VERSIONES

Fecha	N° de Versión	Detalle
2026/02/24	1.2.0	Creación del manual

MANUAL DE USO

2026

ÍNDICE

INTRODUCCIÓN

El siguiente manual proporciona una guía completa y detallada sobre X-BA, el sistema de interoperabilidad implementado en la Ciudad de Buenos Aires. El objetivo principal es facilitar la comprensión y aplicación por parte de los usuarios. Se presenta dividido en 6 secciones:

Sección 1: Sistema de Interoperabilidad
Esta sección se enfoca en resaltar la relevancia de los sistemas de interoperabilidad, explorando aspectos cruciales como su definición, implementación a nivel mundial, y el caso específico del Sistema de Interoperabilidad en la Ciudad Autónoma de Buenos Aires (X-BA). Proporciona una visión completa de la interoperabilidad y su aplicación práctica, subrayando la importancia de estos sistemas para la conectividad y eficiencia en situaciones del mundo real.

Sección 2: Estructura de Implementación X-BA
En esta sección, se detallan los diversos roles principales y sus responsabilidades asociadas, ofreciendo una visión completa de la arquitectura y su funcionamiento dentro de X-BA. Esto establece una base sólida para comprender la implementación del sistema y su estructura integral.

Sección 3: Adhesión como Organización Miembro a X-BA
Esta sección proporciona instrucciones detalladas para que las organizaciones se unan y participen en el Sistema de Interoperabilidad, fundamental para comprender y utilizar eficazmente X-BA. Además, se incluye un detalle técnico sobre la instalación del servidor de seguridad necesario para operar dentro del ecosistema.

Sección 4: Gestión de X-BA
En esta sección, se describen en detalle los dos sistemas de gestión para utilizar el Sistema de Interoperabilidad, incluyendo los objetivos de cada uno, sus componentes y los roles y responsabilidades asociados. Esta información es esencial para una gestión eficiente de X-BA.

Sección 5: Implementación de Casos de Uso en X-BA
Enfocándose en la implementación práctica, esta sección guía a través de los pasos desde la detección y análisis hasta la activación de un caso de uso en X-BA. Proporciona recomendaciones tanto a nivel funcional (uso de datos, experiencia de usuario, calidad de datos) como a nivel técnico (protocolos SOAP y REST, adaptación de sistemas, desarrollo de servicios web, mantenimiento y soporte).

Sección 6: Suspensión o Exclusión del Sistema de Interoperabilidad
Esta sección aborda los criterios y procedimientos para la suspensión o exclusión de una Organización Miembro de X-BA en caso de incumplimiento de obligaciones, estableciendo sanciones con el objetivo de preservar la calidad del Sistema de Interoperabilidad en su totalidad.

SISTEMA DE INTEROPERABILIDAD

A. ¿Qué es un Sistema de Interoperabilidad?

Un Sistema de Interoperabilidad es una estructura diseñada para permitir la comunicación y el intercambio de información entre diferentes entidades o sistemas, sin importar las diferencias en sus tecnologías, plataformas o protocolos, ya que establece estándares, y define mecanismos de comunicación compatibles y políticas de seguridad consistentes.

Es importante destacar que un sistema de interoperabilidad debe ser flexible y escalable, capaz de adaptarse a los cambios tecnológicos y a las necesidades futuras. Además, debe garantizar la privacidad y la protección de los datos personales, cumpliendo con las regulaciones y normativas vigentes.

Durante los últimos años, la tecnología y las comunicaciones tomaron un rol fundamental en la administración pública, logrando crear sistemas que faciliten la integración y colaboración entre distintas agencias gubernamentales, departamentos y proveedores de servicios. Su objetivo principal es facilitar el intercambio eficiente y seguro de información entre estos actores, promoviendo la transparencia, facilitando la automatización de procesos y mejorando la experiencia de los ciudadanos.

B. ¿Qué nos llevó a implementar un Sistema de Interoperabilidad?

A partir del 2009, con la política de modernización, el Gobierno de la Ciudad comenzó la transición de un modelo tradicional a uno digital, digitalizando trámites mediante portales y ventanillas virtuales. Aunque esto logró agilizar el proceso de acudir presencialmente a los departamentos gubernamentales, los ciudadanos aún enfrentan filas virtuales desde casa, navegando entre diversas plataformas y repitiendo la gestión de documentación. Con la implementación de un Sistema de Interoperabilidad se busca superar esta dinámica al eliminar la necesidad de que los ciudadanos proporcionen documentación ya en posesión de la administración pública, evitando repeticiones y avanzando hacia un Estado Inteligente.

En la adopción de un Sistema de Interoperabilidad, nos inspiramos en las experiencias exitosas de países como Suecia, Estonia e Islandia, que optimizaron los servicios gubernamentales al ciudadano al reducir costos y tiempos mediante la implementación de sistemas similares. Estonia, pionera desde el 2001, ha asegurado la confiabilidad en el intercambio de datos entre entidades gubernamentales y proveedores de servicios. Finlandia, siguiendo esta línea, ha mejorado la colaboración y reducido la duplicación de esfuerzos.

C. X-BA: el sistema de interoperabilidad de la Ciudad de Buenos Aires

En el contexto del Decreto N°118/22 GCABA y en consonancia con el Plan de Modernización de la Administración Pública de la Ciudad de Buenos Aires en el año 2022, se estableció la implementación del sistema de interoperabilidad "X-BA". Este sistema, impulsado por la Secretaría de Innovación y Transformación Digital, tiene como objetivo facilitar la comunicación y el intercambio de datos entre sistemas gubernamentales **mediante servicios web**, garantizando la seguridad y confidencialidad en el intercambio de información.

La Resolución N°303/SECITD/22 y su modificatoria N°236/SECITD/23 designaron a la Dirección General de Eficiencia Administrativa (DGEADM) para coordinar la implementación de X-BA, mientras que la Agencia de Sistemas e Información (ASI) se encarga de definir estándares y directrices conforme a la Ley N° 2.689. Además, la Subsecretaría de Políticas Públicas Basadas en Evidencia (SSPPBE) asumió la responsabilidad de elaborar lineamientos para la gobernanza de datos.

Posteriormente, mediante el Decreto 387/23 se modificó la estructura orgánica funcional del Poder Ejecutivo del Gobierno de la Ciudad de Buenos Aires, generando una nueva distribución de competencias y responsabilidades. En este contexto, el Sistema de Interoperabilidad, junto con las obligaciones previamente asignadas a la SSPPBE y a la DGEADM, fueron transferidas a la Dirección General de Gobernanza de Datos (DGGDA). Este cambio implica que la DGGDA ahora asume el rol de liderar la elaboración de políticas y lineamientos para la gobernanza de datos, y la coordinación para la implementación de X-BA.

En el año 2025, el Decreto N° 335/2025 generó un nuevo impulso para el Sistema de Interoperabilidad, definiéndolo como política del Gobierno de la Ciudad de Buenos Aires, instruyendo a las diferentes áreas a interoperar datos y abstenerse de solicitar información a los ciudadanos que la administración ya dispone o es la propia fuente auténtica.

La incorporación de X-BA como herramienta de interoperabilidad busca lograr un ahorro significativo de costos y tiempo tanto para los ciudadanos como para la administración pública en el proceso de realizar trámites y procedimientos administrativos.

ESTRUCTURA DE IMPLEMENTACIÓN X-BA

A. Roles y Responsabilidades en X-BA

El Sistema de Interoperabilidad está compuesto por tres roles fundamentales: el Operador, los Proveedores de Servicios de Confianza y las Organizaciones Miembro que se unen a esta red.

Operador del Sistema de Interoperabilidad

Es el principal responsable de la definición de políticas y protocolos en X-BA. La Secretaría de Innovación y Transformación Digital (SECITD) es la responsable de ejercer este rol, y trabajará coordinadamente con las Organizaciones pertenecientes a X-BA. Dentro de sus tareas están incluidas:

- Establecer regulaciones y prácticas para el funcionamiento del sistema.
- 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 Sistema de Interoperabilidad.
- 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 Sistema de Interoperabilidad.

Proveedor de Servicio de Confianza

Es la entidad que ofrece servicios de sellado de tiempo y certificación para la seguridad y transparencia de la herramienta. A todos los mensajes intercambiados a través de X-BA se les aplica una marca de tiempo y son registrados por los servidores de seguridad intervinientes.
Todos los nodos de los Servidores de Seguridad de X-BA requieren que les sean asignados dos tipos de certificados:

- **Certificado de Autenticación**
  Determina la identidad y asegura la conexión segura entre distintos Nodos de Seguridad dentro del Sistema.
- **Certificado de Firma**
  Todo mensaje que se comparte entre Nodos de Seguridad 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.

Para la implementación inicial del Sistema de Interoperabilidad, se definió la utilización de la PKI del GCBA para la provisión de certificados y la TSA Buenos Aires como autoridad de sellado de tiempo. A futuro el Operador del Sistema podrá autorizar autoridades de certificación provistas por otras organizaciones.

Organizaciones Miembro (OM)

Las Organizaciones Miembro en el contexto del Sistema de Interoperabilidad tienen la capacidad de producir y/o consumir servicios dentro de la red. Pueden desempeñarse como proveedores, consumidores o ambas funciones, abarcando tanto entidades de gestión pública del GCABA u otras jurisdicciones como organizaciones de gestión privada.

Cada Organización Miembro debe gestionar al menos un nodo por Servidor de Seguridad para

facilitar el intercambio eficiente de servicios digitales y debe acceder a los servicios de confianza TSA(s) y CA(s) para desencriptar y verificar la autoría de los mensajes. Es fundamental designar un Administrador de usuarios para establecer responsables de la gestión de accesos, y supervisar la operación del Servidor de Seguridad, así como garantizar el funcionamiento adecuado de los nodos y servicios hacia otros miembros dentro de X-BA.

Ser parte de X-BA implica tanto beneficios como obligaciones. Los beneficios incluyen el intercambio eficiente de datos, comunicación ágil entre organizaciones, procedimientos administrativos simplificados y la prestación de mejores servicios a los ciudadanos. Sin embargo, junto con estos beneficios, hay obligaciones, como cumplir con estándares de seguridad y privacidad, garantizar la ética y privacidad en el uso de la información, mantener la infraestructura tecnológica actualizada, lo que garantiza el correcto funcionamiento del sistema en su totalidad. y, en caso de incompatibilidades, el operador del sistema puede suspender a las Organizaciones Miembro.

Es importante destacar que, frente a la detección de incompatibilidades conforme a estas obligaciones, el operador del sistema tiene la potestad de suspender a Organizaciones Miembro que formen parte del Sistema de Interoperabilidad.

