EDI MENDOZA

Dirección General de Informática y Comunicaciones

Gobierno de Mendoza 2.025

ÍNDICE

Control del Documento

Versión: 1.1 26.03.2025

Historial de versiones

Fecha	Versión	Descripción
13/11/2024	0.1	Versión Inicial
21/11/2024	0.2	Revisión y Ajustes
25/11/2024	0.3	Revisión y Ajustes
28/11/2024	0.4	Revisión y Ajustes
27/12/2024	1.0	Reestructuración del contenido, mejora de las imágenes y gráficos.
26/03/2024	1.1	Se agrega el manejo de índice en base de datos del Servidor de Seguridad

Introducción

El siguiente manual proporciona una guía completa sobre el EDI-Mendoza, el Ecosistema Digital de Integrabilidad Implementado en la Provincia de Mendoza por la Dirección de Informática y Comunicaciones.
El objetivo principal es facilitar la comprensión y aplicación por parte de los usuarios.

¿Qué es interoperabilidad?

La interoperabilidad es la capacidad que tienen distintos sistemas de operar entre sí, sin limitaciones, trabajando de forma coordinada y, además, con facultad para discernir la información que reciben desde todos los puntos de la red.
Es decir, no solo intercambian información, también comparten conocimiento sin restricciones.

¿Qué es un Ecosistema de Integrabilidad Digital?

Un Ecosistema Digital de Integrabilidad (EDI) genera un entorno informático en el cual conviven diversos sistemas y aplicaciones. Un EDI es una plataforma de intercambio de alta seguridad, basada en una arquitectura distribuida, altamente resistente a fallas, independiente de la tecnología, arquitectura y software con los que están desarrollados los sistemas que se interconectan.

Es una comunidad de organizaciones miembros de un mismo ecosistema que:

1. Respeta mínimas reglas de convivencia digital,
2. Aplica estándares y componentes de software para poder utilizar y reutilizar los servicios comunes del ecosistema.

Es importante destacar que un Ecosistema de Integrabilidad debe ser flexible, capaz de adaptarse a los cambios tecnológicos y a las necesidades futuras. Su objetivo principal es facilitar el intercambio eficiente y seguro de información entre los actores, promoviendo la transparencia, facilitando la automatización de procesos y mejorando la experiencia de los ciudadanos.

¿Qué es X-Road?

Para la implementación del EDI en la Provincia de Mendoza se ha tomado como base tecnológica X-Road, software de licencia pública mantenido por el Instituto Nórdico de Interoperabilidad (NIIS).

X-ROAD le aporta al Ecosistema las siguientes características:

- El intercambio de datos se produce directamente entre las entidades sin intermediarios en un modelo par a par o peer 2 peer.
- Las entidades son las que autorizan el acceso a los servicios de intercambio de información expuestos ejerciendo la soberanía de sus datos.
- La propiedad de los datos no cambia, la autoridad administradora de los datos controla quién puede acceder al servicio de intercambio de información.
- Cada miembro es autenticado a través de certificados digitales para el acceso a la plataforma.
- El intercambio de datos se realiza con protocolos criptográficos seguros a través HTTPS con TLS 1.2 y los mensajes cifrados aplicando el algoritmo RSA con la función Hash SHA512.
- Todos los mensajes intercambiados a través de X-ROAD son estampados cronológicamente, y se utiliza para estampar todas las solicitudes salientes, solicitudes entrantes, respuestas salientes y respuestas entrantes entre los miembros del ecosistema.
- Los mensajes intercambiados en el EDI Mendoza tienen valor jurídico y pueden ser usados como evidencia digital de envío y recepción del mensaje intercambiado, debido a que son firmados digitalmente.
- No hay roles predeterminados, una vez que una entidad se ha unido al ecosistema de X-ROAD, puede actuar como cliente y proveedor de servicios web sin tener que realizar ningún registro adicional.
- Se registran las transacciones y se establecen auditoría sobre los mensajes intercambiados, , lo que permite junto con la firma digital y la estampa de tiempo, el no repudio de la información de intercambio.

Estructura del EDI-Mendoza

El Ecosistema Digital de Integrabilidad está compuesto por tres roles fundamentales:

1. Operador del sistema de interoperabilidad
2. Proveedor de servicios de confianza
3. Organización miembro que se une al ecosistema.

Operador del Ecosistema Digital de Integrabilidad

Es el coordinador y principal responsable de la definición de políticas y protocolos en EDI- Mendoza.
La Dirección de Informática y Comunicaciones es la responsable de ejercer este rol en la Provincia de Mendoza, y trabaja en conjunto con las organizaciones pertenecientes al ecosistema.

Dentro de sus tareas se destacan:

- Establecer regulaciones y buenas prácticas para el funcionamiento del Ecosistema
- Supervisar y asegurar el cumplimiento de estas regulaciones
- Definir y aplicar configuraciones globales que mejoren el rendimiento y la estabilidad del servidor central y los componentes del Ecosistema Digital de Integrabilidad
- Publicar estándares que deben ser seguidos por las organizaciones miembro
- Gestionar las solicitudes de ingreso de nuevas organizaciones miembro
- Brindar apoyo y operar los servicios centrales del Ecosistema Digital de Integrabilidad
- Registrar los miembros verificando su identidad (mantener el catálogo de miembros).
- Controlar la correcta registración y mantenimiento del Catálogo de servicios.
- Monitorear la operación del EDI.
- Instalar y/o dar soporte para el despliegue de servidores de seguridad del EDI.
- Capacitar y concientizar sobre los beneficios del EDI.
- Implementar las decisiones establecidas por la Gobernanza del EDI.

Proveedor de Servicios de Confianza

Es la entidad que ofrece servicios de sellado de tiempo (TSA) y Autoridad Certificante (CA) que genera los certificados utilizados para la seguridad y transparencia de la herramienta. A todos los mensajes intercambiados a través de EDI-Mendoza se les aplica una marca de tiempo y son registrados por los servidores de seguridad intervinientes.

Todos los nodos de los servidores de seguridad del ecosistema requieren que les sean asignados dos tipos de certificados:

- Certificado de autenticación: Identifica cada una de las Entidades y Organismos participantes del EDI, y asegura la conexión entre los distintos nodos de seguridad X-Road dentro del ecosistema.
- Certificado de firma: Todo mensaje que se comparte entre nodos de seguridad X-Road será firmado digitalmente con el objeto de validar la identidad del emisor del mensaje, asegurando la trazabilidad e inalterabilidad del mensaje enviado y recibido, garantizando el no repudio.

Organización Miembro (OM)

Las Organizaciones Miembro son entidades públicas o privadas que tienen la capacidad de producir y/o consumir servicios dentro del ecosistema. Pueden desempeñarse como proveedores, consumidores (clientes) o ambas funciones.

Cada OM debe gestionar al menos un subsistema para facilitar el intercambio eficiente de servicios digitales y debe acceder a los servicios de confianza TSA(s) y CA(s) para verificar la validez de los certificados de los clientes y la estampa de tiempo de los mensajes intercambiados, y certificar su existencia en un momento determinado.

Las OM deben designar un usuario administrador que se responsabilice de la gestión de accesos, supervisar la operación del servidor de seguridad, así como garantizar el funcionamiento adecuado de los subsistemas y servicios hacia otros miembros.

Componentes de la plataforma de Integrabilidad

El Ecosistema Digital de Integrabilidad se basa en una arquitectura descentralizada que permite a diferentes sistemas de información comunicarse entre sí a través de servicios web, de manera segura, confidencial y estandarizada. La que cuenta con los siguientes componentes claves:

- **Servidor central**

  El servidor central gestiona la base de datos de miembros del Ecosistema y servidores de seguridad. Contiene la política de seguridad de instalación de X-ROAD, que cuenta con los siguientes elementos:

  - Lista de autoridades de Certificación Digital confiables.
  - Lista de autoridades confiables de Estampado Cronológico de Tiempo.
  - Parámetros ajustables de configuración de los servicios de administración.

  Se aclara que ninguna comunicación pasa a través del servidor central; este podría no estar presente en la red durante unos minutos sin ningún impacto en la disponibilidad de los servicios en la plataforma de integrabilidad.

- **Servidor de Seguridad:**

  Los miembros son organizaciones, instituciones gubernamentales o empresas privadas que participan en la plataforma.
  Cada miembro tiene un *servidor de seguridad* (Nodo) que actúa como puerta de entrada y salida para proveer o consumir datos a través de servicios web.

  Este servidor de seguridad, gestiona las llamadas y respuestas de servicio entre los sistemas de información de los miembros y encapsula los aspectos de seguridad involucrados en el intercambio de datos: gestión de claves para la firma y autenticación, envío de mensajes a través de un canal seguro, creación del valor de prueba para mensajes con firmas digitales y sellado de tiempo.

  El servidor de seguridad (SS) es la puerta de entrada/salida segura de los servicios a internet abierta. Los SS se deben instalar junto a las instalaciones donde corren los sistemas de cada organización miembro. Esto implica que según las locaciones que tenga cada Miembro deberían tener un SS en cada locación.

  Soberanía de datos: Los SS permiten ejercer la soberanía de los datos administrando el control de acceso a determinados subsistemas. Esto implica que una misma organización

independientemente de la locación, debería tener un SS por cada actor interno que necesite ejercer el total control sobre sus datos.

- **Subsistemas:**

  Dentro de cada miembro, existen subsistemas que representan *sistemas* o aplicaciones individuales. Los subsistemas una vez que se registran en el servidor central, pueden proporcionar y/o consumir servicios.

  Un subsistema representa una parte del sistema de información de un miembro de X-Road.

  Los miembros de X-Road deben declarar partes de su sistema de información o aplicación como subsistemas para utilizar o proporcionar servicios de X-Road.

  Un subsistema siempre está asociado a una sola organización.

  El subsistema puede estar conectado a uno o más servidores de seguridad.

  Una organización puede tener N subsistemas o simplemente uno solo. Esto responde a la necesidad de diferenciar las partes de los sistemas de información dentro de la organización.

  Por ej: subsistema RRHH, subsistema COMPRAS, subsistema PROVEEDORES, subsistema VACUNAS, subsistema MÉDICOS.

  Puede ser razonable tener diferentes subsistemas para diferentes registros (sistemas de proveedores de datos) o también para evitar el mal uso de los datos por organismos.

- **Servicios:**

  Son los servicios web (microservicios, APIs) que una organización miembro puede ofrecer o solicitar a otros subsistemas. Los mismos se definen mediante descripciones técnicas y se publican en los subsistemas de cada servidor de seguridad.

Control de accesos y auditoría de intercambios

- **Derechos de acceso:**

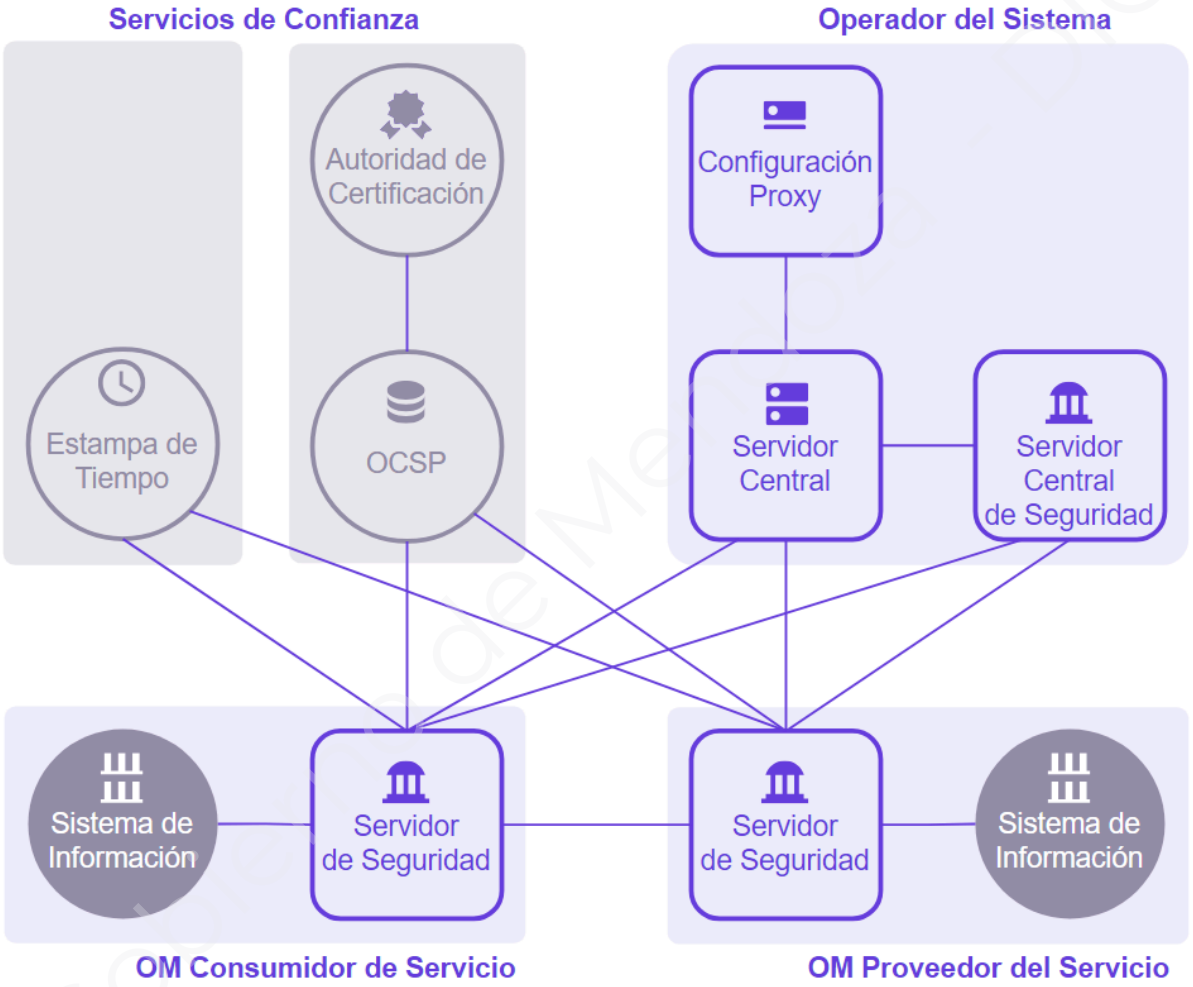
  Se deben realizar acuerdos formales que especifiquen las condiciones bajo las que los servicios pueden ser utilizados, donde se define la autorización y restricciones de uso.

