOL)** | Documental | Postulaciones web con datos personales y respaldo documental en PDF; revisión manual apoyada en Excel. | Protección de datos personales y control de acceso (Ley 19.628). | El tratamiento posterior basado en revisión manual y soportes documentales requiere controles consistentes de acceso y custodia para asegurar la protección de los datos personales durante todo el proceso. | Clasificación de datos, definición de roles de acceso y auditoría de accesos a la plataforma y a los repositorios documentales. |
| **F-05 Eventos Masivos** | Documental / Operativo | Recepción de resoluciones judiciales en PDF, sistematización interna y redistribución operativa. | Trazabilidad documental y deber de secreto (DS 55; Dec. 10). | La interoperabilidad del flujo se encuentra condicionada por la dependencia de insumos documentales provenientes de órganos autónomos y por la necesidad de asegurar trazabilidad y custodia reforzada desde su recepción. | Convenios interinstitucionales, procedimientos formales de recepción y gestión documental trazable. |
| **F-06 DACRIM – Consolidados periódicos** | Analítico | Recepción periódica de planillas Excel multifuente para consolidación y análisis estadístico nacional. | Interoperabilidad federada y calidad del dato. | La consolidación analítica depende de procesos posteriores de estandarización y documentación de esquemas, debido a la heterogeneidad de las fuentes de origen. | Catálogo de datos común, reglas de versionamiento de esquemas y documentación técnica de las fuentes. |

| ID / Flujo | Dominio funcional | Descripción sintética del flujo | Exigencia normativa crítica | Tensión normativo-operativa | Condición habilitante y control |
|---|---|---|---|---|---|
| **F-07 DACRIM – Reportes diarios críticos** | Operativo | Reportes diarios sensibles enviados por correo y WhatsApp en formato PDF. | Seguridad de la información y uso de canales institucionales. | El uso de canales no sistémicos y formatos documentales para información sensible dificulta asegurar niveles homogéneos de trazabilidad y resguardo exigidos por la normativa. | Sustitución progresiva de canales informales por mecanismos de intercambio institucional seguros y trazables. |
| **F-08 SPD/DDT – Sistemas municipales** | Analítico | Plataformas de reporte municipal con extracción a Excel para análisis y control de cumplimiento. | Mandato de coordinación y trazabilidad (Ley 21.730). | La heterogeneidad de capacidades y estructuras municipales, junto con el análisis a partir de extracciones, requiere mecanismos comunes de estandarización y control de calidad para asegurar trazabilidad y comparabilidad. | Estándares comunes, control de calidad y monitoreo institucional. |
| **F-09 SPD/CEAD** | Analítico | Recepción de DBF por correo y soportes físicos (CD) para análisis estadístico. | Seguridad de la información y trazabilidad reforzada. | El uso de formatos legados y soportes físicos para el intercambio de información sensible limita la trazabilidad y el resguardo exigidos por los estándares de seguridad vigentes. | Sustitución de soportes físicos por intercambio seguro. |

| ID / Flujo | Dominio funcional | Descripción sintética del flujo | Exigencia normativa crítica | Tensión normativo-operativa | Condición habilitante y control |
|---|---|---|---|---|---|
| **F-10 SITIA Patentes** | Operativo | Streaming de datos estructurados en tiempo real para apoyo operativo territorial. | Seguridad, control de acceso y disponibilidad del servicio. | La operación en tiempo real requiere asegurar disponibilidad continua del servicio y controles de acceso proporcionales al uso operativo de la información. | Accesos por rol, trazabilidad y monitoreo central. |
| **F-11 SITIA Evidencias** | Operativo | Consulta estructurada de evidencias bajo requerimiento institucional. | Deber de secreto y protección reforzada de datos sensibles. | La naturaleza altamente sensible del contenido exige un acceso estrictamente acotado y controlado, incompatible con esquemas de interoperabilidad abierta. | Autorización expresa, entornos segregados y auditoría completa. |
| **F-12 CICPOL – Consultas interinstitucionales** | Operativo | Acceso y consulta a sistemas de terceros para coordinación policial. | Custodia del dato en la institución de origen y cumplimiento de finalidades específicas de seguridad (Ley 21.730; DS 55). | La diversidad de instituciones de origen implica reglas de negocio y niveles de madurez disímiles que dificultan una integración estandarizada inmediata. | Intercambio mediante convenios específicos, perfiles de acceso definidos por la institución de origen y controles centralizados de auditoría. |