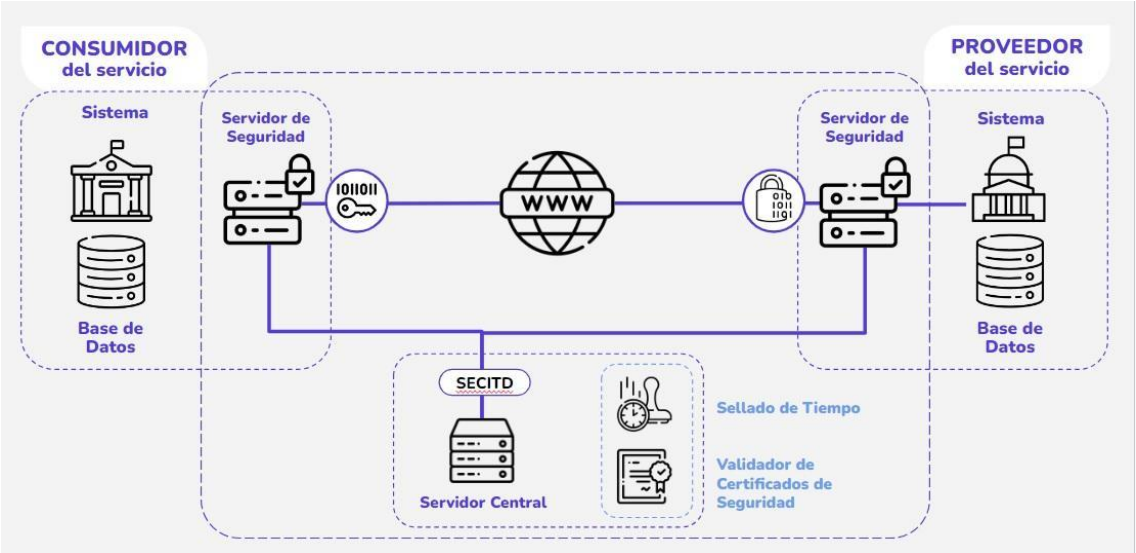
B. Arquitectura

El Sistema de Interoperabilidad se basa en una arquitectura descentralizada que permite a diferentes sistemas de información comunicarse entre sí a través de servicios web, de manera segura y estandarizada. La misma consta de los siguientes componentes clave:

- **Servidor Central**
  Es el componente central del sistema. El mismo administra y coordina todas las transacciones entre las organizaciones miembro. Sus funciones incluyen la autenticación, autorización, registro de eventos y registro de auditoría.
- **Miembros**
  Los miembros son organizaciones, instituciones gubernamentales o empresas que participan en la red. Cada miembro tiene al menos un servidor de seguridad que actúa como puerta de entrada y salida para proveer o consumir datos a través de servicios web.
- **Subsistemas**
  Dentro de cada miembro, existen subsistemas que representan sistemas de información individuales. Los subsistemas se registran en el Servidor Central y pueden proporcionar y/o consumir servicios.
- **Servicios**
  Son los servicios web 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.
- **Derechos de Acceso**
  Se deben realizar acuerdos formales que especifiquen las condiciones bajo las que los servicios pueden ser utilizados. Definen la autorización y restricciones de uso.
- **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 registran en un registro de auditoría para garantizar la trazabilidad.

La arquitectura del Sistema de Interoperabilidad, en una instancia básica entre dos Organizaciones Miembro con servidores de seguridad que funcionan con nodos únicos, sigue el siguiente esquema:



En instancias complejas, el Sistema de Interoperabilidad contendrá múltiples Organizaciones Miembro, dónde si bien se conectarán a la red 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 el principio de Alta Disponibilidad.

Cuando una Organización Miembro, a través de un subsistema consumidor desea consultar un servicio web de otro subsistema proveedor, perteneciente a otra Organización, a través del Sistema de Interoperabilidad, se sigue el siguiente flujo:

1. Autenticación: El subsistema consumidor se autentica mediante su certificado digital. El Servidor Central verifica la identidad y los privilegios del solicitante.
2. Solicitud: El subsistema consumidor envía una solicitud al subsistema proveedor, indicando qué servicio desea utilizar.
3. Autorización: El Servidor Central verifica si el consumidor tiene autorización para acceder al servicio específico. Esto se basa en los derechos de acceso definidos.
4. Procesamiento de la Solicitud: El subsistema proveedor procesa la solicitud y genera una respuesta.
5. Respuesta: El resultado se envía de vuelta al subsistema consumidor a través del Módulo Central.
6. Registro de Auditoría: Cada paso de la transacción se registra en el registro de auditoría para fines de trazabilidad y seguridad.

Esta arquitectura ofrece varios beneficios, incluyendo:

- **Seguridad**
  Garantiza transacciones seguras y autenticadas mediante certificados digitales.

- **Flexibilidad**
  Facilita la comunicación entre sistemas heterogéneos.
- **Gobernanza**
  Su estructura descentralizada permite que la fuente auténtica de los datos tenga control sobre los accesos a sus servicios.
- **Eficiencia**
  Reduce la duplicación de datos y procesos, lo que ahorra tiempo y recursos.
- **Trazabilidad**
  Registra todas las transacciones para auditoría y seguimiento.

ADHESIÓN COMO ORGANIZACIÓN MIEMBRO A X-BA

A. Proceso de registro como Organización Miembro

Las Organizaciones Miembro (OM), como se detalló anteriormente, son entidades o instituciones que forman parte de X-BA, 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 Ciudad de Buenos Aires u otras jurisdicciones, o Entidades Privadas. Dependiendo de esto, deben seguir las acciones detalladas a continuación.

Entidades Públicas dependientes de la Ciudad de Buenos Aires

El primer contacto debe realizarse vía mail a sistemadeinteroperabilidad@buenosaires.gob.ar, expresando la voluntad de formar parte de X-BA. Se coordinará una primera reunión entre ambas partes para realizar la presentación formal del proyecto.

Una vez decidida la incorporación como Organización Miembro, la máxima autoridad de la entidad interesada deberá enviar mediante SADE una Comunicación Oficial (CCOO) con el acrónimo NOSOM dirigida al Secretario de la Secretaría de Innovación y Transformación Digital, o a la máxima autoridad del organismo que a futuro la reemplace. En la misma, es necesario que se establezcan la/s persona/s que será/n responsable/s de la gestión y monitoreo del Servidor de Seguridad. Lo ideal es que, además de alguien técnico, se designe un responsable de gestión que pueda tomar decisiones sobre los servicios a habilitar y lo que no. Para registrarlos, se requerirá el CUIT y un mail para enviar las credenciales de acceso al Servidor.

Cuando la Comunicación Oficial haya sido atendida, se considerará que la Organización se ha integrado a X-BA. En este proceso, los Gestores del Servidor de Seguridad recibirán una capacitación detallada sobre la arquitectura de X-BA. Durante esta formación, se abordarán aspectos como la creación de Subsistemas, la configuración de accesos para que otras Organizaciones Miembro consuman servicios, así como otros procedimientos pertinentes.

El ente puede optar por instalar su servidor de seguridad en infraestructura propia, si la tuviera, siguiendo el procedimiento que se detalla en la siguiente sección, o solicitar la instalación del mismo en la infraestructura de la Agencia de Sistemas de Información de GCBA (ASI).

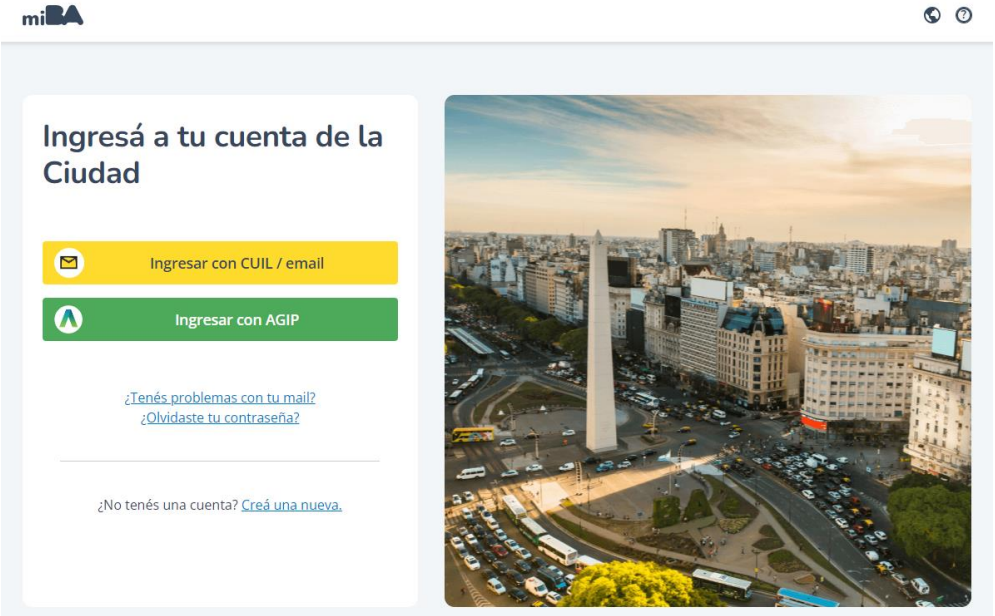
Entidades Públicas de Otras Jurisdicciones o Entidades Privadas

El primer contacto debe realizarse vía mail a sistemadeinteroperabilidad@buenosaires.gob.ar, expresando la voluntad de formar parte de X-BA. Se coordinará una primera reunión entre ambas partes para realizar la presentación formal del proyecto.

La suscripción de un Convenio constituye un requisito fundamental para que una entidad adquiera la condición de Organización Miembro, siendo un hito clave en el proceso de integración. A continuación, se describen los pasos para dar inicio a este procedimiento:

Se debe Iniciar el Trámite vía TAD, accediendo a: https://tad.buenosaires.gob.ar/tramitesadistancia/nuevo-tramite:

El trámite deberá ser iniciado por el Representante Legal de la Entidad, que también debe ser apoderado en TAD, ya que será quien posteriormente firmará el Convenio.



Se debe buscar el trámite "Solicitud para ser Organización Miembro – X-BA". Dentro del trámite, se encuentran dos botones: uno para ver los detalles, incluyendo pasos y documentación necesaria, y otro para iniciar la tramitación.

Al hacer click en “Iniciar Trámite”, se dará inicio al mismo y se podrá cargar la documentación necesaria.

La documentación obligatoria es la siguiente:

1. Nota del interesado en ser parte del Sistema de Interoperabilidad. Dentro de los detalles del trámite encontrará un archivo modelo adjunto.
2. Estatuto Constitutivo.

3. Inscripción en IGJ.
4. Acta de Designación de Autoridades (Si hubiera facultades delegadas, es necesario acompañar Poder de Representación debidamente certificado)
5. DNI del firmante (frente y dorso). En caso de tener nivel 2 o 3 en miBA al momento de loguearse en el sistema, el mismo se validará automáticamente a través de X-BA.
6. Modelo de convenio: se encuentra dentro del detalle de trámite. Sólo se deben completar los campos correspondientes y adjuntarlo -sin firmar-.
7. Declaración Jurada.

La documentación tendrá que estar en formato PDF y en el caso de la Nota del interesado, tendrá la posibilidad de firmarlo digitalmente. De no contar con el certificado para firmar, tendrá que completarlo, imprimirlo, firmarlo holográficamente y subirlo en el campo correspondiente.

Tener en cuenta que el Representante Legal de la persona jurídica que firme la nota, deberá ser la misma que firme el Convenio posteriormente.

Luego de que el área de legales analice toda la documentación, se solicitará mediante notificación por TAD, que se impriman 3 ejemplares y se firmen de forma ológrafa, para luego ser enviado a la dirección designada. Una vez recibido el convenio, la máxima autoridad del organismo responsable de X-BA (SECITD) lo firmará y se adjuntará al expediente previamente creado. Se notificará a la entidad sobre la recepción del convenio y se le enviará una copia del mismo.

Para llevar a cabo la instalación del Servidor de Seguridad, el que estará alojado en la infraestructura de la entidad, se establecerá la comunicación por correo electrónico con los referentes técnicos responsables. Se proporcionará un manual instructivo para guiar al equipo técnico en el proceso de instalación, manteniendo un contacto constante para garantizar el éxito en esta etapa del proceso.

B. Instalación de Servidor de Seguridad

Para completar el proceso de convertirse en Organización Miembro después de la aprobación administrativa y la confirmación del Operador de X-BA, es necesario avanzar con la instalación del Servidor de Seguridad. Esta fase implica una colaboración estrecha entre el responsable técnico de la Organización Miembro y el Operador del Sistema de Interoperabilidad, requiriendo una comprensión sólida de la plataforma y la infraestructura de la entidad.

