Anexo 5: Reglas de Uso de la Plataforma de Interoperabilidad del Sector Trabajo y Previsión Social (Reglas de Uso)

Autor: Unidad IoP, DTI-SPS

Versión: 17-oct-25, 15:00

Contenido

Capítulo 1. Objeto y alcance

Este documento fija, en términos simples, cómo se usa la Plataforma de Interoperabilidad del Sector Trabajo y Previsión Social —compuesta por el Nodo Laboral y Previsional (Nodo L&P) y la Ficha Única de Información Laboral y Previsional (Ficha L&P)— para que el intercambio de datos entre instituciones sea seguro, trazable y estrictamente ajustado a finalidades públicas definidas. Las presentes reglas complementan el Convenio Marco; en caso de duda, prevalece lo dispuesto en el Convenio y en la normativa aplicable.

1.1 A quién aplica

Aplica a todas las instituciones que adhieran al Convenio, a sus equipos y usuarios autorizados que operen la Plataforma y, cuando corresponda, a terceros o encargados que actúen por cuenta de dichas instituciones, quienes quedan sujetos a obligaciones equivalentes en seguridad, confidencialidad y trazabilidad.

1.2 Qué cubre

Cubre las reglas comunes para habilitar, operar y auditar flujos de datos del Nodo L&P y el consumo de la Ficha L&P; define deberes mínimos de seguridad, trazabilidad, niveles de servicio y uso adecuado de la información, y su relación con los instrumentos habilitantes (formularios/anexos) que detallan cada flujo o conjunto de datos.

1.3 Relación con el Convenio

Estas Reglas forman el “Anexo 5” del Convenio Marco. No crean nuevas bases legales ni alteran la titularidad de los datos. Su función es operativizar cómo se accede, usa y verifica el cumplimiento del Convenio, incluyendo los procedimientos, métricas y medios de prueba que la Subsecretaría podrá requerir.

1.4 Vigencia y ámbito territorial

Rigen desde su publicación oficial y mientras el Convenio esté vigente; se aplican a operaciones realizadas en Chile y a los servicios externos o en la nube que soporten la Plataforma para dichas operaciones.

1.5 Qué no regula

No define bases legales de acceso a datos (cada flujo debe fundarse en su finalidad y base legal declaradas en su instrumento habilitante) ni impone tecnologías o proveedores específicos: los aspectos técnicos concretos se fijan caso a caso en los anexos correspondientes, manteniendo neutralidad tecnológica.

Capítulo 2. Principios rectores

Los principios rectores orientan todas las decisiones y actuaciones de quienes operan la Plataforma de Interoperabilidad del Sector Trabajo y Previsión Social. Son criterios prácticos y verificables: sirven para diseñar flujos, configurar accesos, ejecutar consumos y auditar el uso de los datos. Cada principio exige evidencias documentales y técnicas que deberán conservarse y presentarse cuando la Subsecretaría lo requiera.

2.1 Legalidad y finalidad pública

Toda provisión y consumo de datos debe fundarse en una atribución legal y responder a una finalidad pública explícita, descrita en el instrumento habilitante del flujo. No se permiten usos "genéricos" ni fines distintos a los declarados. Cómo se aplica: cada flujo debe identificar norma habilitante y propósito concreto, y adjuntar el acto o resolución que lo respalda.

2.2 Necesidad y proporcionalidad (minimización de datos)

Solo se solicitarán y compartirán los datos estrictamente necesarios para cumplir la finalidad declarada, evitando atributos redundantes o excesivos. Cómo se aplica: antes de publicar un catálogo o solicitar un consumo, se justifican uno a uno los campos y se descartan los no esenciales.

2.3 Titularidad y calidad de la información

La titularidad de los datos no se altera por el intercambio; la institución de origen sigue siendo responsable de su veracidad y actualización. Cómo se aplica: las publicaciones deben indicar fuente, fecha de actualización y reglas de versión; los consumidores deben validar coherencia básica y reportar inconsistencias al proveedor.

2.4 Seguridad y confidencialidad por diseño

Los flujos deben incorporar medidas de seguridad "desde el diseño": control de acceso por roles y principios de menor privilegio, cifrado en tránsito y en reposo donde corresponda, segregación de ambientes y resguardo de secretos (claves, tokens). Cómo se aplica: todo consumo se autentica, toda operación se autoriza, y toda credencial tiene responsable nominativo, vigencia y rotación.

2.5 Trazabilidad y rendición de cuentas (accountability)

Cada operación debe quedar registrada con quién, qué, cuándo, dónde (sistema/origen) y para qué finalidad. Cómo se aplica: el Nodo y las instituciones mantienen bitácoras inmutables de publicación y consumo, con conservación por el plazo fijado y capacidad de reconstruir la historia de un dato.

2.6 Exactitud, integridad y no repudio

Las respuestas publicadas deben ser íntegras, y su integridad verificable mediante huellas de versión; las solicitudes deben ser auténticas y no repudiables. Cómo se aplica: las publicaciones incluyen identificador de versión y huella de integridad (p. ej., hash del payload); los consumidores validan firma o huella y conservan el comprobante de verificación.

2.7 Transparencia operativa y auditabilidad

Las instituciones deben poder explicar sus consumos y publicaciones ante auditorías internas o externas, sin revelar información sensible innecesaria. Cómo se aplica: se mantiene un expediente operativo por flujo (formulario, base legal, pruebas UAT, controles, métricas, bitácoras y responsables), disponible para revisión.

2.8 Neutralidad tecnológica e interoperabilidad abierta

La Plataforma promueve especificaciones abiertas y evita dependencias exclusivas de proveedor. Cómo se aplica: los catálogos de datos usan definiciones y formatos estandarizados; las APIs documentan contratos, códigos de error y esquemas; los cambios de versión siguen controles de compatibilidad y avisos previos.

2.9 Privacidad y protección de datos personales

Cuando los datos sean personales, su tratamiento debe ajustarse al marco vigente, aplicando medidas reforzadas de seguridad y limitaciones de finalidad. Cómo se aplica: se evalúan riesgos de privacidad para cada flujo, se aplican políticas de acceso granular, y se minimiza la exposición en ambientes no productivos.

2.10 No discriminación y uso legítimo

Se prohíbe usar la Plataforma para prácticas discriminatorias, perfilamientos indebidos o evaluaciones masivas ajenas a la finalidad declarada (por ejemplo, fines de estudio o investigación sin base legal). Cómo se aplica: los instrumentos habilitantes excluyen expresamente usos incompatibles; los monitores de consumo detectan patrones anómalos.

2.11 Continuidad del servicio y mejora continua

La operación debe asegurar disponibilidad acorde a los niveles de servicio definidos, gestión oportuna de incidentes y mejora continua de desempeño y capacidad. Cómo se aplica: se monitorean SLA, se ejecutan planes de normalización ante desvíos y se documentan medidas correctivas y preventivas (RCA).

2.12 Gobernanza y corresponsabilidad

La Subsecretaría lidera la gobernanza sectorial; cada institución es responsable de su conducta de publicación y consumo, y de controlar a sus encargados o terceros. Cómo se aplica: existen roles formales (responsable institucional, responsables técnicos y de seguridad), con sustitutos, canales de escalamiento y matriz RACI vigente por flujo.

Capítulo 3. Roles y responsabilidades

La Plataforma se gobierna bajo un modelo de corresponsabilidad: la Subsecretaría de Previsión Social conduce, las instituciones participantes operan sus publicaciones y consumos, y ciertos órganos transversales apoyan con lineamientos y supervisión. Este capítulo describe cada rol "en lenguaje de uso", delimitando su ámbito de acción, decisiones que puede tomar y evidencias mínimas que debe mantener. Cuando un mismo organismo asume más de un rol, deberá separar funciones y responsabilidades para evitar conflictos y asegurar control cruzado.

3.1 Subsecretaría de Previsión Social (SPS) – Gobernanza sectorial

La SPS lidera la gobernanza de la Plataforma, define reglas de uso, aprueba altas y cambios relevantes de flujos, y coordina incidentes críticos.

- Qué hace: dicta lineamientos, aprueba o rechaza publicaciones/consumos nuevos o sus versiones mayores, convoca y dirige la Mesa de Interoperabilidad, verifica cumplimiento y coordina auditorías.
- Puede decidir sobre: ingreso/suspensión de instituciones, ventanas de mantenimiento extraordinarias, planes de normalización por desvíos de SLA, y medidas especiales de seguridad/contingencia.
- Evidencias mínimas: resoluciones o actas de aprobación/rechazo, bitácoras de incidentes y RCA, métricas de cumplimiento, comunicaciones oficiales.

3.2 Mesa de Interoperabilidad del Sector Trabajo y Previsión Social (Mesa IoP)

Instancia operativa y de coordinación entre las instituciones (OAEs) adheridas.

- Qué hace: revisa catálogos y cambios, alinea agendas técnicas y operativas, prioriza mejoras y pruebas, y hace seguimiento de riesgos.
- Puede decidir sobre: priorización de iteraciones y mejoras no críticas, acuerdos de compatibilidad y plazos de adopción.
- Evidencias: actas, acuerdos operativos, backlog priorizado y calendario de UAT/paso a entorno productivo (Go-Live).

3.3 Comité Directivo (SPS)

Órgano de decisión estratégica que resuelve controversias y define prioridades mayores.

- Qué hace: valida planes anuales, financiamiento y metas de servicio.
- Puede decidir sobre: ampliación de alcance funcional y asignación de recursos.
- Evidencias: actas, resoluciones y cuadro de control de metas.

3.4 Operación de Plataforma (Unidad IoP-SPS)

Responsable técnico-operativo del Nodo y la Ficha en ambientes sandbox, UAT y producción.

- Qué hace: administra la infraestructura y los servicios de integración, publica y mantiene documentación técnica, opera monitoreo, despliegues y respaldo; gestiona mesa de ayuda de la Plataforma.
- Puede decidir sobre: cambios menores (hotfixes, parches de seguridad urgentes), escalamiento de incidentes y ejecución de planes de continuidad.

- Evidencias: bitácoras de cambios (CAB), manuales vigentes, tableros de monitoreo, reportes de disponibilidad y capacidad, inventario de credenciales/secretos y su rotación.

3.5 MINHAC (Secretaría de Modernización del Estado y Secretaría de Gobierno Digital)

Rol normativo y de articulación con lineamientos de transformación digital e interoperabilidad del Estado.

- Qué hace: emite lineamientos y buenas prácticas, revisa consistencia con estándares estatales y facilita articulación con plataformas transversales.
- Puede decidir sobre: observaciones técnicas y de cumplimiento transversal; recomendaciones vinculantes cuando así se establezca.
- Evidencias: oficios, informes de revisión y matrices de cumplimiento.

3.6 Instituciones Publicadoras de datos (Proveedor)

Cada institución que expone un flujo o catálogo de datos mediante el Nodo.

- Qué hace: define la finalidad del flujo, su base legal y catálogo mínimo; mantiene calidad, oportunidad y seguridad de la publicación; gestiona versiones y comunicados de cambio.
- Puede decidir sobre: evolución del catálogo (en los márgenes aprobados), ventanas de actualización propias y suspensión preventiva por riesgo.
- Evidencias: formulario/instrumento habilitante, especificación del contrato de servicio (endpoint, esquema, códigos de error), changelog, registros de publicación y controles de integridad.

3.7 Instituciones Consumidoras de datos (Consumidor)

Cada institución que invoca flujos publicados mediante el Nodo.

- Qué hace: solicita habilitación de consumo fundado en finalidad y base legal; implementa controles de acceso por rol y registra cada operación con su finalidad.
- Puede decidir sobre: perfiles de acceso internos y suspensión de consumos ante incidentes o desvíos.
- Evidencias: formulario de consumo habilitado, matriz de perfiles/roles, evidencia de pruebas UAT, registros de consumo y comprobantes de verificación de integridad/firma.

3.8 Responsables institucionales (por cada institución adherida)

Figura nominativa que responde por la conducta de publicación y/o consumo ante SPS.

- Qué hace: actúa como punto único de contacto; asegura que existan responsables técnico y de seguridad, y que la documentación esté al día.
- Puede decidir sobre: solicitudes de alta/cambio/baja de flujos y perfiles.
- Evidencias: designación formal, RACI vigente, expediente operativo por flujo (base legal, pruebas, métricas, bitácoras, controles).

3.9 Responsable técnico (por flujo y por institución)

- Qué hace: implementa y mantiene las integraciones; gestiona versiones y pruebas; atiende incidentes técnicos y participa en RCA.
- Evidencias: plan de pruebas, resultados UAT/Go-Live, bitácora de cambios, documentación de APIs/contratos y planes de reversa.

3.10 Responsable de seguridad y confidencialidad (por institución)

- Qué hace: define y verifica controles de acceso, segregación de ambientes, gestión de secretos y resguardo de logs; valida que cada operación tenga trazabilidad y finalidad.
- Puede decidir sobre: suspensión preventiva del flujo por riesgo o incidente; exigencia de rotación de credenciales y endurecimiento (hardening).
- Evidencias: matriz de controles, reportes de accesos, registros de autenticación/autorización, políticas de retención y destrucción segura.

3.11 Administrador funcional de catálogos/datos (lado proveedor)

- Qué hace: asegura que los campos publicados sean necesarios y suficientes; mantiene definiciones de datos y reglas de negocio; coordina cambios funcionales y comunica impactos.
- Evidencias: diccionario de datos, glosario de términos, justificación de minimización y actas de cambios funcionales.

3.12 Administrador de usuarios y perfiles (lado consumidor)

- Qué hace: habilita y revoca usuarios, revisa periódicamente vigencias y privilegios; mantiene segregación de funciones y registra altas/bajas con trazabilidad.
- Evidencias: listado vigente de usuarios/perfiles, registros de auditoría de altas/bajas y constancias de revisiones periódicas.

3.13 Soporte y Mesa de Ayuda de la Plataforma

- Qué hace: atiende requerimientos, categoriza incidentes (S1/S2/S3), deriva y monitorea SLA.
- Evidencias: tickets con causa, impacto y resolución; tableros de tiempos de atención y cumplimiento de SLA.

3.14 Encargados o terceros que operen por cuenta de una institución

- Qué hace: ejecutan tareas delegadas bajo instrucciones de la institución responsable, con obligaciones equivalentes en seguridad, confidencialidad y trazabilidad.
- Reglas: toda delegación debe constar por escrito, delimitar finalidades y plazos, y prever auditorías y sanciones por incumplimiento.
- Evidencias: contratos o convenios de encargo, anexos de seguridad y privacidad, informes de auditoría y registros de acceso del encargado.