  Los derechos de acceso en X-Road se otorgan a nivel de Subsistema, si se necesita gestionar niveles de acceso por usuario deberán resolverse en la aplicación que lo requiere.

- **Seguridad y autenticación:**

  El sistema cuenta con una seguridad sólida, utilizando certificados digitales para autenticar y autorizar a los miembros y subsistemas. Además, todas las transacciones se almacenan en un registro de auditoría para garantizar la trazabilidad.

La arquitectura del Ecosistema Digital de Integrabilidad , en una instancia básica entre dos Organizaciones Miembro con servidores de seguridad, sigue el siguiente esquema:



En instancias complejas, el Ecosistema Digital de Integrabilidad contendrá múltiples Organizaciones Miembro, dónde si bien se conectarán a la plataforma a través de un único servidor de seguridad, este podrá funcionar con múltiples nodos de seguridad actuando en grupo. Las Organizaciones Miembro deberán utilizar la configuración necesaria para garantizar alta disponibilidad.

Cuando una aplicación o sistema de información de una Organización Miembro, requiera consumir un servicio de otro miembro del ecosistema, únicamente puede hacerlo a través del subsistema que lo representa, se debe seguir el siguiente flujo:

1. **Solicitud**: la aplicación que consume (representado por el subsistema consumidor) envía una solicitud al subsistema proveedor, indicando qué servicio desea utilizar y se identifica mediante su certificado digital.
2. **Autenticación**: el servidor de seguridad consumidor, auténtica a la aplicación o sistema de información verificando su certificado digital según los requisitos establecidos en la configuración del subsistema.
3. **Autorización**: el servidor de seguridad proveedor verifica si el consumidor (cliente) tiene autorización para acceder al servicio específico. Esto se basa en los derechos de acceso definidos.
4. **Procesamiento de la solicitud**: la aplicación o sistema de información (representado por el subsistema proveedor) procesa la solicitud y genera una respuesta.
5. **Respuesta**: el resultado se envía de regreso al subsistema consumidor.
6. **Registro de auditoría**: cada paso de la transacción se almacena en el registro de auditoría de ambos servidores de seguridad intervinientes para fines de trazabilidad y seguridad.

Adhesión como Organismo Miembro

Las Organizaciones Miembro (OM), como se detalló anteriormente, son entidades o instituciones que forman parte del EDI-Mendoza, y una vez reconocidas y autorizadas por el servidor central, tienen la capacidad de operar su propio servidor de seguridad dentro del sistema, lo que implica proveer y consumir servicios web.

En este modelo, cada unidad organizacional puede definirse a nivel de Ministerio, Secretaría, Subsecretaría, o según la jerarquía correspondiente en función de su relevancia en la gestión de datos.

Las Organizaciones Miembro pueden ser entidades públicas, pertenecientes al Gobierno de la Provincia de Mendoza o del Gobierno Nacional u otras jurisdicciones, o entidades privadas.
Según las características de la organización se le asignará alguna de las clases siguientes:

- **GPL**: Gobierno Poder Legislativo
- **GPE**: Gobierno Poder Ejecutivo
- **GPJ**: Gobierno Poder Judicial
- **GM**: Gobierno Municipal
- **GN:** Gobierno Nacional
- **OP**: Organizaciones Privadas.

Los requerimientos necesarios para formar parte del Ecosistema EDI-Mendoza, se debe contar con los siguientes perfiles:

1. Responsable Técnico (Infraestructura), deberá gestionar y monitorear el servidor de seguridad, administrar certificados.
2. Responsable de sistemas (Desarrollo), deberá exponer servicios, mantenerlos actualizados y administrar los subsistemas que contenga, implementar certificados, etc.
   Es el responsable de informar las actualización o baja de servicio a sus respectivos clientes.
3. Responsable de Gestión, deberá tomar decisiones sobre la habilitación de servicios para el consumo de otros miembros.

En caso de no contar con alguno de estos perfiles debe comunicarlo a la Dirección Informática y Comunicaciones, para que se evalúen las acciones a seguir.

Pasos a seguir para formar parte del ecosistema:

1. Completar el formulario para solicitud de alta de nuevo miembro.
2. Realizada la solicitud, será contactado para coordinar la primera reunión entre el equipo de implementación de X-Road y el solicitante para realizar la presentación formal de los motivos por los que desea incorporarse al EDI.
3. Una vez decidida la incorporación como organización miembro, la máxima autoridad de la entidad interesada deberá comunicar los datos de los responsables técnicos y de gestión.

   Para todos los casos se debe enviar nombre y apellido, número de celular, mail de contacto de los responsables designados.
4. Firmar el convenio de adhesión, el modelo de convenio se encuentra disponible dentro del siguiente sitio.

Durante proceso, los responsables técnicos del servidor de seguridad recibirán una capacitación detallada sobre la arquitectura del EDI-Mendoza, donde se abordarán aspectos como el monitoreo y seguimiento de auditoría, utilización y consumo de certificados, creación de subsistemas, configuración de accesos para que otras organizaciones miembro consuman servicios, etc.

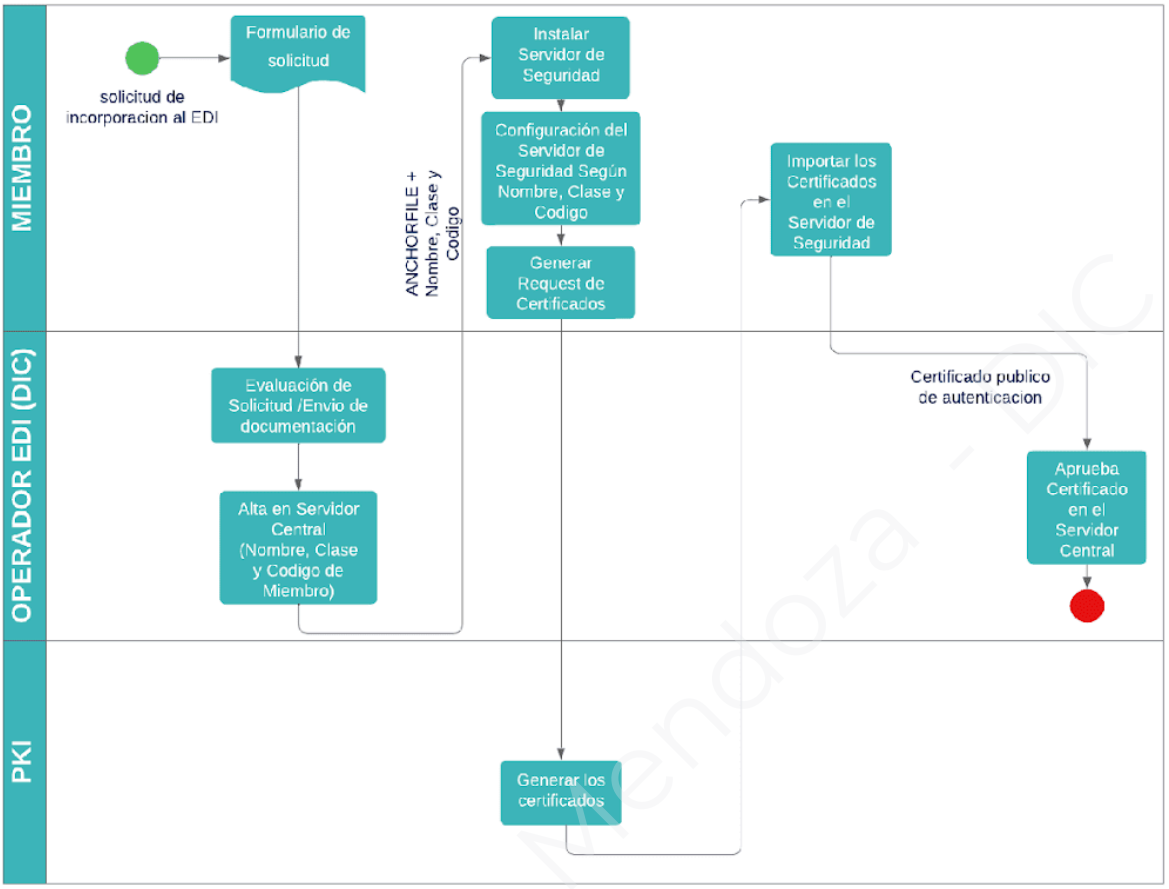
La entidad puede optar por instalar su servidor de seguridad en infraestructura propia, si la tuviera, siguiendo los lineamientos que detalle la Dirección de Informática y Comunicaciones (adjunto siguiente sección) o solicitar la instalación del mismo en la infraestructura de la Dirección de Informática y Comunicaciones la cual quedará sujeta a la evaluación y aprobación de la Dirección.

Instalación del servidor de seguridad X-Road

Para completar el proceso de convertirse en organización miembro, después de la aprobación administrativa y la confirmación del operador de EDI-Mendoza, es necesario avanzar con la instalación del servidor de seguridad. Esta fase implica un trabajo conjunto colaborativo entre el responsable técnico de la organización miembro y el Operador del Ecosistema Digital de Integrabilidad, requiriendo una comprensión sólida de la plataforma y la infraestructura de la entidad.

Si se decide que la instalación del servidor de seguridad se encuentre alojado en la infraestructura del organismo miembro, se establecerá una comunicación con los referentes técnicos responsables, y se proporcionará los instructivos para el equipo técnico, manteniendo un contacto constante de forma de garantizar el éxito en esta etapa del proceso.

Diagrama de flujo de alta de Miembro



1) **Miembro**: Completa formulario de solicitud de alta de miembro (generación de ticket*)

2) **Operador EDI:** Evaluación de solicitud y coordinación de capacitación inducción y envío de documentación del EDI.

3) **Operador EDI:** Envía Nombre, Clase y Código del Miembro + Anchorfile a correo ingresado en el formulario.

4) **Miembro:** Instalar servidor de seguridad hasta el punto de generar request de certificados.

5) **Miembro:** Enviar solicitud de certificados a través del ticket generado para el alta.

6) **Operador EDI:** Genera y envía los certificados a través del ticket.

7) **Miembro:** Importa los certificados en el Servidor de Seguridad solicita a través del ticket generado la aprobación del certificado al Operador.

8) **Operador EDI:** Aprueba certificado en el Servidor Central.

***El ticket emitido por el interesado es el principal medio de comunicación

desde el proceso de solicitud de alta de miembro hasta la finalización del alta como miembro del EDI Mendoza, donde se da por finalizado el ticket.

Requerimientos:

Los *requerimientos mínimos necesarios* que se requieren para instalar la plataforma X-Road de un servidor de seguridad son:

- Procesador de 64-bit dual-core Intel, AMD o compatible.
- 4 GB RAM
- Placa de red de 100 Mbps.
- Si se van a usar tokens en hardware, interfaces para estos.
- El hardware debe estar soportado por Ubuntu.
- SO: Ubuntu 22.04 LTS, 24.04 TLS
- Disco: 8GB

Los requerimientos recomendados, son los siguientes:

- 3 discos/particiones:
    - 16 GB para la partición raíz
    - 250 GB para logs
    - 100 GB para BD

Para consulta de última actualización oficial del NIIS la misma se encuentra en: Requerimientos UBUNTU , Requerimientos para RHEL

Instalación:

La instalación requiere del agregado de un repositorio y la instalación del X-Road, a continuación se dejan las líneas de comando paso a paso para realizar la instalación de nodo de seguridad de X-Road.

```
useradd webadmin

apt-get install locales software-properties-common

echo "LC_ALL=en_US.UTF-8" >> /etc/environment

locale-gen en_US.UTF-8

curl https://artifactory.niis.org/api/gpg/key/public | apt-key add
-

apt-add-repository                    -y                    "deb
https://artifactory.niis.org/xroad-release-deb       $(lsb_release
-sc)-current main"

apt update
```

```
apt install --assume-yes xroad-securityserver
xroad-addon-opmonitoring
```

Durante el proceso de instalación habrá que completar algunos datos:

- CN: Common Name del servidor
- IP: Aliases y/o direcciones ip del servidor.