<u>Requisitos tecnológicos</u>

Sistema Operativo (SO): Red Hat Enterprise Linux (RHEL) versión 8 - Red Hat Enterprise Linux release 8.7 o superior.
Procesador (CPU): 64-bit dual-core.
Almacenamiento (Disco): 60 GB.
Memoria RAM: 4 GB.
Red: Tarjeta de interfaz de red de 100 Mbps.

<u>Preparación del hardware</u>

Asegúrese de que el servidor cumpla con los requisitos mínimos de hardware, incluida la capacidad de almacenamiento, la memoria RAM y la capacidad de procesamiento.

Sistema operativo

X-Road es compatible con varios sistemas operativos, como Linux y Windows Server. Seleccione el sistema operativo más adecuado y realice una instalación limpia. En este caso, se recomienda Red Hat Enterprise Linux (RHEL) versión 8 - Red Hat Enterprise Linux release 8.7 o superior.

Conexión a Internet

Asegúrese de que el servidor tenga acceso a Internet para descargar actualizaciones y componentes necesarios.

Instalación del Servidor de Seguridad

Descarga de X-Road: Visite el sitio web oficial de X-Road para obtener la versión más reciente y la documentación relacionada con la instalación.

Instalación del software: Siga las instrucciones proporcionadas en la documentación para instalar X-Road en el servidor. Esto generalmente implica la ejecución de comandos en la línea de comandos o el uso de un asistente de instalación.

Configuración inicial

Defina un nombre único para el servidor de seguridad, validándolo con el Operador del Sistema, quien designará un "Member Class" y "Member Code" a utilizar.

Configure las direcciones IP y los puertos para la comunicación.

Configure el almacenamiento de claves y certificados necesarios para la autenticación y seguridad.

Una vez completadas estas configuraciones, el Operador del Sistema de Interoperabilidad registrará el servidor de seguridad en el Servidor Central.

GESTIÓN DE X-BA

Para realizar las gestiones administrativas y técnicas necesarias para activar un caso de uso, se requiere acceder a dos portales distintos: el “Servidor de Seguridad (SS)” y el “Portal de Gestión de Servicios de Interoperabilidad (PGSI)”.

El Servidor de Seguridad será utilizado únicamente de manera directa, para la realización de pruebas en ambientes bajos. Es decir, aquellas organizaciones miembro que cuenten con un servidor de HML, podrán crear subsistemas y disponibilizar servicios en esa instancia. Aquellas que no disponen de un servidor de HML, deberán realizar esa gestión con el equipo de XBA.

El Portal de Gestión de Servicios será utilizado para la gestión en producción, por los gestores y administradores de cada organización miembro. A. Servidor de Seguridad (SS)

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 crear subsistemas, disponibilizar servicios, gestionar accesos y agregar certificados.

Roles, permisos y responsabilidades

Para poder acceder al SS 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:

- **Administrador del sistema**
  Responsable de la instalación, configuración y mantenimiento del servidor de seguridad.
- **Oficial de seguridad**
  Es responsable de la aplicación de la política de seguridad y los requisitos de seguridad, incluida la gestión de la configuración de claves, claves y certificados.
- **Oficial de Registro**
  Es responsable del registro y eliminación de los clientes del servidor de seguridad.
- **Administrador de servicios**
  Es responsable de gestionar los datos y los derechos de acceso a los servicios.
- **Security Server Observer**
  Puede ver el estado del servidor de seguridad sin tener derechos de acceso para editar la configuración.

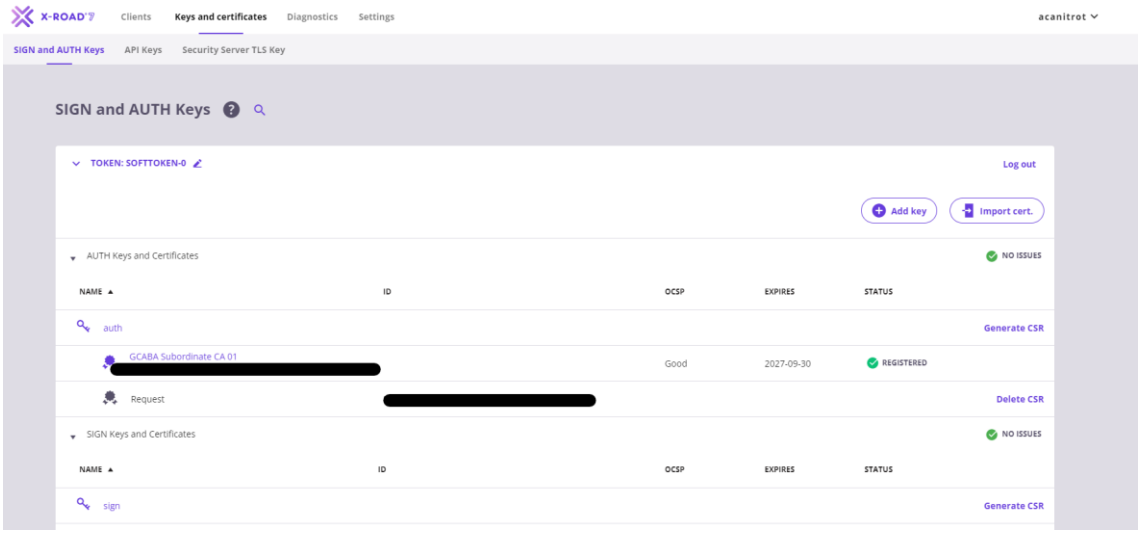
Componentes del Servidor de Seguridad

Vamos a dividir los componentes del servidor de seguridad en dos: Componentes de Configuración y Componentes de Gestión.

1. Componentes de Configuración del Servidor de Seguridad

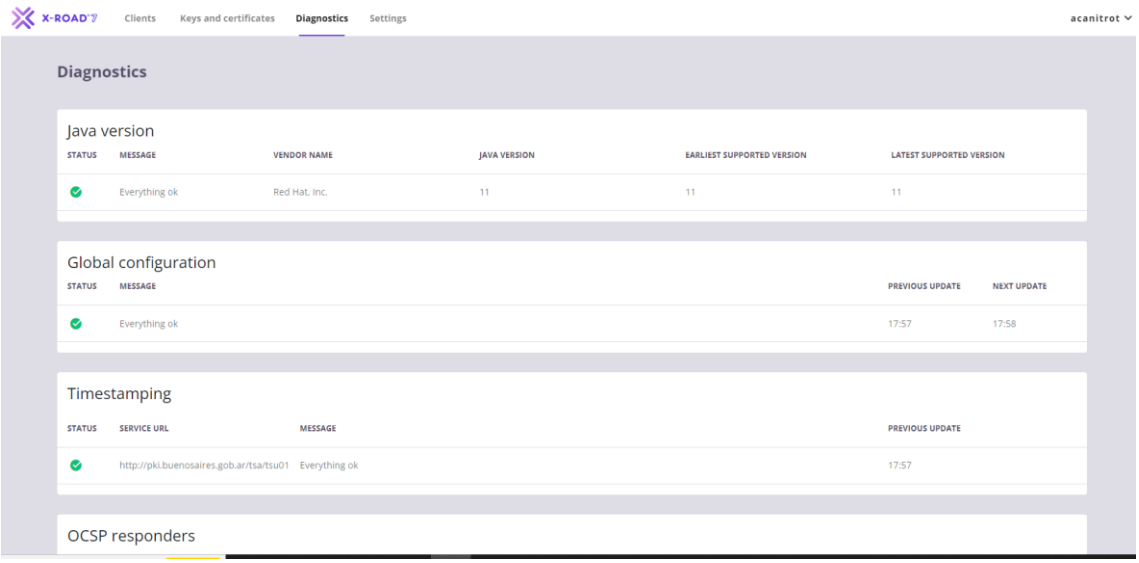
Dentro del servidor de seguridad las solapas “Keys and Certificates”, “Diagnostics” y “Settings” se deben utilizar inicialmente para la instalación del servidor de seguridad, y después es recomendable no hacer modificaciones sobre las mismas, excepto que el Operador del Sistema de Interoperabilidad lo 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.

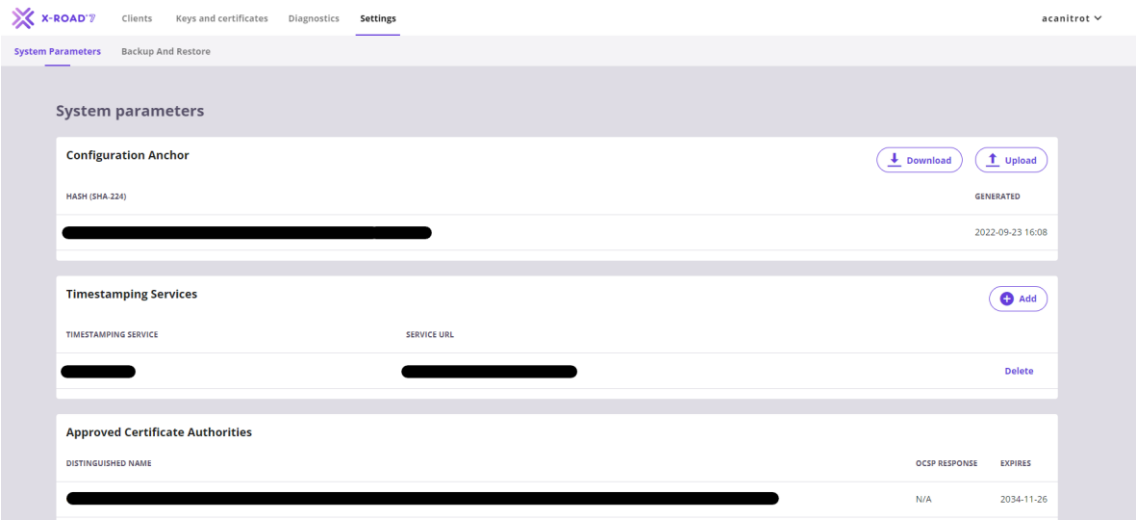
Diagnóstico (Diagnostics)



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

Los OCSP Responder hacen frecuentemente verificaciones con el Servidor Central para verificar que los certificados estén actualizados.

Ajustes (Settings)

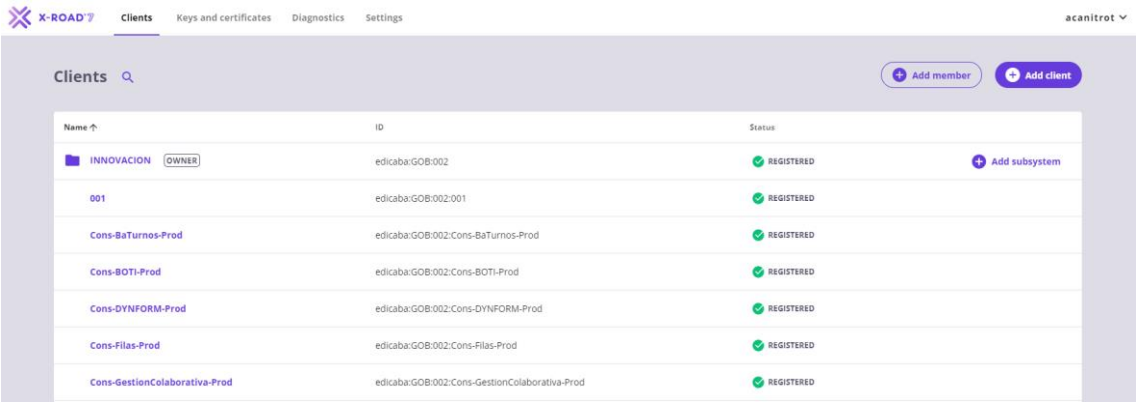


Se visualizan los parámetros del sistema. La configuración del Anchor, el timestamp y la Autoridad certificante habilitada. Todas provistas por el Gobierno de la Ciudad de Buenos Aires.