3.15 Auditoría interna/externa (cuando aplique)

- Qué hace: revisa el cumplimiento de reglas de uso, seguridad, trazabilidad, niveles de servicio y correcta aplicación de finalidades.
- Evidencias: planes y reportes de auditoría, hallazgos, planes de acción y verificaciones de cierre.

3.16 Reglas comunes para todos los roles

- Principio de mínimo privilegio: accesos sólo a lo necesario, por el tiempo estrictamente requerido.
- No repudio y trazabilidad: toda acción queda registrada y debe poder atribuirse a una persona o sistema responsable.
- Separación de ambientes: pruebas y capacitación nunca usan datos reales salvo autorización expresa y controles reforzados.
- Gestión de cambios: ninguna modificación se promueve a producción sin documentación, pruebas y plan de reversa.
- Deber de colaboración: ante incidentes o auditorías, todas las partes deben aportar antecedentes de forma completa y oportuna.

Capítulo 4. Reglas de publicación y consumo

Este capítulo establece, en lenguaje de uso, cómo una institución publica datos en el Nodo y cómo otra los consume mediante la Plataforma. Las reglas son comunes para todo flujo y aplican adicionalmente a lo que cada instrumento habilitante señale (formulario de alta de publicación o de consumo).

4.1 Reglas para publicar datos (rol Proveedor)

a) Finalidad y base habilitante, por escrito.
Antes de exponer un flujo, la institución debe declarar para qué se publican los datos y la norma/acto que lo habilita. Esa información queda en su instrumento de publicación y se mantiene disponible para revisión.

b) Catálogo mínimo y justificación de campos.
Cada publicación identifica su "contrato" (endpoint, esquema, campos, códigos de error) y explica por qué cada atributo es necesario para la finalidad. Campos redundantes o no esenciales no deben publicarse.

c) Versionado y compatibilidad.
Las publicaciones tienen versión (v1, v1.1, v2…). Los cambios menores mantienen compatibilidad; los mayores requieren aprobación previa y aviso con plazo razonable a consumidores.

d) Calidad y oportunidad.
El proveedor asegura que los datos estén completos, coherentes y actualizados según lo comprometido. Debe corregir a la brevedad errores detectados y comunicar impactos.

e) Seguridad y acceso.
Solo se expone lo indispensable. El acceso se controla por autenticación y autorización de la Plataforma; no se usan credenciales compartidas. Las claves/tokens tienen responsable nominativo y rotación.

f) Trazabilidad e integridad.
Cada respuesta se registra (quién, cuándo, qué se sirvió). La publicación indica su identificador de versión y su huella de integridad; el proveedor conserva logs por el plazo definido.

g) Ambientes segregados.
Toda publicación tiene, cuando corresponda, sandbox/UAT para pruebas con datos ficticios o enmascarados. Nunca se usan datos reales en pruebas salvo autorización expresa y controles reforzados.

h) Comunicación de cambios e incidencias.
El proveedor avisa anticipadamente ventanas y cambios que afecten a consumidores; ante incidentes, informa causa, impacto y medidas (RCA) en los plazos definidos.

4.2 Reglas para consumir datos (rol Consumidor)

a) Consumo fundado y proporcional.
Cada consumo declara finalidad pública y base habilitante en su instrumento de consumo. Se pide solo lo estrictamente necesario; no se encadenan consultas para finalidades distintas.

b) Uso transaccional, no "scraping".
La Plataforma se usa dentro de procedimientos administrativos o servicios definidos. No se permiten barridos masivos o prácticas de extracción sistemática no vinculadas a un caso/acto administrativo.

c) Gestión de usuarios y perfiles.
La institución define roles mínimos, habilita y revoca accesos con trazabilidad. Revisa periódicamente vigencias y privilegios.

d) Verificación de integridad y resguardo de evidencia.
El consumidor valida la integridad de la respuesta (huella/firma cuando aplique) y guarda el comprobante junto a la referencia del expediente o caso que motivó la consulta.

e) Responsabilidad por el uso.
Los datos se emplean solo para la finalidad declarada, sin cederlos internamente a fines distintos ni a terceros, salvo autorización habilitante.

f) Desempeño y buenas prácticas.
Las integraciones deben implementar manejo de errores, reintentos prudentes y backoff. No se ejecutan pruebas de carga sin coordinación sectorial.

4.3 Contratos de servicio (API/servicio) y catálogos

a) Especificación clara.
Toda publicación cuenta con: (i) endpoint y método, (ii) esquema de datos con tipos y reglas de negocio, (iii) códigos de error y mensajes, (iv) límites de uso/cuotas, (v) ventanas y calendario de operación.

b) Estándares y consistencia.
Se priorizan formatos abiertos y convenciones coherentes (nombres de campos, estados, códigos). Las definiciones funcionales se mantienen en un catálogo sectorial actualizado.

c) Cambios controlados.
Cada modificación indica impacto, plan de transición, pruebas requeridas y fecha de entrada en vigor.

4.4 Pruebas, paso a producción y reversa

a) UAT obligatorio.
Antes del "Go-Live", proveedor y consumidor realizan pruebas funcionales y de seguridad en UAT, con casos representativos. Los resultados quedan documentados.

b) Criterios de aprobación.
Para pasar a producción se requiere: (i) casos de prueba aprobados, (ii) documentación vigente, (iii) monitoreo y alertas configuradas, (iv) plan de reversa probado.

c) Plan de reversa y contingencia.
Todo despliegue define cómo volver a la versión anterior sin pérdida de trazabilidad ni integridad.

4.5 Seguridad mínima aplicable a toda operación

a) Autenticación y autorización.
Cada llamada se autentica; cada operación se autoriza por perfil. Se aplica principio de mínimo privilegio y segmentación de redes/servicios cuando corresponda.

b) Protección de secretos y cifrado.
Las credenciales se almacenan en cofres seguros; se usa cifrado en tránsito y, cuando corresponda, en reposo.

c) Logs inmutables y preservación.
Los registros de publicación y consumo son completos, protegidos contra alteraciones y conservados por el plazo definido para auditoría.

4.6 Trazabilidad y rendición de cuentas

a) Datos mínimos del evento.
Toda operación registra: identificador del sistema/usuario, fecha y hora, finalidad del consumo, identificador de expediente/proceso, endpoint invocado, parámetros relevantes y resultado.

b) Acceso a auditoría.
Proveedor y consumidor deben poder exhibir sus registros ante requerimientos de la Subsecretaría o auditorías internas/externas.

4.7 Cuotas, límites y protección de la Plataforma

a) Límites por diseño.
Cada publicación define límites de tasa y de concurrencia. Su propósito es proteger disponibilidad y evitar abusos.

b) Excepciones gestionadas.
Necesidades transitorias (p. ej., incrementos por contingencias) se canalizan para evaluación y, de aprobarse, se habilitan con medidas de control y un plazo acotado.

4.8 Ventanas de mantenimiento y cambios

a) Calendario y aviso.
Las ventanas regulares se comunican con antelación razonable y se concentran fuera de horarios críticos. Cambios de alto impacto requieren coordinación sectorial.

b) Emergencias.
Ante riesgos de seguridad o disponibilidad, se podrán aplicar ventanas extraordinarias, con comunicación posterior del detalle y medidas adoptadas.

4.9 Reglas de ambientes (sandbox / UAT / producción)

a) Separación estricta.
Cada ambiente tiene propósitos y controles propios. Los endpoints y credenciales son distintos y no reutilizables entre ambientes.

b) Datos de prueba.
Se utilizarán datos sintéticos o debidamente enmascarados. Sólo por excepción fundada y controles reforzados se podrán usar datos reales fuera de producción.

4.10 Evidencias obligatorias por flujo (expediente operativo)

Toda publicación y todo consumo debe mantener, al menos: instrumento habilitante (Convenio y anexo(s)), especificación del servicio, plan y resultados de pruebas, registro de pases a producción, bitácoras de cambios y operaciones, métricas e informes de incidentes y su RCA.

4.11 Prohibiciones y usos indebidos

- Usar datos para fines distintos a los declarados o sin base habilitante.
- Ejecutar scraping, barridos masivos o pruebas de carga sin autorización.
- Compartir credenciales o eludir controles de la Plataforma.
- Replicar o almacenar datos fuera de lo necesario para la finalidad y el plazo declarados.
- Usar ambientes de prueba con datos reales sin autorización y controles reforzados.

Capítulo 5. Niveles de servicio, incidentes y continuidad operativa

Este capítulo fija, en lenguaje práctico, cómo medimos el servicio, cómo reaccionamos ante incidentes y cómo aseguramos la continuidad de la Plataforma (Nodo L&P y Ficha L&P). Sus parámetros se declaran por flujo en su instrumento habilitante; cuando exista un SLA sectorial publicado por la Subsecretaría, servirá como referencia por defecto.

5.1 Objetivo

Tener expectativas claras y medibles de disponibilidad, desempeño, soporte y comunicación de cambios, para que proveedores y consumidores planifiquen su operación y controlen desvíos con evidencia.

5.2 Métricas y umbrales (qué se mide)

Como mínimo, cada flujo define: (1) disponibilidad mensual, (2) latencia p95 en consultas síncronas, (3) tasa de error aplicable, (4) capacidad/cuotas por institución y por flujo, (5) RPO/RTO para lotes y eventos, (6) soporte: tiempos de primera respuesta/atención por severidad, y (7) mantenibilidad (MTBF/MTTR) cuando aplique. Toda métrica declara umbral, fuente de medición y periodicidad de reporte.

5.3 Medición y reporte

La operación del Nodo/Ficha publica indicadores y gestiona un tablero sectorial; los informes incluyen resultados versus umbrales, tendencias y, cuando aplique, reporte post-incidente con causa, acciones y plazos. El historial queda versionado en el Repositorio Digital Sectorial.

5.4 Severidad y tiempos de atención

Se clasifica el incidente por impacto: S1 (crítico), S2 (alto) y S3 (medio/bajo). Como referencia: S1 primera respuesta ≤1 h y escalamiento en ≤2 h con actualizaciones cada 2 h; S2 primera respuesta ≤4 h y escalamiento en ≤8 h con comunicación diaria; S3 primera respuesta ≤1 día hábil y resolución/escalamiento en ≤5 días hábiles. Los tiempos exactos se fijan en el instrumento del flujo o en el SLA sectorial.

5.5 Procedimiento de gestión de incidentes

Detectado un evento, la institución afectada registra síntoma/alcance preliminar y severidad; si es S1/S2, notifica de inmediato a la Subsecretaría por el canal oficial. Se clasifica y escala (≤1 h), se contiene (p. ej., revocar credenciales, aplicar throttling o cambiar temporalmente de síncrono a lotes), se emite comunicación inicial (S1 ≤2 h; S2 ≤4 h), se remedia y recupera según RPO/RTO del flujo, y se cierra con RCA completo en ≤10 días hábiles. La Subsecretaría coordina S1/S2 y valida el cierre sectorial.

5.6 Ventanas de mantenimiento y cambios

Las ventanas programadas se concentran en horarios de bajo tráfico, con aviso mínimo definido (fecha, horario, impacto y contingencia). Cambios de alto impacto requieren coordinación sectorial. Las emergencias se comunican de inmediato con estado, alcance y próxima actualización, aplicando la matriz de severidad. La coordinación de ventanas de los sistemas institucionales y del Nodo/Ficha queda detallada en estas Reglas (Anexo 5).

5.7 Continuidad operativa y resiliencia

La Plataforma opera con desacoplamiento, escalabilidad y recuperación automática ante indisponibilidades, reteniendo mensajes hasta que fuente o destino restauren su servicio. Los planes de contingencia consideran DRP y despliegues en infraestructura elástica para absorber picos; cada parte realiza pruebas de restauración y continuidad

con la frecuencia y condiciones definidas en estas Reglas, registrando resultados y planes de mejora. Además, se prevén degradaciones planificadas (por ejemplo, de síncrono a lotes), retención temporal en colas y reprocesos documentados.

5.8 Cuotas y protección del servicio

Cada publicación define límites de tasa y concurrencia para proteger los orígenes; los consumidores respetan cuotas y manejan reintentos sin sobrecargar. Excepciones transitorias se solicitan, evalúan y, si proceden, se habilitan con medidas de control y plazos acotados.

5.9 Incumplimientos y plan de normalización

Cuando una métrica cae bajo su umbral, se activa un Plan de Mejora con acciones, responsables y fechas, con seguimiento en la instancia operativa sectorial. Si el incumplimiento de SLA es reiterado, se activa un plan de normalización con metas y plazos; su inobservancia habilita medidas temporales y proporcionales (por ejemplo, ajuste de cuotas o de ventanas, priorización o degradación controlada), las que cesan una vez restablecidos los estándares o, en último caso, se reflejan en los anexos técnicos.

5.10 Exenciones y causas no imputables

El SLA no aplica en casos de fuerza mayor, emergencias nacionales, exceso de cuota o errores del consumidor, ni por mantenimientos de terceros debidamente acreditados. Estas situaciones deben dejar evidencia en el repositorio de seguimiento.

Capítulo 6. Seguridad, trazabilidad y resguardo

Este capítulo establece los controles mínimos y verificables para proteger la información, asegurar que cada acceso quede registrado y conservar evidencias que permitan auditar la operación de la Plataforma —Nodo L&P y Ficha L&P— de manera proporcional al riesgo. Las reglas se aplican a proveedores y consumidores y se complementan con lo que declare cada instrumento habilitante del flujo.

6.1 Enfoque y objetivos

La seguridad y la privacidad se incorporan "desde el diseño", con controles de acceso, cifrado, monitoreo y resguardo acordes a la sensibilidad del dato; toda transacción debe quedar registrada en registros inalterables y auditables.

6.2 Acceso: autenticación, autorización y mínimo privilegio

El acceso se otorga por perfil (p. ej., Operador/a de Consulta, Administrador/a Institucional, Auditor/a) y se limita estrictamente a lo necesario para la finalidad del flujo. Se exige autenticación robusta: MFA para perfiles sensibles y para cuentas de servicio con alcances críticos; dichas cuentas deben rotarse, tener expiración y mantener registro de uso. Todo cambio de autorización se documenta con motivo y aprobaciones.

Las altas y bajas de usuarios son trazables; las revisiones de vigencia y privilegios son, al menos, semestrales, y la baja procede de inmediato ante desvinculación o inactividad prolongada.

6.3 Gestión de secretos, cifrado y endurecimiento

Las credenciales se resguardan en cofres o mecanismos equivalentes y se usan sólo por cuentas nominativas o de servicio autorizadas. El cifrado en tránsito es obligatorio, y en reposo se aplica cuando el riesgo lo amerite. Se exige parcheo oportuno, tratamiento documentado de vulnerabilidades y respaldo con pruebas periódicas de restauración, de acuerdo con los RPO/RTO del flujo.