Se debe verificar que todos los componentes se hallan instalados correctamente, para eso se ejecuta lo siguiente y posteriormente se verifica que se encuentren activos todos los servicios:

```
sudo systemctl list-units "xroad*"

UNIT                                      LOAD   ACTIVE SUB     DESCRIPTION
xroad-base.service                        loaded active exited  X-Road initialization
xroad-center-management-service.service   loaded active running X-Road Central Server
xroad-center-registration-service.service loaded active running X-Road Central Server
xroad-center.service                      loaded active running X-Road Central Server
xroad-signer.service                      loaded active running X-Road signer
```

Luego de que el software se encuentre instalado se procede a la configuración del mismo con el fin de agregarlo al ecosistema.

XROAD hace uso de PAM. Por lo que es necesario generar un usuario y agregar el mismo a distintos grupos, por lo general el usuario generado es: webadmin.

Una vez realizado, se procede a ingresar a la interfaz web de administración: https://[servidor]:4000, usando el usuario y contraseña ya mencionados.

En la primera interacción con el sistema, se va a solicitar que se completen tres pasos:

1. Cargar el archivo anchor: Este archivo lo envía la administración del EDI al responsable del nodo e indica, a qué servidor central se debe conectar el nodo de seguridad.
2. Luego se debe ingresar los datos del miembro (owner) del nodo: Los datos del miembro deben ser dados por la administración del EDI, ya que deben estar pre cargados en el servidor central. Ingresar un nombre no válido, implicaría borrar todo el software del servidor y empezar de nuevo.
3. Generación del PIN: Se solicita el ingreso de un PIN para la inicialización de los servicios. Este PIN sirve para proteger el almacenamiento de los certificados generados que usa el nodo de seguridad para interactuar entre los nodos de seguridad, y se debe ingresar cada vez que el servidor se reinicie. En caso de querer

automatizar este proceso, ver el punto de **autologin**, detallado más abajo.

Si todo está bien, el operador del ecosistema de integrabilidad podrá agregar el nodo al ecosistema.

Se recomienda migrar las base de datos a la unidad de 100GB y la carpeta de los logs a la unidad de 250GB, a traveś de un bind a la partición en la carpeta donde se guarda la base de datos del postgresql y se debe hacer lo mismo con los logs del servidor, ubicados respectivamente en:

- /var/lib/postgresql
- /var/lib/xroad/

Esta recomendación, es por la cantidad de datos que generan los nodos de seguridad.

Configuración y agregado del nodo al EDI-Mendoza

Para agregar el nodo al ecosistema, es necesario generar los certificados para autenticarse y firmar los paquetes, y se deben seguir los siguientes pasos:

- Desde la pestaña Keys and certification -> SIGN and AUTH Keys -> Softtoken-0
- Luego “Add Key”
- Luego se debe colocar AUTH para la llave de autenticación y SIGN para firmar.
- Luego se completa el resto según el uso que debamos dar.
- Para ambos casos, se genera un csr
- Se debe enviar el CSR al correo del soporte de la DIC (dic-infraestructura@mendoza.gov.ar) para ser firmado con la CA del ecosistema.
- Se debe importar los certificados firmados en el paso anterior a los correspondientes keys.
- En el certificado con nombre AUTH hacer click en el nombre del certificado y click en “activate” y luego hacer click en “register”. Al hacer click en “register” hay que informar el FQDN del nodo.
- Se deberá ingresar al ticket emitido en la solicitud de alta de miembro para solicitar la aprobación del certificado.

Autologin

Este es un módulo que ingresa automáticamente el pin del servidor cuando se reinicia. La implementación del mismo, queda a consideración del operador del nodo de seguridad. Para instalar el módulo, se debe instalar el paquete: xroad-autologin,para eso ejecutar en la terminal:

```
~# apt install xroad-autologin
```

Una vez instalado, generar el archivo:

```
/etc/xroad/autologin
```

Dentro de este archivo poner el password en texto plano y reiniciar el nodo.

Ventajas de su configuración:
En caso de que esté todo en orden, el sistema debe inicializarse sin solicitar el pin code.

Manejo de índices en la Base de Datos

Una vez que el Servidor de Seguridad se encuentre operativo, se podrán consultar los registros de logs específicos utilizando el "message-id" de cada transacción, lo que facilita la recuperación del detalle del pedido realizado y de la respuesta correspondiente. Estos registros se almacenan en la base de datos messagelog.

Para optimizar la consulta de registros específicos, se puede agregar un índice a la tabla logrecord dentro de esta base de datos realizando los siguientes pasos:

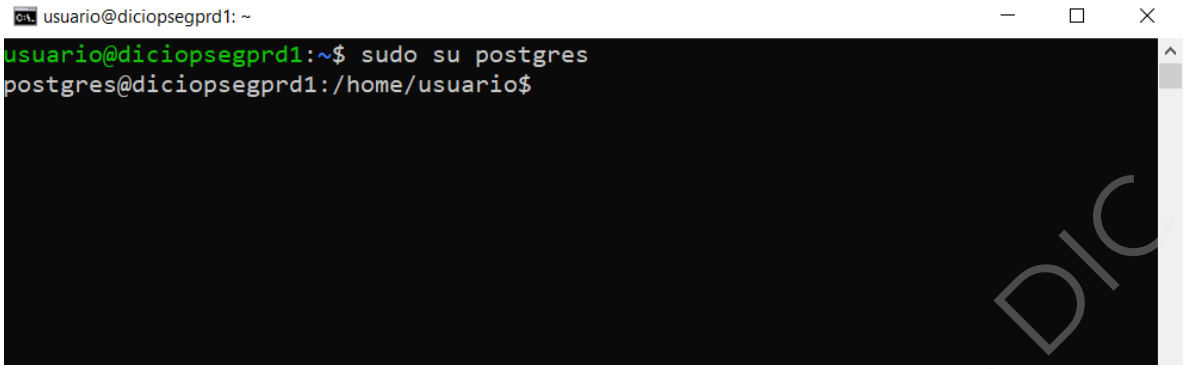
1. **Acceso al Servidor**

Para realizar esta tarea, es necesario acceder al servidor mediante SSH y cambiar al usuario postgres.

a. **Conectarse al servidor con SSH:**

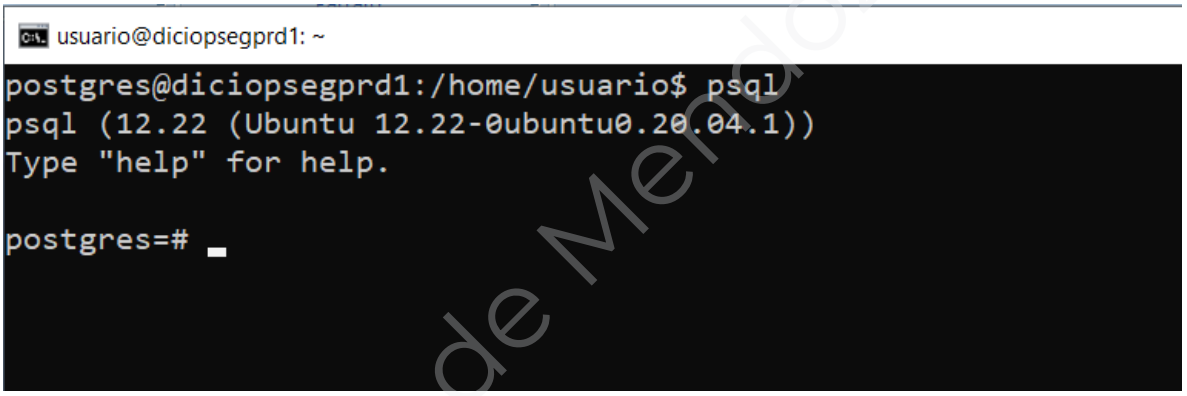
b. Cambiar al usuario postgres:

sudo su postgres



c. Iniciar la consola de PostgreSQL:

Psql



d. Conectar a la base de datos messagelog:

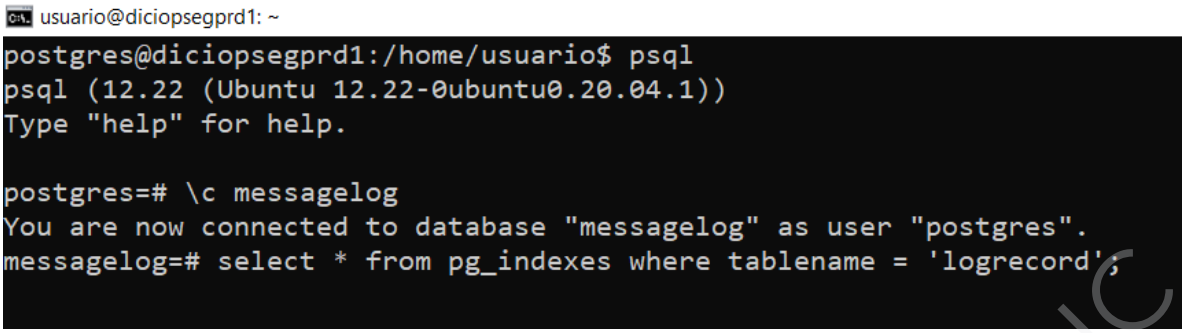
\\c messagelog

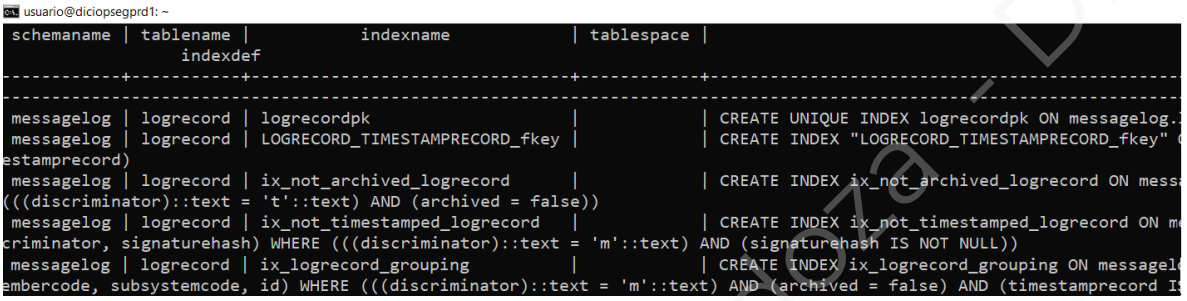
2. Verificación de Índices Existentes

Antes de agregar un nuevo índice, es recomendable verificar los índices existentes en la tabla logrecord:

SELECT * FROM pg_indexes WHERE tablename = 'logrecord';

Este comando devuelve la lista de índices actuales sobre la tabla logrecord.





3. Creación del Índice

Para mejorar la velocidad de las consultas basadas en la columna queryid, se debe agregar un índice B-Tree a la tabla logrecord:

CREATE INDEX logrecord_queryid ON messagelog.logrecord USING btree (queryid);

4. Beneficios del índice

La creación de este índice proporciona los siguientes beneficios:

- Mayor eficiencia en la recuperación de registros de log.
- Reducción del tiempo de respuesta al ejecutar consultas basadas en queryid.
- Optimización del rendimiento de la base de datos de auditoría.

Gestión del Ecosistema

Una vez que la Entidad esté plenamente incorporada al EDI-Mendoza, contará con dos herramientas para realizar la gestión de sus subsistemas y servicios:

- UI Servidor de Seguridad.
- Plataforma de auditoría y mantenimiento del catálogo de servicios.

UI Servidor de Seguridad

Con la instalación del servidor de seguridad de X-Road en cada Organización Miembro, se permite el acceso a una interfaz de usuario llamada “X-Road Security Server” que permitirá incorporar subsistemas, disponibilizar servicios, gestionar accesos y agregar certificados.

Para poder acceder al servidor de seguridad propio de la organización miembro, existe un único rol llamado “Gestor del Servidor de Seguridad” al que se le pueden otorgar uno o más permisos para accionar dentro del mismo.

