MARCO DE INTEROPERABILIDAD INSTITUCIONAL

INS

Institución Benemérita de la Patria

Contenido

Introducción

El Marco de Interoperabilidad Institucional del Instituto Nacional de Seguros (INS) se crea con el fin de ser el instrumento normativo-técnico derivado y sub normado del CNTD, que define las políticas, principios, lineamientos, estándares y estructuras de gobernanza precisos para asegurar el intercambio eficiente, seguro, semánticamente coherente y técnicamente estandarizado de información entre sistemas, aplicaciones, plataformas y actores externos con sistemas e información interoperable del INS.

Este Marco toma como referencia base lo expuesto en el Código Nacional de Tecnologías Digitales (CNTD) del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), la cual figura como normativa obligatoria para todo el sector público costarricense según el decreto de oficialización. El CNTD establece que todas las instituciones del sector público deben adoptar las disposiciones técnicas, incluyendo las relacionadas con integración, seguridad, accesibilidad y, especialmente, interoperabilidad, que constituye un capítulo formal dentro del Código.

El documento vigente del CNTD incorpora y sistematiza principios, políticas generales, políticas específicas y estándares que toda institución deben cumplir para llegar a garantizar la integración digital del Estado, incluyendo lineamientos para las distintas dimensiones de la interoperabilidad como la técnica, semántica, legal y organizacional, los cuales conforman la base estructural de este Marco de Interoperabilidad Institucional del INS.

Asimismo, este Marco reconoce las características esenciales del entorno tecnológico institucional del INS, documentadas en los lineamientos de arquitectura y desarrollo internos de la institución, donde se especifican estándares para integraciones, APIs, nomenclatura, buenas prácticas de datos, seguridad y comunicación entre aplicaciones. Estos insumos constituyen un componente necesario para alinear el modelo institucional con el marco nacional.

Objetivos

La creación de un Marco de Interoperabilidad Institucional para el Instituto Nacional de Seguros busca cumplir con distintos objetivos:

- Establecer directrices institucionales para el diseño, implementación, operación y gobernanza en la interoperabilidad e intercambio de datos.
- Alinear la interoperabilidad institucional con lo descrito en el CNTD del MICITT.
- Estandarizar los modelos de interoperabilidad completando diferentes lineamientos para la integración con la institución.
- Incluir mecanismos de seguimiento, actualización y mejora continua los cuales contemplen cambios normativos, tecnológicos, organizacionales y de seguridad alineados al cumplimiento del CNTD.

Alcance

El alcance de este documento abarca todas las integraciones expuestas por dependencias, unidades, sistemas y plataformas tecnológicas del INS, así como soluciones desarrolladas internamente, adquiridas, integradas o consumidas por la institución.

En el ámbito de interoperabilidad, se regula las dimensiones técnica, semántica, organizacional y legal. La interoperabilidad técnica se basa en las Políticas Generales del CNTD e incorpora protocolos, APIs, formatos, seguridad, modelos de mensajería y patrones de integración definidos por dicho ente. La interoperabilidad semántica establece glosarios, catálogos y reglas de calidad de datos, también basados en lineamientos del CNTD. La interoperabilidad organizacional define los procesos, roles, responsabilidades, estructuras de gobernanza y reglas institucionales necesarias para habilitar el intercambio de información; y la interoperabilidad legal establece el marco jurídico para el intercambio de información tanto interna como externamente, fundamentado en las políticas del CNTD sobre cumplimiento normativo y respaldo legal.

En cuanto al ámbito tecnológico, se comprende todos los medios definidos a nivel interno de la institución, incluyendo APIs REST, estándares y patrones oficiales y el Portal del Desarrollador como repositorio central de publicación de APIs. Este Marco es permanente y requiere actualización ante cambios relevantes en normas, tecnologías o estructura institucional, manteniéndose alineado con los mecanismos de control de versiones del CNTD.

Responsables

El Marco de Interoperabilidad institucional debe de contar con un equipo Ad Hoc interno e interdisciplinario el cual se encargue de mantenerlo actualizado, en el Instituto Nacional de Seguros este se encuentra conformado de la siguiente manera:

Equipo interdisciplinario con representantes de:

- Dirección de Tecnologías de Información.
- Dirección Jurídica.
- Transformación digital.
- Areas de negocio (Comercialización, Dirección de Cliente Corporativo y Pyme, Direcciones Técnicas y Mercadeo).

Las jefaturas de estas dependencias definirán un representante designado y un suplente, para la atención de temas relacionados al Marco de Interoperabilidad en cuanto a su actualización, los cuales deberán contar con conocimiento y capacidad de decisión o articulación en temas relacionados con interoperabilidad.

Se deberá mantener un registro actualizado de los miembros del Equipo Ad Hoc, el cual deberá contener como mínimo: nombre completo, área o dependencia, fecha de designación.

Marco de Interoperabilidad

El presente Marco de Interoperabilidad establece la estructura integral mediante la cual el INS define, organiza y regula los procesos de intercambio de información entre sus sistemas y actores externos.

A través de este documento se detallan los principios, políticas, lineamientos y mecanismos que permiten implementar la interoperabilidad conforme a lo dispuesto en el CNTD, incorporando de manera articulada las dimensiones técnica, semántica, legal y organizacional que rigen el intercambio de información en el sector público.

El Marco desarrolla los elementos necesarios para la correcta adopción de la interoperabilidad en el INS, incluyendo la definición de estándares tecnológicos, modelos de datos, estructuras de gobernanza, roles institucionales, procesos operativos y controles asociados. Asimismo, establece los mecanismos de seguimiento, actualización y evaluación del nivel de capacidad que garantizan su aplicación, sostenibilidad y mejora continua.

De esta forma, el documento constituye una guía integral para el diseño, implementación y gestión de integraciones, proporcionando a las diferentes áreas institucionales un marco común que facilita la consistencia, la coordinación y el cumplimiento normativo en los procesos de interoperabilidad.

Principios para la interoperabilidad

Los principios de interoperabilidad se derivan del CNTD, el cual establece lineamientos, políticas generales y estándares obligatorios para la adopción de interoperabilidad en las empresas del sector público costarricense. El CNTD define el propósito que las instituciones públicas operen con mayor cohesión, eficiencia, seguridad y consistencia en los intercambios de datos y servicios digitales.

Principios:

- La información debe de ser intercambiada de una forma segura, estable y en el momento en el que es requerido por el cliente.
- Desarrollo de interoperabilidad en tecnologías con estándares abiertos, reconocidos y compatibles.
- Tener a disposición definiciones estandarizadas (campos, catálogos, mensajes) de las integraciones.
- Diseño y desarrollos de integraciones que permitan la reutilización.
- Legalidad y protección de datos basados en normas jurídicas que se encuentren vigentes para el intercambio de información.
- Cumplir los principios de la seguridad de la información, manteniendo la confidencialidad, integridad y autenticidad.
- Uso de métodos de seguridad con acceso robustos y mecanismos de autenticación y autorización que brinden protección contra ataques y exposición de datos sensibles.
- Permitir mecanismos, para el seguimiento, trazabilidad y auditoría de la integración.
- Seguir el proceso de mejora continua con revisiones periódica para la incorporación de ajustes organizacionales, tecnológicos y normativos.

Dimensiones

El marco de interoperabilidad se encuentra fundamentado en 4 dimensiones propuestas por el CNTD del MICITT, las cuales funcionan como la base de este, siendo estas las dimensiones técnica, semántica, legal y organizacional.