| ID / Flujo | Dominio funcional | Descripción sintética del flujo | Exigencia normativa crítica | Tensión normativo-operativa | Condición habilitante y control |
|---|---|---|---|---|---|
| **F-13 DCOTSF – SIREGARD** | Operativo / Regulatorio | Sistema de registro y control de sustancias químicas controladas para fiscalización administrativa y apoyo a funciones de seguridad. | Deber de secreto, protección de datos sensibles y trazabilidad reforzada. | La articulación con otros sistemas debe resguardar el rol rector y la custodia administrativa de los datos. | Convenio específico, segmentación de accesos por rol y trazabilidad completa. |

## A.3. Glosario de términos

**Conceptos Estratégicos y Normativos**

- **Arquitectura Federada:** Modelo de integración de datos donde la información permanece en los sistemas de las instituciones de origen y solo se accede a ella mediante consultas en tiempo real. Esto permite la interoperabilidad sin centralizar físicamente las bases de datos ni vulnerar la custodia original.
- **Gobernanza de Datos:** Marco de reglas, roles y procesos que aseguran que la información sea precisa, privada, segura y utilizada de acuerdo con la normativa legal (Ley 21.730 y Ley 19.628).
- **Interoperabilidad:** Capacidad de dos o más sistemas o instituciones para intercambiar información y utilizar los datos intercambiados de manera coherente (técnica, semántica y organizacionalmente).
- **Ley 21.730:** Marco legal que crea el Ministerio de Seguridad Pública y establece el mandato de interoperabilidad para las instituciones del Sistema de Seguridad Pública en Chile.
- **Soberanía de Datos:** Principio que establece que cada institución mantiene la propiedad legal, la responsabilidad técnica y el control sobre quién accede a los datos que genera en el ejercicio de sus funciones.

**Conceptos Técnicos de Arquitectura**

- **API (Application Programming Interface):** Conjunto de reglas que permite que una aplicación se comunique con otra para solicitar datos o servicios de forma automatizada.
- **Catálogo de Datos:** Inventario centralizado que describe qué datos existen, dónde están, quién es su dueño y qué nivel de sensibilidad tienen, facilitando su descubrimiento por parte de analistas autorizados.
- **Data Lake (Lago de Datos):** Repositorio de almacenamiento que contiene una gran cantidad de datos en su formato original ("en crudo") hasta que son necesarios para procesamiento o análisis.
- **Data Warehouse (Bodega de Datos):** Sistema de almacenamiento optimizado para el análisis de datos estructurados, diseñado para generar reportes, estadísticas y apoyo a la toma de decisiones estratégicas.
- **JDBC (Java Database Connectivity):** Estándar tecnológico que permite a una aplicación (como el motor de consultas del MSP) conectarse a diferentes bases de datos institucionales de forma uniforme.
- **Motor de Consultas Federadas:** Componente de software que recibe una pregunta de un usuario, busca la respuesta en múltiples bases de datos externas simultáneamente y entrega un único resultado consolidado.

**Seguridad y Privacidad**

- **Anonimización:** Proceso técnico que elimina la posibilidad de identificar a una persona a partir de sus datos, requisito legal para el análisis de políticas públicas en el Ministerio.
- **mTLS (Mutual TLS):** Protocolo de seguridad donde tanto el emisor como el receptor de la información deben presentar certificados digitales para validar su identidad antes de intercambiar datos.
- **Transport Layer Security (TLS)** es un protocolo de seguridad ampliamente adoptado, diseñado para facilitar la privacidad y la seguridad de los datos en las comunicaciones por Internet.
- **Trazabilidad:** Capacidad de reconstruir el historial de uso de un dato, permitiendo saber exactamente quién accedió a qué información, en qué momento y con qué justificación.
- **Zero Trust (Confianza Cero):** Modelo de ciberseguridad que asume que ninguna conexión es segura por defecto. Requiere verificación estricta para cada persona y dispositivo que intente acceder a recursos en la red, incluso si están "dentro" del perímetro institucional.