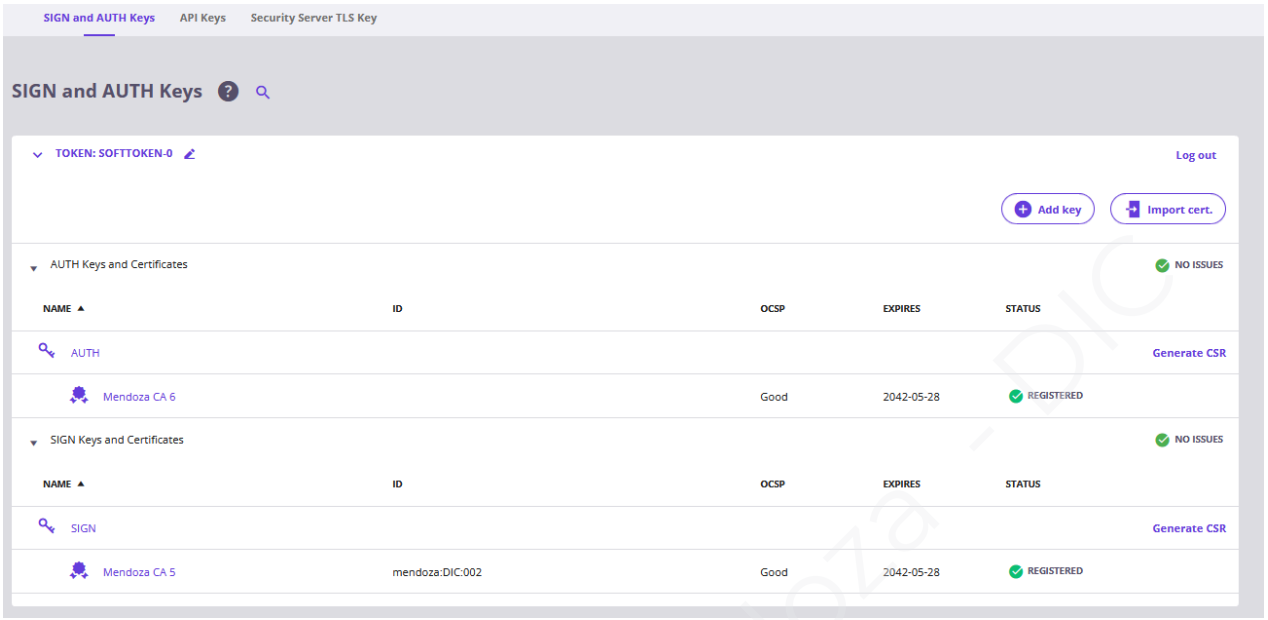
Componentes del servidor de seguridad

Los componentes del servidor se dividen en: componentes de configuración y componentes de gestión.

1. Componentes de configuración del servidor de seguridad

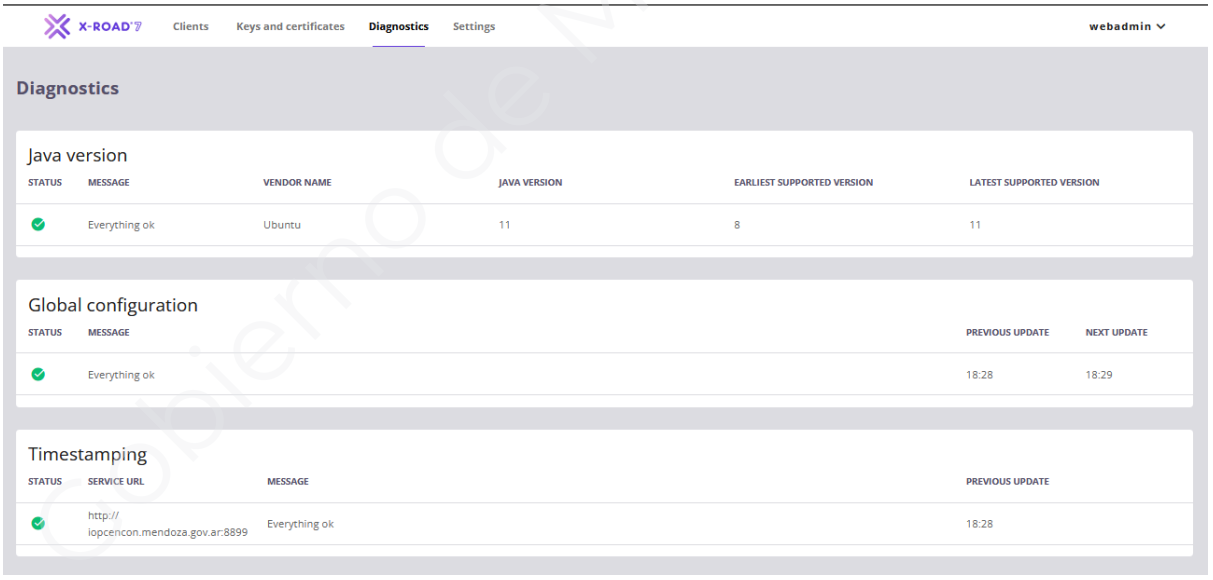
Dentro del servidor de seguridad las solapas Keys and certificates, Diagnostics y Settings se debe utilizar inicialmente para la instalación del servidor de seguridad, y después es recomendable no hacer modificaciones sobre las mismas, excepto que el operador del Ecosistema Digital de Integrabilidadlo solicite al responsable técnico de la organización.

Llaves y certificados (Keys and certificates)



Se visualizan los certificados y firmas registradas en el servidor de seguridad.

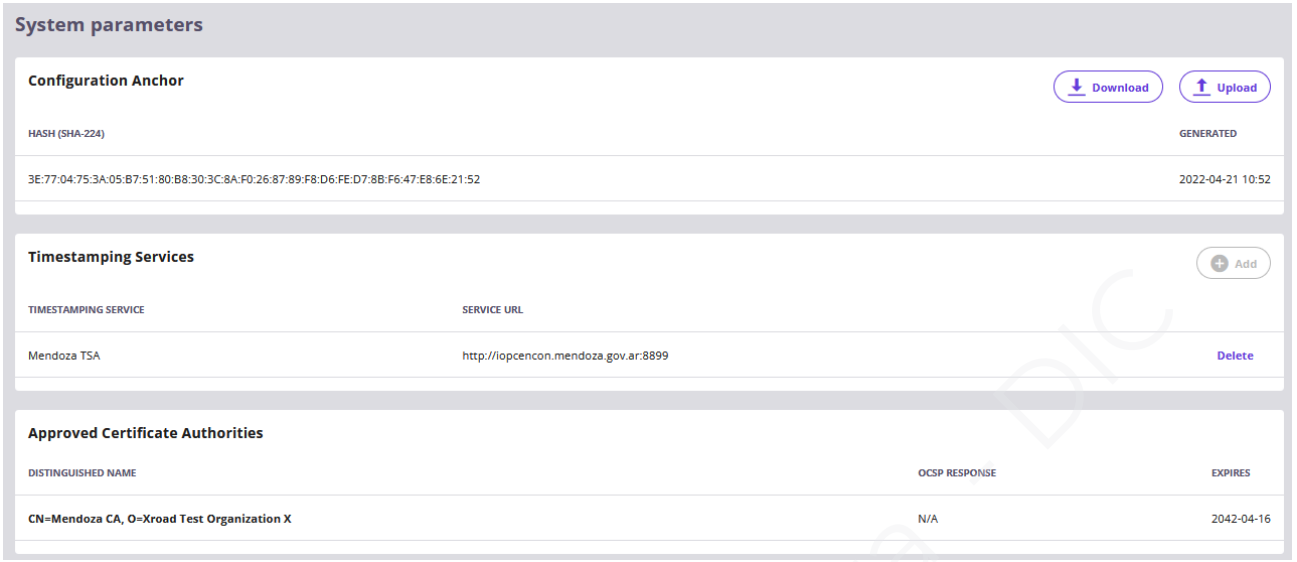
Diagnóstico (Diagnostics)



Se podrá verificar la versión del servidor y que la configuración global del ecosistema, el *timestamping* y el *OCSP Responders* se encuentren funcionando correctamente.

Los OCSP Responder es el servicio que dispone la CA y que utiliza el servidor de seguridad, para verificar el estado de los certificados de los nodos X-Road cliente.

Ajustes (Settings)

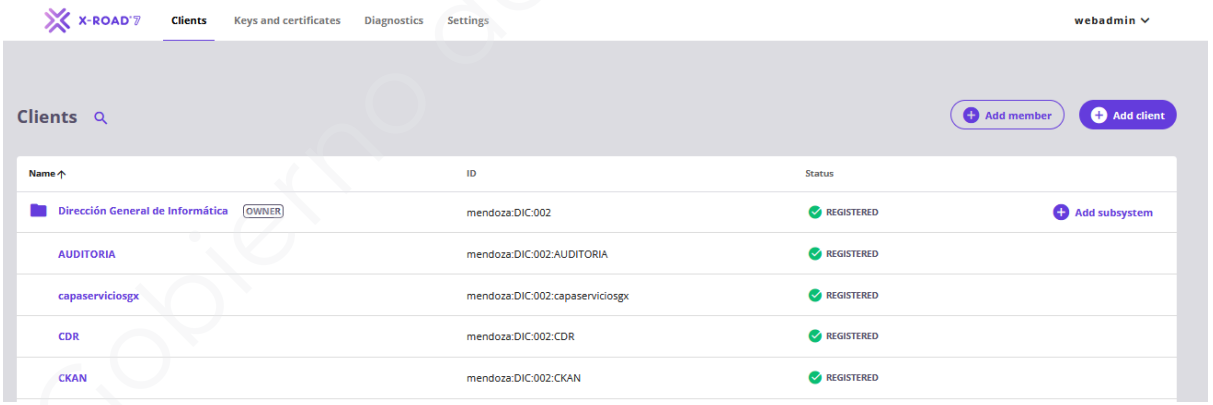


Se visualizan los parámetros del sistema. La configuración del Anchor, el timestamp y la autoridad certificante habilitada. Todas provistas por el Gobierno de la Provincia de Mendoza

2. Componentes de gestión del servidor de seguridad

La solapa Clients es la que va a ser utilizada por los gestores del servidor de seguridad y se identifican varias acciones.

Clientes (Clients)



Refiere a la organización miembro propietaria del servidor de seguridad. Cabe aclarar que se pueden crear más de un cliente por servidor de seguridad, pero para la implementación de EDI-Mendoza se requiere un servidor por miembro. Por lo tanto, no será necesario agregar miembros o clientes.

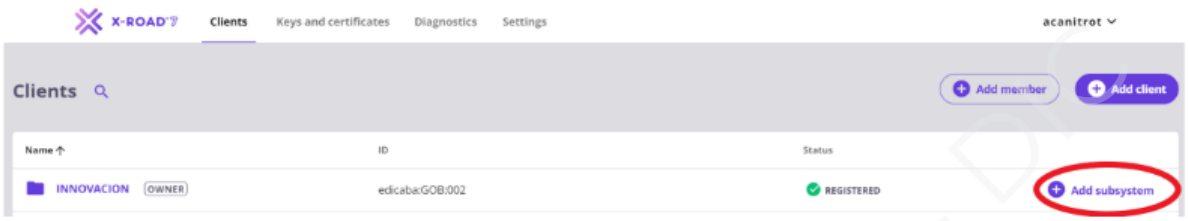
Subsistemas (Subsystems)

Los subsistemas en EDI-Mendoza se definen como el medio por el que se conectan las distintas aplicaciones o sistemas de información para el

intercambio de datos. El propósito específico de cada uno puede variar entre proveer servicios o consumirlos.

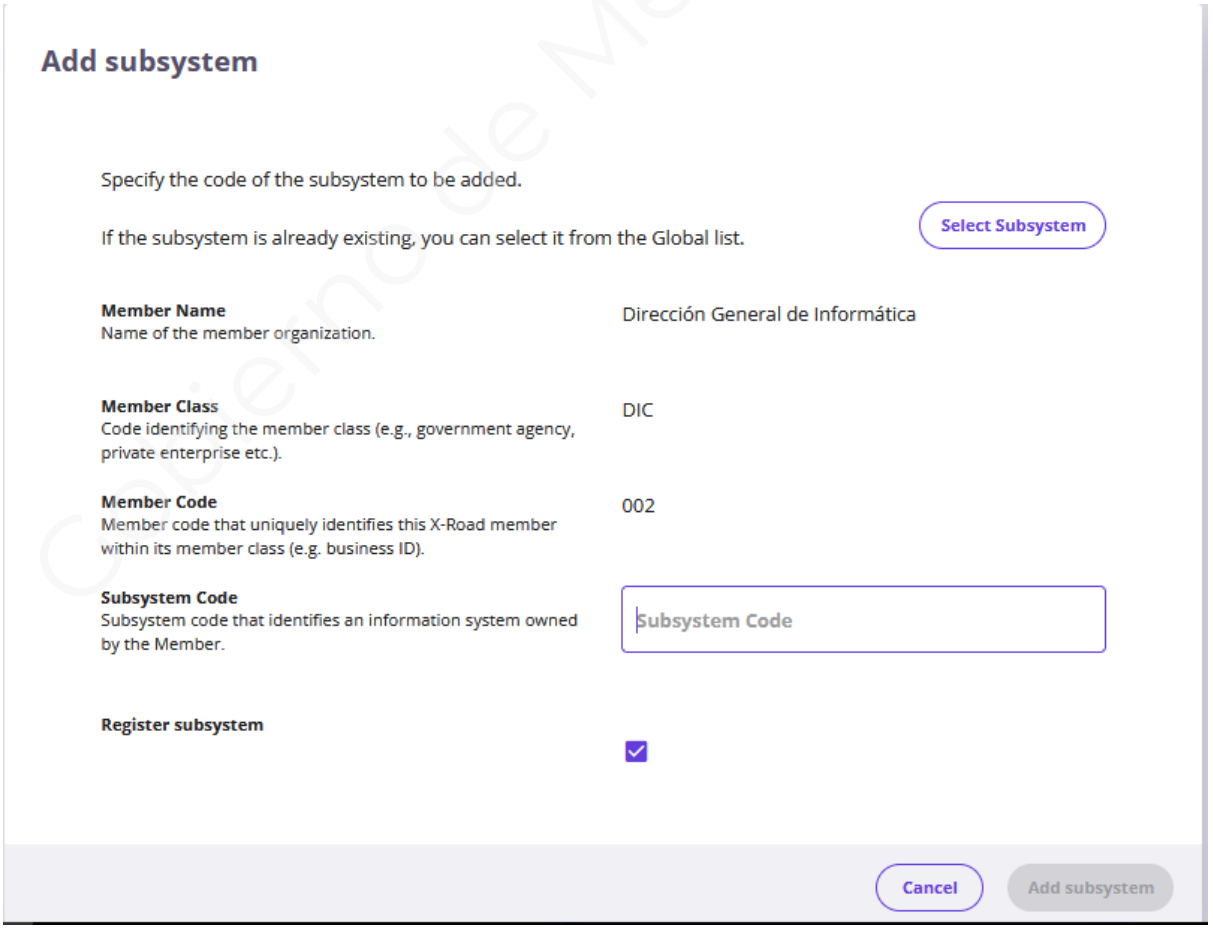
Los subsistemas pueden ser agregados al servidor de seguridad (Nodo) del organismo.