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 podemos identificar varias acciones.

Clientes (Clients)



Refiere a la Organización Miembro dueña del Servidor de Seguridad. Cabe aclarar que se pueden crear más de un cliente por Servidor de Seguridad, pero para la implementación de X-BA se va a requerir de un servidor por miembro. Por lo tanto, no se va requerir agregar miembros o clientes.

Subsistemas (Subsystems)

Los subsistemas en X-BA se definen como el medio por el que se conectan los distintos sistemas de información para el intercambio de datos. El propósito específico de cada uno puede variar entre proveer servicios o consumirlos.

Para garantizar la estandarización en la creación de subsistemas, se utiliza una nomenclatura de tres partes, dependiendo de su finalidad:

[Prov/Cons]-[SistemaDeInformación]-[Ambiente]

- Si el subsistema está diseñado para proporcionar servicios, se utiliza "Prov".
- Si el subsistema está destinado a consumir servicios, se utiliza "Cons".
- Se incluye el nombre del sistema de información con el cual se establecerá la conexión.
- Se agrega el nombre del ambiente, ya sea desarrollo (dev), calidad (qa), homologación (hml) o producción (prd).

Ejemplo Práctico:

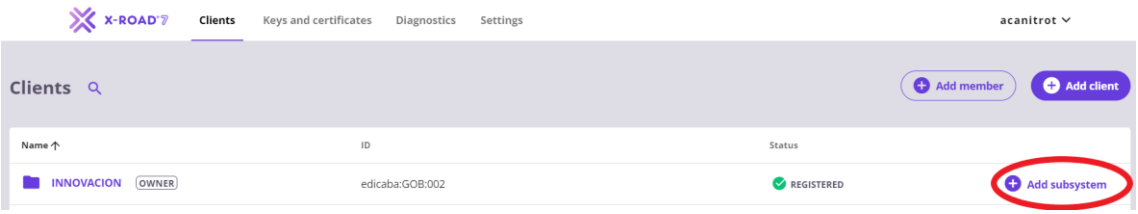
En el caso de un escenario donde el sistema "Mi Escuela" requiere consumir datos sobre "Vacunas" proporcionados por el sistema de Salud a través de SIGHEOS, y se están realizando pruebas en un entorno de calidad (QA), se crearán dos subsistemas:

Un subsistema en el servidor de Educación, llamado "Cons-MiEscuela-QA".

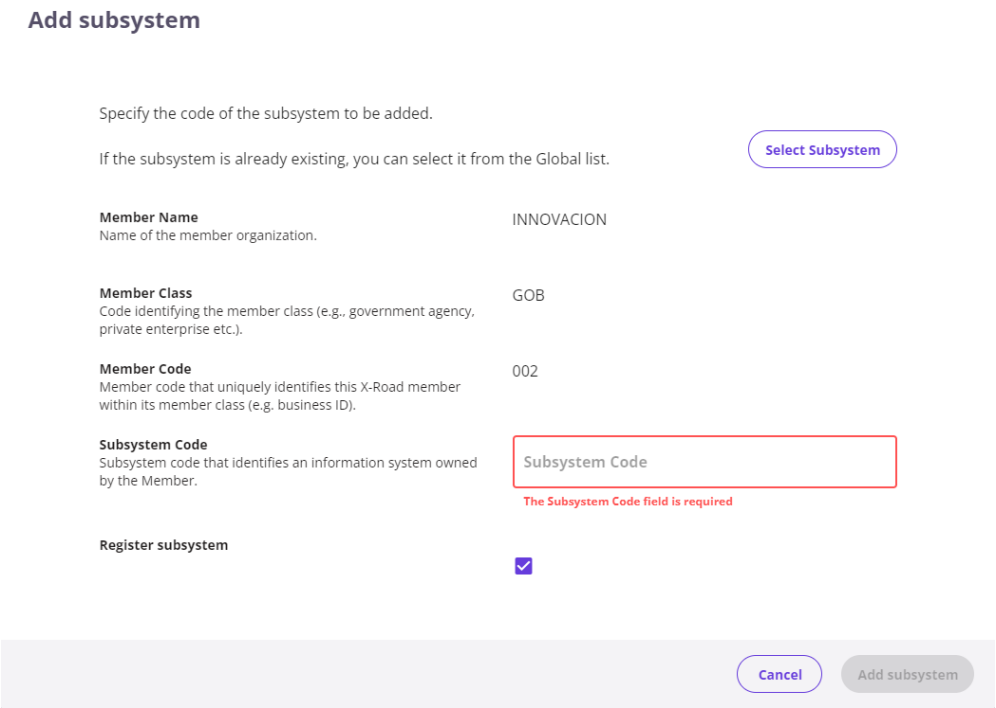
Otro subsistema en el servidor de Salud, llamado "Prov-SIGHEOS-QA".

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 entorno X-BA.

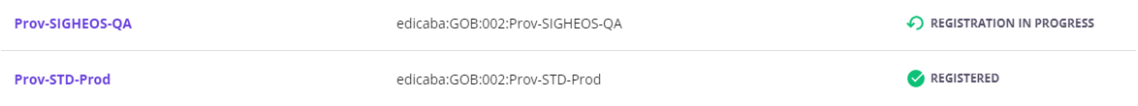
Para crear un nuevo subsistema, debe seleccionar “Add subsystem”



Asignarle en “subsystem code” un nombre con la estructura anteriormente mencionada.

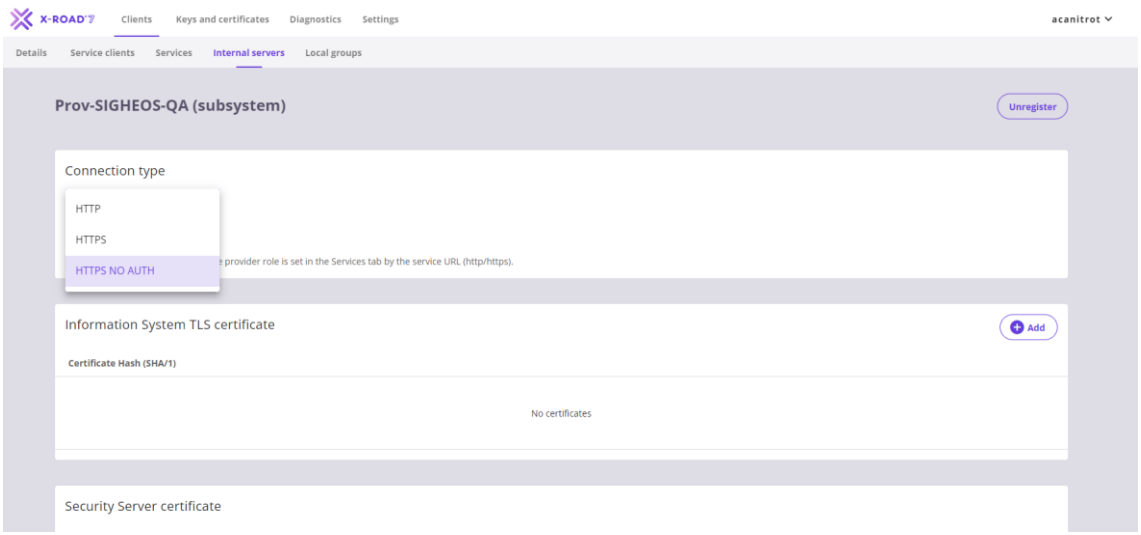


Una vez creado, se enviará la solicitud de registración al servidor central, y quedará el subsistema en el listado de “Clients”, con el estado “Registration in Progress”



Aceptada la solicitud desde el Servidor Central, aparecerá con el estado “Registered”, ya listo para ser utilizado.

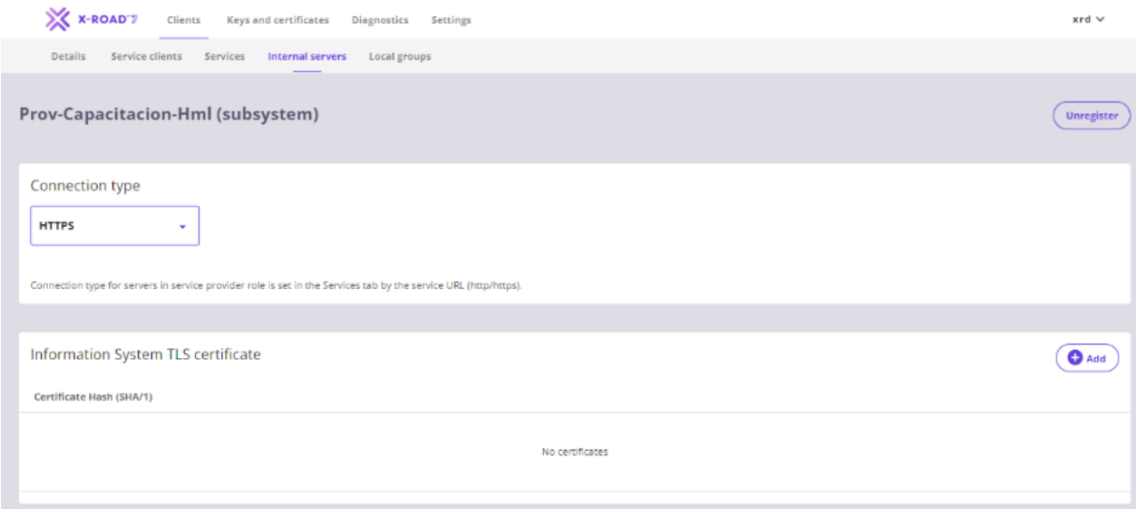
La interfaz del Servidor de Seguridad ofrece tres tipos de conexión en la solapa "Internal Servers": HTTP, HTTPS y HTTPS NO AUTH.



La elección entre HTTP, HTTPS y HTTPS NO AUTH dependerá de los requisitos de seguridad específicos de su entorno y de la sensibilidad de la información que se transmite entre los servidores. En X-BA se recomienda utilizar HTTPS NO AUTH ya que existe una cadena de confianza entre los servidores de seguridad y sus certificados autenticados.