6.4 Encargados y terceros

El acceso de encargados o subcontratistas requiere mandato escrito, se limita en tiempo y alcance, y queda bajo responsabilidad de la institución contratante, con obligaciones equivalentes de seguridad y confidencialidad.

6.5 Acceso de emergencia ("break-glass")

Se permite sólo con carácter excepcional y temporal para restaurar servicio o contener un incidente; requiere autorización del Responsable de Seguridad e informe a la SPS. Su uso queda documentado y genera plan de normalización posterior.

6.6 Registros y trazabilidad

Toda acción relevante en la Plataforma debe registrarse, con foco en saber quién hizo qué, cuándo, desde dónde y para qué finalidad. Como mínimo, se registra identidad del usuario o cuenta de servicio, institución y perfil, finalidad asociada, flujo o dataset, fecha y hora (con sincronización horaria), acción y resultado, origen técnico e, idealmente, un identificador único por transacción para correlación interinstitucional.

Los logs residirán en los entornos institucionales y, cuando corresponda, en componentes de observabilidad del Nodo; su integridad se protege con hash o firma y su retención se ajusta a clasificación de datos, políticas internas y normativa aplicable.

6.7 Evidencia y transparencia operativa

Cada institución debe poder exportar registros y artefactos (altas/bajas, cambios de configuración, tickets, reportes) en formatos abiertos y entregarlos a la SPS con cadena de custodia documentada cuando se requiera; a nivel sectorial, se publican tableros e indicadores agregados y reportes post-incidente de severidad alta, sin exponer datos personales o contenidos de transacciones.

Además, el Repositorio Digital Sectorial publica versiones vigentes de reglas, instrumentos y comunicados con control de cambios; toda publicación incorpora metadatos de versión y hash de integridad que permiten verificar autenticidad.

6.8 Continuidad operativa y resguardo

Los planes de contingencia consideran DRP y despliegues en infraestructura elástica; contemplan opciones de degradación planificada (p. ej., pasar temporalmente de síncrono a lotes), colas temporales y reprocesos. Las restauraciones se prueban periódicamente y los resultados quedan registrados, conforme a los RPO/RTO definidos en el instrumento del flujo.

6.9 Límites y protección del servicio

Para resguardar disponibilidad y evitar abusos, cada publicación define límites de tasa y concurrencia; los consumidores deben implementar reintentos prudentes y timeouts. Cualquier excepción transitoria se acuerda sectorialmente y queda acotada en el tiempo.

6.10 Integridad y versionado

Toda interfaz, esquema o catálogo se publica con versión y notas de cambio; los documentos operativos y técnicos se resguardan en el Repositorio con control de versiones y hash de integridad.

6.11 Listas de verificación (mínimos operativos)

Antes y durante la operación de un flujo deben cumplirse, al menos, los siguientes controles: clasificación del dato declarada; MFA activo en perfiles sensibles y en cuentas de servicio críticas; cifrado en tránsito y, cuando aplique, en reposo; logs habilitados y retenidos; parches críticos al día; respaldos probados y RPO/RTO documentados; acuerdos de confidencialidad vigentes.

6.12 Responsabilidad institucional y rendición de cuentas

Cada parte responde por su conducta: el proveedor por la calidad y oportunidad del dato; el consumidor por el uso conforme a la finalidad y por mantener trazabilidad y evidencias. La SPS coordina lineamientos y auditorías en el marco del Convenio y del presente Anexo 5.

Capítulo 7. Comunicación y ventanas de mantenimiento

Este capítulo ordena cómo se informa, coordina y deja evidencia de todo cambio operativo relevante de la Plataforma (Nodo L&P y Ficha L&P): anuncios preventivos, incidentes, ventanas de mantenimiento y publicaciones en el repositorio sectorial. Lo aquí descrito aplica tanto a proveedores como a consumidores y se complementa con lo que cada flujo establezca en su instrumento habilitante.

7.1 Objetivo y criterio general

Asegurar comunicaciones oportunas, claras y con contenidos mínimos verificables, de modo que las instituciones puedan planificar, reaccionar ante incidentes y auditar lo actuado. Prevalece la coordinación sectorial cuando el cambio impacte a múltiples instituciones o la continuidad del servicio.

7.2 Canales oficiales

- **Operación**: mesa de ayuda de la Plataforma y tablero sectorial (estado, métricas y avisos).
- **Seguridad**: canal expedito con el Responsable de Seguridad institucional y la SPS para incidentes S1/S2 y medidas especiales.
- **Repositorio digital**: publicaciones y versiones de reglas, instrumentos, comunicados y reportes con control de cambios e integridad.

7.3 Tipos de comunicación

1. **Preventiva**: anuncios de ventanas, cambios de versión o ajustes de cuotas.
2. **De incidente**: detección, clasificación (S1/S2/S3), contención y avances hasta el cierre.
3. **Post-incidente**: informe de causa raíz (RCA), medidas correctivas y preventivas.
4. **Informativa**: métricas periódicas, tendencias y planes de mejora.

7.4 Contenidos mínimos de cada aviso

Todo comunicado incluye, a lo menos: **título**, **fecha y hora**, **alcance** (flujos afectados), **impacto esperado/observado**, **acciones de mitigación** (si procede), **contacto y próxima actualización**; en post-incidentes, además **causa**, **medidas** y **plazos**. Los documentos se publican en el Repositorio con versión y hash de integridad.

7.5 Ventanas de mantenimiento

- **Programadas**: se concentran en horarios de bajo tráfico y se anuncian con antelación razonable (fecha, horario, impacto, reversa y contingencia). Cambios de alto impacto requieren coordinación sectorial.
- **Extraordinarias** (emergencias de seguridad o disponibilidad): pueden ejecutarse sin preaviso, con comunicación inmediata y detalle posterior según matriz de severidad.
- **Coordinación interinstitucional**: cuando la ventana del Nodo/Ficha o de un proveedor afecte a consumidores, la SPS coordina el calendario para minimizar indisponibilidades.

7.6 Matriz de comunicaciones por severidad (síntesis operativa)

- **S1 – Crítico**: comunicación inicial ≤2 h; actualizaciones cada 2 h; coordinación sectorial por SPS; medidas especiales autorizadas por seguridad (p. ej., throttling, degradación temporal).

- **S2 – Alto**: comunicación inicial ≤4 h; seguimiento diario; coordinación operativa entre instituciones afectadas.
- **S3 – Medio/Bajo**: comunicación dentro del día hábil; consolidación en tablero e informe mensual.
  Los umbrales exactos se fijan por flujo o en el SLA sectorial y se reflejan en el repositorio.

7.7 Cambios de versión y congelamientos

Los cambios **menores** mantienen compatibilidad y se comunican con notas de cambio; los **mayores** requieren aprobación previa y plan de transición con pruebas UAT y reversa. En períodos críticos, la SPS podrá establecer **congelamientos** (freeze) para proteger la continuidad.

7.8 Ajustes de cuotas y protección del servicio

Ante desvíos reiterados de SLA o riesgo a la disponibilidad, se podrán aplicar medidas proporcionales y temporales: ajuste de cuotas, reprogramación de ventanas o degradación controlada, con comunicación sectorial y término al normalizar.

7.9 Break-glass y comunicaciones de seguridad

El acceso de emergencia (“break-glass”) es excepcional, temporal y autorizado por el Responsable de Seguridad; su uso se comunica a la SPS y se documenta con justificativo, alcance, duración y plan de normalización.

7.10 Evidencia y archivo

Todos los avisos, actas y reportes (incluido el RCA) se conservan en el expediente operativo del flujo y en el Repositorio Digital Sectorial con control de versiones y verificación de integridad.

Capítulo 8. Privacidad, confidencialidad y protección de datos personales

Este capítulo fija reglas simples y operativas para tratar datos personales en la Plataforma (Nodo L&P y Ficha L&P). Su propósito es asegurar que toda publicación y consumo respete la finalidad pública, minimice exposición y mantenga controles razonables y verificables. Complementa el Convenio, sin crear nuevas bases legales.

8.1 Régimen aplicable y principios prácticos

Toda operación se rige por la normativa vigente y por las Reglas de Uso. En la práctica, esto significa: (i) licitud y finalidad pública explícita por flujo; (ii) minimización de datos; (iii) confidencialidad y seguridad desde el diseño; (iv) trazabilidad y rendición de cuentas. Estas salvaguardas se reflejan en los instrumentos habilitantes y en el repositorio sectorial.

8.2 Finalidad y base habilitante, por flujo

Para publicar o consumir, la institución declara la base legal y la finalidad específica en su instrumento habilitante. Esa autorización delimita qué puede pedirse, quién puede acceder y por cuánto tiempo. Cualquier cambio relevante exige actualizar el instrumento.

8.3 Clasificación del dato y controles asociados

Cada flujo clasifica su dato (básico/restringido/sensible) y aplica, como mínimo, los controles organizativos y técnicos definidos en las Reglas de Uso: políticas y acuerdos de confidencialidad; autenticación robusta (MFA en perfiles sensibles y cuentas de servicio críticas); autorización por perfil/bajo mínimo privilegio; cifrado en tránsito y, cuando proceda, en reposo; logging y monitoreo correlacionable; protección antiabuso.

8.4 Minimización, calidad y exactitud

Sólo se exponen y consumen los campos estrictamente necesarios; el proveedor mantiene la calidad y oportunidad del dato, y el consumidor valida integridad y conserva evidencia del uso.

8.5 Confidencialidad (obligación y alcance)

La información no puede divulgarse ni reutilizarse fuera de la finalidad declarada. La obligación de confidencialidad es indefinida y subsiste al término del flujo o del Convenio. El acceso de encargados/subcontratistas requiere mandato escrito y controles equivalentes.

8.6 Encargados y terceros

Cuando una institución delega, sigue siendo responsable. Debe delimitar finalidad, plazos y salvaguardas; exigir deber de confidencialidad y permitir auditoría y trazabilidad del encargado.

8.7 Anonimización, seudonimización y ambientes de prueba

Para reducir riesgos, se aplican técnicas de seudonimización/anonimización cuando proceda, según finalidad y proporcionalidad. En sandbox/UAT se utilizan datos sintéticos o debidamente enmascarados; sólo por excepción fundada se usarán datos reales, con controles reforzados.

8.8 Trazabilidad y conservación de evidencias

Todo acceso y operación queda registrado (quién/qué/cuándo/para qué), con integridad protegida y retención por los plazos definidos en las Reglas y en el instrumento del flujo. Las evidencias deben poder exportarse en formatos abiertos y ponerse a disposición de la Subsecretaría.

8.9 Derechos de las personas y transparencia operativa

Los procedimientos sectoriales deben facilitar el ejercicio de derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición, considerando la distribución inter-institucional de los datos. La verificación de identidad se realizará por los mecanismos habilitados para servicios del Estado (p. ej., ClaveÚnica).

8.10 Notificación y gestión de incidentes con datos personales

Todo incidente que afecte confidencialidad, integridad o disponibilidad se gestiona conforme a la matriz de severidad y al procedimiento sectorial (contención, remediación, RCA). Cuando corresponda, se efectuarán las notificaciones a las autoridades competentes, además de informar a la Subsecretaría.

8.11 Repositorio y control de cambios

El Repositorio Digital Sectorial mantiene versiones vigentes de estas Reglas y de los instrumentos de cada flujo. Toda publicación incorpora metadatos de versión y hash de integridad, y se comunica a los adherentes según lo previsto en el Convenio y el presente Anexo 5.

Capítulo 9. Instrumentos habilitantes (formularios por flujo)

Los "instrumentos habilitantes" son los formularios oficiales que documentan, por cada flujo, la autorización de **publicación** o de **consumo** de datos en la Plataforma. Su propósito es dejar por escrito la finalidad pública, la base legal, el catálogo y las condiciones operativas y de seguridad, de modo que el uso sea verificable y auditable. Todo flujo debe tener su instrumento vigente, versionado y disponible en el Repositorio Digital Sectorial.

9.1 Estructura general del instrumento

Cada instrumento —de **publicación** o de **consumo**— se desarrolla en prosa clara y contiene, como mínimo:

- Identificación del flujo (título, institución responsable y punto de contacto).
- **Finalidad pública** concreta y **base legal** que habilita la operación.
- Alcance funcional y **catálogo**: datos/atributos necesarios y reglas de negocio.
- Condiciones operativas: **SLA/umbrales clave**, **cuotas/límites**, ventanas y ambientes.
- Controles de **seguridad, confidencialidad y trazabilidad** aplicables.
- Evidencias de pruebas (**UAT/Go-Live**) y plan de reversa.
- Versionado, fecha de entrada en vigor y archivo en repositorio.

9.2 Formulario de publicación (proveedor)

El instrumento de publicación deja constancia de que la institución **expone** un flujo a través del Nodo:

- **Finalidad y base habilitante**: norma o acto y descripción de la necesidad pública que se satisface.
- **Catálogo mínimo**: lista de campos con su justificación de necesidad (minimización) y esquema/contrato del servicio (endpoint, tipos, reglas y códigos de error).
- **Ciclo y oportunidad**: frecuencia de actualización, retrasos máximos tolerados y dependencias.
- **SLA y desempeño**: disponibilidad mensual objetivo, latencia p95 cuando aplique, tasa de error, RPO/RTO si existen procesos por lotes.
- **Cuotas y protección**: límites por institución y políticas de reintentos/backoff para evitar abusos.
- **Ambientes**: sandbox/UAT/producción, datos sintéticos o enmascarados en pruebas.
- **Seguridad y confidencialidad**: autenticación/autorización por perfil, resguardo de secretos, cifrado en tránsito (y en reposo cuando corresponda), gestión de vulnerabilidades y respaldos.
- **Trazabilidad**: qué se registra y por cuánto tiempo; hash/firma y versión de la publicación.
- **Pruebas y Go-Live**: resultados UAT, checklist de paso a producción y plan de reversa.
- **Comunicaciones**: régimen de avisos de cambios/ventanas e incidentes.
- **Versionado**: número de versión, notas de cambio y fecha de vigencia.