Para agregar un nuevo subsistema, se utiliza la opción “Add subsystem”.



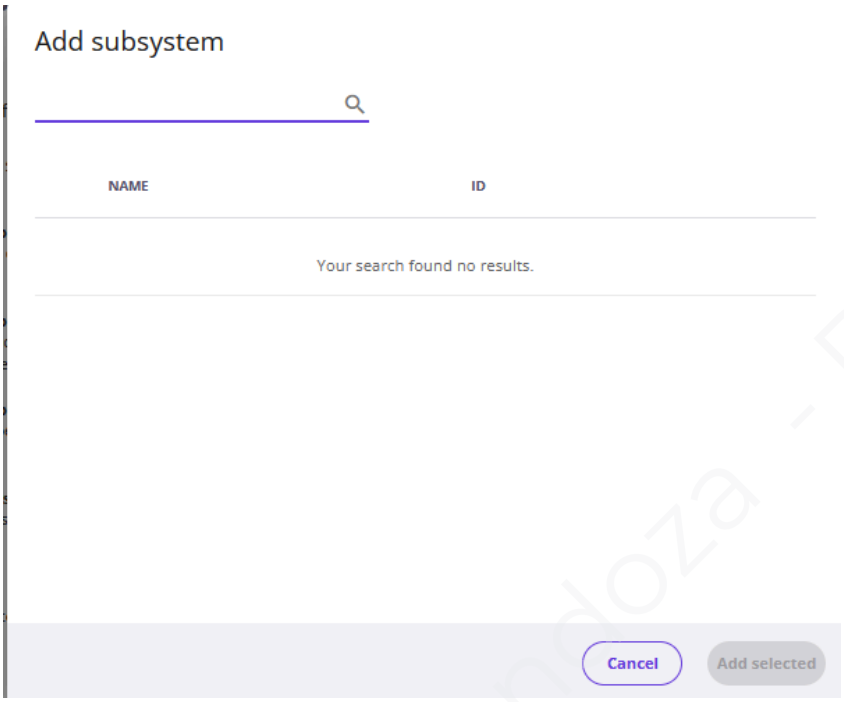
El nombre del subsistema deberá ser definido en mayúsculas y ser representativo de la aplicación o sistema de información al que representa.

Esta metodología de nomenclatura proporciona claridad y consistencia en la creación y gestión de subsistemas, facilitando la identificación y comprensión de sus funciones dentro del ecosistema.



Otra alternativa es seleccionar el subsistema de la lista de subsistemas disponibles presionando en el botón “Select Subsystem”, siempre que se

haya solicitado previamente la creación del subsistema al administrador de EDI-Mendoza.



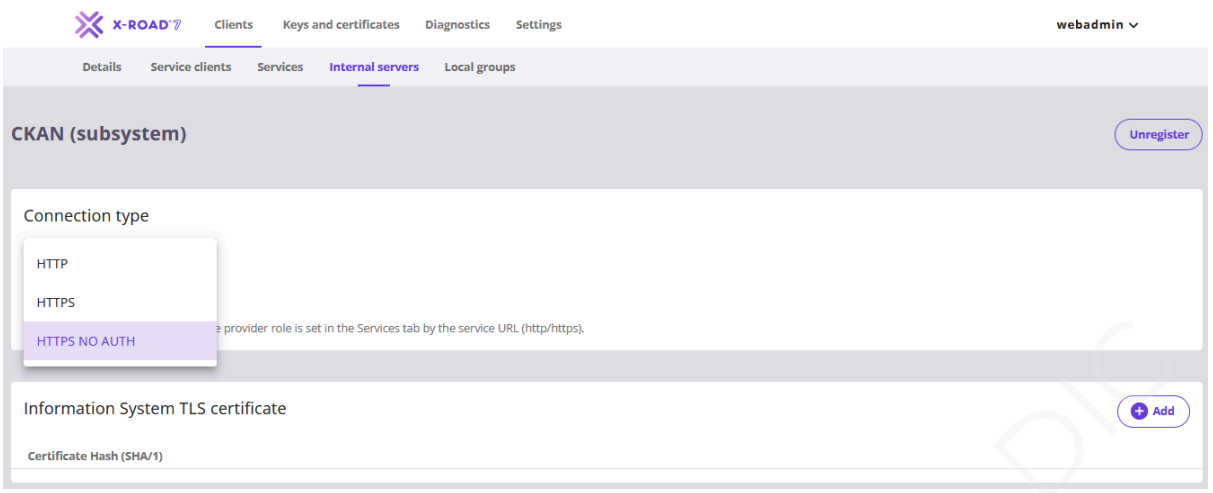
Para garantizar la estandarización en la creación de subsistemas y la no duplicidad de nombres de subsistemas, se deberá solicitar la autorización del mismo al operador del Ecosistema mediante el siguiente formulario brindando información sobre la aplicación o sistema de información, el uso que se dará y los datos del responsable.

Una vez enviada la solicitud, en caso de ser correcta y no haber duplicidad el operador del ecosistema, enviará al responsable del servidor de seguridad Central del EDI-Mendoza para que se autorice el subsistema y quede habilitado para comenzar a operar.

Si el nombre del subsistema solicitado se encuentra ya registrado en EDI-Mendoza, el operador del Ecosistema se comunicará para que se hagan las correcciones necesarias y poder continuar con la habilitación del mismo.

Conexión del Servidor de Información al Subsistema como cliente

La interfaz del servidor de seguridad ofrece tres tipos de conexión en la solapa Internal Servers: HTTP, HTTPS y HTTPS NO AUTH.



La elección del tipo de conexión dependerá de los requisitos de seguridad específicos de su entorno y de la sensibilidad de la información que se transmite entre los servidores. En EDI-Mendoza se recomienda evitar utilizar el protocolo HTTP y usar el protocolo HTTPS .

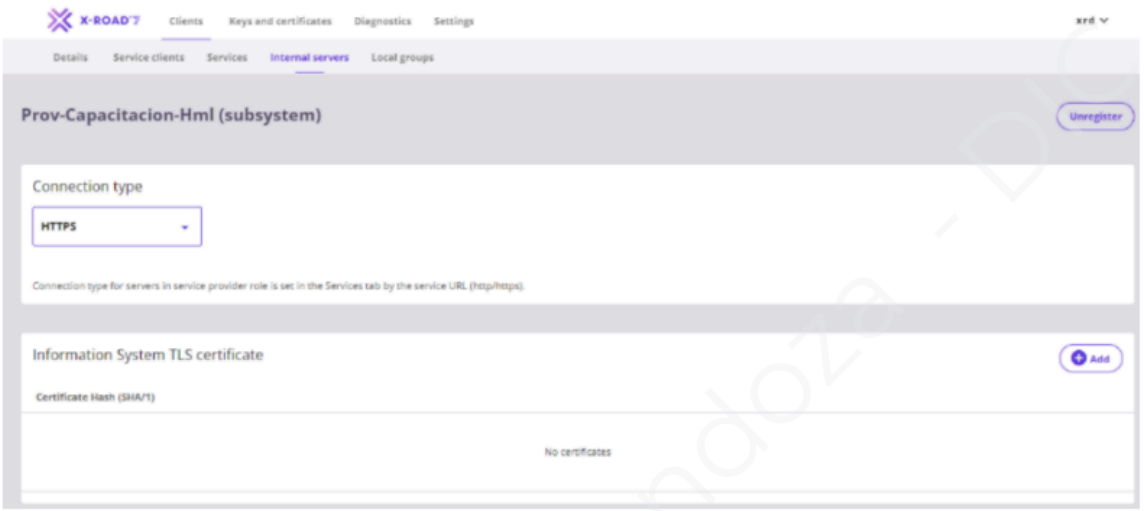
Un servidor de seguridad puede usar los protocolos HTTP, HTTPS o HTTPS NOAUTH para comunicarse con los sistemas de información del cliente, sistemas de información que actúan como clientes de servicio y consumen servicios a través de X-Road.

Se recomienda encarecidamente utilizar siempre el protocolo HTTPS. La diferencia entre las alternativas se explica a continuación.

- Se puede usar el protocolo HTTP si el servidor de la aplicación o sistema de información y el servidor de seguridad se comunican en un segmento de red privada donde no hay otras computadoras conectadas. Además, el servidor del sistema de información no debe permitir el inicio de sesión interactivo.
- El protocolo HTTPS (predeterminado para nuevos clientes) debe usarse si no es posible proporcionar un segmento de red separado para la comunicación entre el servidor del sistema de información y el servidor de seguridad. En ese caso, se utilizan métodos criptográficos para proteger su comunicación contra posibles escuchas e intercepciones. Antes de que se pueda usar HTTPS, se deben crear certificados TLS internos para los servidores de aplicación o sistema de información y cargarlos en el servidor de seguridad.
- Se debe utilizar el protocolo HTTPS NOAUTH si desea que el servidor de seguridad omita la verificación del certificado TLS del sistema de información. Si se selecciona el método de conexión HTTP, pero el sistema de información se conecta al servidor de seguridad a través de HTTPS, entonces se acepta la conexión, pero no se verifica el certificado TLS interno del cliente (mismo comportamiento que con HTTPS NOAUTH).

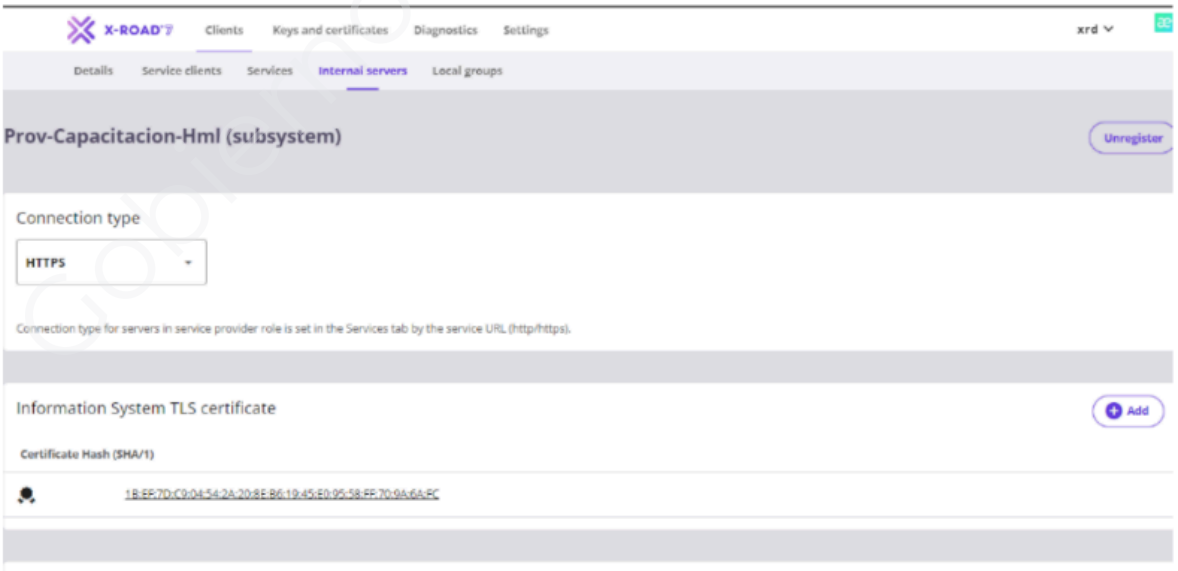
De manera predeterminada, el tipo de conexión para todos los clientes de servidor de seguridad se establece en HTTPS para evitar el uso no autorizado de los clientes.

En el caso de que se utilice este último, se deberá cargar el certificado TLS siguiendo las siguientes acciones:



Desplegando el icono HTTPS que está debajo de Connection Type, selecciona la opción “HTTPS”. Luego hacé clic en el botón “+Add” dentro del campo Information System TLS Certificate y seleccioná el archivo con el certificado que se desea cargar.