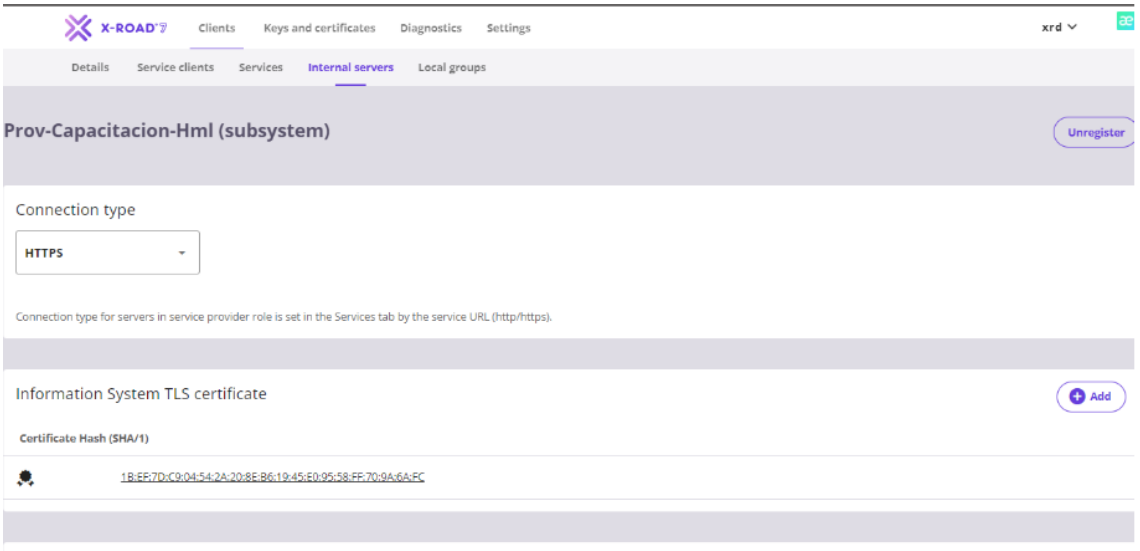
- **HTTP (Hypertext Transfer Protocol)**
  Se utiliza cuando la comunicación entre los servidores internos puede realizarse de manera abierta y sin cifrado.Puede ser adecuado para comunicaciones internas donde la seguridad no es una preocupación principal, o cuando la red interna ya cuenta con medidas de seguridad sólidas.
- **HTTPS NO AUTH (Hypertext Transfer Protocol Secure sin autenticación)**
  Se utiliza cuando la autenticación en la capa de transporte no es necesaria, pero aún se desea cifrar la comunicación. Es útil en situaciones donde la autenticación se maneja en un nivel superior, por ejemplo, a través de la aplicación o capa de aplicación.
- **HTTPS (Hypertext Transfer Protocol Secure)**
  Se recomienda cuando la seguridad de la comunicación es crucial y se requiere cifrado para proteger la información transmitida. Debería utilizarse en entornos donde la privacidad y la integridad de los datos son prioridades, especialmente cuando la comunicación se realiza a través de redes no seguras, como internet.

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, debemos seleccionar la opción “HTTPS”. Luego clickear el botón +Add dentro del campo Information System TLS Certificate y seleccionar el archivo con el certificado que se desea cargar.

Una vez cargado el Certificado nos 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, podríamos hacer una consulta de prueba contando con el archivo KEY (asociado al certificado) que debe ser cargado en la herramienta que utilicemos 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 disponibilizarán los servicios que se proveen desde el sistema de información.

En el Sistema de Interoperabilidad 'X-BA' se promueve el acceso a servicios mediante la adopción de estándares reconocidos, ofreciendo a los usuarios la posibilidad de utilizar tanto el protocolo SOAP como REST. Estos proporcionan las bases para la comunicación y el intercambio

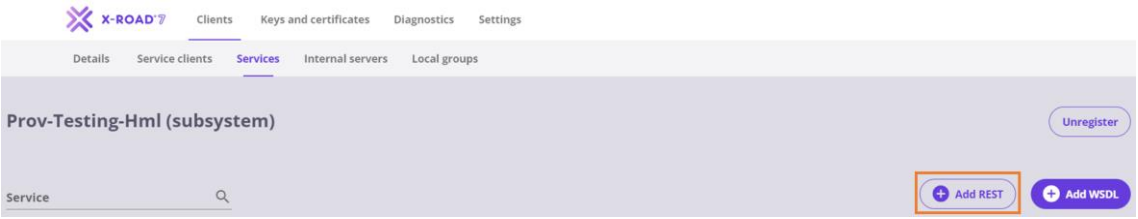
de datos dentro del sistema, permitiendo la integración entre distintas aplicaciones.

Dentro de estas opciones, se destaca la utilización del protocolo REST, el que se recomienda como la elección preferente en X-BA. Esto se fundamenta en su enfoque flexible, su simplicidad de implementación y su eficiencia en el manejo de recursos en comparación con SOAP.

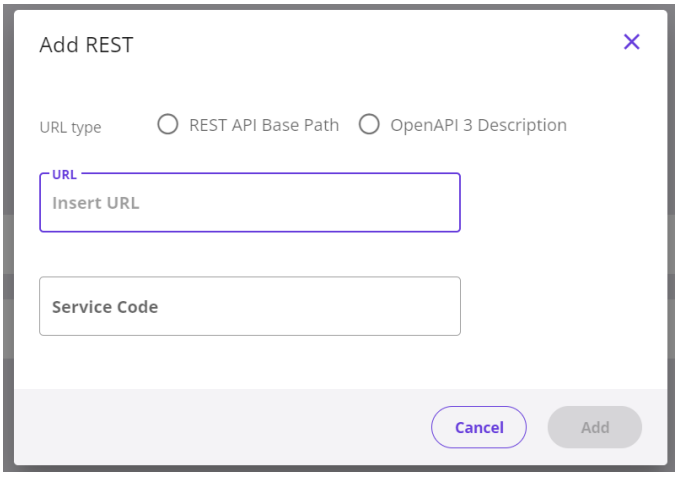
A continuación, se detallan los pasos a seguir para la publicación de los servicios en X-BA:

- **Servicios de tipo REST**

Para publicar servicios de tipo REST es necesario seleccionar un subsistema en particular y dirigirse a la solapa "Services". En la misma, seleccionar "Add REST"

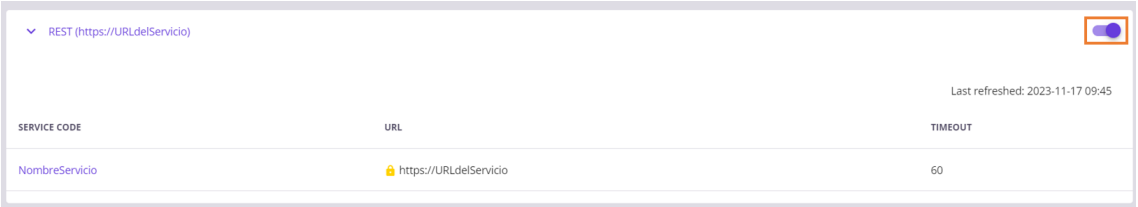


Luego se debe seleccionar la opción del tipo de URL, comúnmente se utiliza "REST API Base Path". Se debe completar con la base de la URL, en caso de que cuente con múltiples endpoints, o la URL completa si no los tuviera.



En el campo **Service Code** se le asigna una etiqueta a dicho servicio, la que servirá para conformar la URL de X-BA y realizar el llamado posteriormente.

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

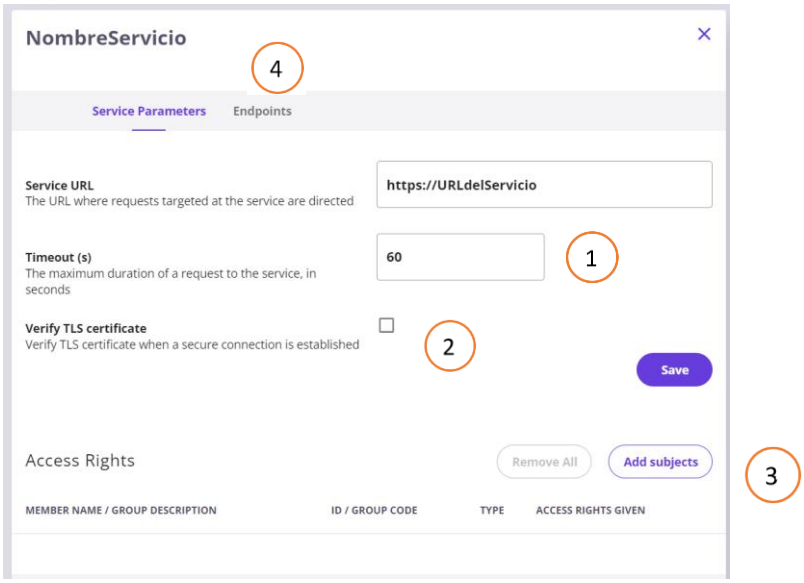


Haciendo click en el Service Code, accederemos a una pantalla que nos permite realizar distintas gestiones relacionadas al servicio.

1. Modificar el tiempo máximo de duración de llamado al servicio -en segundos- (se

encuentra preestablecido por defecto).

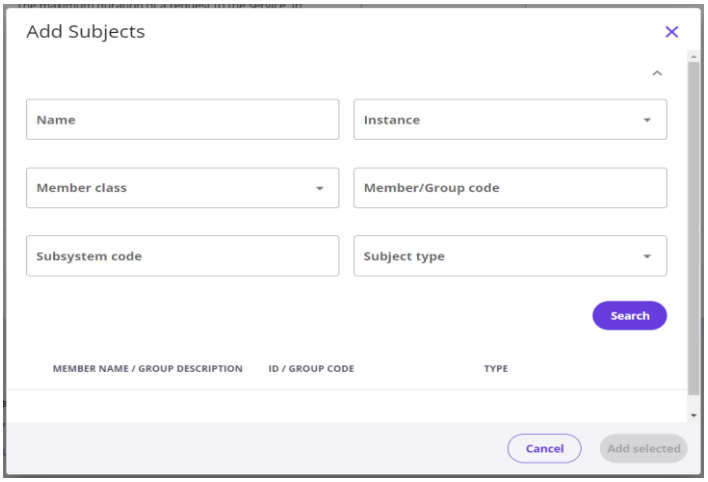
2. Desactivar el certificado TLS (se encuentra activado por defecto cuando el servicio es https). En el caso de que se deje activado, para poder consumir el servicio, se requerirá, además del certificado del servidor de seguridad, un certificado por sistema de información.
3. Añadir/quitar subsistemas habilitados para consumir el servicio
4. De ser necesario, agregar endpoints



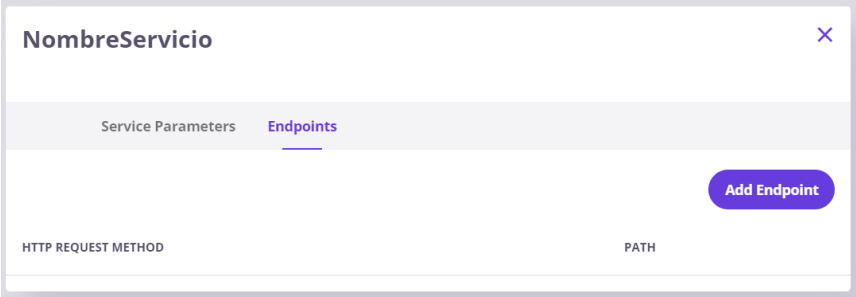
Para que se apliquen los cambios de los puntos 1 y 2, es necesario hacer click en “Save”, de lo contrario se perderá la configuración seleccionada.

La idea principal de la plataforma es que 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 deben administrar esos acceso de servicio a subsistema.

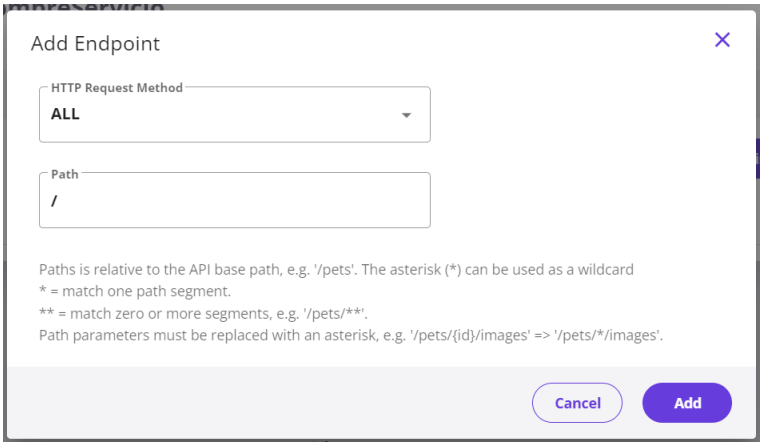
Para añadir consumidores (3), se puede buscar mediante algún dato o simplemente tocando el botón “Search”, lo que devolverá todos los subsistemas existentes en X-BA para elegir a cuál otorgarle el permiso.