Dimensión técnica

La Interoperabilidad Técnica constituye el conjunto de políticas, lineamientos, estándares, procesos y mecanismos tecnológicos que permiten a los sistemas del INS intercambiar información de forma segura, eficiente, estandarizada y confiable, con entidades externas. Esta dimensión se apega estrictamente a lo dispuesto por las Políticas Generales de Interoperabilidad Técnica del CNTD, normativa obligatoria para todas las instituciones del sector público costarricense.

Asimismo, se sustenta en los lineamientos institucionales internos, que definen modos de diseño, construcción y operación de soluciones tecnológicas dentro del INS, y adopta buenas prácticas internacionales respaldadas, que promueven la estandarización, la gobernanza técnica centralizada y la administración del ciclo de vida de las integraciones.

Propósito

El propósito de esta dimensión es garantizar que todas las integraciones del INS cumplan con los requisitos solicitados por CNTD como lo son:

- Basadas en estándares abiertos.
- Mantengan la coherencia estructural entre sistemas.
- Ser seguros, auditables y escalables.
- Aseguren continuidad operativa y trazabilidad.
- Faciliten la reutilización de componentes.

Principios técnicos

- Estándares abiertos y neutralidad tecnológica: Las integraciones expuestas por la institución deben adoptar estándares abiertos ampliamente aceptados (REST, JSON, HTTPS, TLS).
- Seguridad transversal: Los mecanismos técnicos deben garantizar confidencialidad, integridad y autenticidad, siguiendo políticas institucionales y los lineamientos de seguridad del CNTD.
- Reutilización obligatoria: Los servicios, modelos y componentes deben diseñarse para uso transversal, evitando duplicidad y facilitando la eficiencia técnica.
- Continuidad y disponibilidad: La operación técnica debe asegurar niveles adecuados de disponibilidad, resiliencia y recuperación.
- Calidad, trazabilidad y auditoría: Las integraciones deben poder monitorearse, medirse y auditarse como lo exige el CNTD.

Tipos de integraciones

El Instituto Nacional de Seguros, en el ámbito de la interoperabilidad, dispone de una amplia variedad de APIs que permiten la integración con diversos procesos de negocio. Estas integraciones emplean tanto tecnologías sincrónicas como asincrónicas, según las necesidades de cada caso.

Sincrónica

En las integraciones de tipo sincrónico, el INS dispone de múltiples APIs que operan bajo este modelo, permitiendo que el cliente reciba la respuesta dentro de la misma solicitud HTTP realizada.

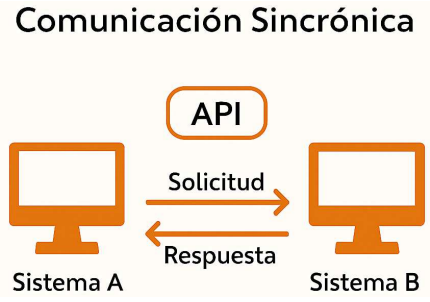

Ilustración 1. Diagrama ejemplo de comunicación sincrónica

Asincrónica

En las integraciones de tipo asincrónico, aunque su uso es menos frecuente, el cliente debe proporcionar un endpoint al cual se enviará la respuesta una vez finalizada el proceso. Este endpoint debe cumplir con los lineamientos, estándares y estructuras JSON definidos por el INS en la especificación correspondiente.

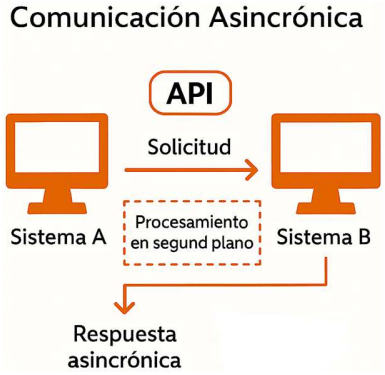

Ilustración 2. Diagrama ejemplo de comunicación asincrónica

Estándares de los recursos

Según lo establecido por el CNTD, las instituciones públicas deben ofrecer sus integraciones mediante estándares abiertos, interoperables y ampliamente adoptados en el mercado. En este contexto, el INS optó por el uso de tecnologías basadas en RESTful APIs, lo que permite brindar a los clientes una amplia variedad de integraciones para distintos procesos de negocio.

RESTFul APIs

Las integraciones que ofrece el INS se construyen bajo un modelo arquitectónico de comunicación basado en RESTful APIs por medio del protocolo de comunicación HTTPS. Este enfoque permite disponer de un catálogo amplio y estructurado de recursos que respaldan diversos procesos de negocio, incluyendo pólizas, reclamos, clientes, comercio electrónico, utilitarios, contabilidad y bienes asegurados.

Las integraciones están diseñadas de manera que aseguran su portabilidad y se desarrollan siguiendo prácticas que garantizan a los clientes la disponibilidad,

continuidad, integridad, autenticidad y confidencialidad en el uso de cada uno de los recursos disponibles.

Estas integraciones utilizan cuerpos de mensajes en formato JSON como estándar principal, dado que se trata de un formato ligero, ampliamente adoptado y reconocido en el ámbito de las APIs REST. Gracias a ello, los clientes pueden recibir respuestas claras y consistentes para sus consultas o transacciones, según corresponda.

Es importante destacar que los detalles específicos de cada integración, incluyendo los distintos escenarios de respuesta, se encuentran documentados en el Portal del Desarrollador. En la siguiente sección se proporciona más información para su correcta implementación.

Documentación de las integraciones

La documentación de los APIs y sus recursos en el INS se elabora utilizando la especificación OpenAPI, la cual permite describir de manera estructurada y comprensible tanto para personas como para sistemas automatizados los endpoints, descripción de la funcionalidad, métodos, parámetros, modelos de datos (descripción, obligatoriedad, longitud y tipo de dato), ejemplos de tramas, catálogos, códigos de respuesta o error, y reglas de negocio que conforman cada API institucional.

Este enfoque aporta beneficios significativos a la institución, como la estandarización de la información técnica y una mayor claridad para los desarrolladores que implementan integraciones. Asimismo, el uso de definiciones centralizadas facilita la actualización continua y simplifica la gestión del ciclo de vida de cada API.

El INS cuenta con un Portal del Desarrollador, que actúa como repositorio oficial para la publicación, consulta y versionamiento de las APIs institucionales. De esta manera, toda API creada se encuentra registrada, documentada, publicada y con su versión vigente en dicho portal, sin limitar a que pueden existir distintas versiones vigentes al mismo momento, lo cual se visualiza de una forma sencilla utilizando la versión explícitamente en el path del recurso. A través de esta plataforma es posible visualizar la documentación generada en OpenAPI, realizar pruebas, revisar ejemplos, consultar políticas de uso, modelos de seguridad y verificar las versiones vigentes de cada recurso. El portal se encuentra disponible en: https://portaldesarrollador.grupoins.com.

Políticas de Seguridad establecidas

Para garantizar el intercambio seguro, confiable y controlado de información entre los sistemas del INS y externos, se establecen diferentes políticas de seguridad aplicables a todas las integraciones y recursos expuestos mediante APIs institucionales.