9.3 Formulario de consumo (consumidor)

El instrumento de consumo acredita que una institución **invoca** un flujo con base legal y fines definidos:

- **Finalidad y base habilitante** del uso; referencia al acto administrativo que la sustenta.
- **Alcance de uso**: quiénes (perfiles) y para qué casos administrativos se realizan las consultas; exclusiones expresas (no investigación, no scraping, no usos genéricos).
- **Necesidad de campos**: correspondencia entre atributos solicitados y finalidad (minimización).
- **Controles internos**: administración de usuarios/perfiles, MFA en perfiles sensibles y cuentas de servicio críticas, segregación de ambientes, rotación de credenciales.
- **Evidencia operativa**: validación de integridad (hash/firma) y archivo del comprobante junto al expediente del caso; bitácoras de consumo exportables.
- **SLA y cuotas**: compromisos de uso responsable, manejo de errores y reintentos prudentes.
- **Pruebas UAT** y plan de puesta en producción.

9.4 Procedimiento de alta, cambio y baja del flujo

- **Alta**: la institución presenta el instrumento completo; la Subsecretaría revisa coherencia con las Reglas y con estándares sectoriales, y aprueba o solicita ajustes.
- **Cambio**: los cambios **menores** (compatibles) se notifican con notas de cambio; los **mayores** requieren revisión y plan de transición con UAT y reversa.
- **Baja**: se documenta el cierre, comunicación a consumidores, fecha efectiva y resguardo de evidencias/logs.

9.5 Validaciones previas y causales de rechazo

La Subsecretaría puede rechazar o devolver un instrumento cuando falte base legal o la finalidad sea ambigua; cuando el catálogo incluya campos no necesarios; cuando no se definan controles mínimos de seguridad/trazabilidad; o cuando el SLA/cuotas sea incompatible con la protección del servicio. La decisión queda registrada con fundamento y referencias.

9.6 Evidencias obligatorias anexas

Cada instrumento adjunta: acto o resolución habilitante; **especificación** del servicio (endpoint, esquema, reglas y errores); resultados de UAT y checklist de Go-Live; matriz de roles/perfiles y registro de altas/bajas; política de retención de logs y respaldos; plan de reversa; y, cuando corresponda, evaluación de riesgos de privacidad.

9.7 Archivo y publicación

Los instrumentos vigentes y su historial se conservan en el **Repositorio Digital Sectorial**, con control de versiones, metadatos y **hash de integridad** para verificación. Toda actualización se comunica por los canales oficiales y queda trazada.

9.8 Ejemplo orientativo de llenado

A modo orientativo, el **objeto del flujo**, la **finalidad**, la **base legal**, el **catálogo** y las **condiciones operativas** se redactan en prosa breve y verificable, siguiendo la estructura anterior y el estilo de los ejemplos sectoriales

disponibles. El detalle práctico debe reproducir las mejores prácticas de los ejemplos oficiales publicados para el sector.

9.9 Vigencia y revisión

El instrumento rige desde su publicación y hasta que una nueva versión lo reemplace o se dicte su baja. Los cambios mayores se someten a revisión previa; los menores se publican con notas de cambio y fecha de vigencia.

9.10 Responsables y rendición de cuentas

El **responsable institucional del flujo** (proveedor o consumidor) asegura que el instrumento esté vigente, que las personas usuarias tengan los perfiles correctos y que las evidencias estén disponibles para auditoría o requerimientos de la Subsecretaría.

Capítulo 10. Gestión de cambios, versionado y compatibilidad

Este capítulo ordena, en lenguaje de uso, cómo se proponen, aprueban, comunican y despliegan los cambios en la Plataforma (Nodo L&P y Ficha L&P), asegurando compatibilidad y trazabilidad. Aplica a publicaciones de datos, contratos de servicio (APIs), catálogos y documentación operativa.

10.1 Objetivo y alcance

Que toda modificación sea predecible, reversible y auditable; que los consumidores dispongan de tiempo razonable para adaptar sus integraciones; y que la continuidad del servicio prevalezca sobre la velocidad del cambio. Cubre cambios **técnicos** (endpoints, esquemas, seguridad), **funcionales** (reglas de negocio, catálogos) y **operativos** (SLA, cuotas, ventanas).

10.2 Tipos de cambio y política de versiones

Se usa una convención de versionado comprensible y consistente (p. ej., Mayor.Menor.Parche):

- **Cambio mayor (Mayor)**: rompe compatibilidad hacia atrás (breaking change). Ej.: eliminación o renombrado de campos obligatorios; cambios semánticos en códigos de respuesta; autenticación distinta no compatible.
    - Requiere: aprobación de la Subsecretaría, plan de transición, pruebas UAT, reversa definida y calendario de coexistencia de versiones.
- **Cambio menor (Menor)**: mantiene compatibilidad. Ej.: agregar campo **opcional**; ampliar dominios válidos; agregar códigos de error no disruptivos.
    - Requiere: comunicación previa y notas de cambio; no exige coexistencia prolongada.
- **Parche (hotfix)**: corrige defectos sin afectar el contrato ni la semántica.
    - Requiere: comunicación posterior (si procede) y registro en bitácora de cambios.

Cada servicio y cada catálogo exhiben su **número de versión vigente**, fecha de publicación y **notas de cambio** claras.

10.3 Reglas de compatibilidad (contratos y catálogos)

- **Nunca** eliminar ni cambiar el significado de un campo **obligatorio** en una línea de versión. Para ello, publicar una **versión mayor** y ofrecer período de coexistencia.
- Al **agregar** campos, que sean **opcionales** y con valores por defecto claros.
- Mantener **estables** los nombres de campos, tipos y códigos de error.
- Para catálogos (códigos, estados): toda **reclasificación** o **deprecación** documenta equivalencias (mapping) y fecha de retiro.
- Cuando haya **feature flags** o encabezados de versión, documentar su uso y límites.
- Firmar los artefactos (esquemas, ejemplos) con **hash** y guardarlos en el repositorio.

10.4 Flujo de gestión de cambios (resumen operativo)

1. **Propuesta** del proveedor (o de la operación de Plataforma) con justificación, impacto y tipo de cambio.
2. **Revisión** técnica/funcional y de seguridad; clasificación como mayor/menor/parche.
3. **Aprobación**:
    - Mayor: por la Subsecretaría; Menor/Parche: por operación Plataforma (con control posterior).
4. **Comunicación**: aviso preventivo (contenido mínimo: alcance, impacto, versión, fechas, pruebas requeridas, reversa).
5. **Pruebas** en UAT y **criterios de paso a producción** (casos de prueba, monitoreo, reversa).
6. **Despliegue** en ventana definida; **coexistencia** cuando aplique.
7. **Cierre**: publicación de notas de cambio, evidencias y actualización de documentación.

Todo el ciclo queda trazado en el **expediente operativo del flujo** y en el **Repositorio Digital Sectorial**.

10.5 Coexistencia, transición y deprecaciones

- **Coexistencia**: ante cambios mayores, mantener al menos dos versiones activas por un período definido (ej.: 3–6 meses, según impacto) para permitir la migración.
- **Deprecación**: anunciar con antelación la fecha de retiro; durante el período de gracia, monitorear consumos e informar rezagos a responsables institucionales.
- **Corte**: al retirar una versión, bloquear su uso y conservar evidencias (logs, contratos) por los plazos de retención.

10.6 Cambios urgentes y de seguridad

- **Hotfix de seguridad**: puede aplicarse en ventana extraordinaria, minimizando impacto. Debe acompañarse de comunicación inmediata y notas de corrección.
- **Medidas temporales** para proteger el servicio (p. ej., throttling, cuotas, degradación controlada de síncrono a lotes) son **proporcionales**, **acotadas en el tiempo** y **auditables**.

10.7 Cambios operativos: SLA, cuotas y ventanas

- **SLA**: umbrales y fuentes de medición se actualizan por versión de flujo; los cambios relevantes requieren aviso y fecha de vigencia.
- **Cuotas**: se podrán ajustar por riesgo o capacidad; excepciones transitorias se documentan con responsable y plazo.
- **Ventanas**: los cambios que las modifiquen deben coordinarse sectorialmente y reflejarse en el calendario operativo.

10.8 Evidencias mínimas por cambio

- Propuesta y clasificación (Mayor/Menor/Parche), con análisis de impacto.
- Acta o resolución de aprobación (según tipo).

- Esquema actualizado, ejemplos de payload y **notas de cambio**.
- Resultados de **UAT** (casos aprobados) y **plan de reversa** probado.
- Registro de **pase a producción** con fecha/hora y responsables.
- Publicación en el **Repositorio** con versión y **hash de integridad**.

10.9 Gobernanza y responsabilidades

- **SPS**: define lineamientos, aprueba cambios mayores, coordina congelamientos (freeze) en períodos críticos y valida cierres de incidentes vinculados a cambios.
- **Unidad IoP (operación Plataforma)**: gestiona el pipeline de cambios, monitoreo, despliegues y reversas; mantiene la documentación técnica y los tableros.
- **Proveedor**: custodia la evolución del catálogo/servicio; comunica impactos y garantiza compatibilidad según este capítulo.
- **Consumidor**: adapta integraciones dentro de los plazos, respeta notas de deprecación y reporta hallazgos de compatibilidad.

10.10 Matriz práctica de ejemplos (orientativa)

Tipo de cambio	Ejemplo concreto	¿Rompe compatibilidad?	Requisitos clave
Mayor	Cambiar id_trabajador de string a entero; eliminar campo obligatorio estado_cotización	Sí	Aprobación SPS; coexistencia v1/v2; UAT; reversa; cronograma de migración
Menor	Agregar correo_contacto como **opcional**; añadir código de error 429 (rate limit)	No	Aviso preventivo; notas de cambio; pruebas funcionales básicas
Parche	Corregir validación de formato RUT; fix en mensaje de error	No	Comunicación posterior si impactó; registro en bitácora

10.11 Reversa y restauración

Todo cambio define **cómo volver** a la versión anterior sin perder trazabilidad ni integridad: condiciones de activación, pasos técnicos, duración estimada y criterios de éxito. La reversa se **prueba** en UAT y se mantiene documentada junto al cambio.

Capítulo 11. Monitoreo, métricas y tablero sectorial

Este capítulo define cómo se miden los servicios del Nodo L&P y la Ficha L&P, cómo se publican los resultados y qué responsabilidades asume cada parte para asegurar transparencia operativa y mejora continua. El objetivo es disponer de indicadores simples, verificables y comparables en el tiempo, con una **fuente única de medición** y un **tablero sectorial** accesible a las instituciones adherentes.

11.1 Qué medimos (métricas base)

Para cada flujo y para el servicio del Nodo/Ficha se definen, como mínimo, las siguientes métricas con su umbral, fuente de medición y periodicidad de reporte: **(i)** disponibilidad mensual; **(ii)** latencia p95 en consultas síncronas; **(iii)** tasa de error aplicable; **(iv)** capacidad/cuotas por institución y por flujo; **(v)** RPO/RTO para eventos o lotes; **(vi)** soporte (tiempos de primera respuesta/atención/escalamiento por severidad); y **(vii)** mantenibilidad (MTBF/MTTR), cuando corresponda.

11.2 Fuentes y métodos de medición

Las métricas se obtienen desde el monitoreo de la Plataforma y/o de cada flujo, declarando expresamente la **fuente única de medición** para evitar discrepancias. Cada resultado se contrasta con su umbral y se expone la tendencia. El historial de mediciones queda **versionado en el repositorio oficial** para trazabilidad.

11.3 Tablero sectorial

La Subsecretaría/Operación del Nodo-Ficha **mide y publica indicadores**, gestiona el **tablero sectorial** y coordina ventanas e incidentes de alto impacto. El tablero presenta resultados mensuales por flujo y consolidado del servicio, junto con comparaciones contra umbrales y tendencias. En incidentes S1/S2 se incorpora el **post-incidente** (RCA, acciones y plazos).

11.4 Periodicidad y formatos

Como regla, el **reporte es mensual** (y trimestral para RPO/RTO si así se define en el instrumento del flujo). Los formatos deben ser abiertos y estandarizados para permitir su reutilización y auditoría. La plantilla referencial incluye campos pre-llenables de métricas, ventanas, severidades y planes de mejora, para homogeneidad sectorial.

11.5 Incidentes y reportes post-incidente

Ante incidentes S1/S2, además del flujo operativo descrito en capítulos previos, se exige **reporte post-incidente** con causa, medidas correctivas y preventivas, y plazos de implementación. Estos reportes se integran al tablero y al repositorio, manteniendo versiones y evidencias.

11.6 Responsables y corresponsabilidad

- **SPS/Operación del Nodo-Ficha**: publica métricas, gestiona el tablero, coordina ventanas y comunica incidentes de alto impacto.
- **Proveedor**: sostiene calidad y disponibilidad del origen, informa cambios que afecten al flujo.
- **Consumidor**: usa responsablemente, respeta cuotas y maneja reintentos y errores sin sobrecargar el servicio.
  Estas responsabilidades están expresamente establecidas en las Reglas de Uso.

11.7 Repositorio Digital Sectorial (RDS)

Los indicadores, comunicaciones, versiones y reportes se publican en el **Repositorio Digital Sectorial**, administrado por la Subsecretaría. Cada artefacto posee **identificador de versión, fecha de publicación, vigencia y hash de integridad**; las versiones allí publicadas son las únicas oficiales. El acceso a **evidencias sensibles** (p. ej., logs o RCA detallados) se gestiona bajo control de la Subsecretaría.

11.8 Mejora continua y planes de normalización

Cuando una métrica cae **bajo su umbral**, se configura y activa un **Plan de Mejora** con acciones, responsables y fechas, cuyo seguimiento se realiza en la instancia operativa sectorial (mesa/comité). Si el origen o el consumidor son la causa del desvío, ello se deja **expresamente** consignado, acordando medidas específicas.

11.9 Exenciones y pausas de conteo

No computan para el SLA los eventos de **fuerza mayor** o emergencias nacionales, ni interrupciones atribuibles a exceso de cuota o mantenimientos de terceros **debidamente acreditados**. Estas situaciones se documentan y archivan en el repositorio.

11.10 Lista breve de verificación (antes de operar)

Métricas y umbrales declarados; **fuente de medición** y tablero definidos; **cuotas** por institución/flujo configuradas; calendario y aviso de **ventanas**; **matriz de severidad** y tiempos acordados; procedimiento de **post-incidente**; publicación en RDS con versión y hash.

Capítulo 12. Catálogos, API/servicio y documentación operativa

Este capítulo ordena, en lenguaje de uso, cómo se describen los datos, cómo se publica el "contrato" del servicio (API o mecanismo de intercambio) y qué documentación operativa debe mantenerse para que el flujo sea comprensible, integrable y auditable por cualquier institución adherente. La regla general es simple: **lo que no está documentado no existe** a efectos de habilitación, soporte y auditoría.