El Certificado aparecerá en Certificate Hash (SHA/1) de la siguiente manera:



Una vez verificado que el certificado está cargado como se muestra en la imagen anterior, será posible hacer una consulta de prueba contando con

el certificado que debe ser cargado en la herramienta que se utilice para la consulta.

Nota: tanto la configuración HTTPS como HTTPS NO AUTH utilizan el puerto 443, mientras que la configuración HTTP utiliza el puerto 80.

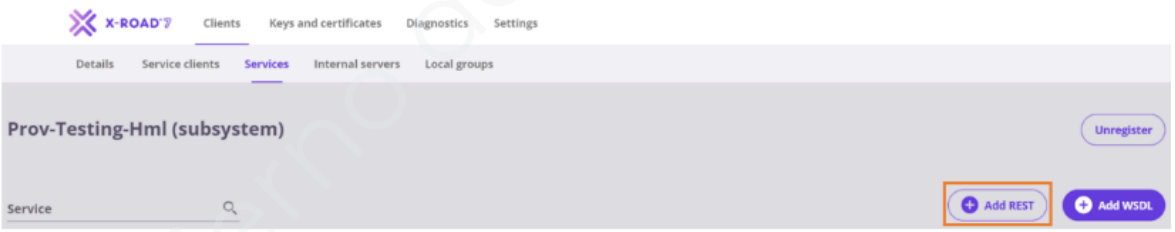
Servicios (Services)

Dentro de los subsistemas proveedores, se van a disponibilizar los servicios que se proveen desde la aplicación o sistema de información. En el Ecosistema Digital de Integrabilidad se promueve el acceso a servicios mediante la adopción de estándares, ofreciendo a los usuarios la posibilidad de utilizar tanto el protocolo SOAP como REST. Estos proporcionan las bases para la comunicación y el intercambio de datos dentro del ecosistema, permitiendo la integración entre distintas aplicaciones.

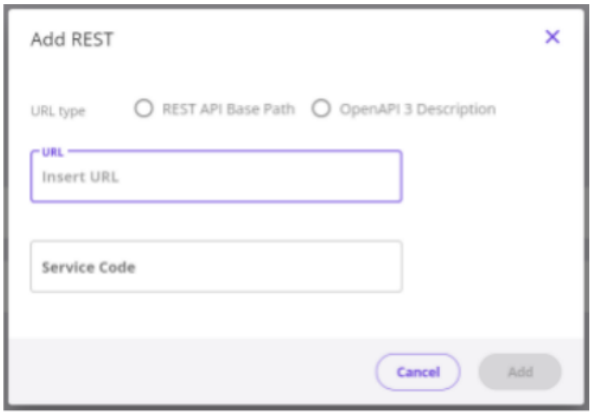
Dentro de estas opciones, se recomienda la utilización del protocolo REST, en el EDI-Mendoza, lo que se fundamenta en su enfoque flexible, la simplicidad de implementación y la eficiencia en el manejo de recursos en comparación con SOAP.

Servicios de tipo REST

Para publicar servicios de tipo REST, se debe seleccionar el subsistema al que pertenece el servicio y luego ingresar en la solapa Services para utilizar la opción “Add REST”**.**



Luego seleccionar la opción tipo de URL, se utiliza “REST API Base Path”. Se completa con la base de la URL, en caso de que se cuente con múltiples endpoints, o en su defecto la URL.

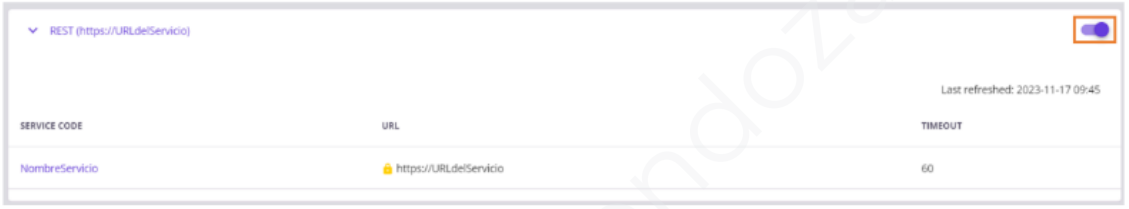


Por otro lado, si el servicio desarrollado cuenta con un archivo de especificación openAPI 3.0 se puede optar por cargarlo directamente desde la opción “OpenAPI 3 Description”.

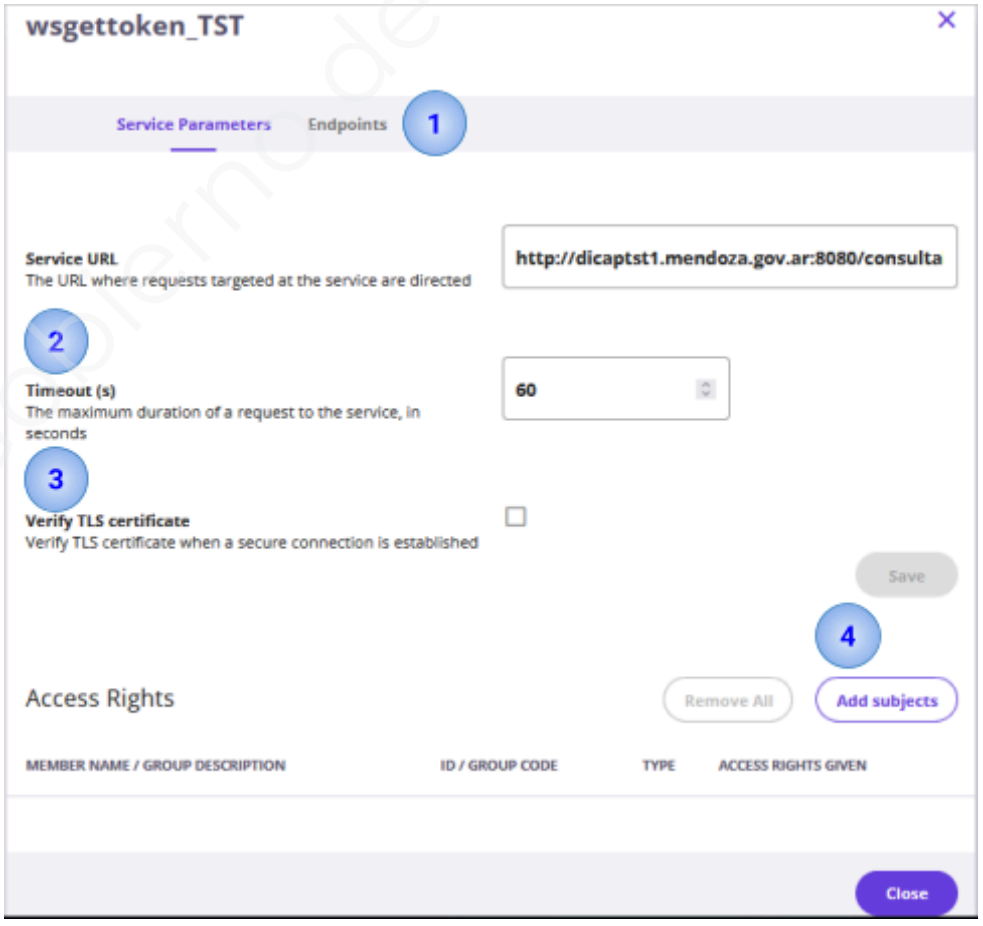
En el campo “Service Code” se asigna una etiqueta a dicho servicio que servirá para conformar la URL en X-Road y realizar el llamado posteriormente.

Para definir el “Service Code” se deberá emplear una estructura en lenguaje natural utilizando la notación “Pascal Case” definiendo el inicio de cada palabra en mayúscula. Con la intención que la funcionalidad del servicio sea clara para todos los miembros del ecosistema.

Una vez añadido el servicio, es necesario habilitarlo para que pueda ser utilizado:



Se debe hacer click en el “Service Code” para acceder a la pantalla que permite realizar distintas gestiones relacionadas al servicio.



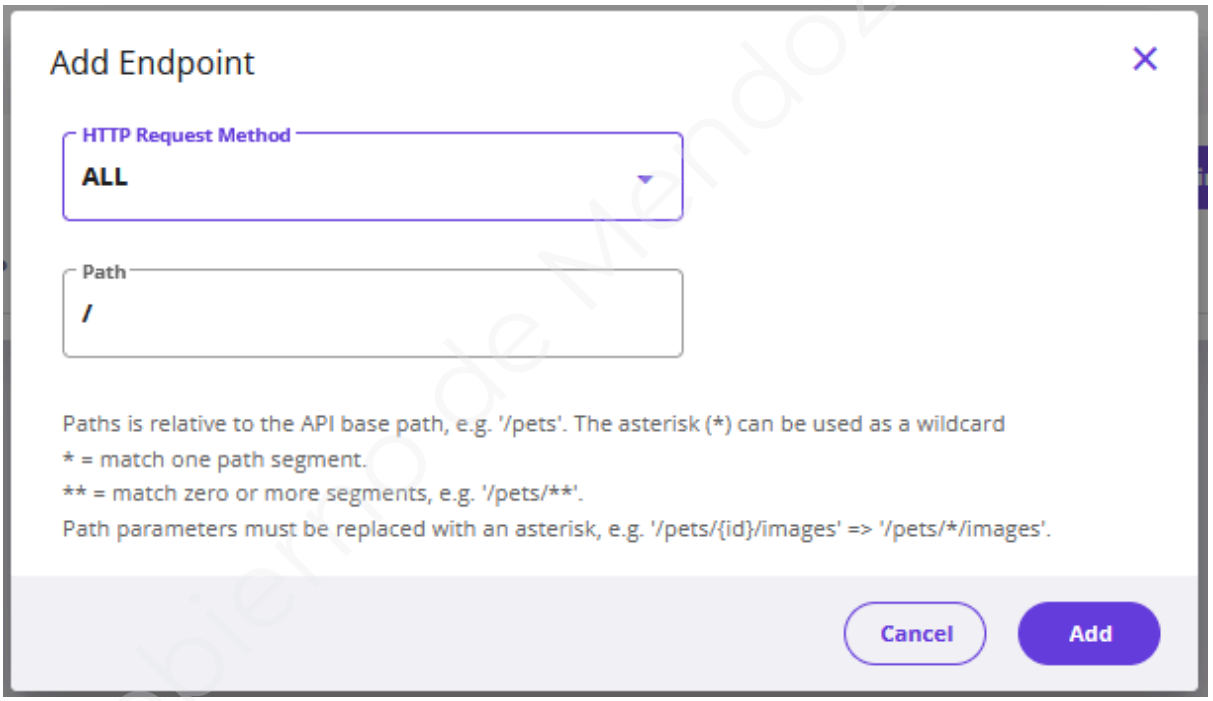
1. La solapa de Endpoints se utiliza para definir cada uno de los endpoints de una API y poder autorizar el consumo en forma individual a los distintos subsistemas.

2. Modificar el tiempo máximo de duración de llamado al servicio -en segundos (se encuentra preestablecido por defecto).

3. Verificar el certificado TLS (se encuentra activo por defecto cuando el servicio es https). En el caso de que se deje activado, para consumir el servicio se requiere del certificado del servidor de seguridad. Se aclara que es un certificado por aplicación o sistema de información.

4. Añadir/quitar subsistemas habilitados para consumir el servicio

Respecto al punto 1 (añadir endpoints), se observa la siguiente pantalla:



Al hacer click en Add Endpoint, añadir el tipo de llamado (GET/POST/PUT/DELETE) y el endpoint específico.

IMPORTANTE: como se visualiza en la imagen, los parámetros que se envían mediante URL deben sustituirse por asteriscos (*). La cantidad de asteriscos estará determinada por los parámetros a ingresar.

Para que se apliquen los cambios de los puntos 2 y 3, se debe hacer click en “Save”, de lo contrario se perderá la configuración seleccionada.

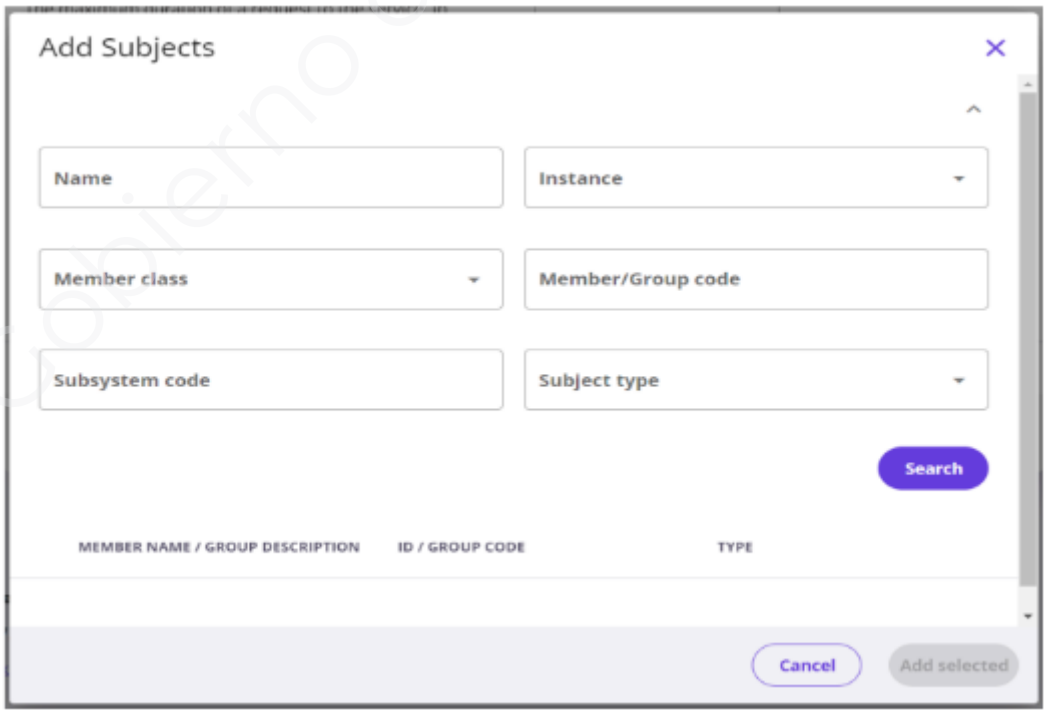
El método de conexión para los servidores de red internos en el rol de proveedor de servicios está determinado por el protocolo en la URL del extremo del servicio.