- **Protocolo HTTPs:** Todas las integraciones deben realizarse exclusivamente mediante el protocolo HTTPS, con el cual se logra asegurar la comunicación cifrada de extremo a extremo entre los consumidores y las APIs del INS, protegiendo la confidencialidad e integración y evitando la manipulación o intercepción del tráfico.

- **Autenticación OAuth 2.0:** El acceso a los recursos expuestos mediante las APIs del INS debe realizarse utilizando el mecanismo de autenticación y autorización OAuth 2.0, garantizando que únicamente los clientes autorizados puedan consumir los servicios institucionales. La obtención y uso de las credenciales de acceso se ejecutará conforme al flujo definido por el INS, empleando el grant client_credentials, a partir del cual el cliente recibirá un token de autorización utilizando su *client_id* y *client_secret*. El token generado tendrá una vigencia de 60 minutos, por lo que deberá ser renovado para continuar realizando consumos. La descripción detallada de este proceso se encuentra disponible en el Portal del Desarrollador del INS: https://portaldesarrollador.grupoins.com/security.

- **Tokens JWT (JSON Web Token):** El INS utiliza tokens JWT para enviar la autorización otorgada mediante OAuth 2.0, a través del encabezado estándar: “Authorization: Bearer <jwt_token>”.

  Las principales características de los tokens JWT emitidos por el INS son:
  - Incluyen los scopes autorizados, que representan los recursos y operaciones que el consumidor está habilitado para ejecutar.
  - Están firmados digitalmente según los estándares definidos por JWT y utilizando un certificado digital definido por el INS.
  - Poseen tiempos de expiración alineados con prácticas seguras, garantizando la vigencia mínima necesaria, en el caso del INS de 60 minutos.

- Transporta información verificable e íntegra

- **Subscription-key:** Además del token JWT, todo consumo de los recursos expuestos por el INS debe incluir una "subscription key", la cual actúa como un mecanismo adicional de control, identificación y trazabilidad del consumo. Esta debe enviarse en el encabezado: "subscription-key: <subscription_key>". El uso de esta clave permite al INS realizar controles sobre la cantidad de llamadas, trazabilidad, auditoría y aplicar una revocación inmediata en caso de incidentes de seguridad. La descripción detallada de este proceso se encuentra disponible en el Portal del Desarrollador del INS: https://portaldesarrollador.grupoins.com/security.

- **Web Application Firewall:** La institución cuenta en su arquitectura con un WAF, el cual procesa todo el tráfico HTTPS de los llamados a los recursos APIs, aplicando una capa extra de seguridad.

- **Auditoría, trazabilidad y seguimiento:** Cada solicitud realizada a los recursos del INS genera registros que permiten su seguimiento, auditoría y análisis, tanto para transacciones exitosas como para aquellas que presentan errores. Estos registros incluyen información como: subscription key, identidad del consumidor según el token JWT, recurso accedido, fecha y hora de la operación, tramas de entrada, tramas de salida y el resultado final de la solicitud.

Contratos de servicio (SLA)

Para garantizar una comunicación confiable y efectiva con los APIs del INS, se establecen Acuerdos de Nivel de Servicio (SLA) que deben ser cumplidos tanto por la institución como por los clientes. Estos acuerdos aseguran que los consumos y procesos asociados a las integraciones se realicen de manera correcta, cumpliendo con los requisitos técnicos, los compromisos de disponibilidad, los tiempos de respuesta, la capacidad operativa, los lineamientos de seguridad y los límites de consumo definidos.

- **Disponibilidad:** El INS cuenta con APIs que funcionan en un esquema 24/7, del cual se tiene una disponibilidad del 99.9%, sin embargo, aquellas que no se encuentran dentro de este esquema tienen una disponibilidad del 66.67%, esto debido a que las mismas cuentan con una ventana de mantenimiento programada entre 22:00 y 6:00.

- **Tiempo Máximo de Respuesta:** La institución cuenta con límites de tiempos para sus recursos dependiendo del tipo de acción que realizan; teniendo las consultas en un monto de 15 segundos en promedio, y en las transacciones de 60 segundos en promedio.

- **Atención de Incidentes:** La atención de incidentes se clasifica según su prioridad, de la cual se tienen 4 niveles, teniendo una cantidad de horas disponibles para la atención y resolución de la situación teniendo como tiempos estimados:

Tiempo Solicitudes de Servicios	
Prioridad	**Tiempo de respuesta**
Procesos masivos	112 horas.
3 Bajo	56 horas.
2 Alto	48 horas.
1 Crítico	24 horas.

- **Límites y Restricciones:** Para asegurar una operación controlada, segura y eficiente, se establecen los siguientes límites de llamados por cliente/aplicación, en el que se tiene una base de 480 llamadas por minuto, obteniendo un total de 28.800 llamados por hora o 691.200 llamados por día.

Diseño técnico

El diseño técnico de cualquier integración dentro del INS debe responder al principio fundamental establecido por el CNTD, el cual es garantizar que todos los servicios digitales sean construidos utilizando estándares abiertos, metodologías consistentes y estructuras técnicamente estables, de forma que puedan interoperar con sistemas externos sin generar ambigüedades, dependencias innecesarias ni riesgos operativos.

El diseño técnico se guía por reglas estrictas de normalización, que establecen nomenclaturas predecibles, consistentes y estandarizadas para la definición de recursos, atributos, estructuras de datos, catálogos y endpoints. La normalización incluye adoptar identificadores claros, seguir patrones uniformes en camelCase en sus campos, utilizar atributos significativos y preservar la consistencia entre APIs.

Cada API o servicio se diseña bajo un enfoque que priorice la reutilización, evitando desarrollar integraciones duplicadas o específicas para un sistema y fomentando la creación de componentes que puedan servir múltiples procesos institucionales, permitiendo que la institución avance en los niveles de madurez técnica, reduciendo costos, evitando redundancia y mejorando la calidad de la arquitectura.

También se definen modelos de error estandarizados, en el nivel técnico como los códigos HTTP y estructuras de mensajes el cual se encuentra basado en el estándar internacional RFC 7807 con el fin de garantizar respuestas predictibles y acciones claras para el consumo de APIs.

Finalmente, el diseño técnico debe incorporar desde su concepción los criterios de seguridad definidos en el apartado Políticas de Seguridad establecidas, además de validar todos los datos de entrada, definir límites de consumo, garantizar la autenticación y autorización robusta.

Ciclo de vida

El ciclo de vida técnico de las integraciones del INS constituye el proceso formal que rige la planificación, desarrollo, implementación, operación y retiro de cualquier mecanismo de interoperabilidad.

El ciclo inicia con la fase de diseño técnico, donde se analiza la necesidad del servicio, se definen los requerimientos funcionales, y se elabora el diseño de alto nivel considerando los lineamientos de interoperabilidad, seguridad y arquitectura.

Se ejecuta la revisión arquitectónica, en la que se valida el cumplimiento de estándares, verifica el alineamiento con patrones institucionales (REST, JSON, OpenAPI) y garantiza que el diseño no genere acoplamientos indebidos, duplicidades o riesgos técnicos.

La fase de desarrollo debe realizarse respetando los lineamientos internos del INS, asegurando separación de capas, consistencia en las estructuras de datos y uso de librerías institucionales aprobadas. Al finalizar el desarrollo, se

requiere la generación completa de la documentación técnica en OpenAPI y su publicación provisional en el Portal del Desarrollador para revisión.