Respecto al punto 4 (añadir endpoints), se observa la siguiente pantalla:



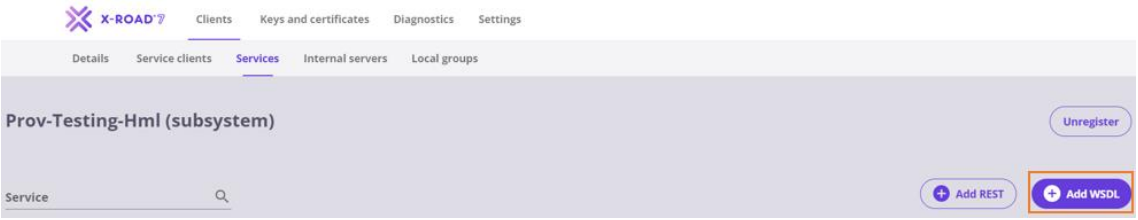
Se deberá clickear “Add Endpoint”, añadir el tipo de llamado (GET/POST/PUT/DELETE..) y el endpoint específico.



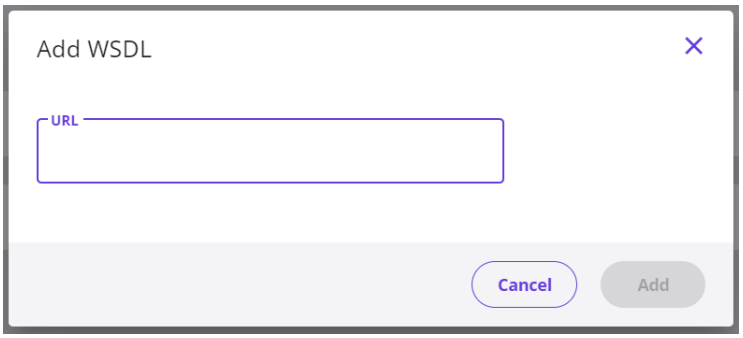
IMPORTANTE: como se visualiza en la imagen, los parámetros que se envían mediante url deben sustituirse por asteriscos (*). La cantidad de asteriscos estará determinada por los parámetros a ingresar.

- **Servicio de tipo SOAP**

Para publicar servicios de tipo SOAP es necesario seleccionar un subsistema en particular y dirigirse a la solapa “Services”. En la misma, seleccionar “Add WSDL”



Se desplegará la siguiente pantalla, en la que se deberá colocar la URL del servicio a publicar:



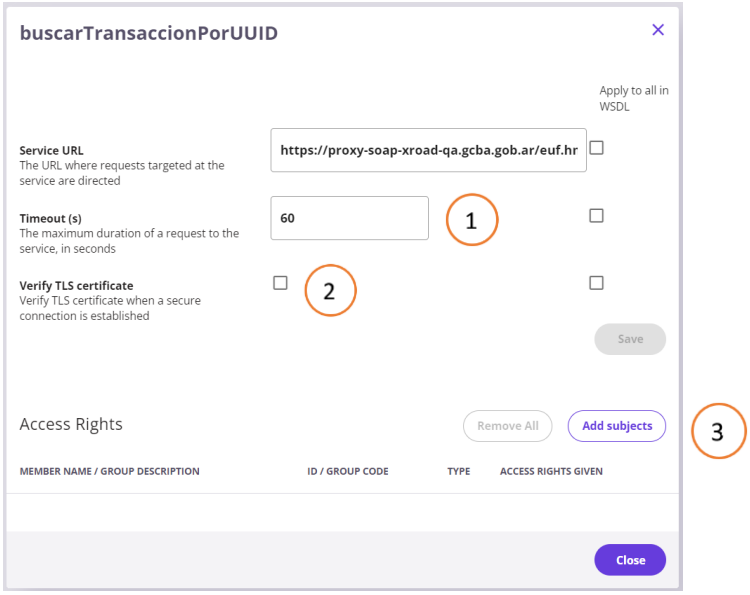
Una vez añadido el servicio, es necesario habilitarlo y, en este tipo de protocolo, se debe añadir un conector en los métodos específicos, previo a la URL, para su correcto funcionamiento:

Conector para ambientes de prueba(DEV/QA/HML): https://proxy-soap-xroad-qa.gcba.gob.ar
Conector PRD: https://proxy-soap-xroad.buenosaires.gob.ar

* (1) Método con conector | (2) método sin conector

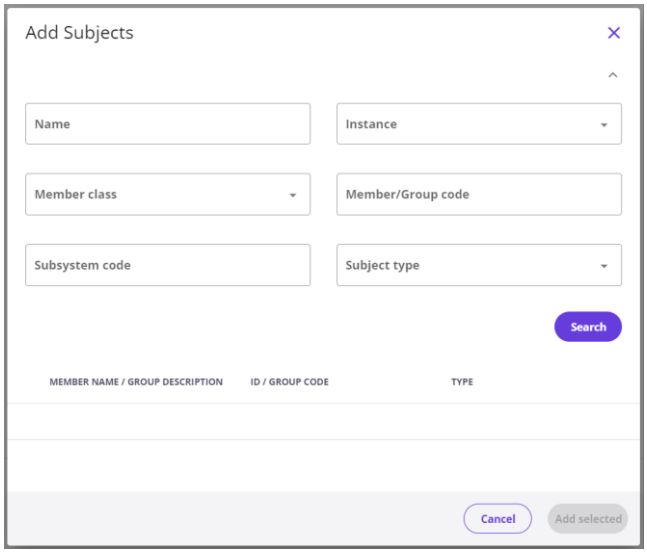
Haciendo click en el Service Code de cada método, accederemos a una pantalla que nos permite realizar distintas gestiones:

1. Modificar el tiempo máximo de duración de llamado al servicio -en segundos- (se encuentra preestablecido por defecto).
2. Desactivar el certificado TLS.
3. Añadir/quitar subsistemas habilitados para consumir el servicio



Para que se apliquen los cambios de los puntos 1 y 2, es necesario hacer click en “Save”, de lo contrario se perderá la configuración seleccionada.

Para añadir consumidores (3), se puede buscar mediante algún dato o simplemente tocando el botón “Search”, lo que devolverá todos los subsistemas existentes en X-BA para elegir a cuál otorgarle el permiso.



B. Portal de Gestión de Servicios de Interoperabilidad (PSGI)

Con el objetivo de mejorar la eficiencia en la comunicación y gestión entre las Organizaciones Miembro, se ha lanzado el Portal de Gestión de Servicios de Interoperabilidad (PGSI). Este recurso contribuye a simplificar la gestión, eliminando procesos administrativos innecesarios y optimizando el tiempo dedicado a estas tareas.

La gestión centralizada de políticas de acceso garantiza que solo los usuarios autorizados de la Organización Miembro tengan acceso al portal. Además, se mantiene un registro detallado de los subsistemas registrados en el Servidor de Seguridad, servicios en funcionamiento y solicitudes de consumo, brindando una visión completa y controlada de la actividad dentro de X-BA.

Roles y Responsabilidades en el PGSI

Para llevar a cabo la implementación de casos de uso en X-BA, es esencial realizar una adecuada gestión de accesos a los servicios ofrecidos por las Organizaciones Miembro. Con este propósito, se han establecido roles diferenciados en el Portal, cada uno con funciones específicas, que se detallan a continuación.

<u>Administrador del Sistema</u>

Es designado por la Secretaría de Innovación y Transformación Digital y realiza las siguientes tareas:

- Supervisa el funcionamiento integral del Portal, garantizando disponibilidad y rendimiento óptimo.
- Realiza auditorías periódicas para verificar el cumplimiento de normas y asegurar la integridad y seguridad de los datos.
- Mantiene actualizado el catálogo de Organizaciones Miembro y sus usuarios.
- Brinda soporte técnico y capacitación a administradores de usuarios y gestores de servidores de seguridad de organizaciones miembro.

Administrador de Usuarios de la Organización Miembro

Es designado en la solicitud de adhesión como miembro, por la máxima autoridad de cada organización, y realiza las siguientes tareas:

- Gestiona usuarios que actuarán como gestores del servidor de seguridad de la organización.
- Garantiza que estos usuarios cuenten con los permisos y accesos necesarios para realizar las gestiones correspondientes.
- Responsable de mantener actualizada y precisa la información de estos usuarios, así como de revocar permisos en caso de cambios en funciones.
- Supervisa el estado de los nodos de seguridad y tiene acceso para monitorear los servicios utilizados por el servidor de seguridad.

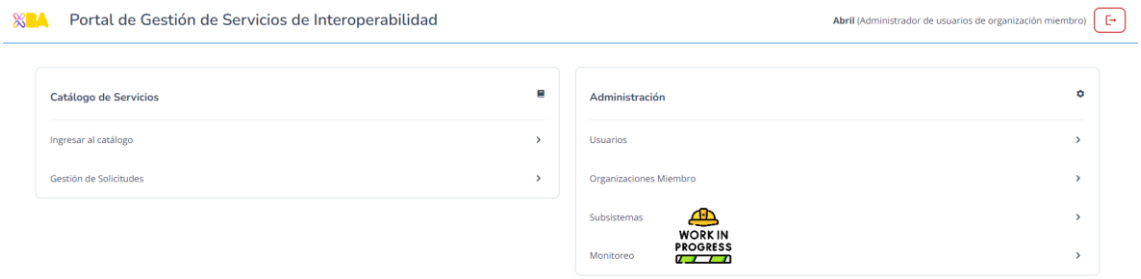
Gestor del Servidor de Seguridad

Es designado por el Administrador de Usuarios de la Organización Miembro, a través de la sección “Usuarios del portal”, y realiza las siguientes tareas:

- Administra y registra subsistemas dentro del servidor de seguridad, así como publica nuevos servicios web.
- Solicita y gestiona permisos de acceso a servicios por parte de otras organizaciones miembro a través del portal.
- Supervisa el estado de los servicios que administra.

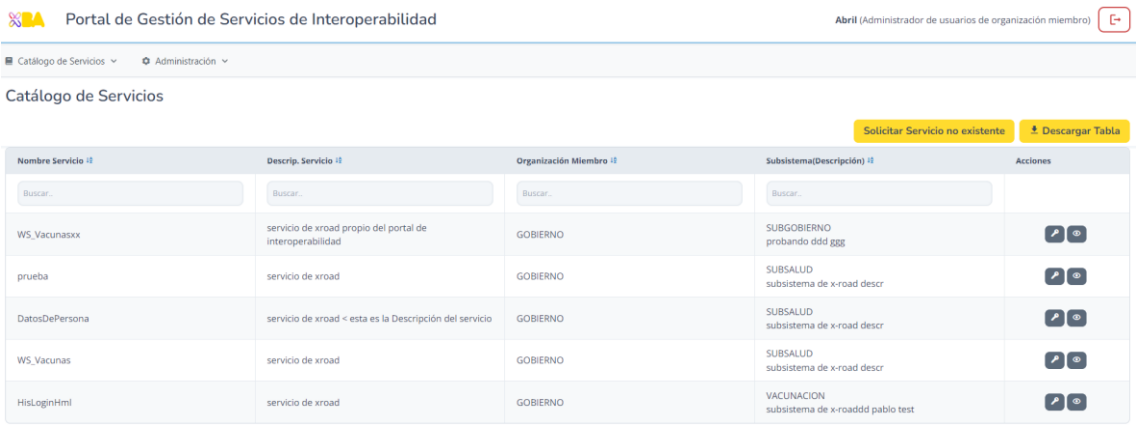
Componentes del Portal de Gestión de Servicios de Interoperabilidad

El portal está compuesto por un conjunto de componentes que fortalecen la colaboración, transparencia y la eficiencia del Sistema de Interoperabilidad.