12.1 Catálogo de datos (qué es y para qué sirve)

El catálogo es la descripción funcional de los **atributos** que se publican o consumen en un flujo: nombres, definiciones en lenguaje claro, reglas de negocio, formatos y ejemplos. Su finalidad es doble: (i) **minimización** (justificar por qué cada campo es necesario para la finalidad pública) y (ii) **consistencia sectorial** (que "el mismo dato" signifique lo mismo en todas las instituciones).

- Contenido mínimo del catálogo:
    - **Identificación del flujo** y versión del catálogo.
    - **Tabla de atributos**: nombre, descripción en prosa, tipo de dato, dominio/valores permitidos, obligatoriedad (obligatorio/opcional), regla de cálculo o validación, **justificación de necesidad**.
    - **Relaciones y claves**: identificadores, llaves compuestas y referencias externas (p. ej., RUT, RUN, códigos de organismo).
    - **Reglas de integridad**: unicidad, no nulos, longitudes máximas, formatos (p. ej., ISO 8601 para fechas).
    - **Ejemplos representativos** (payloads de requisa y respuesta) que cubran casos normales y bordes.
- Buenas prácticas:
    - Nombres **estables y autoexplicativos** ("fecha_inicio_vigencia" mejor que "fch_ini").
    - Mantener un **glosario** de términos y sinónimos para evitar ambigüedades.
    - Declarar **equivalencias** cuando un estado/código cambie (mapping de versiones).

12.2 API/servicio

El "contrato" es la descripción técnica y operativa de **cómo** se invoca un flujo y **qué** responde.

- Contenido mínimo del contrato:
    - **Endpoint y método** (o mecanismo de entrega si es por lotes/eventos) y **versión**.
    - **Autenticación y autorización**: tipo, alcance, perfiles habilitados, límites de uso/cuotas.
    - **Esquemas de solicitud y respuesta** (JSON/XML/CSV): tipos, cardinalidades, reglas de validación y campos obligatorios.
    - **Códigos de error** y semántica (incluidos 4xx/5xx frecuentes, con mensajes breves de diagnóstico).
    - **Rendimiento esperado**: latencia de referencia (p95 si es síncrono), tamaños máximos, concurrencia admitida.

    - **Restricciones**: idempotencia, ordenamiento, paginación, filtros, ventanas de consistencia.
    - **Política de versionado**: mayor/menor/parche y compatibilidad (véase Cap. 10).
    - **Ejemplos** completos (OK y error) con valores creíbles.
- Buenas prácticas:
    - **Neutralidad tecnológica** y formatos abiertos.
    - Mantener **estabilidad** del contrato; cambios disruptivos sólo por versión mayor y con coexistencia.

12.3 Documentación operativa

Conjunto de documentos vivos que facilitan integración, soporte y auditoría. Debe alojarse en el repositorio oficial y vincularse al flujo/instrumento correspondiente.

- Contenido mínimo:
    - **Guía funcional** del flujo (finalidad, casos de uso, precondiciones y límites).
    - **Procedimiento de integración**: prerequisitos, pasos de onboarding, credenciales/roles, ambientes (sandbox/UAT/prod), datos de prueba.
    - **Plan de pruebas** (UAT) con resultados y criterios de aprobación.
    - **Monitoreo y alertas**: qué se observa, umbrales y responsables.
    - **Operación diaria**: runbook (errores comunes, reintentos, backoff, cómo escalar).
    - **Gestión de cambios**: historial, notas de versión y fechas de vigencia.
    - **Seguridad y privacidad**: matriz de controles aplicados y evidencias mínimas (accesos, logs, respaldos).
    - **Plan de reversa y continuidad**: condiciones de activación, pasos y validaciones.

12.4 Convenciones y estándares

- **Nombres de campos**: snake_case o camelCase consistentes; evitar abreviaturas opacas; prefijar booleanos con verbos o auxiliares (“es_”, “tiene_”).
- **Fechas y horas**: ISO 8601; declarar zona horaria si aplica; siempre en UTC internamente si el flujo lo requiere.
- **Identificadores**: inmutables dentro de una versión del flujo; declarar formato (p. ej., dígitos + verificador).
- **Catálogos de códigos**: publicar **tablas de referencia** con versión, descripciones y estados (vigente/deprecado/retirado).
- **Ejemplos**: válidos y coherentes con la semántica; incluir al menos un caso de borde (sin dato, límite, error).

12.5 Gobernanza del catálogo y del contrato

- **Proveedor**: custodia la evolución del catálogo/contrato; propone cambios, justifica impacto y ejecuta pruebas.

- **Consumidor**: revisa impactos, adapta integraciones y verifica compatibilidad en UAT.
- **SPS/Operación Plataforma**: valida lineamientos, aprueba cambios mayores, coordina ventanas y congela cambios en periodos críticos.
- **Evidencias**: propuesta de cambio, clasificación (mayor/menor/parche), notas de versión, resultados UAT, pase a producción, publicación en repositorio.

12.6 Ejemplos orientativos

- **Ejemplo de solicitud** (síncrona): query con parámetros típicos, encabezados de autenticación y correlación.
- **Ejemplo de respuesta OK**: objeto con todos los **campos obligatorios** y opcionales representativos; incluir version_publicacion, id_transaccion y **huella de integridad** si aplica.
- **Ejemplo de respuesta de error**: estructura con codigo, mensaje_corto, detalle (opcional), timestamp y trace_id.

12.7 Calidad y validación

Antes de la puesta en productivo (Go-Live), cada flujo debe pasar por:

- **Validación de esquema** (automática) y **validación semántica** (reglas de negocio).
- **Casos de prueba** acordados (exitosos, errores, bordes, volumen razonable).
- **Ensayo de reversa** documentado.
- **Revisión de seguridad** (autenticación/autorización, secretos, cifrado, logs).
- **Checklist final**: contrato publicado; catálogo completo y justificado; runbook disponible; métricas y monitoreo activos; canales de soporte definidos.

12.8 Conservación, versión y trazabilidad (después del despliegue)

- Todo artefacto (catálogo, contrato, guías, planes y evidencias) se **versiona** y se archiva en el repositorio oficial con metadatos (versión, fecha de publicación, vigencia) y **huella de integridad**.
- Los cambios **menores** se documentan con notas y fecha efectiva; los **mayores** mantienen coexistencia por un plazo definido.
- Los **registros operativos** (logs, métricas, tickets, reportes) se conservan durante el período de retención establecido y deben ser **exportables** en formatos abiertos.

12.9 Lista breve de verificación (para publicar o consumir)

- Catálogo completo con **justificación de campos** y ejemplos.
- Contrato con endpoint, esquemas, errores, límites y **política de versión**.
- Guía de integración, plan de pruebas y resultados **UAT aprobados**.
- Monitoreo, métricas y **cuotas** configuradas.
- Runbook operativo y plan de **reversa probado**.

- Artefactos publicados en el **repositorio oficial** con versión y hash.

Capítulo 13. Gestión de usuarios, perfiles y acceso por roles

La Plataforma opera bajo el principio de **mínimo privilegio**: cada persona o sistema accede sólo a lo estrictamente necesario, por el tiempo indispensable y con trazabilidad completa. Este capítulo explica, en lenguaje de uso, cómo se crean, administran y retiran los accesos; cómo se definen los perfiles; y qué evidencias deben conservar las instituciones para auditoría y control.

13.1 Objetivo y alcance

El control de accesos protege la confidencialidad, integridad y disponibilidad de los datos publicados y consumidos por la Plataforma (Nodo L&P y Ficha L&P). Se aplica a usuarios humanos, cuentas de servicio, herramientas automatizadas y a cualquier tercero que opere por cuenta de una institución adherente.

13.2 Tipos de cuentas y titulares

- **Cuenta personal nominativa**: usada por funcionarios/as para operar flujos según su rol. Prohibido compartir credenciales.
- **Cuenta de servicio**: destinada a integraciones de sistemas. Debe tener alcance acotado, vigencia definida y responsable nominativo.
- **Cuenta técnica/operativa** (p. ej., mesa de ayuda): sólo para tareas de soporte, con capacidades predefinidas y registro reforzado.

13.3 Perfiles y permisos (modelo base)

La Plataforma define perfiles sectoriales de referencia; cada institución mapea sus cargos a estos perfiles:

- **Operación de consulta** (consumidor): invoca flujos habilitados y consulta bitácoras propias.
- **Operación de publicación** (proveedor): gestiona catálogos/contratos del flujo y monitorea su salud.
- **Administrador/a institucional**: habilita y revoca usuarios de su institución, asigna perfiles, verifica revisiones periódicas.
- **Responsable técnico**: administra integraciones, versiones y pruebas (sin acceso a datos más allá de lo requerido).
- **Responsable de seguridad**: revisa privilegios, políticas y registros; autoriza medidas excepcionales.
- **Auditor/a**: acceso de sólo lectura a evidencias y reportes (sin datos operacionales salvo autorización expresa).

Los permisos finos (endpoints, operaciones, ambientes) se definen por flujo en su instrumento habilitante.

13.4 Alta de usuarios: requisitos y evidencia

Toda alta debe quedar respaldada por una **solicitud** con: identidad del titular, institución, perfil solicitado, finalidad operativa, aprobaciones (responsable institucional y seguridad), y **fecha de expiración** o evento de revisión. La creación efectiva del acceso genera un registro (quién, cuándo, qué privilegios) y un aviso al titular.

13.5 Asignación de perfiles y mínimo privilegio

La regla es asignar el **perfil mínimo** que permita cumplir la función. Las ampliaciones de privilegio requieren justificación y vencimiento. Cuando una persona asuma funciones múltiples, se preferirá la **separación de perfiles** y, si es posible, de cuentas (operación vs. administración) para evitar conflictos y facilitar auditoría.

13.6 Autenticación fuerte y gestión de sesiones

- **MFA obligatorio** para perfiles sensibles (administración, seguridad, publicación) y para **cuentas de servicio** con alcances críticos.
- Políticas de sesión: expiración por inactividad, bloqueo tras intentos fallidos razonables y cierre forzado al revocar el acceso.
- Federaciones/autenticaciones externas se permiten si cumplen los requisitos de seguridad y registro; la responsabilidad por la identidad sigue siendo de la institución usuaria.

13.7 Gestión de credenciales y secretos

Las credenciales (claves, tokens, certificados) se almacenan en **cofres de secretos** o mecanismos equivalentes, con **rotación** periódica y obligatoria ante incidentes o cambios de responsable. Está prohibido incrustarlas en código, planillas o repositorios no seguros. Toda entrega/renovación de credencial deja evidencia.

13.8 Revisión periódica y recertificación

Las instituciones revisan **al menos semestralmente** la vigencia y adecuación de accesos y perfiles; los resultados se documentan con fecha, universo revisado, hallazgos y bajas/ajustes ejecutados. En áreas críticas o con alta rotación, se recomienda **periodicidad trimestral**. La recertificación incluye cuentas de servicio y accesos de terceros.

13.9 Baja, suspensión y cambios de función

La baja procede **de inmediato** ante desvinculación, traspaso de funciones o inactividad prolongada. Las suspensiones temporales por ausencia o investigación interna se ejecutan con igual celeridad. Todo cambio de función obliga a **revaluar** el perfil. Debe conservarse evidencia del retiro (fecha, responsable, alcance) y de la revocación de credenciales asociadas.

13.10 Cuentas de servicio e integraciones

Las cuentas de servicio se crean **por flujo** y **por ambiente** (sandbox/UAT/producción), con permisos mínimos y **límites de uso** (cuotas/tasa). Deben registrar responsable nominativo, **vigencia** y controles de **origen** (p. ej., listas de permitidos por IP, restricciones de horario). La rotación de tokens/certificados es obligatoria y documentada.

13.11 Separación de funciones (SoD)

Cuando el mismo actor pudiera autorizar y ejecutar acciones de alto impacto (p. ej., aprobar y desplegar un cambio), se implementan **controles compensatorios**: doble autorización, revisión independiente o monitoreo reforzado. La SoD se documenta por flujo y se valida en auditoría.

13.12 Acceso de emergencia (“break-glass”)

Permitido sólo para restaurar servicio o contener un incidente. Requiere autorización del Responsable de Seguridad, tiene **duración acotada** y deja registros con motivo, alcance, acciones y **plan de normalización**. Su uso se informa a la Subsecretaría según el procedimiento de comunicaciones de seguridad.

13.13 Auditoría de accesos y registros mínimos

Toda operación relevante debe poder atribuirse a un titular o a una cuenta de servicio. Los registros incluyen: identidad, perfil, institución, flujo/endpoint, finalidad (en consumos), fecha/hora, origen técnico y resultado. Las instituciones deben **exportar** estos registros a requerimiento, manteniendo su integridad y la cadena de custodia.

13.14 Acceso de terceros y encargados

El acceso de proveedores o subcontratistas exige **mandato escrito**, definición de finalidad, alcance y plazo, y controles equivalentes a los institucionales. La institución contratante sigue siendo responsable y debe poder **auditar** el uso realizado por el encargado.

13.15 Lista breve de verificación (operación diaria)

- Solicitudes de alta/baja con aprobaciones y fechas.
- Perfiles asignados bajo mínimo privilegio y con expiración.
- MFA activo en perfiles sensibles y cuentas de servicio críticas.
- Cofre de secretos en uso y rotación vigente.
- Recertificación semestral/trimestral ejecutada y documentada.
- SoD definida para tareas de alto impacto.
- Procedimiento de **break-glass** habilitado y probado.
- Registros de acceso completos y exportables.

Capítulo 14. Cumplimiento, auditoría y mejora continua

Este capítulo establece cómo se verifica el cumplimiento de las Reglas de Uso, cómo se ejecutan las auditorías y cómo se corrigen y previenen las no conformidades, asegurando un ciclo sistemático de mejora continua. Aplica a todas las instituciones proveedoras y consumidoras que operan la Plataforma (Nodo L&P y Ficha L&P), incluyendo a sus encargados o terceros.

14.1 Objetivo y enfoque

Garantizar que la operación de la Plataforma sea **legal, segura, trazable y eficiente**, mediante controles proporcionales al riesgo, evidencias verificables y un proceso ordenado de corrección y mejora (planificar–hacer–verificar–actuar).

14.2 Qué significa "cumplir" en la práctica

Una institución está en cumplimiento cuando:

- Opera cada flujo con **finalidad pública y base legal** declaradas en su instrumento habilitante, y respeta su **catálogo** y **contrato de servicio**.
- Mantiene **seguridad**, **confidencialidad** y **trazabilidad** en los términos definidos en estas Reglas.
- Respeta **SLA**, **cuotas**, **ventanas** y procedimientos de comunicación.
- Conserva y **puede exhibir evidencias**: expedientes de flujo, pruebas UAT/Go-Live, bitácoras, métricas, RCA y documentación vigente en el Repositorio Digital Sectorial.