En la fase de pruebas técnicas, el servicio debe someterse a pruebas unitarias, integrales, de rendimiento y de seguridad. Una vez completadas, se valida los resultados y autoriza el despliegue al ambiente de producción.

La fase de publicación implica realizar la entrega oficial al solicitante, el servicio opera bajo monitoreo continuo durante la fase de operación, donde se supervisan métricas de disponibilidad, consumo, latencia, errores y amenazas por medio de los controles de auditoría, trazabilidad y gobernanza.

Por último, se contempla las fases de depreciación y retiro, donde se planifica la sustitución o eliminación del servicio, asegurando comunicación oportuna a los consumidores y manteniendo la estandarización institucional.

Pruebas técnicas

Las pruebas técnicas son un elemento crítico para garantizar la calidad y confiabilidad de las integraciones del INS, para asegurar continuidad, seguridad y estabilidad de los servicios digitales.

Cada integración se somete a un conjunto de pruebas estructuradas que comprueban su funcionamiento desde distintos ángulos. En primera instancia, con las pruebas unitarias se valida la lógica interna de los componentes desarrollados, asegurando que cada módulo cumpla correctamente su funcionalidad sin depender de otros servicios.

Las pruebas de integración verifican el comportamiento conjunto entre componentes internos, sistemas backend y consumidor. Este tipo de pruebas permite detectar errores de comunicación, incompatibilidades de modelos y desviaciones del diseño técnico.

Las pruebas de contrato aseguran que el servicio cumple fielmente con la especificación OpenAPI publicada, estas son indispensables, pues evitan que cambios inadvertidos rompan a consumidores existentes.

Las pruebas de rendimiento y carga miden la capacidad del servicio para responder adecuadamente bajo demanda creciente, estableciendo límites aceptables de latencia, con estas se garantiza la continuidad, lo cual incluye validar que la integración mantenga niveles aceptables de desempeño bajo condiciones normales y elevadas de uso.

Además, se aplican pruebas de seguridad de validación de tokens, pruebas de límites de consumos y verificación de configuración de OAuth2.

Todas las pruebas deben documentarse y archivarse como parte del requerimiento técnico del servicio, ningún servicio puede pasar a producción sin haber superado satisfactoriamente la totalidad de estas pruebas, garantizando así un alto nivel de estabilidad, confiabilidad y seguridad para todos los consumidores.

Dimensión semántica

En la dimensión semántica se garantiza que la información intercambiada entre el INS y terceros sea comprendida de la misma manera por todas las partes, eliminando ambigüedades, inconsistencias y divergencias interpretativas.

Los objetivos que se buscan con esta dimensión son:

- Estandarizar el significado de los datos.
- Alinear vocabularios, conceptos, definiciones y estructuras.
- Evitar duplicidad semántica.
- Definir catálogos oficiales.

Principios semánticos

Los recursos expuestos por INS en la dimensión semántica deben de considerar diferentes principios que logran adecuar la interoperabilidad de la institución con lo solicitado en el CNTD, los principios utilizados son:

- Las definiciones deben ser únicas, consensuadas, publicadas y accesibles.
- Existencia de catálogos, metadatos y definiciones formalizadas.
- Gobernanza semántica.

- Los datos intercambiados deben ser válidos, completos, consistentes y trazables.
- Documentación estandarizada y reutilizable.
- Trazabilidad del origen y evolución de los datos.

Gobernanza

La gobernanza semántica del INS debe entenderse como el conjunto de estructuras, responsabilidades y procesos que garantizan que los datos se definan de manera uniforme, las definiciones se mantengan actualizadas, las integraciones usen los artefactos oficiales, se eviten duplicidades, conflictos o interpretaciones erróneas, esta labor estará a cargo del equipo Ad Hoc.

Artefactos semánticos

Se entiende por artefactos semánticos los entregables institucionales que documentan y estandarizan el significado, estructura y reglas de uso de los datos, para asegurar una interpretación uniforme en los intercambios de información.

Glosario institucional de términos

El INS desarrollará y mantendrá un glosario de datos institucionales en el cual, se encuentran incluidos los conceptos de negocio, teniendo de esta manera las definiciones formales y precisas de cada uno de estos. El glosario es un instrumento de la interoperabilidad semántica, en el cual debe incluir como mínimo:
Ver Anexo 1

- Nombre del dato.
- Definición clara y comprensible.

Estos glosarios deberán:

- Ser reutilizables entre proyectos.
- Estar disponibles para los equipos técnicos, funcionales y de negocio.
- Actualizarse de manera controlada conforme a cambios normativos, tecnológicos u organizacionales.

Catálogo de datos institucional

El INS cuenta para cada uno de sus recursos, con la definición de cada uno de los campos del mismo, en el cual se encuentran documentados los campos para el uso del recurso, esta documentación tiene el detalle por campo del nombre, descripción, tipo de datos, longitud del dato, catálogos de posibles valores y formato en el caso de que aplique, un ejemplo de esto se puede ver en el siguiente sitio: https://portaldesarrollador.grupoins.com/api-details#api=api-de-administraci-n-de-p-lizas-del-ins-v2&operation=ConsultaRiesgosPoliza

Modelo canónico de información

El INS adoptará un Modelo Canónico de Información como referencia semántica común para los datos que sean interoperados entre sistemas internos y con entidades externas.

El modelo canónico:

- Define estructuras de información estandarizadas y reutilizables.
- Representa el significado institucional de los datos, independiente de su implementación técnica.
- Reduce la complejidad de integraciones punto a punto.
- Facilita la evolución controlada de los servicios interoperables.

El Modelo Canónico será utilizado como base para:

- Definición de servicios interoperables.
- Diseño de APIs.
- Integración de nuevos sistemas o plataformas.

Para dar inicio al proceso, deberá presentarse una solicitud formal por parte de una empresa o de una persona. El equipo responsable deberá identificar el servicio existente que atienda la necesidad y determinar si requiere personalización. Asimismo, deberán aplicarse las normas correspondientes para garantizar el intercambio correcto de la información. Una vez que el servicio se encuentre en producción y en uso, deberá evaluarse la retroalimentación de la parte usuaria.

Esquemas semánticos

El INS definirá y mantendrá esquemas semánticos que describan:

- La estructura lógica de los datos.
- Las relaciones entre conceptos.
- Las restricciones y reglas semánticas aplicables.

Estos esquemas podrán expresarse mediante:

- Glosario de datos.
- Catálogos de metadatos.
- Modelos de información.

Los esquemas semánticos deberán estar alineados con:

- El Modelo Canónico de Información.
- El Glosario Institucional de Términos.
- Los lineamientos del CNTD y el Marco de Interoperabilidad Nacional.

Procesos semánticos

Proceso de creación y aprobación de definiciones

Dentro del Equipo Interno de Interoperabilidad, designado por el INS el Equipo Ad Hoc responsable de:

- Velar por la correcta definición y uso del significado de los datos interoperables.
- Coordinar con las áreas funcionales y técnicas para validar definiciones.
- Asegurar la alineación semántica entre sistemas internos y externos.
- Participar en procesos de revisión y actualización del Marco.

Las áreas funcionales propietarias de la información serán responsables de:

- Validar el significado de los datos bajo su competencia.
- Notificar cambios que impacten definiciones, estructuras o uso de la información.

Proceso de mantenimiento semántico

El INS establecerá un proceso de mantenimiento semántico, orientado a:

- Revisar definiciones existentes.
- Identificar términos obsoletos o inconsistentes.
- Ajustar definiciones ante cambios normativos, organizacionales o de negocio.
- Registro institucional de servicios interoperables.