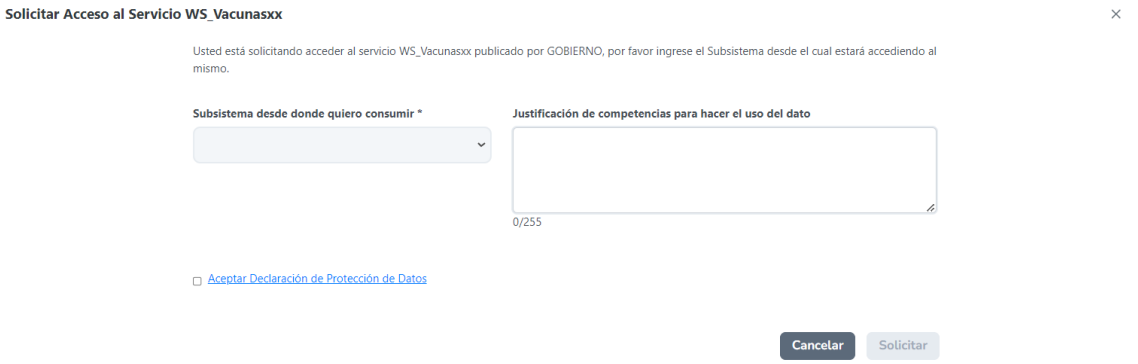


Catálogo de Servicios (CAS)

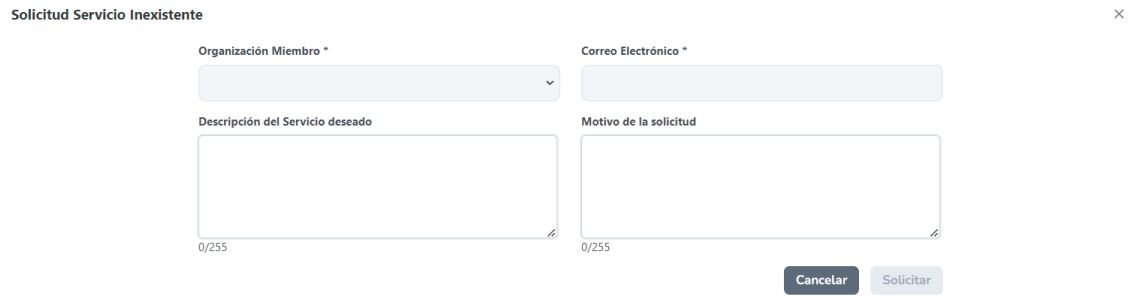
Listado de los servicios web disponibles en el Sistema de Interoperabilidad (X-BA). Estos servicios están diseñados para ser utilizados por las organizaciones miembro en sus sistemas de información. El CAS proporciona información detallada sobre cada servicio, incluyendo su descripción, métodos de acceso, parámetros requeridos, documentación funcional y cualquier información relevante.

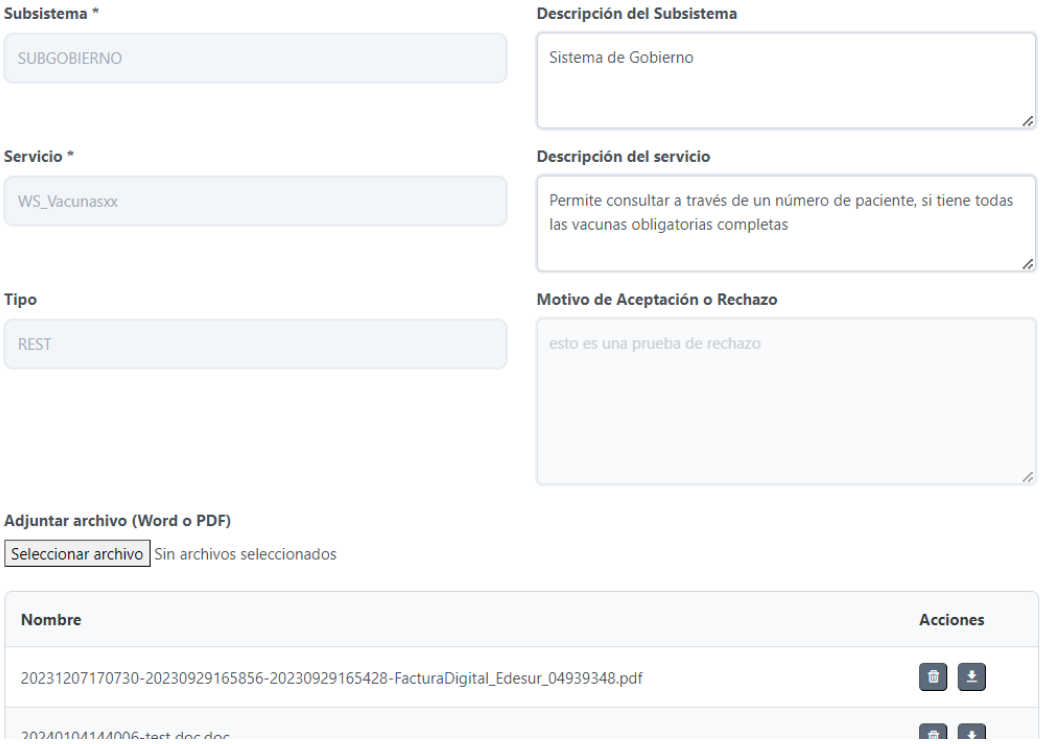


Es responsabilidad de todas las organizaciones miembro, al disponibilizar un servicio en el Servidor de Seguridad, agregar en el catálogo información relevante, como documentos funcionales y descripciones sobre el mismo.



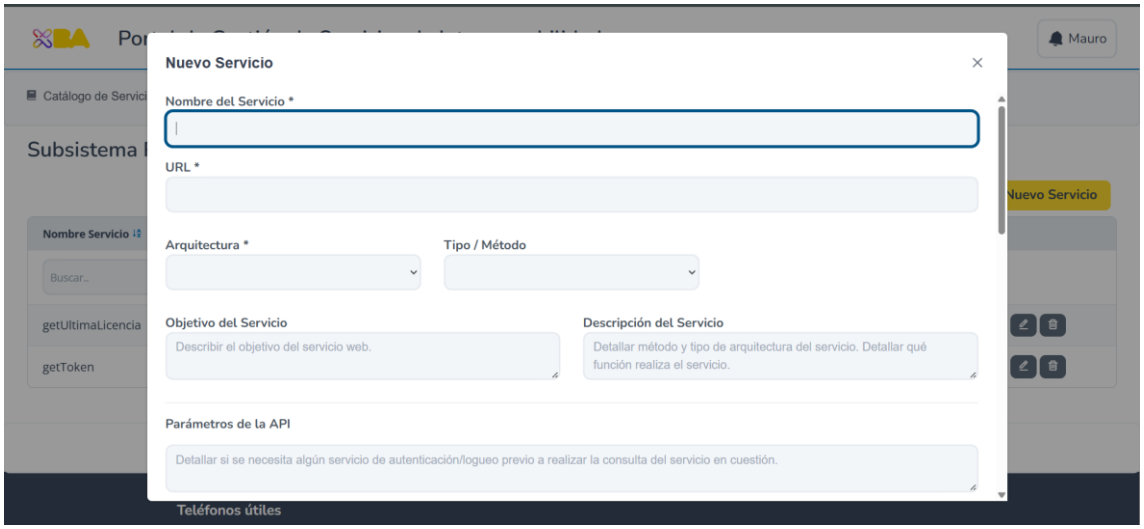
En el caso de que el servicio que se desea consumir no se encuentre disponible en el catálogo, es posible realizar una solicitud a la Organización Miembro, que es fuente auténtica del dato, para que lo ofrezca.

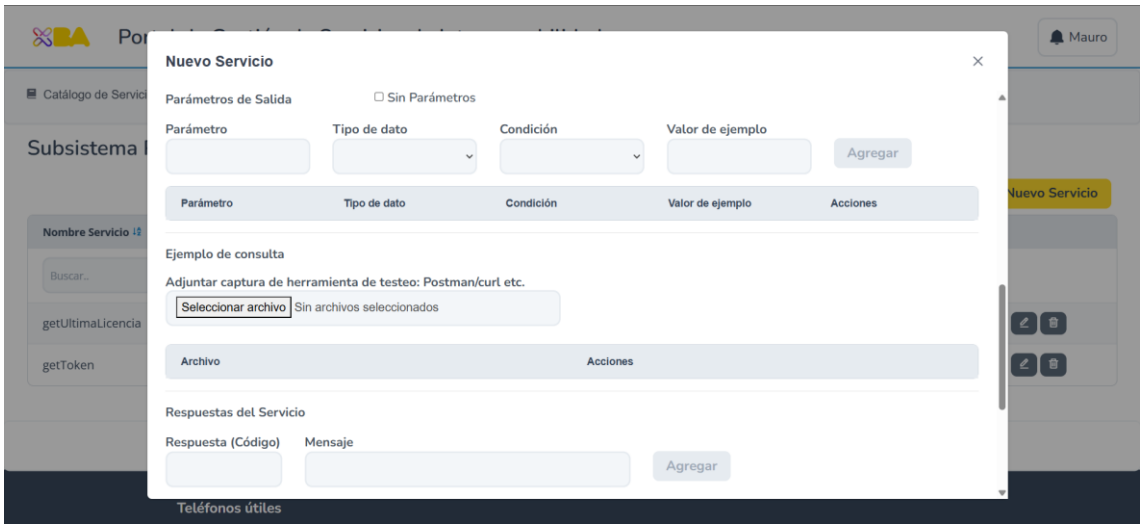


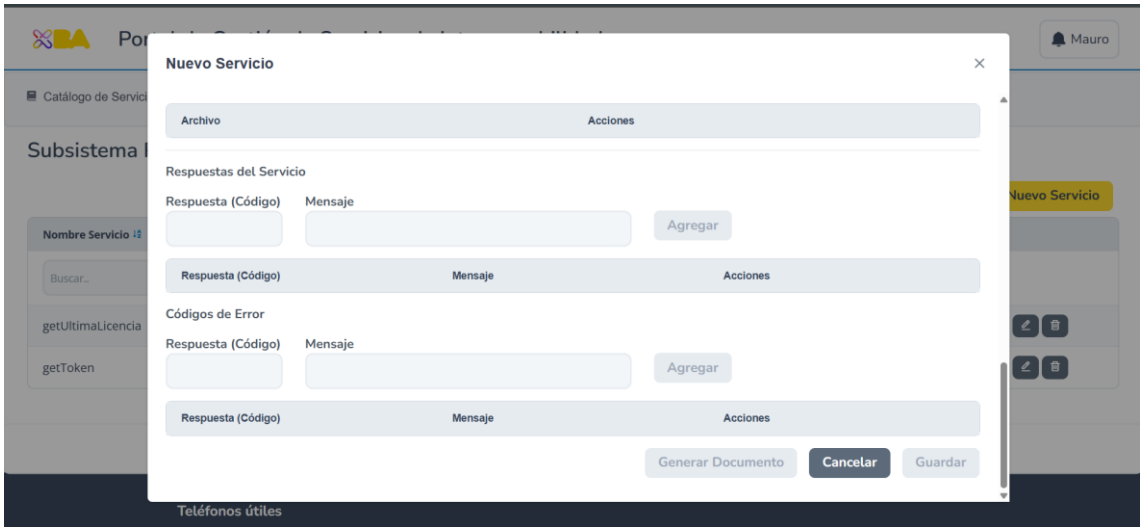


A través de este catálogo, el Gestor del Servidor de Seguridad podrá realizar las solicitudes de acceso de los servicios que desea consumir.