14.3 Tipos de verificación

- **Autoevaluación** (institucional): revisión periódica del cumplimiento por flujo, con plan de acción cuando haya brechas.
- **Auditoría operativa sectorial** (coordinada por la Subsecretaría): verifica reglas transversales (SLA, comunicación, cuotas, seguridad/trazabilidad mínima) y el estado del repositorio.
- **Auditoría específica** (temática o por incidente): focalizada en seguridad, privacidad, integridad de datos o continuidad, activada por hallazgos, reclamos o incidentes S1/S2.
- **Auditoría de terceros/encargados**: la institución contratante verifica obligaciones equivalentes del encargado (accesos, logs, confidencialidad y segregación de ambientes).

14.4 Alcance mínimo de una auditoría (qué se revisa)

1. **Instrumento habilitante**: finalidad, base legal, catálogo y controles declarados.
2. **API/servicio y versión**: compatibilidad, notas de cambio, coexistencia y reversa.
3. **Seguridad y acceso**: MFA en perfiles sensibles y cuentas de servicio, mínimo privilegio, gestión de secretos, segregación de ambientes.
4. **Trazabilidad**: completitud de logs (quién/qué/cuándo/para qué), integridad (hash/firma) y retención.
5. **Operación**: métricas vs. umbrales, cuotas y manejo de reintentos/backoff.

6. **Continuidad**: RPO/RTO, respaldos y ensayos de restauración.
7. **Comunicación**: avisos de ventanas/cambios, reportes post-incidente, publicación en repositorio.

14.5 No conformidades (NC) y observaciones

- **NC Mayor**: incumplimiento que compromete legalidad, confidencialidad, integridad o disponibilidad (p. ej., uso sin base legal; ausencia de trazabilidad; credenciales compartidas; ruptura de servicio sin coexistencia).
- **NC Menor**: desviación que no afecta la continuidad ni la finalidad (p. ej., metadatos desactualizados en el repositorio; omisiones formales).
- **Observación**: oportunidad de mejora sin incumplimiento.

Cada NC se documenta con **evidencia**, **riesgo**, **responsable** y **plazo**.

14.6 Planes de acción y plazos de corrección

- **Plan Correctivo (PC)** para **NC Mayor**: acciones, responsables, hitos y fecha comprometida; puede incluir medidas temporales de protección (ajuste de cuotas, degradación controlada, ventanas extraordinarias).
- **Plan de Mejora (PM)** para **NC Menor**/observación: acciones y fechas de implementación.
- **Seguimiento**: reporte quincenal o mensual (según severidad) hasta cierre verificado por la Subsecretaría.

14.7 Tratamiento ante incumplimientos reiterados

Si una institución **repite desvíos** o no ejecuta su plan en los plazos:

- Se **eleva** a la instancia sectorial correspondiente.
- Se aplican **medidas proporcionales y temporales** para proteger el servicio (ajuste de cuotas, reprogramación de ventanas, suspensión parcial/temporal del flujo).
- Persistiendo el incumplimiento, se podrá **suspender** la publicación/consumo involucrado hasta regularizar, dejando constancia en el repositorio.

14.8 Evidencias y repositorio (trazabilidad de cumplimiento)

Todos los elementos de cumplimiento (informes, listas de verificación, PC/PM, actas y cierres) se **versionan y archivan** en el Repositorio Digital Sectorial, con metadatos (versión, fecha, vigencia) y huella de integridad. Las instituciones mantienen el **expediente operativo del flujo** actualizado y exportable.

14.9 Indicadores de cumplimiento

A nivel de tablero sectorial se publican, al menos:

- **% de flujos con instrumentos vigentes** y completos.
- **% de auditorías** realizadas vs. plan.
- **Tasa de NC** (mayores/menores) y **tiempo medio de cierre**.
- **Incidentes S1/S2** y cumplimiento de plazos de **RCA**.

- **Publicaciones de versión** y **cumplimiento de coexistencia** en cambios mayores.

14.10 Roles y responsabilidades (síntesis)

- **Subsecretaría**: define lineamientos y plan anual de auditoría; coordina verificaciones; valida cierres de NC Mayores; puede disponer medidas temporales de protección del servicio.
- **Unidad IoP (operación de Plataforma)**: facilita evidencias técnicas, métricas y tableros; apoya en verificaciones y en el seguimiento de PC/PM.
- **Instituciones proveedoras/consumidoras**: mantienen expedientes, ejecutan PC/PM y aseguran control sobre sus encargados.
- **Encargados/terceros**: se someten a verificación y aportan evidencias equivalentes a las institucionales.

14.11 Integración con gestión de riesgos

Los hallazgos de auditoría alimentan el **registro de riesgos** del flujo y del servicio; cada riesgo relevante debe tener **tratamiento** (qué/cómo/quién/cuándo/evidencia) y revisión periódica. La resolución de incidentes S1/S2 debe cerrar sus **acciones preventivas** asociadas.

14.12 Cierre y mejora continua

Una auditoría cierra cuando: (i) todas las NC están **corregidas y verificadas**, o (ii) existe un **plan aprobado** con medidas de mitigación temporal y fecha cierta. La mejora continua se evidencia en la **reducción de NC**, en la **estabilidad de métricas** y en la **menor recurrencia** de incidentes vinculados a causas ya tratadas.

Capítulo 15. Disposiciones finales y vigencia

Este capítulo establece cómo se aplican, mantienen y actualizan estas Reglas de Uso, así como su relación con el Convenio y con los instrumentos habilitantes de cada flujo. Su objetivo es dar certezas simples: qué prevalece si hay dudas, desde cuándo rigen y qué obligaciones subsisten aún cuando un flujo se modifique o termine.

15.1 Naturaleza y carácter vinculante

Estas Reglas de Uso forman parte integrante del Convenio como su Anexo operativo. Obligan a la Subsecretaría, a las instituciones proveedoras y consumidoras y a sus encargados o terceros, en todo lo relativo a publicación, consumo, seguridad, trazabilidad, comunicación y auditoría del Nodo L&P y de la Ficha L&P.

15.2 Orden de prelación y coherencia

Ante dudas o aparentes conflictos, se aplica el siguiente orden:

1. **Convenio** (cuerpo principal y cláusulas),
2. **Estas Reglas de Uso (Anexo 5)**,
3. **Instrumentos habilitantes** (formularios de publicación/consumo de cada flujo),
4. **Documentación operativa** (catálogos, contratos de servicio, guías y runbooks).
   En lo no previsto, rige la normativa sectorial y transversal aplicable y los lineamientos de la Subsecretaría.

15.3 Vigencia y actualización

Las Reglas rigen desde su **publicación oficial** y permanecen vigentes hasta que una nueva versión las reemplace. La Subsecretaría puede emitir **actualizaciones** para mejorar claridad, reforzar controles o alinear con cambios normativos.

- Los cambios **menores** (que no alteran obligaciones sustantivas) se publican con **notas de cambio** y fecha de vigencia.
- Los cambios **mayores** (que introducen nuevas exigencias sustantivas o modifican procedimientos clave) se comunican con antelación razonable y, cuando corresponda, consideran período de transición.

15.4 Publicación y control de versiones

La versión vigente y su historial se mantienen en el **Repositorio Digital Sectorial** con metadatos (número/fecha de versión, vigencia) y verificación de integridad. La versión publicada en el Repositorio es la **única oficial** para todos los efectos.

15.5 Interpretación y resolución de controversias

Las consultas de interpretación operativa se canalizan inicialmente a la **Operación de Plataforma** y, de persistir, a la **Subsecretaría**. Las controversias sobre aplicación de estas Reglas se resuelven conforme al mecanismo establecido en el Convenio, priorizando soluciones que **protejan la continuidad del servicio** y la finalidad pública del flujo.

15.6 Fuerza mayor y suspensiones

Eventos de fuerza mayor o de seguridad que impidan el cumplimiento oportuno de ciertos compromisos operativos (p. ej., SLA o ventanas) se documentan y comunican por los canales oficiales. Superado el evento, se restablecen los parámetros y, si procede, se ejecuta un **plan de normalización** proporcional.

15.7 Obligaciones que sobreviven

Terminado un flujo o suspendido su consumo/publicación, **subsisten**:

- el deber de **confidencialidad**,
- las obligaciones de **resguardo y trazabilidad** de evidencias por los plazos aplicables,
- el respeto a la **titularidad** y a la finalidad con que fueron tratados los datos,
- la obligación de colaborar en auditorías relativas al período en que el flujo estuvo activo.

15.8 Modificaciones del documento y mejoras

Las propuestas de mejora a estas Reglas pueden originarse en la operación del Nodo/Ficha o en la Mesa de Interoperabilidad. Toda modificación conserva **trazabilidad** (propuesta, revisión, aprobación, publicación) y se alinea con el modelo de **gestión de cambios** descrito en el Capítulo 10 (cuando impacte documentación o contratos de servicio).

15.9 Derogación de versiones previas

Con la entrada en vigor de una nueva versión, quedarán **derogadas** las versiones anteriores, salvo que la propia publicación establezca un período acotado de **coexistencia** para permitir la transición documental.

15.10 Entrada en vigor por flujos

Si una actualización de estas Reglas introduce exigencias operativas que requieren ajustes por flujo, la Subsecretaría podrá establecer un calendario de **entrada en vigor gradual**, priorizando flujos críticos y resguardando la continuidad.

15.11 Preguntas frecuentes y soporte

Las instituciones adherentes cuentan con: (i) **mesa de ayuda** para operación diaria, (ii) canal expedito de **seguridad** para incidentes S1/S2 y (iii) un repositorio de **preguntas frecuentes** actualizado. La información oficial se comunica exclusivamente por los **canales definidos** en estas Reglas.

Anexo A. Instrumento habilitante de Publicación (Proveedor)

Propósito del anexo. Plantilla detallada y auditable para que una institución publique un flujo de datos en la Plataforma (Nodo L&P y Ficha L&P). Se completa en prosa breve y con los cuadros siguientes. Todo lo declarado aquí debe ser **verificable** y mantenerse **actualizado**.

Nota importante: este anexo es referencial, los anexos válidos son los publicados en el cuerpo del Convenio.

A.1 Identificación del flujo

Ítem	Contenido a completar
Título del flujo	*(Nombre claro y único)*
Institución publicadora	*(Nombre oficial)*
Responsable institucional del flujo	*(Nombre, cargo, correo, teléfono)*
Responsable técnico	*(Nombre, correo)*
Responsable de seguridad	*(Nombre, correo)*
Versión de la publicación	*(v1.0, v1.1, etc.)*
Fecha de entrada en vigor	*(dd-mm-aaaa)*
Alcance resumido	*(1–3 líneas en prosa clara)*

A.2 Finalidad pública y base habilitante

Finalidad pública (prosa, 3–5 líneas).
(Describir qué necesidad pública satisface el flujo y para qué procedimientos se usará.)

Base legal habilitante (citar acto/norma).

- Norma/acto: *(Ley/Reglamento/Resolución/oficio)*
- Identificador y fecha: *(p. ej., Res. Ex. 1234/2025)*
- Extracto habilitante (1–2 líneas): *(¿Qué autoriza?)*

Regla de llenado: No se aceptan finalidades genéricas; la finalidad debe permitir evaluar qué campos son **estrictamente necesarios**.

A.3 Catálogo de datos (necesidad y reglas)

Nº	Campo/atributo	Descripción funcional (prosa)	Tipo/formato	Oblig.	Regla de negocio/validación	Justificación de necesidad (1 línea)
1						
2						

Relaciones y claves (si aplica).
(Identificadores, claves compuestas, referencias externas p. ej. RUT/RUN, códigos institucionales.)

Regla de llenado: Si la justificación es "por si acaso", elimine el campo. Documente equivalencias/mapeos si cambia el dominio de un código.

A.4 Contrato de servicio (API / mecanismo)

Ítem	Contenido a completar
Modalidad	*(Síncrono REST / Lotes / Eventos)*
Endpoint / Canal	*(URL o mecanismo; no incluir secretos)*
Método / Frecuencia	*(GET/POST, o frecuencia de lotes/eventos)*
Autenticación & Autorización	*(Tipo; perfiles habilitados; alcance mínimo)*
Esquema de **solicitud**	*(Resumen de parámetros esenciales)*
Esquema de **respuesta**	*(Resumen; incluir version_publicacion e id_transaccion si corresponde)*
Códigos de error principales	*(p. ej. 400, 401, 403, 404, 409, 429, 5xx con semántica breve)*
Límites/cuotas por consumidor	*(p. ej. 50 req/min; burst 10; concurrencia 5)*
Tamaños y paginación	*(p. ej. máx. 1 MB / 100 ítems por página)*
Idempotencia/orden	*(Cuando aplique)*

Ejemplos representativos (adjuntos).

- 1 solicitud **válida** y 1 **inválida**
- 1 respuesta **OK** y 1 **error** (con codigo, mensaje_corto, timestamp, trace_id)

A.5 Condiciones operativas (SLA y continuidad)

Métrica	Umbral/objetivo	Fuente de medición	Periodicidad
Disponibilidad mensual (%)			
Latencia p95 (ms) (si es síncrono)			
Tasa de error permitida (%)			
RPO/RTO (si hay lotes/eventos)			
Soporte (S1/S2/S3: primera respuesta)			

Cuotas y protección del servicio.

(Definir límites por institución/flujo; política de reintentos/backoff recomendada.)

Continuidad y reversa.

(Descripción breve del plan de reversa y degradación controlada —p. ej., de síncrono a lotes—.)