Todo cambio semántico deberá:

- Evaluar impacto en sistemas y procesos.
- Quedar registrado bajo control de versiones.
- Ser comunicado a las partes interesadas.

Proceso de alineación semántica con APIs

El INS establece el Proceso de Alineación Semántica con APIs como un mecanismo obligatorio para garantizar que la información intercambiada mediante servicios interoperables sea comprendida de manera uniforme, inequívoca y consistente entre los sistemas productores y consumidores, tanto internos como externos.

Antes de la publicación, modificación o consumo de APIs institucionales, el INS deberá asegurar la alineación semántica entre los elementos que definen el significado de los datos intercambiados, considerando como mínimo los siguientes artefactos:

- El Modelo Canónico de Información, como referencia semántica común institucional.
- Los esquemas semánticos definidos, que establecen relaciones, reglas y restricciones del significado.
- El Glosario Institucional de Términos y el Diccionario de Datos y Metadatos Institucionales.
- Las estructuras de datos expuestas o consumidas por las APIs.

El proceso de alineación semántica con APIs debe aplicarse a:

- Nuevas APIs institucionales.
- Nuevas versiones de APIs existentes.
- Consumo de APIs de terceros cuando éstas intercambien datos con significado institucional del INS.

- Cambios que impacten el significado, uso o estructura de los datos interoperables.

El proceso inicia con la identificación de la API y de los datos que serán intercambiados, luego, se realiza la verificación de los artefactos semánticos oficiales para confirmar que los datos cuenten con definiciones aprobadas y vigentes.

En caso de que los datos no se encuentren definidos o aprobados, deberá activarse el proceso de creación y aprobación de definiciones, asegurando su incorporación formal en los artefactos semánticos institucionales.

Cuando los datos cuentan con definiciones vigentes, se procede a la validación de alineación semántica, la cual deberá confirmar que se cumpla:

- Los nombres de campos y atributos reflejen fielmente su significado institucional.
- Los valores permitidos, estados y catálogos correspondan a los definidos oficialmente.
- El uso del dato sea coherente con su finalidad y contexto de negocio.
- No existan duplicidades, sinónimos no controlados o contradicciones semánticas entre APIs o servicios interoperables.
- El significado del dato sea independiente de su representación técnica o formato.

Cuando se identifiquen desviaciones o inconsistencias semánticas, deberán realizarse los ajustes correspondientes mediante el proceso de mantenimiento semántico, incluyendo la evaluación de impacto, el control de versiones y la comunicación a las partes interesadas.

Una vez confirmada la alineación semántica, deberá registrarse la validación y autorizarse formalmente la publicación o consumo de la API.

Responsabilidades:

- El Equipo Ad Hoc de Interoperabilidad será responsable de velar por el cumplimiento del proceso de alineación semántica con APIs.
- Las áreas funcionales propietarias de la información deberán validar el significado y el uso de los datos bajo su competencia.

- Los equipos técnicos deberán utilizar exclusivamente los artefactos semánticos oficiales como referencia para el diseño, evolución y consumo de APIs.

El Proceso de Alineación Semántica con APIs garantiza que:

- La información intercambiada sea interpretada de forma uniforme y consistente.
- Se preserve la coherencia semántica entre servicios interoperables.
- Se reduzcan errores operativos derivados de interpretaciones divergentes.
- La interoperabilidad técnica se sustente en una base semántica gobernada y controlada.

Esta alineación constituye un requisito obligatorio para asegurar una interoperabilidad técnica efectiva y sostenible en el INS.

Mecanismos de Validación Semántica

El INS implementará mecanismos de validación semántica que permitan verificar:

- Coherencia entre definiciones y uso real de los datos.
- Cumplimiento de esquemas y reglas semánticas.
- Alineación con el Modelo Canónico y el Glosario Institucional.
- Consistencia entre productor y consumidor de la información.

Estos mecanismos podrán incluir:

- Revisiones semánticas en diseño de servicios.
- Validaciones previas a la puesta en producción.
- Evaluaciones de impacto ante cambios relevantes.

Dimensión legal

La Interoperabilidad en la dimensión legal comprende el conjunto de normas, disposiciones jurídicas, lineamientos institucionales, acuerdos y responsabilidades que habilitan, delimitan y regulan el intercambio de información entre los sistemas del Instituto Nacional de Seguros (INS) y otros actores externos.

De conformidad con el Código Nacional de Tecnologías Digitales (CNTD), la interoperabilidad no puede limitarse a aspectos técnicos o semánticos; debe contar con un respaldo jurídico explícito que garantice que el intercambio de datos se realice dentro de un marco de legalidad, respeto a los derechos fundamentales, seguridad jurídica, protección de datos personales y cumplimiento normativo.

Esta dimensión asegura que toda iniciativa de interoperabilidad del INS se encuentre debidamente sustentada desde el punto de vista legal, evitando riesgos institucionales, incumplimientos normativos o uso indebido de la información.

Objetivo de la Dimensión Legal

La Dimensión Legal del Marco de Interoperabilidad Institucional del INS tiene como objetivos:

- Garantizar que el intercambio de información interoperable se realice conforme al ordenamiento jurídico costarricense vigente.
- Asegurar la protección de los datos personales, confidenciales y sensibles tratados mediante integraciones.
- Establecer los instrumentos jurídicos habilitantes necesarios para la interoperabilidad externa.
- Definir responsabilidades legales claras entre las partes involucradas en el intercambio de información.
- Brindar certeza jurídica a los servicios interoperables expuestos por el INS.
- Toda iniciativa de interoperabilidad y desarrollo de infraestructura tecnológica interoperable deberá cumplir con el marco jurídico vigente aplicable a los servicios digitales, infraestructura tecnológica, seguridad de la información y protección de datos personales

Principios de Interoperabilidad Legal

Los siguientes principios rigen la Dimensión Legal y orientan todas las decisiones relacionadas con el intercambio de información:

- **Principio de Legalidad**

Toda interoperabilidad debe sustentarse en normas legales vigentes, habilitaciones expresas y competencias institucionales claramente definidas.

- **Principio de Finalidad**

Los datos intercambiados solo podrán utilizarse para los fines específicos para los cuales fueron solicitados y autorizados.

- **Principio de Proporcionalidad**

El intercambio de información debe limitarse estrictamente a los datos necesarios para cumplir con el objetivo definido, evitando exposiciones innecesarias.

- **Principio de Responsabilidad**

Cada parte involucrada en la interoperabilidad es responsable del tratamiento adecuado de la información bajo su custodia, así como de la protección de la confidencialidad de la información.

- **Principio de Protección de Datos**

  Debe garantizarse la confidencialidad, integridad y disponibilidad de la información intercambiada, en coherencia con la normativa de protección de datos personales y la normativa de protección del secreto industrial, comercial y económico del INS.

Marco Normativo Aplicable

La interoperabilidad legal del INS se encuentra respaldada, entre otros instrumentos, por:

- Código Nacional de Tecnologías Digitales (CNTD) – MICITT.
- Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (Ley N.º 8968).
- Ley Reguladora del Mercado de Seguros.
- Ley Reguladora del Contrato de Seguros.
- Código de Comercio y sus reformas.
- Código Civil y sus reformas.
- Normativa sectorial aplicable al INS.
- Contratos, convenios y acuerdos interinstitucionales vigentes.