El protocolo en la URL del servicio puede ser HTTP o HTTPS. Cuando se utiliza HTTPS, la casilla de verificación "Verificar certificado TLS" alterna la verificación del certificado cuando se establece una conexión TLS. De acuerdo con los parámetros del servicio, la conexión con el servidor de la red interna se crea utilizando uno de los siguientes protocolos:

- HTTP: la URL del servicio/adaptador comienza con "http://...".
- HTTPS: la URL del servicio/adaptador comienza con "https://" y la casilla de verificación Verificar certificado TLS está seleccionada. Antes de que se pueda usar HTTPS, se debe descargar el certificado TLS del servidor web y cargarlo en el servidor de seguridad.
- HTTPS NO AUTH: la URL del servicio/adaptador comienza con "https://" y la casilla Verificar certificado TLS no está seleccionada.

En el EDI-Mendoza cada proveedor de servicios es dueño de sus datos y responsable de los derechos de acceso a cada servicio, es decir que disponibilizar el servicio no significa que automáticamente se encuentra accesible para todas las organizaciones miembro, sino que se debe administrar esos accesos de servicio al subsistema.

Para añadir consumidores (4), se puede buscar mediante algún dato o tocando el botón “Search”, lo que devolverá todos los subsistemas existentes en el ecosistema (y los ecosistemas federados) para elegir a cuál otorgarle el permiso.



Recomendaciones para implementar la comunicación segura en EDI Mendoza

Consumidores o clientes de servicios

Las aplicaciones consumidoras de servicios deben utilizar un certificado TLS. Cada aplicación cliente deberá tener su propio certificado, preferentemente en formato pfx, protegido con una passphrase.

En la aplicación antes de invocar el servicio se debe abrir el archivo pfx, utilizando la passphrase para poder acceder al contenido y agregar el certificado a las credenciales del objeto que ejecuta el Request HTML.

En el servidor de seguridad se debe dar de alta al certificado público correspondiente a la aplicación cliente en la solapa Internal Servers, dentro del subsistema que representa a la aplicación cliente.

El organismo responsable de administrar el servidor de seguridad o nodo deberá proveer los certificados TLS para cada aplicación que actúe como consumidora de servicios.

Proveedores de servicios

Las aplicaciones que publiquen servicios o APIs deben publicarlo en un servidor de aplicación que tenga habilitado el protocolo https, para lo cual el servidor debe contar con un certificado TLS válido.

En el servidor de seguridad se debe dar de alta el certificado público del servidor de aplicación en la solapa Internal Servers del subsistema donde se define el servicio.

Al definir un servicio que utiliza https, se debe marcar la casilla “Verify TLS certificate” para que se realice la verificación del certificado del servidor al momento de establecer la comunicación desde el servidor de seguridad.

Dentro de la aplicación que implementa el servicio web o API, también se debe validar el certificado del servidor de seguridad, este certificado se puede exportar desde la solapa Internal Servers para que el servicio web o API pueda utilizarlo para comparar los datos internos o para agregarlo en un almacén de “certificados reconocidos” del sistema operativo o servidor de aplicación.

La generación de los certificados TLS de los servidores de aplicación es responsabilidad del organismo que publica los servicios.

Para ambos casos:

Si el organismo miembro no tuviera los recursos necesarios para generar los certificados, la Dirección de Informática y Comunicaciones deberá prestar asistencia para generar los certificados para los servidores de aplicación.

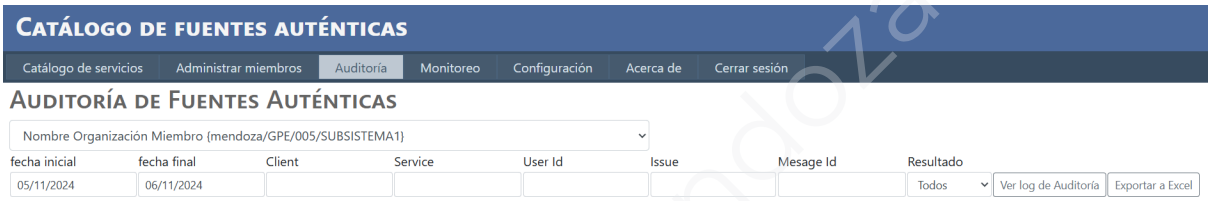
El organismo responsable debe controlar la vigencia de los certificados para renovarlos en el momento que sea necesario y volver a agregarlos al servidor de seguridad.

Plataforma de auditoría y administración del catálogo

Los gestores del servidor de seguridad también tendrán un acceso a la auditoría y monitoreo del mismo. Desde allí podrán visualizar el tráfico que ocurre entre sus subsistemas y el resto del ecosistema.

Los accesos para el sitio web https://xroadauditoria.mendoza.gov.ar serán entregados al responsable técnico del organismo miembro.

Auditoría



En la solapa “Auditoría” podrá acceder al reporte de las transacciones realizadas por cada uno de los subsistemas que pertenecen al organismo miembro.

Para visualizar el registro deberá filtrar por fecha inicial, fecha final y resultado. Otros filtros son posibles para la búsqueda de transacciones específicas.

Monitoreo

Permite la verificación de los parámetros operativos del servidor de seguridad, tales como el espacio físico de memoria, carga de procesamiento, espacio libre de memoria y otros datos del sistema operativo.

Catálogo de Fuentes Auténticas

El catálogo de fuente auténtica tiene como objetivo publicitar los servicios o APIs que se encuentran disponibles en EDI-Mendoza, para que las entidades públicas o privadas que deseen consumirlas puedan realizar las gestiones correspondientes para su acceso. Comprende la lista de servicios publicados por los organismos miembros a través de sus subsistemas.

El catálogo proporciona información detallada sobre cada servicio o API expuesta en el EDI-Mendoza, incluyendo descripción, métodos de acceso, parámetros requeridos, documentación funcional, etc.

Cada responsable técnico de servidor de seguridad (Nodo) es el encargado de cargar la información y documentación de los servicios o APIs publicadas, para ello deberá contar con una clave de acceso que será otorgada por el operador del sistema de Integrabilidad, para cumplir con tal requisito deberá seguir las indicaciones explicadas en el título: “Administrar Miembros”.

Cualquier organismo miembro puede solicitar el acceso de los servicios que desea consumir, por medio del responsable de gestión del organismo miembro proveedor.

Administrar Miembros

En la pestaña de Administrar Miembros deberá ingresar con sus credenciales para acceder a la lista de subsistemas pertenecientes al organismo miembro.

Allí podrá seleccionar un subsistema para visualizar la lista de servicios disponibles en el ecosistema.

Es responsabilidad de todas las organizaciones miembro, al disponibilizar un servicio en el servidor de seguridad (Nodo), agregar en el catálogo información relevante, como documentos funcionales y descripciones sobre el mismo.

Para ello deberá seleccionar el servicio y presionar el botón “Editar datos del servicio”.

Para que el servicio sea publicado en el Catálogo de Servicios es necesario completar todos los campos que se detallan a continuación:

- Descripción: Alcance del servicio y objetivos funcionales de manera resumida.
- Parámetros: Definición sobre los parámetros de entrada que requiere el consumo del servicio.
- Respuesta esperada: El resultado del servicio para el caso de éxito.
- Responsables del servicio: Persona a cargo de atender las solicitudes de consumo y mantenimiento del servicio, se debe cargar en este campo el correo electrónico donde se recibirán dichas consultas.
- Documento adjunto: Documentación técnica con mayor nivel de detalle para su consumo, descargar la documentación de Ejemplo.
- URL para solicitud de consumo: si el organismo miembro tiene establecido un canal de comunicación y gestión de las peticiones de autorización para consumo del servicio puede indicar en este campo la URL correspondiente.
  De otro modo, se establece el siguiente formulario para la solicitud de autorización a la Dirección de Informática y Comunicaciones.

Una vez completos los campos, el sistema permitirá seleccionar la casilla “¿Mostrar en el catálogo?” En caso de no seleccionarla el servicio no será visible en el Catálogo de Fuentes Auténticas.

Consumo de Servicios

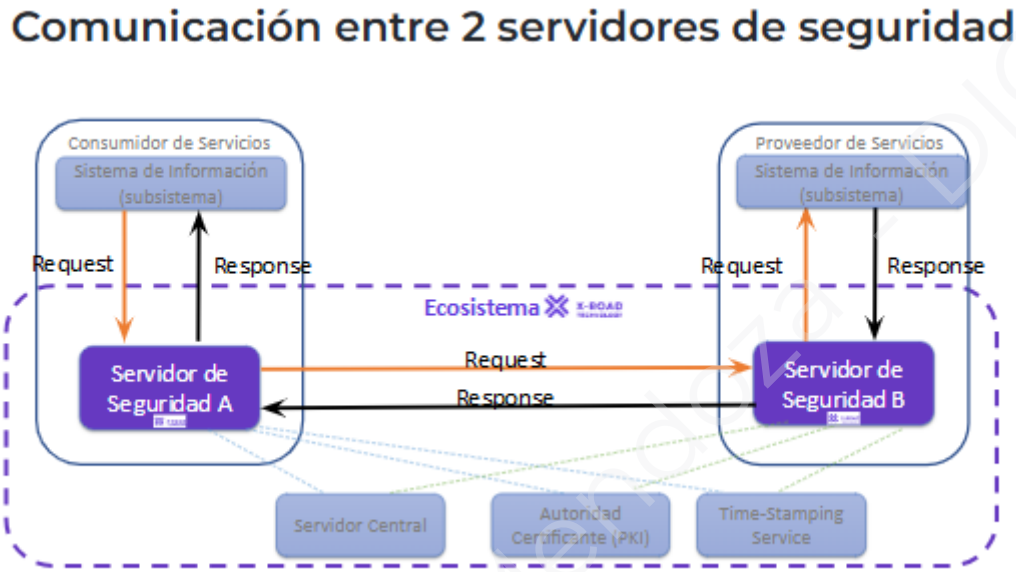
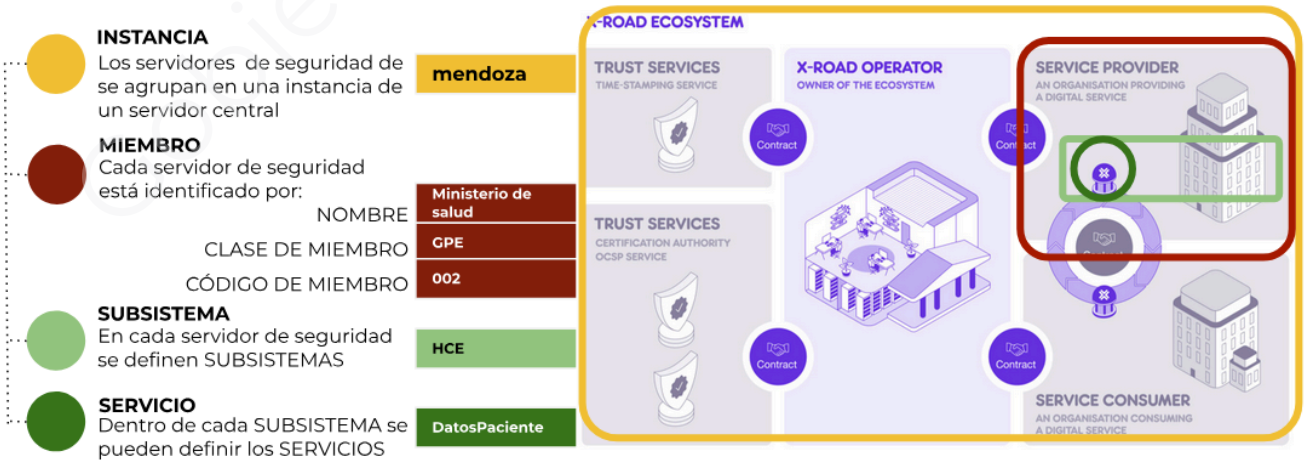


Gráfico de ruteo de servicios

Para poder generar la URL del servicio a consumir se ingresan los datos dependiendo el FQDN del servidor desde el cuál se están consumiendo.
Así mismo, el tipo de conexión “ConnectionType” va a depender de cómo tenga configurado el subsistema consumidor, esta configuración se visualiza en la solapa ”Internal Servers” dentro de cada subsistema.