A.6 Seguridad, confidencialidad y trazabilidad

Control	Declaración mínima
Autenticación	*(Mecanismo; MFA en perfiles sensibles y cuentas de servicio críticas)*
Autorización	*(Perfiles, mínimo privilegio; alcance por flujo/endpoint)*
Gestión de secretos	*(Cofre/rotación; sin secretos en código)*
Cifrado	*(En tránsito obligatorio; en reposo cuando aplique)*
Ambientes	*(Segregación sandbox/UAT/prod; datos sintéticos/enmascarados en pruebas)*
Logs y retención	*(Quién/qué/cuándo/para qué; plazo de retención; exportables)*
Integridad	*(Hash/firma de respuestas o de artefactos de publicación)*

A.7 Ambientes y pruebas

Ítem	Sandbox	UAT	Producción
Endpoint/Canal declarado	☐	☐	☐
Datos sintéticos/enmascarados	☐	☐	—
Casos de prueba aprobados	☐	☐	—
Monitoreo/alertas configuradas	—	☐	☐
Plan de reversa ensayado	—	☐	☐

Acta de Go-Live (adjunta). *(Fecha/hora; responsables; criterios de aceptación cumplidos.)*

A.8 Comunicación y ventanas

Tipo	Contenido mínimo	Anticipación / Frecuencia
Ventanas programadas	Fecha, impacto, contingencia, reversa	*(p. ej., ≥5 días hábiles)*
Cambios de versión	Alcance, impacto, pruebas requeridas	*(según mayor/menor/parche)*
Incidentes (S1/S2)	Estado, severidad, avance, RCA	*(según matriz sectorial)*

A.9 Versionado y deprecaciones

Ítem	Contenido
Esquema de versionado	*(Mayor.Menor.Parche)*
Coexistencia en cambios mayores	*(p. ej., v1 y v2 por 4 meses)*
Fecha de deprecación de versión anterior	*(dd-mm-aaaa)*
Notas de versión (resumen)	*(Cambios y compatibilidad)*

A.10 Evidencias obligatorias (adjuntar)

- Acto/norma habilitante (copia digital).
- Catálogo completo (cuadro A.3) y contrato del servicio (A.4).
- Plan de pruebas y **resultados UAT**.
- Checklist de **Go-Live** y plan de **reversa** probado.
- Matriz de **roles/perfiles** y registro de altas/bajas.
- Política de **retención de logs** y respaldos.
- Publicación en **Repositorio Digital Sectorial** (versión + hash de integridad).

A.11 Declaraciones y firmas

Rol	Nombre y cargo	Firma/fecha
Responsable institucional		
Responsable técnico		
Responsable de seguridad		
V°B° Subsecretaría (aprobación)		

A.12 Ejemplo orientativo (prosa breve)

Finalidad. "Publicar la vigencia de afiliación y entidad administradora para verificar **en línea** requisitos de acceso a subsidios del Ministerio X dentro del procedimiento Y."
Base habilitante. "Res. Ex. 1234/2025 de la Institución Z, que encomienda la provisión de datos para fines de verificación de requisitos del procedimiento Y."
Catálogo (extracto). rut_persona *(string, obligatorio; valida DV)* — **necesidad**: identificar unívocamente al solicitante. estado_afiliacion *(enum: vigente/no_vigente)* — **necesidad**: determinar elegibilidad. fecha_actualizacion *(fecha ISO 8601)* — **necesidad**: saber la vigencia de la respuesta.
Contrato (extracto). GET /v1/afiliacion?rut_persona={rut}; auth por token institucional; cuota inicial: 30 req/min por institución; errores: 400 formato de RUT inválido, 404 sin registro, 429 límite excedido.
SLA (extracto). Disponibilidad ≥ 99,5% mensual; p95 ≤ 800 ms; tasa de error ≤ 1%; RPO/RTO no aplica (síncrono).
Seguridad. MFA para administradores; secretos en cofre; cifrado TLS; logs con id_transaccion, finalidad y resultado, retención 12 meses.
Pruebas y Go-Live. 24 casos exitosos + 12 de error; monitoreo listo; reversa a v1.0 si falla v1.1.

A.13 Lista rápida de verificación (antes de enviar a aprobación)

- Finalidad **específica** y base legal **citada**.
- Catálogo completo con **justificación de necesidad** por campo.
- Contrato con **endpoint, esquema, errores y cuotas**.
- Métricas/SLA con **fuente de medición**.
- Seguridad y **trazabilidad** declaradas; MFA en perfiles sensibles y cuentas de servicio críticas.
- UAT **aprobado** y **plan de reversa** probado.
- Publicación preparada para el **Repositorio** (versión + hash).

Anexo B. Instrumento habilitante de Consumo (Consumidor)

Propósito del anexo. Plantilla simple y auditable para que una institución **consuma** un flujo de datos a través de la Plataforma (Nodo L&P y Ficha L&P). Se completa en prosa breve y con los cuadros siguientes. Todo lo declarado debe ser **verificable**, **proporcional a la finalidad** y mantenerse **actualizado**.

Nota importante: este anexo es referencial, los anexos válidos son los publicados en el cuerpo del Convenio.

B.1 Identificación del consumo

Ítem	Contenido a completar
Título del consumo	*(Nombre claro y único, referenciando el flujo publicado)*
Institución consumidora	*(Nombre oficial)*
Responsable institucional del consumo	*(Nombre, cargo, correo, teléfono)*
Responsable técnico (integración)	*(Nombre, correo)*
Responsable de seguridad	*(Nombre, correo)*
Versión del consumo	*(v1.0, v1.1, etc.)*
Fecha de entrada en vigor	*(dd-mm-aaaa)*
Alcance resumido	*(1–3 líneas en prosa clara)*

B.2 Finalidad pública y base habilitante del consumo

Finalidad (prosa, 3–5 líneas).
(Describir el caso/acto administrativo que habilita el consumo y el beneficio público concreto.)

Base legal/acto administrativo.

- Norma/acto: *(Ley/Reglamento/Resolución/Oficio)*
- Identificador y fecha: *(p. ej., Res. Ex. 1234/2025)*
- Extracto habilitante (1–2 líneas): *(¿Qué autoriza?)*

Regla de llenado: No se aceptan finalidades genéricas ni "por si acaso". El consumo debe estar explícitamente vinculado a **un** procedimiento o servicio.

B.3 Alcance de uso y perfiles habilitados

Ítem	Contenido
Procedimientos/servicios donde se usará	*(Listar. Ej.: Subsidio X; Fiscalización Y; Trámite Z)*
Perfiles que podrán consumir	*(p. ej., Operador Trámite X; Cuenta de servicio backend)*
Justificación de cada perfil	*(1 línea de necesidad por perfil)*
Exclusiones expresas	*(No investigación; no scraping; no usos masivos no transaccionales; no reprocesamientos fuera de finalidad)*

B.4 Necesidad de datos (minimización)

Nº	Campo requerido (según catálogo del proveedor)	Uso en el procedimiento (prosa breve)	Justificación de necesidad (1 línea)
1			
2			

Regla de llenado: Solicita **sólo** los atributos que respaldan la decisión del caso administrativo. Si la justificación es débil, elimínalo.

B.5 Contrato de consumo e integración

Ítem	Contenido a completar
Publicación consumida	*(Nombre del flujo y versión: p. ej., "Afiliación v1")*
Modalidad	*(Síncrono REST / Lotes / Eventos)*
Endpoint/canal invocado	*(URL o mecanismo; sin secretos)*
Autenticación & autorización	*(Mecanismo; perfiles autorizados; alcance mínimo)*
Parámetros de consulta	*(Listar los esenciales y su origen en el expediente/caso)*
Manejo de errores	*(Códigos esperados; política de reintentos con backoff; límites)*
Límites/cuotas respetadas	*(p. ej., 30 req/min por institución; concurrencia 5)*
Tiempos de espera (timeouts)	*(p. ej., 2 s app; 5 s backend; 10 s total)*
Idempotencia y correlación	*(Uso de id_transaccion/trace_id si aplica)*

B.6 Evidencia operativa y trazabilidad (no repudio)

Requisito	Declaración mínima
Registro por transacción	*(Quién/qué/cuándo/para qué; identificador de caso/expediente; endpoint/versión; resultado)*
Verificación de integridad	*(Validación de hash/firma cuando aplique; guardar comprobante)*
Conservación de evidencia	*(Plazo de retención; formato exportable; ubicación)*
Exportabilidad	*(Capacidad de entregar registros a SPS/auditoría con cadena de custodia)*

B.7 Seguridad y confidencialidad

Control	Declaración mínima
Gestión de usuarios	*(Altas/bajas trazables; recertificación al menos semestral)*
MFA y cuentas de servicio	*(MFA en perfiles sensibles; cuentas de servicio con alcance acotado y rotación de secretos)*
Segregación de ambientes	*(Endpoints y credenciales distintas para sandbox/UAT/prod; sin datos reales en pruebas)*
Cifrado y secretos	*(TLS en tránsito; cofres de secretos; sin claves en código)*
Política de uso	*(Datos sólo para la finalidad declarada; prohibida redistribución interna/terceros sin habilitante)*

B.8 Condiciones operativas del consumo

Métrica	Compromiso del consumidor	Observaciones
Uso responsable	*(Respetar cuotas y backoff; no pruebas de carga sin coordinación)*	
Manejo de errores	*(Reintentos con jitter y límites; no bucles acelerados)*	

Ventanas y cambios	*(Adaptación a ventanas programadas; seguimiento de avisos del proveedor)*	
Continuidad	*(Degradación planificada si falla síncrono: p. ej., colas y reintentos diferidos)*	

B.9 Pruebas y paso a producción

Ítem	Sandbox	UAT	Producción
Casos de prueba (éxito/error/borde)	☐	☐	—
Validación de integridad y trazas	☐	☐	—
Monitoreo/alertas del consumo	—	☐	☐
Ensayo de reversa/rollback	—	☐	☐

Acta de Go-Live (adjunta). *(Fecha/hora; responsables; criterios de aceptación cumplidos.)*

B.10 Comunicaciones e incidentes

Tipo	Contenido mínimo	Tiempo/Canal
Aviso de cambios del proveedor	Alcance, impacto y pruebas	*(Seguir canales oficiales)*
Incidente S1/S2	Severidad, contención, causa preliminar	*(Notificación inmediata a SPS según matriz sectorial)*
Post-incidente	RCA, medidas correctivas/preventivas y plazos	*(Publicación en repositorio cuando aplique)*

B.11 Versionado y compatibilidad

Ítem	Contenido
Versión de la publicación consumida	*(vX.Y)*
Política de actualización	*(Plazos de adaptación; coexistencia en cambios mayores)*
Notas internas de cambio	*(Efectos en procesos; capacitación; ajustes de sistemas)*

B.12 Evidencias obligatorias (adjuntar)

- Acto/norma **habilitante** del consumo.
- Mapa de **perfiles** y matriz de acceso por rol.
- Lista de **campos** solicitados con **justificación de necesidad** (B.4).
- Plan de **pruebas UAT** y resultados; **checklist de Go-Live**.
- Política de **retención y exportación** de registros (trazabilidad).
- Publicación del instrumento en el **Repositorio Digital Sectorial** (versión + hash).

B.13 Declaraciones y firmas

Rol	Nombre y cargo	Firma/fecha

Responsable institucional del consumo		
Responsable técnico (integración)		
Responsable de seguridad		
V°B° Subsecretaría (aprobación)		

B.14 Ejemplo orientativo (prosa breve)

Finalidad. "Verificar en línea la **vigencia de afiliación** de solicitantes para el otorgamiento del Subsidio X dentro del procedimiento Y (etapa de evaluación)."

Base habilitante. "Res. Ex. 5678/2025 de la Institución A, que autoriza el consumo del flujo 'Afiliación' para el procedimiento Y."

Alcance y perfiles. Operadores del **Trámite Y** y una **cuenta de servicio** backend para validación automática; queda **excluido** el uso para investigación/estudios o barridos masivos.

Necesidad de datos (extracto). rut_persona (identificación única del solicitante) y estado_afiliacion (determinar elegibilidad); fecha_actualizacion (vigencia de la respuesta).

Integración. GET /v1/afiliacion?rut_persona={rut}; autenticación con token institucional; timeouts app 2 s / backend 5 s; reintentos con backoff exponencial (máx. 2).

Evidencia y trazabilidad. Registro por transacción con id_expediente, finalidad, endpoint, version_publicacion, resultado y trace_id; validación de integridad de la respuesta; retención 12 meses.

Seguridad. MFA para administradores; tokens en cofre con rotación trimestral; sandbox/UAT con datos sintéticos; sin pruebas de carga.

UAT/Go-Live. 18 casos de éxito y 10 de error cubiertos; monitoreo activo; reversa documentada.

B.15 Lista rápida de verificación (previa a aprobación)

- **Finalidad específica** y **base legal** citadas (sin ambigüedades).
- **Perfiles** acotados al mínimo necesario y **exclusiones** declaradas.
- **Campos** solicitados con **justificación de necesidad** (minimización).
- **Contratos** y parámetros de consumo definidos (errores, reintentos, cuotas, timeouts).
- **Trazabilidad** por transacción y verificación de **integridad** habilitadas.
- **Seguridad**: MFA en perfiles sensibles; secretos en cofre; ambientes segregados.
- **UAT aprobado**; **monitoreo activo**; **plan de reversa** probado.
- Publicación en **Repositorio** (versión + hash).

Anexo C. Matriz RACI y Escalamiento (resumen operativo)

Propósito del anexo. Unificar "quién hace qué" y "cómo se escala" ante cambios e incidentes del Nodo L&P y la Ficha L&P. La matriz permite auditabilidad y es coherente con los capítulos de este Anexo.

Leyenda RACI: **R** (Responsible: ejecuta) · **A** (Accountable: decide/aprueba) · **C** (Consulted: participa/asesora) · **I** (Informed: informado)

Actores (referencia):
SPS (gobernanza) · Mesa IoP (coordinación operativa) · Comité Directivo (estratégico, cuando exista) · Unidad IoP (operación Plataforma) · MINHAC (lineamientos transversales) · Institución **Proveedor (Prov.)** · Institución **Consumidor (Cons.)** · Responsable Institucional (por OAE) · Resp. Técnico (por flujo) · Resp. Seguridad (por institución) · Admin. Usuarios/Perfiles · Mesa de Ayuda · Encargado/Tercero · Auditoría (interna/externa).