Este Marco no sustituye la normativa legal, sino que operativiza su cumplimiento en el contexto tecnológico y digital.

Instrumentos Jurídicos para la Interoperabilidad

Para habilitar el intercambio de información, el INS podrá utilizar, según corresponda, los siguientes instrumentos jurídicos:

- **Convenios Interinstitucionales**
  Documentos formales que establecen condiciones, alcances, responsabilidades y compromisos para el intercambio de información entre entidades.

- **Memorandos de Entendimiento**
  Instrumentos que regulan colaboraciones técnicas o intercambio de información sin carácter contractual estricto, cuando la normativa lo permite.

- **Cláusulas Contractuales**
  En el caso de proveedores tecnológicos o terceros, los contratos deberán incorporar cláusulas específicas sobre interoperabilidad, protección de datos y seguridad de la información.

- **Acuerdos de Nivel de Servicio (SLA)**
  Complementan los instrumentos legales al definir responsabilidades operativas, tiempos de respuesta y obligaciones técnicas.

Protección de Datos Personales

Toda interoperabilidad del INS deberá cumplir estrictamente con las disposiciones relacionadas con la protección de datos personales, garantizando:

- Identificación y su correcto etiquetado del tipo de datos intercambiados (públicos, confidenciales, sensibles).
- Definición clara de responsables y encargados del tratamiento.
- Implementación de controles técnicos y organizacionales para la protección de los datos.
- Mecanismos de consentimiento cuando aplique.
- Registro y trazabilidad del acceso y uso de la información.

La Dimensión Legal se articula directamente con la Dimensión Técnica (controles de seguridad) y la Dimensión Semántica (clasificación y significado de los datos).

Responsabilidades Legales en la Interoperabilidad

En el proceso de interoperabilidad se definen claramente los siguientes roles:

- **Responsable del tratamiento del dato**, usualmente el área funcional propietaria de la información: Direcciones Técnicas, Comerciales o de Negocio.
- **Encargado del tratamiento**, un tercero o sistema procesa información por delegación: Socios comerciales o de negocio y clientes.
- **Responsable técnico**, garantiza el cumplimiento de los controles establecidos: Dirección de Tecnologías de Información.
- **Responsable Semántico,** área o rol designado por dominio de datos.
- **Instancia legal del INS**, encargada de validar los instrumentos jurídicos asociados: Dirección Jurídica con apoyo de la Oficialía de Cumplimiento y Gobernanza de Datos.

Trazabilidad, Auditoría y Evidencia Legal

El CNTD exige que las instituciones cuenten con mecanismos que permitan demostrar el cumplimiento de las disposiciones legales. En este sentido, el INS deberá:

- Mantener registro de convenios y acuerdos asociados a cada integración.
- Documentar el cumplimiento de los principios de protección de datos.
- Conservar evidencias de accesos, intercambios y autorizaciones.
- Facilitar procesos de auditoría interna y externa relacionados con interoperabilidad.
- Mantener el registro que permite identificar y verificar el movimiento e intercambio de la información, incluyendo su origen, destino, momento y condiciones de transmisión, con fines de control, seguimiento y auditoría. Políticas de Seguridad establecidas

Dimensión organizacional

La Interoperabilidad Organizacional comprende las estructuras de gobernanza, roles, responsabilidades, procesos y mecanismos de coordinación que permiten al Instituto Nacional de Seguros (INS) gestionar, controlar y sostener la interoperabilidad de manera coherente, ordenada y alineada con sus objetivos institucionales.

De acuerdo con el Código Nacional de Tecnologías Digitales (CNTD), la interoperabilidad no puede depender únicamente de soluciones técnicas o acuerdos informales; requiere una organización institucional clara, con instancias responsables, procesos definidos y mecanismos de decisión que aseguren su continuidad, trazabilidad y mejora continua.

Objetivo de la Dimensión Organizacional

La Dimensión Organizacional tiene como objetivos:

- Establecer una estructura formal de gobernanza para la interoperabilidad institucional.
- Definir roles y responsabilidades claras en los procesos de interoperabilidad.
- Asegurar la coordinación entre las áreas funcionales, TI, legal, ciberseguridad, datos y negocio.
- Estandarizar los procesos de solicitud, evaluación, aprobación y mantenimiento de integraciones.
- Garantizar la sostenibilidad y evolución del Marco de Interoperabilidad.
- Alinear la interoperabilidad con la estrategia institucional del INS.

Principios de la Interoperabilidad Organizacional

Los siguientes principios orientan la organización de la interoperabilidad en el INS:

- **Gobernanza Institucional**

La interoperabilidad debe ser gestionada mediante instancias formales y procesos documentados.

- **Responsabilidad**

Debe sustentarse en la asignación clara, explícita y formal de responsabilidades entre las instancias institucionales y/o socios comerciales involucrados, de manera que cada rol tenga definidas sus funciones, alcances y obligaciones en los procesos de intercambio de información.

- **Coordinación Interdisciplinaria**

La interoperabilidad requiere la participación coordinada de áreas funcionales, TI, legal, ciberseguridad, datos y negocio.

- **Alineación Estratégica**

Las iniciativas de interoperabilidad deben alinearse con los objetivos estratégicos del INS.

- **Mejora Continua**

La estructura organizacional debe permitir ajustes y mejoras conforme evolucionan los procesos, tecnologías y normativas.

Estructura de Gobernanza de la Interoperabilidad en el INS

- **Equipo Ad Hoc Institucional de Interoperabilidad**

El INS deberá contar con un equipo Ad Hoc institucional de interoperabilidad, como órgano de gobernanza de esta.

Funciones principales:

- Aprobar el Marco de Interoperabilidad Institucional y sus actualizaciones.
- Definir lineamientos estratégicos y prioridades de interoperabilidad.
- Validar integraciones entre las instancias institucionales y/o socios comerciales.
- Evaluar solicitudes de interoperabilidad.
- Validar cumplimiento técnico y semántico.
- Coordinar revisiones arquitectónicas.
- Administrar el ciclo de vida de integraciones.
- Mantener el catálogo institucional de servicios interoperables.
- Proveer soporte técnico y lineamientos.

Roles Organizacionales Clave

- **Responsable del Tratamiento del Dato,** área funcional propietaria de la información: Direcciones Técnicas, Comerciales o de Negocio.

  Responsabilidades:

  - Autorizar el intercambio de información.
  - Definir finalidad y alcance.
  - Validar uso permitido de la información.

- **Encargado del Tratamiento,** un tercero o sistema procesa información por delegación: Socios comerciales o de negocio y clientes.

  Responsabilidades:
  - Procesar información conforme a lo autorizado.
  - Cumplir obligaciones legales y técnicas.
  - Respetar acuerdos de interoperabilidad.

- **Responsable Técnico,** garantiza el cumplimiento de los controles establecidos: Dirección de Tecnologías de Información.

Responsabilidades:
- Implementar controles técnicos.
- Garantizar seguridad, disponibilidad y trazabilidad.
- Operar y monitorear integraciones.

- **Responsable Semántico,** área o rol designado por dominio de datos.

  Responsabilidades:
  - Validar definiciones y modelos de datos.
  - Garantizar coherencia semántica.
  - Aprobar artefactos semánticos.