Ruta completa al servicio: mendoza/GPE/002/HCE/DatosPaciente

Composición de URL:

[ConnectionType]://[FQDN_SecurityServer_Consumer]/[protocoloXRoad]/[instancia]/[MemberClass_Provider]/[MemberCode_Provider]/[SubsystemCode_Provider]/[ServiceCode]

https://hostservidorseguridad.mendoza.gov.ar/r1/mendoza/GPE/002/HCE/DatosPaciente

Ejemplo práctico:

En el siguiente cuadro, tenemos los datos correspondientes a la configuración de diferentes Servidores de Seguridad y sus subsistemas registrados y si tienen algún Service Code agregado o no.

Miembro	FQDN Servidor de Seguridad	protocolo & instancia	Member Class	Member Code	Subsistem Code	Service Code
Educación	iopdge.mendoza.gov.ar	r1/mendoza	GPE	005	GEM	-
Salud	iopsalud.mendoza.gov.ar	r1/mendoza	GPE	007	SAMEP	-
Registro Civil	iopregcivil.mendoza.gov.ar	r1/mendoza	GPE	010	PARTIDAS	FechaDef

A continuación, se muestra cómo se define la URL para consultar el Servicio Web de Fecha de defunción del sistema de PARTIDAS del Registro Civil desde distintos consumidores:

SecurityServer Consumidor	URL	valor del encabezado: X-Road-Client
Educación	https://iopdge.mendoza.gov.ar/r1/mendoza/GPE/010/PARTIDAS/FechaDef	mendoza/GPE/005/GEM
Salud	https://iopsalud.mendoza.gov.ar/r1/mendoza/GPE/010/PARTIDAS/FechaDef	mendoza/GPE/007/SAMEP

Encabezados

Adicionalmente, para poder consumir servicios a través del Ecosistema Digital de Integrabilidad, se deberá agregar (además de los headers que pueda tener el servicio web en sí) los siguientes encabezados:

- X-Road-Client
- X-Road-Issue
- X-Road-UserId

X-Road-Client

El HEADER “X-Road-Cient” como key y en el value se deberá cargar el ID del subsistema (Ej. mendoza/GPE/005/TEST) que se ha habilitado como consumidor.
La Key siempre va a ser la misma (“X-Road-Client”), el valor va a depender del nombre del subsistema habilitado como consumidor.

Key: X-Road-Client

Value:
[ecosistema]/[MemberClass]/[MemberCode_Consumer]/[SubsystemCode_

Consumer]

Si el subsistema ha sido configurado con conexión HTTPS debe asegurarse de agregar a la petición el envío del certificado correspondiente, de lo contrario el servicio responderá con el siguiente error:


```
{
    "type": "Server.ClientProxy.SslAuthenticationFailed",
      "message": "Client (SUBSYSTEM:mendoza/GPE/005/TST) specifies HTTPS but did not supply TLS certificate",
    "detail": "50e2b7a0-548b-4b08-849b-69a337365a03"
}
```


Si el subsistema ha sido configurado con conexión HTTPS pero no se ha cargado ningún certificado en la solapa de ”Internal Server TLS” el servicio responderá con el siguiente error


```
{
    "type": "Server.ServerProxy.SslAuthenticationFailed",
    "message": "Client (SUBSYSTEM:mendoza/GPE/005/TST) has no IS certificates",
    "detail": "50e2b7a0-548b-4b08-849b-69a337365a03"
}
```


X-Road-Issue

El encabezado “X-Road-Issue” como key y en el value se deberá cargar un identificador de la transacción único que origina el pedido de datos.

La implementación de la Cabecera “X-Road-Issue” permite registrar su valor en la base de datos de Auditoría de X-Road, permitiendo identificar unívocamente cada transacción. Lo cual es sumamente útil para lograr una trazabilidad de la transacción (issue) cuando se trata de varios servicios que colaboran entre sí mediante el intercambio de mensajes.

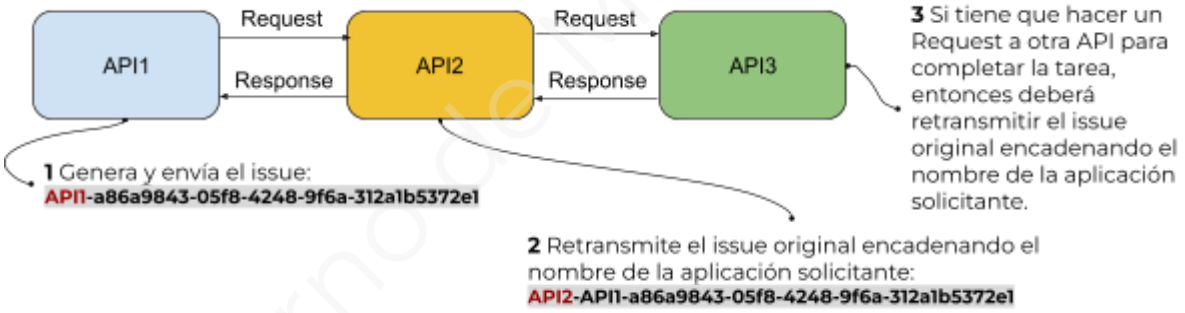
Para generar el X-Road-Issue se recomienda utilizar UUID (Universal Unique Identifier) en su versión 4. Se sugiere agregar el nombre de la aplicación que genera el issue. El nombre de la aplicación se debe anteponer al código UUID generado.

Por ejemplo:

X-Road-Issue: NombreApp-a86a9843-05f8-4248-9f6a-312a1b5372e1

Si la aplicación que genera el issue tiene su propia base de datos de auditoría, puede almacenar el UUID junto con la información enviada en la petición HTTP.

En el caso de una tarea encadenada, donde intervienen varias aplicaciones, es necesario registrar la trazabilidad del issue. Esto suele darse en casos donde varias aplicaciones colaboran entre sí mediante el intercambio de mensajes, por ejemplo:



En este ejemplo, puede observarse en el punto 2) que la API2 no necesita generar un nuevo issue, ya que para cumplir la tarea solicitada por la API1, tiene que hacer una nueva petición a la API3 y retransmitir el issue original para que X-Road registre la trazabilidad completa del mismo.

X-Road-UserId

Este encabezado permite identificar al usuario que opera el sistema que origina la solicitud de datos a través de X-Road. Dependiendo del servicio desplegado puede implementarse su uso como herramienta de autorización a nivel de aplicación.

Buenas prácticas y Recomendaciones

Funcionales

Uso ético de datos

El organismo miembro dueño del servicio, debe analizar las solicitudes que recibe de otros OM, y cumplir con las leyes de protección de datos personales al habilitar cualquier acceso.

Se deben establecer un ANS - Acuerdo de Nivel de Servicio LINK.

Ante el incumplimiento o mal uso de los servicios por parte de la organización habilitada para consumirlo, la organización proveedora tiene la potestad para suspender o revocar el acceso al mismo.

Uso eficiente de datos

En la utilización de los servicios o APIs, se busca promover el uso de sistemas de validaciones para romper con la lógica de transporte de documentos entre diferentes sistemas utilizando efectivamente la información en beneficio de la sociedad en su conjunto, asegurando un equilibrio adecuado entre la disponibilidad de datos y la utilización de criterios simples (SI/NO) para reducir no solo el tiempo de carga de información del ciudadano sino el chequeo de ésta por parte de la entidad que recibe la información.

Minimizar el pedido de información al ciudadano

Principio Once Only (Sólo una vez)

Uno de los principios fundamentales del EDI-Mendoza es:

- No solicitarle al ciudadano un documento o dato que el mismo ya lo haya provisto alguna vez a alguna entidad tanto público como privada.

Lo que significa que, en la medida de lo posible, el sistema debe aprovechar las fuentes de datos existentes y simplificar el pedido al ciudadano de información que pueda obtener mediante un servicio web que lo otorgue automáticamente.

Mecanismos para corregir datos

Es necesario que el sistema ofrezca canales claros y fácilmente accesibles que permitan a los usuarios rectificar cualquier información incorrecta. Asimismo, se debe tener en cuenta la posibilidad de que, al realizar la consulta, el sistema o el servicio web pueda no estar operativo, o que la información no esté disponible debido a deficiencias en la base de datos o en la calidad de los datos.

que en algunos casos puede estar incompleta. En consecuencia, es esencial implementar las medidas necesarias para evitar que esto obstaculice el avance en el proceso de trámite, permitiendo que se pueda llevar a cabo de la misma manera que antes de la validación automática.

Técnicas

Desarrollo de servicios web

Un buen diseño de la estructura y organización de datos, es esencial para que los consumidores puedan entender fácilmente cómo interactuar con el servicio web. A continuación se detallan recomendaciones para su desarrollo.

- Tipo REST: Adoptar el estilo arquitectónico REST para su API proporciona una interfaz uniforme y fácil de usar.
- Buen manejo de errores: Implementar un manejo de errores robusto que brinde mensajes claros y significativos. Los códigos de estado HTTP adecuados y los mensajes de error descriptivos ayudan a los usuarios a comprender y solucionar problemas.
- Multiplicidad de endpoints: Proporcionar varios endpoints que permitan a los usuarios realizar diferentes acciones. Utilizar parámetros claros y específicos para cada endpoint, facilitando así las consultas y operaciones.
- Limitar la información exponencial: Evitar exponer demasiada información en las respuestas. Diseñar el servicio o API para que los usuarios puedan obtener solo la información necesaria. Usar opciones como filtros y campos de selección para controlar los datos devueltos.
- Utilización de datos estructurados: Proporcionar datos estructurados que puedan ser utilizados directamente para validaciones. Esto mejora la eficiencia y reduce el ancho de banda necesario para las solicitudes.
- Documentación funcional completa: Se debe crear una documentación completa del servicio, que incluya detalles sobre el objetivo del servicio, la descripción, los endpoints, los parámetros necesarios, códigos de respuesta, y ejemplos claros de solicitudes y respuestas. Además, es necesario especificar las instrucciones de consulta.
  La documentación debe ser comprensible para que los desarrolladores puedan integrar fácilmente el servicio o API en sus aplicaciones. Consultar el modelo de documentación (Agregarlo como Anexo).
  Es importante que no se agreguen en la documentación las URL originales que no incluyen la capa de seguridad del EDI-Mendoza

Estas prácticas y requisitos mínimos garantizan una API bien diseñada, fácil de usar y que cumple con las necesidades de los usuarios de manera eficaz.

Mantenimiento y soporte

El mantenimiento y soporte de cada servicio que se provee es responsabilidad del organismo miembro proveedor del servicio.

Es crucial entender que el proveedor del servicio no solo es responsable de la disponibilización y gestión de permisos de sus servicios, sino también de su funcionamiento continuo y de la calidad de los servicios proporcionados. Es importante que tenga en cuenta los siguientes puntos a la hora de ofrecer un servicio dentro del EDI-Mendoza;

- Actualización continua: Mantener actualizada la base de datos. Las actualizaciones de la infraestructura tecnológica, en el caso que las haya, deben ser planificadas y ejecutadas de manera que no interrumpan el servicio para los usuarios finales.

- Integridad y calidad de datos: Implementar medidas rigurosas para garantizar la integridad y calidad de los datos almacenados y transmitidos.
  Esto implica la validación constante, la limpieza de datos y la adopción de estándares de calidad reconocidos. La precisión y confiabilidad de los datos son fundamentales para el buen funcionamiento del servicio o API.

- Monitoreo y resolución de problemas: Realizar un monitoreo constante de los servicios para detectar posibles problemas en tiempo real. Además, se espera que se cuente con un equipo de soporte dedicado que pueda abordar rápidamente cualquier problema reportado por los usuarios finales. La resolución oportuna y efectiva de problemas es esencial para mantener la satisfacción del cliente.

- Evaluación y mejora continua: Realizar evaluaciones periódicas para identificar áreas de mejora en el servicio web. Los comentarios de los usuarios y las métricas de rendimiento deben ser considerados para implementar mejoras continuas en la funcionalidad y calidad del servicio.

Comunicación transparente

Mantener una comunicación abierta y transparente con los usuarios finales. Cualquier interrupción planificada, actualización importante o problema de calidad de datos debe ser comunicado de manera clara y anticipada.
La transparencia contribuye a establecer la confianza con los usuarios y demuestra el compromiso del proveedor con la calidad del servicio.

Es fundamental contar con referentes definidos para cada Servidor de Seguridad (Nodo) con el fin de asegurar la efectividad y la comunicación constante en el entorno del ecosistema. Estos referentes brindan a los usuarios una clara dirección sobre a quién recurrir en caso de requerir apoyo técnico y/o asesoramiento. Asimismo, se establece un canal directo para resolver problemas y facilitar la coordinación entre diferentes entidades dentro del ecosistema.

Datos de contacto

Para consultas sobre este material u otros temas relacionados al EDI Mendoza, puede comunicarse vía correo electrónico a xroad@mendoza.gov.ar.