C.1 Matriz RACI sectorial (síntesis por proceso)

C.1.1 Reglas de Uso (Anexo 5) y actualizaciones menores

Actividad	SPS	Mesa IoP	Comité Dir.	Unidad IoP	MINHAC	Prov.	Cons.	Resp. Inst.	Resp. Téc.	Resp. Seg.	Mesa Ayuda	Auditoría
Emitir/actualizar Reglas de Uso	A	C	I	R	C	I	I	I	I	C	I	I
Nota aclaratoria menor	A	C	I	R	C	I	I	I	C	C	I	I
Publicar versión en Repositorio	A	I	I	R	I	I	I	I	I	I	I	I

C.1.2 Catálogos y contratos de servicio (publicación/cambio)

Actividad	SPS	Mesa IoP	Unidad IoP	Proveedor	Consumidor	Resp. Inst.	Resp. Téc.	Resp. Seg.
Proponer cambio **menor** (compatible)	C	C	C	R	C	A	R	C
Aprobar cambio **mayor** (no compatible)	A	C	C	R	C	C	C	C
Documentar catálogo/contrato y notas	C	I	R	R	C	I	R	C
Coexistencia y plan de transición	A	C	R	R	R	C	R	C

C.1.3 Cuotas, límites y protección del servicio

Actividad	SPS	Unidad IoP	Proveedor	Consumidor	Resp. Seg.	Mesa IoP
Definir cuota inicial por flujo	A	C	R	C	C	C
Ajuste **temporal** por riesgo/incidente	A	R	R	R	C	I
Monitorear/alertar excesos	I	R	R	R	C	I

C.1.4 UAT, Go-Live y reversa

Actividad	SPS	Unidad IoP	Proveedor	Consumidor	Resp. Inst.	Resp. Téc.
Plan de pruebas (casos éxito/error/borde)	C	C	R	R	A	R
Aprobación de UAT	A	C	R	R	A	C
Pase a producción (ventana definida)	A	R	R	R	A	R
Plan de **reversa** (ensayo y evidencia)	C	R	R	R	A	R

C.1.5 Métricas, tablero y reportes post-incidente

Actividad	SPS	Unidad IoP	Proveedor	Consumidor	Mesa IoP	Auditoría
Tablero sectorial (publicación mensual)	A	R	C	C	C	I
Post-incidente S1/S2 (RCA y plan)	A	R	R	R	C	I
Seguimiento de planes de mejora	A	R	R	R	C	I

C.1.6 Mantenimientos (programados y extraordinarios)

Actividad	SPS	Unidad IoP	Proveedor	Consumidor	Mesa IoP
Calendario y aviso (programados)	A	R	R	I	C
Ventana **extraordinaria** (seguridad/dispo)	A	R	R	I	C
Comunicación y cierre (acta/resumen)	A	R	R	I	C

C.1.7 Incidentes S1/S2 y RCA

Actividad	SPS	Unidad IoP	Proveedor	Consumidor	Resp. Seg.	Mesa de Ayuda
Clasificar severidad y escalar	A	R	R	R	C	R
Contención y restauración	A	R	R	R	C	C
RCA + medidas correctivas/preventivas	A	R	R	R	C	I

C.1.8 Break-glass (acceso de emergencia)

Actividad	SPS	Unidad IoP	Resp. Seg.	Proveedor/Consumidor	Mesa IoP
Autorización puntual	A	C	A/R (según institución)	R (ejecución)	I
Documentación y normalización	A	R	R	R	I

C.1.9 Gestión de usuarios y perfiles

Actividad	SPS	Unidad IoP	Admin. Usuarios	Resp. Inst.	Resp. Seg.	Auditoría
Altas/bajas y asignación de perfiles	I	I	R	A	C	I

Recertificación periódica	I	I	R	A	C	I

C.1.10 Auditorías y cumplimiento

Actividad	SPS	Auditoría	Unidad IoP	Proveedor	Consumidor	Resp. Inst.
Plan anual y lineamientos	A	C	C	I	I	I
Ejecución de auditoría	A	R	C	C	C	C
Planes Correctivos/Mejora (PC/PM)	A	C	R	R	R	A

C.2 Escalamiento operativo (S3, S2, S1)

Objetivo: resolver rápido, con trazabilidad y comunicaciones claras. Los tiempos son **máximos**; si se puede antes, mejor.

C.2.1 Definiciones rápidas

- **S3 (Medio/Bajo)**: impacto acotado; sin afectación crítica a servicio.
- **S2 (Alto)**: degradación relevante o indisponibilidad parcial; usuarios afectados.
- **S1 (Crítico)**: caída general o riesgo severo (seguridad/disponibilidad); múltiples instituciones afectadas.

C.2.2 Flujo y tiempos de actuación

Paso	S3	S2	S1
1) Detección y registro (mesa de ayuda)	≤ 4 h	≤ 1 h	≤ 30 min
2) Clasificación + **escalamiento**	≤ 8 h a Resp. Téc.	≤ 2 h a SPS/Resp. Seg.	≤ 30 min a SPS + Unidad IoP + Resp. Seg.
3) Comunicación inicial	Dentro del día hábil	≤ 4 h	≤ 2 h
4) Contención / medidas temporales	Según runbook	≤ 8 h	≤ 2 h
5) Restauración del servicio	≤ 5 días hábiles	≤ 24 h	**Lo antes posible** (objetivo horas)
6) **RCA** + plan (PC/PM)	≤ 10 días hábiles	≤ 7 días hábiles	≤ 5 días hábiles
7) Cierre validado por SPS	Sí	Sí	Sí

C.2.3 Quien lidera en cada severidad

- **S3**: Proveedor/Consumidor (según origen) con apoyo de Unidad IoP; SPS informado.
- **S2**: Unidad IoP lidera; SPS coordina; Proveedor/Consumidor ejecutan acciones en su ámbito.
- **S1**: **SPS lidera la coordinación sectorial**; Unidad IoP dirige operación técnica; Responsables de Seguridad autorizan medidas especiales (throttling, degradación controlada, break-glass) y comunican.

C.2.4 Medidas temporales (proporcionales y auditables)

- **Protección de servicio**: ajuste de **cuotas**, **throttling**, ventanas extraordinarias, degradación de **síncrono → lotes**.
- **Seguridad**: rotación forzada de secretos, bloqueos selectivos, listas de permitidos, **break-glass** con autorización.
- **Comunicación**: avisos periódicos según severidad; publicación de **post-incidente** y actualización de runbooks si aplica.

C.3 Plantillas mínimas de comunicación (orientativas)

A) Aviso de ventana programada (cambio menor)

- Título · Fecha/Hora · Flujos afectados · Impacto esperado · Plan de reversa · Contacto · Próxima actualización.

B) Aviso de incidente S2/S1 (inicial)

- Título · Severidad · Alcance/impacto · Medidas de contención · Próxima actualización (frecuencia) · Equipo a cargo.

C) Cierre post-incidente (RCA)

- Resumen · Causa raíz · Acciones correctivas · Acciones preventivas · Plazos/ responsables · Evidencias adjuntas · Hash/versión del informe.

C.4 Lista rápida de verificación (aplicación diaria)

- Cada flujo tiene **RACI** interno alineado a esta matriz.
- Runbooks vigentes con **escalamiento** y contactos (24×7 si aplica).
- Tablero con **métricas** y alertas configuradas.
- Canales de comunicación validados (operación/seguridad).
- Ensayo anual de **reversa** y de **incidente S1/S2** con acta y mejoras.
- Revisión trimestral de **cuotas** y límites antiabuso.

Anexo D. Glosario y Formatos mínimos del Repositorio Digital Sectorial (RDS)

Propósito del anexo. Establecer un glosario breve y los **formatos mínimos de publicación** en el RDS, de modo que todo artefacto (reglas, instrumentos, catálogos, contratos, métricas, avisos e informes) quede identificable, versionado y verificable (hash), con trazabilidad hacia sus predecesores/sucesores.

D.1 Glosario esencial (definiciones operativas y simples)

Término	Definición breve y de uso
Plataforma	Conjunto Nodo L&P + Ficha L&P y servicios asociados operados sectorialmente.
Flujo	Publicación/consumo de datos habilitado por instrumento formal y operado por la Plataforma.
Catálogo	Descripción funcional de campos, tipos, reglas y justificación de necesidad.
Contrato de servicio	Especificación técnica/operativa del intercambio (endpoint, esquema, errores, límites, versión).
Instrumento habilitante	Formulario oficial (de publicación o consumo) que declara finalidad y base legal del flujo.
SLA	Acuerdo de niveles de servicio (disponibilidad, latencia, error, soporte).
RPO / RTO	Punto Objetivo de Recuperación / Tiempo Objetivo de Recuperación para continuidad/DR.
RCA	Informe de causa raíz y acciones (correctivas/preventivas) post-incidente.
Break-glass	Acceso de emergencia, excepcional, temporal y auditado.
Coexistencia	Periodo en el que conviven dos versiones para permitir migración sin ruptura.
Hash de integridad	Huella (resultado de función criptográfica) para verificar que un artefacto no fue alterado.
Repositorio Digital Sectorial (RDS)	Fuente única y oficial de versiones y evidencias del proyecto/Plataforma.

D.2 Siglas y acrónimos (lista base)

Sigla	Significado
SPS	Subsecretaría de Previsión Social
Unidad IoP	Unidad de Interoperabilidad de la DTI-SPS (operación de Plataforma)
MINHAC	Secretaría de Modernización del Estado y Secretaría de Gobierno Digital
OAE	Organismo de la Administración del Estado
UAT	User Acceptance Test (pruebas de aceptación)
MTBF / MTTR	Mean Time Between Failures / Mean Time To Repair
p95	Percentil 95 de latencia

D.3 Metadatos mínimos para todo artefacto en el RDS

Campo (obligatorio)	Descripción	Ejemplo
id_rds	Identificador único en el repositorio	RDS-REG-000145
título	Nombre claro del artefacto	“Instrumento habilitante – Publicación Afiliación v1.2”
tipo_artefacto	{Reglas, Instrumento, Catálogo, Contrato, Aviso, Informe, Métricas, Acta, Runbook}	Instrumento
versión	Número de versión (Mayor.Menor.Parche)	1.2.0

estado	{Vigente, Deprecado, Borrador, Retirado}	Vigente
propietario	Institución y rol responsable	"Institución X – Responsable Institucional del Flujo"
fecha_publicación	Fecha de incorporación al RDS	2025-10-16
hash_integridad	Huella del archivo publicado	SHA-256: 5f…a9
predecesor	id_rds / versión previa (si aplica)	RDS-REG-000121 (v1.1.0)
sucesor	id_rds / versión siguiente (si aplica)	—
ámbito/flujo	Flujo(s) al que aplica	"Afiliación de Trabajador"
clasificación	{Público, Restringido, Sensible}	Restringido
retención	Plazo de conservación	"24 meses"
observaciones	Notas breves (máx. 200 caracteres)	"Reemplaza v1.1.0; cambio menor (campo opcional)"

Regla: No se publica artefacto sin **versión** ni **hash_integridad**.

D.4 Nomenclatura de archivo (recomendación práctica)

<AAAAMMDD>_<Tipo>_<NombreCorto>_v<Mayor>.<Menor>.<Parche>.<ext>

Ejemplos

- 20251016_InstrumentoPublicacion_Afiliacion_v1.2.0.pdf
- 20251016_ContratoAPI_Afiliacion_v1.2.0.json
- 20251016_RCA_IncidenteS1_Afiliacion_v1.2.0.pdf

Sugerencia: Evitar espacios y acentos en nombres de archivo; usar guiones bajos.

D.5 Metadatos adicionales por tipo de artefacto

D.5.1 Instrumento habilitante (Publicación/Consumo)

Campo adicional	Descripción
finalidad	1–3 líneas claras y específicas
base_legal	Norma/acto con identificador y fecha
contacto	Nombre, cargo y correo del responsable institucional
fecha_vigencia	Fecha desde la cual aplica

D.5.2 Catálogo

Campo adicional	Descripción
tabla_campos	Campos con tipo, obligatoriedad, reglas, justificación
mapeos_equivalencias	Cambios de códigos/estados y equivalencias

D.5.3 Contrato de servicio (API)

Campo adicional	Descripción
endpoint/mecanismo	URL o canal de intercambio

autenticación/autorización	Tipo, perfiles, alcance
códigos_error	Con semántica
límites/cuotas	Por institución/flujo

D.5.4 Aviso de ventana/cambio

Campo adicional	Descripción
fecha_hora	Inicio/fin previstos
impacto	Afectación estimada
reversa	Cómo volver si falla

D.5.5 Informe post-incidente (RCA)

Campo adicional	Descripción
severidad	S1/S2/S3
causa_raíz	Síntesis clara
acciones	Correctivas y preventivas con plazos
evidencias	Logs, capturas, correlaciones (referenciadas)

D.6 Hash de integridad (huella mínima de verificación)

Aspecto	Recomendación simple
Función	Publicar **SHA-256** del archivo (o artefacto JSON firmado si aplica).
Formato	SHA-256: <hexadecimal> (64 caracteres hex).
Dónde	En los **metadatos del RDS** y, cuando sea posible, dentro del propio artefacto (encabezado o campo hash).
Relación	Registrar hash del **predecesor** y del **sucesor** en sus metadatos para facilitar cadena de custodia.

Si el artefacto es **JSON** (p. ej., contrato), se puede incluir un campo hash_contenido calculado sobre el **payload normalizado** (sin espacios/orden inestable).

D.7 Cuadros mínimos por artefacto

D.7.1 Portada corta (todos los artefactos)

Campo	Valor
Título	
Tipo de artefacto	
Flujo/ámbito	
Versión	
Fecha de publicación	
Propietario	
Hash de integridad	

D.7.2 Tabla de control de versiones (todos)

Versión	Fecha	Tipo (Mayor/Menor/Parche)	Resumen del cambio	Aprobación
1.2.0	2025-10-16	Menor	Se agrega campo opcional correo_contacto	SPS

D.7.3 Referencias cruzadas (cuando aplique)

Artefacto relacionado	id_rds / versión	Relación
Instrumento de Publicación Afiliación	RDS-INS-00077 / v1.2.0	Base
Contrato API Afiliación	RDS-CON-00088 / v1.2.0	Implementa
Aviso Ventana 2025-10-20	RDS-AVI-00101 / s/n	Cambio programado

D.8 Ejemplo de metadatos completos (copia de referencia)

Metadatos (JSON legible en RDS):

{

"id_rds": "RDS-INS-001234",

"titulo": "Instrumento habilitante – Publicación Afiliación",

"tipo_artefacto": "Instrumento",

"version": "1.2.0",

"estado": "Vigente",

"propietario": "Institución X – Responsable Institucional del Flujo",

"fecha_publicacion": "2025-10-16",

"hash_integridad": "SHA-256: 7e8a2f1c…9b5d",

"predecesor": "RDS-INS-001101 (v1.1.0)",

"sucesor": null,

"ambito_flujo": "Afiliación de Trabajador",

"clasificacion": "Restringido",

"retencion": "24 meses",

"observaciones": "Cambio menor: se agrega campo opcional en respuesta",

"finalidad": "Verificación en línea de afiliación para Subsidio X",

"base_legal": "Res. Ex. 1234/2025",

"contacto": "Nombre Apellido – correo@institucion.cl",

"fecha_vigencia": "2025-11-01"

}

D.9 Lista rápida para publicar en el RDS

- Archivo con **nomenclatura** estándar y contenido final.

- **Metadatos mínimos** completos (D.3).
- **Hash SHA-256** calculado y registrado.
- Referencias a **predecesor/sucesor** (si aplica).
- Estado correcto (**Vigente/Deprecado/Borrador/Retirado**).
- Tabla de **control de versiones** actualizada.
- Clasificación (**Público/Restringido/Sensible**) y **retención** definidas.
- Publicado y visible en el **RDS**; comunicado por canal oficial si corresponde.