- **Instancia Legal,** encargada de validar los instrumentos jurídicos asociados: Dirección Jurídica con apoyo de la Oficialía de Cumplimiento y Gobernanza de Datos.

  Responsabilidades:
  - Validar convenios, contratos y cláusulas.
  - Asegurar cumplimiento del marco legal.
  - Asesorar sobre riesgos jurídicos.

Procesos Organizacionales de Interoperabilidad

- **Solicitud de Interoperabilidad**

Toda interoperabilidad debe iniciar mediante una solicitud formal, que incluya:

- Justificación de negocio.
- Datos por intercambiar.
- Tipo de socio o consumidor.
- Evaluación preliminar del valor de negocio.

- **Evaluación y Aprobación**

La solicitud será evaluada desde cuatro ejes:

- Técnico.
- Semántico.
- Legal.
- Organizacional.

- **Priorización**

Las iniciativas se priorizan según:

- Impacto institucional.
- Alineación estratégica.
- Urgencia del negocio.

- **Gestión de Cambios**

Todo cambio en una integración debe:

- Evaluarse formalmente.
- Analizar impacto.
- Aprobarse por la instancia correspondiente.
- Registrarse bajo control de versiones.
- Comunicar el cambio.

- **Gestión de incidentes**

- Canales de contacto: Ejecutivo a cargo de la relación comercial.
- Generación del reporte: El socio comercial genera el reporte al Ejecutivo con la información necesaria (detalle, fecha, servicio, evidencias, ambiente, tramas).

- Coordinación interna: El Ejecutivo coordina con Transformación Digital, la validación del reporte para ser remitido a la Dirección de Tecnologías de Información.
- Atención técnica: La Dirección de Tecnologías de Información atiende el incidente conforme a los tiempos establecidos.
- Comunicación de la respuesta: La Dirección de Tecnologías de Información envía la respuesta al Ejecutivo, con copia a Transformación Digital.
- El Ejecutivo coordina el envío de la respuesta al socio comercial.

Este proceso se complementa con lo establecido en la Dimensión Técnica, específicamente en los Acuerdos de Nivel de Servicio (SLA), donde se definen los tiempos de respuesta y resolución de incidentes.

- **Fiscalización del uso de APIs**

El INS establece la facultad institucional de fiscalizar y monitorear el uso correcto de los servicios interoperables expuestos mediante APIs, con el objetivo de garantizar el cumplimiento de los lineamientos técnicos, legales, de seguridad y operativos.

- Alcance de la fiscalización

La fiscalización podrá aplicarse a todos los socios comerciales, consumidores de APIs y terceros que hagan uso de los servicios interoperables del INS, independientemente del tipo de integración o modelo de consumo. Cuando se considere necesario sin que medie una notificación previa al consumidor.

Este proceso podrá abarcar, entre otros aspectos:

- El cumplimiento de los límites de consumo definidos.
- El uso adecuado de credenciales, tokens y mecanismos de autenticación.
- El respeto a las finalidades autorizadas para el uso y protección de la información.
- El cumplimiento de los acuerdos legales, contractuales y de nivel de servicio (SLA).
- La correcta implementación técnica conforme a los lineamientos institucionales.

- La verificación de patrones de consumo que puedan representar riesgos operativos o de seguridad.

- Resultados y acciones derivadas

Como resultado de los procesos de fiscalización, el INS podrá:

- Emitir observaciones al consumidor.
- Solicitar ajustes técnicos o de uso.
- Establecer planes de mejora o regularización.
- Aplicar restricciones temporales o permanentes en el acceso a los servicios.
- Suspender o revocar credenciales en casos de incumplimiento grave o reiterado.
- Escalar situaciones a instancias legales o contractuales, según corresponda.

Mecanismos de seguimiento y actualización

El Marco de Interoperabilidad Institucional del Instituto Nacional de Seguros (INS) debe concebirse como un instrumento dinámico y evolutivo, sujeto a revisiones que permitan su adecuación continua frente a cambios normativos, tecnológicos, organizacionales y operativos.

El Código Nacional de Tecnologías Digitales (CNTD) establece que las instituciones públicas deben contar con mecanismos formales que aseguren la vigencia, cumplimiento y mejora continua de los marcos y lineamientos técnicos adoptados.

En este contexto, el INS establece los siguientes mecanismos de seguimiento y actualización, los cuales garantizan que el Marco de Interoperabilidad se mantenga alineado con la normativa nacional, la estrategia institucional y las necesidades cambiantes del ecosistema digital.

Objetivo de los mecanismos de seguimiento y actualización

Los mecanismos de seguimiento y actualización tienen como objetivo:

- Verificar el cumplimiento efectivo del Marco de Interoperabilidad en las iniciativas institucionales.
- Asegurar la alineación permanente con el CNTD y sus actualizaciones.
- Identificar oportunidades de mejora en las dimensiones técnica, semántica, legal y organizacional.
- Gestionar de manera controlada los cambios que impacten la interoperabilidad.
- Mantener la vigencia y aplicabilidad del Marco en el tiempo.

Instancias responsables del seguimiento

El seguimiento del Marco de Interoperabilidad será responsabilidad del equipo Ad Hoc (Responsables), mismo que deberá actuar de manera coordinada para asegurar una evaluación integral.

Seguimiento del cumplimiento del Marco

El INS realizará seguimientos para verificar que las integraciones y servicios interoperables:

- Cumplan con los lineamientos técnicos establecidos.
- Utilicen los artefactos semánticos oficiales.
- Cuenten con respaldo legal habilitante.
- Se ajusten a los procesos organizacionales definidos.

Este seguimiento se realizará mediante:

- Revisiones técnicas y arquitectónicas.
- Validaciones semánticas previas a la publicación de servicios.
- Verificaciones de cumplimiento de contratos de servicio y SLA.
- Controles de auditoría técnica y funcional.

Actualización por cambios normativos

El INS deberá revisar y actualizar el Marco de Interoperabilidad cuando se presenten:

- Modificaciones al CNTD emitidas por el MICITT.
- Nuevas leyes, reglamentos o directrices aplicables al intercambio de información.
- Cambios en la normativa de protección de datos personales.
- Disposiciones de entes reguladores que afecten al INS.

Ante estos cambios, el equipo Ad Hoc evaluará el impacto y propondrá los ajustes necesarios al Marco, garantizando la continuidad y el cumplimiento normativo.

Actualización por cambios tecnológicos

La evolución de tecnologías, arquitecturas y estándares puede impactar directamente la interoperabilidad institucional. Por ello, el INS deberá revisar el Marco cuando se presenten:

- Adopción de nuevas plataformas de integración.
- Incorporación de nuevos estándares o protocolos.

- Cambios significativos en la arquitectura tecnológica institucional.
- Obsolescencia de tecnologías o mecanismos existentes.

Ante estos cambios, el equipo Ad Hoc evaluará el impacto y propondrá los ajustes necesarios al Marco, garantizando la continuidad y asegurando que las actualizaciones se realicen de manera controlada y documentada.

Actualización por cambios organizacionales y de negocio

Cambios en la estructura organizativa, procesos de negocio, productos o servicios del INS pueden requerir ajustes en el Marco de Interoperabilidad. En estos casos, deberán considerarse:

- Creación o modificación de roles institucionales,
- Cambios en responsabilidades de áreas funcionales,
- Evolución de procesos clave que requieran interoperabilidad.

El equipo Ad Hoc deberá informar oportunamente los cambios para su incorporación en el Marco.

Periodicidad de revisión

Independientemente de la ocurrencia de cambios específicos, el Marco de Interoperabilidad deberá ser revisado:

- Al menos una vez al año, como revisión integral.
- Adicionalmente, cuando se identifiquen cambios relevantes normativos, tecnológicos u organizacionales.

Estas revisiones permitirán validar la vigencia de principios, políticas, lineamientos y procesos definidos.

Gestión de cambios y control de versiones

Toda actualización al Marco de Interoperabilidad deberá:

- Documentarse formalmente.
- Ser aprobada por el Equipo Ad Hoc.

- Registrarse en el historial de versiones del documento.
- Comunicarse oportunamente a las partes interesadas.

El control de versiones garantiza trazabilidad, transparencia y coherencia en la evolución del Marco.

Documentación vinculada

Los siguientes documentos complementan y respaldan los lineamientos, principios y procesos definidos en la Dimensión Semántica del Marco de Interoperabilidad Institucional del Instituto Nacional de Seguros (INS), y regulan su aplicación operativa a nivel institucional:

- Procedimiento institucional para la gestión de interoperabilidad:

Documento de uso interno que regula la atención, análisis, coordinación y aprobación de las solicitudes de interoperabilidad con actores internos y externos del INS. Este procedimiento define los pasos operativos, roles y responsabilidades asociados a la gestión de interoperabilidad, e integra la ejecución de los procesos semánticos establecidos en el presente Marco, incluyendo la alineación semántica con APIs.

- GTI-MAT-0021 Pautas para la Construcción de Soluciones Tecnológicas:

Documento normativo de uso interno que define las directrices, mejores prácticas y estándares institucionales establecidos por el INS para el diseño, desarrollo, implementación y mantenimiento de soluciones tecnológicas. Este instrumento facilita la adopción de criterios homogéneos, asegurando la interoperabilidad, calidad, consistencia y alineación con la arquitectura institucional de los sistemas de información.

Glosario y términos

API (Application Programming Interface): Conjunto de reglas, protocolos y definiciones que permiten la comunicación e intercambio de información entre sistemas, aplicaciones o servicios, facilitando la interoperabilidad entre diferentes plataformas.

API Management: Plataforma que permite la publicación, administración, control, seguridad y monitoreo de APIs, incluyendo funcionalidades como autenticación, control de tráfico, versionamiento y analítica.

Autenticación: Proceso mediante el cual se verifica la identidad de un usuario, sistema o aplicación que solicita acceso a un recurso o servicio.

Autorización: Proceso mediante el cual se determinan los permisos y accesos que un usuario o sistema tiene sobre un recurso o servicio, una vez autenticado.

Catálogo de Datos: Conjunto estructurado de definiciones de datos utilizados en la organización, que incluye su nombre, descripción, tipo, dominio de valores y reglas asociadas.

Confidencialidad: Propiedad de la información que garantiza que solo sea accesible a personas, sistemas o entidades autorizadas.

Convenio Interinstitucional: Acuerdo formal entre dos o más instituciones que regula el intercambio de información, definiendo condiciones, responsabilidades y alcances.

Coherencia Semántica: Propiedad de los datos que asegura que su significado sea consistente y uniforme en todos los sistemas e integraciones donde se utilicen.

Datos Personales: Información que identifica o puede identificar a una persona física, ya sea de forma directa o indirecta.

Datos Sensibles: Categoría especial de datos personales cuya divulgación puede generar discriminación o afectar la privacidad de la persona, tales como datos de salud o financieros.

Dominio de Datos: Agrupación de datos relacionados que pertenecen a un mismo ámbito funcional o de negocio dentro de la organización.

Encargado del Tratamiento: Persona física o jurídica, pública o privada, que procesa datos personales por cuenta del responsable del tratamiento, de acuerdo con las instrucciones establecidas.

Endpoint: Punto de acceso específico de una API donde se puede consumir un servicio o recurso.

Gobernanza de Interoperabilidad: Conjunto de estructuras, roles, procesos y políticas que permiten gestionar, controlar y asegurar la interoperabilidad dentro de la organización.

Glosario de Datos: Repositorio estructurado de términos y definiciones utilizados en la organización para asegurar la comprensión uniforme de la información.

Interoperabilidad: Capacidad de diferentes sistemas, aplicaciones, organizaciones o entidades para intercambiar información y utilizarla de manera efectiva.

Interoperabilidad Técnica: Nivel de interoperabilidad que se ocupa de los aspectos tecnológicos, como protocolos, estándares, formatos y mecanismos de comunicación.

Interoperabilidad Semántica: Nivel de interoperabilidad que garantiza que el significado de la información intercambiada sea comprendido de la misma manera por todas las partes.

Interoperabilidad Organizacional: Nivel de interoperabilidad que define los procesos, roles y estructuras que permiten la colaboración entre distintos actores.

Interoperabilidad Legal: Nivel de interoperabilidad que asegura que el intercambio de información se realice conforme al marco jurídico vigente.

Metadatos: Datos que describen otros datos, proporcionando información sobre su estructura, significado, origen y uso.

Modelo Canónico de Información: Modelo de referencia que define la estructura estándar de los datos de la organización, independiente de los sistemas que los consumen o producen.

Monitoreo: Proceso continuo de supervisión del funcionamiento de sistemas e integraciones para asegurar su disponibilidad, rendimiento y correcto comportamiento.

OAuth 2.0: Protocolo estándar de autorización utilizado para permitir el acceso seguro a recursos mediante el uso de tokens.

Payload: Contenido de datos enviado en una solicitud o respuesta de un servicio o API.

Portal del Desarrollador: Plataforma que permite a los usuarios acceder a la documentación, pruebas y consumo de APIs institucionales.

Proceso de Interoperabilidad: Conjunto de actividades que permiten establecer, operar y mantener integraciones entre sistemas.

Responsable del Tratamiento del Dato: Área o instancia de la organización que define los fines y medios del tratamiento de datos.

Responsable Técnico: Área encargada de implementar, operar y asegurar los mecanismos técnicos utilizados en la interoperabilidad.

Responsable Semántico: Instancia encargada de definir, validar y mantener el significado de los datos, garantizando su coherencia y alineación con los modelos institucionales.

SLA (Service Level Agreement): Acuerdo que define los niveles de servicio que deben cumplir las integraciones, incluyendo disponibilidad, desempeño y tiempos de respuesta.

Seguridad de la Información: Conjunto de prácticas que garantizan la protección de la información en términos de confidencialidad, integridad y disponibilidad.

Token JWT (JSON Web Token): Estructura de datos utilizada para transmitir información de forma segura entre partes, generalmente utilizada para autenticación y autorización.

Trazabilidad: Capacidad de seguir el recorrido de un dato o transacción a través de los diferentes sistemas e integraciones.

Versionamiento: Proceso de gestionar cambios en APIs o servicios mediante la asignación de versiones, permitiendo mantener compatibilidad.

Versionamiento

Historial de Revisión, Aprobación y Divulgación				
Versión:	**Elaborado por:**	**Revisado por:**	**Aprobado por:**	**Oficio y fecha: (rige a partir de):**
1	Abraham Montero Núñez, Departamento Servicios Empresariales de Tecnología. Carolina Fonseca Mora, Unidad de Seguridad TIC. Lilliana Ramirez Chavarria, Transformación Digital.			