Dentro de los subsistemas tendremos la opción de agregar un nuevo servicio.







Se solicitará nombrar el servicio, agregar el endpoint de la API, y luego comenzar a detallar la arquitectura, método de obtención de la respuesta, el objetivo, la descripción, los parámetros de entrada y de salida, códigos y posibles respuestas. Una vez completado todo el detalle, se guardaará y se generará la documentación, lo que nos descargará un archivo ".pdf" sobre las características y funcionamiento del servicio.

Gestor de Solicitudes (GES)

Permite administrar y dar seguimiento a las solicitudes de acceso a servicios web en X-BA, agilizando la aprobación y garantizando un seguimiento eficaz.

En el mismo se podrán gestionar tanto las solicitudes emitidas por la organización miembro, las recibidas por otra organización miembro o las solicitudes de un servicio que no se encuentra publicado y que necesitan que lo desarrolle si no existe, y se lo publique para ser utilizado.

A partir de la versión 1.6.3RC se agregará al Catálogo de Servicios las opciones de ver “Mis Consumos” y “Mis Clientes”, pudiendo ver los clientes que consumen los servicios propios del Servidor de Seguridad, y los consumos del propio servidor.

En ambos casos, en la tabla se verá la columna de “acciones”, que permitirá descargar el contrato de solicitud de servicios.

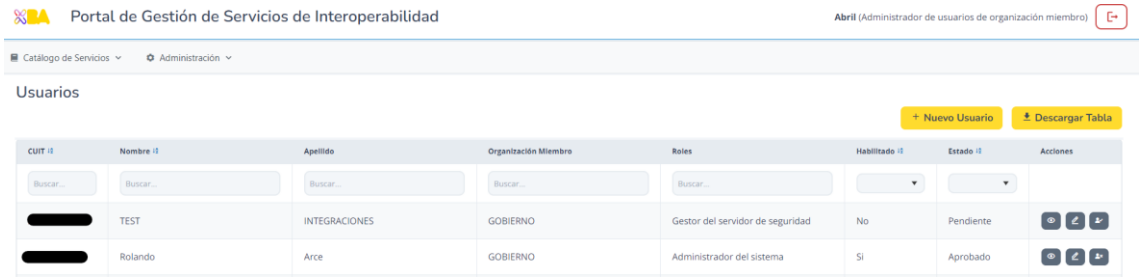
Administrador de Organizaciones Miembro (ADOM)

Permite tener un registro completo de todas las organizaciones que se han convertido en miembros del Sistema de Interoperabilidad, X-BA.

Cada organización miembro está debidamente identificada y se proporciona información de contacto de su principal referente.

Administrador de Usuarios (ADU)

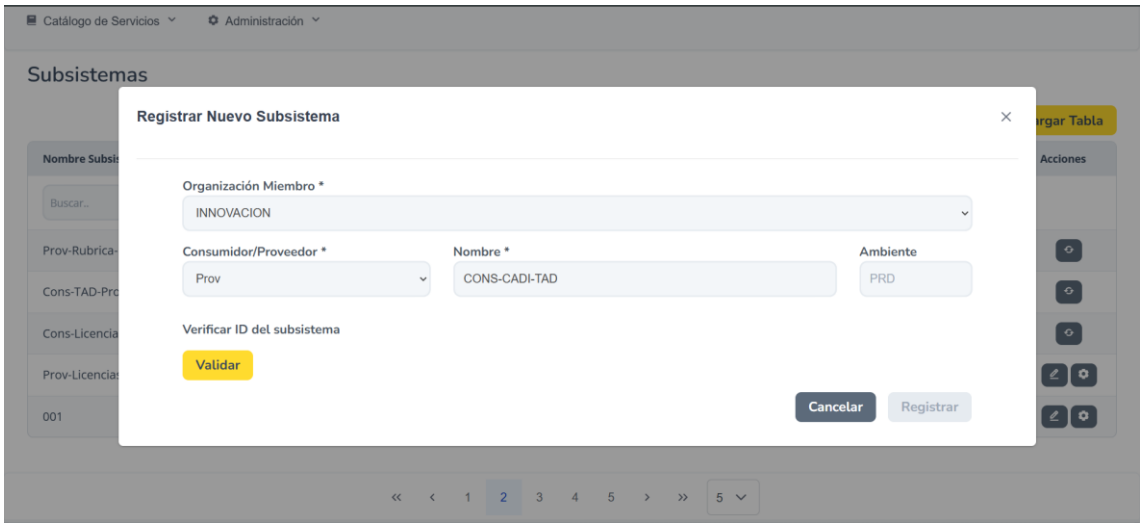
Herramienta que facilita la administración de usuarios y la asignación de permisos. Este componente permite al Administrador de Usuarios de la Organización Miembro, asignar y revocar permisos de Gestor del Servidor de Seguridad.



Administrador de Subsistemas (ADS)

Los subsistemas en producción deben administrarse desde el Portal de Gestión de Servicios y no desde la interfaz.

En la sección de subsistemas se tendrá la opción de agregar nuevo subsistema.



Vendrá predefinida la opción de consumidor o proveedor, como también el ambiente en el que se esté empleando el portal. Se selecciona “validar” para que el portal verifique que en el Servidor de Seguridad no se repita con otros subsistemas. Una vez validado, se aplica registrar el subsistema. De esta forma se obtiene un subsistema funcional.

Centro de Monitoreo (CDM)

Se encuentra en proceso de construcción. En el mismo se podrá monitorear las transacciones de los servicios que provee, y las transacciones de los servicios que consume la Organización Miembro a la que pertenece el usuario.

Para más detalle, es posible consultar el manual del Portal de Gestión de Servicios de Interoperabilidad: Portal de Gestión de Servicios de Interoperabilidad

IMPLEMENTACIÓN DE CASOS DE USO EN X-BA

Como Organización Miembro de X-BA, con un servidor de seguridad instalado, ya es posible avanzar con la implementación de un caso de uso, entendiendo este cómo un trámite o proceso administrativo que involucra a dos o más Organizaciones Miembro, que interoperan a través del Sistema de Interoperabilidad. Para poder lograrlo hay que realizar 3 pasos.

A. Detección

Para encontrar posibles situaciones de interoperabilidad a través de X-BA, resulta fundamental comprender el flujo de trabajo actual para cada trámite o procedimiento. Este entendimiento implica identificar los distintos sistemas implicados y los datos que deben ser validados en cada requisito. Se requiere analizar qué información se valida en cada documento, cómo se solicita, y cómo se procesa y almacena la documentación en cada trámite o procedimiento. Con el objetivo de facilitar este proceso, se ha desarrollado la metodología denominada Mapeo de Integraciones, Documentos y Datos (MIDD), la cual es aplicada de manera uniforme a todos los procesos administrativos y trámites en el ámbito gubernamental.

Mapeo de Integración, Documentos y Datos (MIDD)

El MIDD en el Gobierno de la Ciudad de Buenos Aires proporciona una visión completa de las conexiones gubernamentales, siendo crucial para la gestión eficiente de sistemas, procesos y flujos de información. Esta metodología estructurada complementa el Inventario Único de Trámites (IUT), documentando procesos y requisitos para la Administración Pública. Su objetivo es identificar oportunidades de interoperabilidad, fomentando un intercambio eficiente de información entre sistemas y aplicaciones gubernamentales. El enfoque principal consiste en ofrecer información detallada sobre los trámites, caracterizando requisitos y comprendiendo las necesidades del área solicitante. Este proceso también revela el volumen de trámites, la ubicación de documentación y su impacto en ciudadanos y organizaciones del Sistema de Interoperabilidad. El 'mapeo' se actualiza constantemente mediante la colaboración con las áreas responsables de los procedimientos, garantizando información precisa y actualizada. Para una mayor lectura de la metodología MIDD, es posible visualizar su respectivo Manual en este link: Mapeo de Integraciones, Documentos y Datos

B. Análisis

Se debe analizar la viabilidad técnica y legal de interoperar datos entre los sistemas implicados. Esto incluye evaluar la estructura de datos y competencias legales para el consumo de ese dato. Es importante destacar que el intercambio de datos entre organismos del GCBA está normado por la Ley CABA N° 1.845, eliminando la necesidad de consentimiento personal para datos dentro de las competencias del área consultante.

Dentro de este análisis, se debe evaluar el impacto de la interoperabilidad en los usuarios, los procesos y los sistemas existentes. También es importante considerar cómo afectará la experiencia del usuario y qué cambios serán necesarios en los sistemas de información para que la interoperabilidad sea factible.

C. Activación

Para poder activar un caso de uso entre dos Organizaciones Miembro, se deben haber gestionado previamente los accesos de consumo del mismo.

Una vez que el subsistema desde el cuál deseo consumir el servicio tenga los accesos correspondientes, para poder llegar al servicio web se deberá verificar que se cuente con acceso, desde el backend de la aplicación que se integra o desde el host donde se realiza la consulta (ej: Postman, curl, etc) al DNS del Servidor de Seguridad correspondiente a su área (Ej. xroad-innovacion.buenosaires.gob.ar), de no ser así, solicitar los permisos correspondientes al área de seguridad informática.

Consumo de Servicios

Servicios REST

Para poder generar la URL del servicio a consumir se deben ir cargando los datos dependiendo el DNS del servidor desde el cuál estoy consumiendo (SecurityServer_Consumer) y desde el que se provee el servicio (SecurityServer_Provider). Así mismo, el tipo de conexión (ConnectionType) va a depender de cómo tenga configurado el subsistema consumidor (Subsystem_Consumer), esta configuración se visualiza en la solapa "Internal Servers" dentro de cada subsistema.

Para poder consumir servicios a través del Sistema de Interoperabilidad, se deberá agregar (además de los headers que pueda tener el servicio web en sí) el HEADER "X-ROAD-CLIENT" como key y en el value se deberá cargar el ID del subsistema (Ej. DEV/GOB/12345/Cons-Pruebas-Hml) que se ha habilitado como consumidor. La KEY siempre va a ser la misma, el valor va a depender del nombre del subsistema habilitado como consumidor.

Composición de URL:
[ConnectionType]://[DNS_SecurityServer_Consumer]/[instancia]/[ecosistema]/[MemberClass_Provider]/[MemberCode_Provider]/[SubsystemCode_Provider]/[ServiceCode]

Composición de Header:
Key: X-Road-Client
Value: **[ecosistema]/[MemberClass]/[MemberCode_Consumer]/[SubsystemCode_Consumer]**

Ejemplo práctico:
En el siguiente cuadro, tenemos los datos correspondientes a la configuración de diferentes Servidores de Seguridad y sus subsistemas registrados que según sean proveedores o consumidores, tienen un Service Code agregado o no.

SecurityServer	Instancia	Ecosistema	MemberClass	MemberCode	SubsystemCode	ServiceCode	DNS
Innovación	r1	edicaba	GOB	002	Cons-TAD-Prd	-	xroad-innovacion.buenosaires.gob.ar
Educación	r1	edicaba	GOB	006	Cons-TAD-Prd	-	xroad-educacion.buenosaires.gob.ar

Justicia y Seguridad	r1	edicaba	GOB	020	Prov-RDAM-Prd	DeudorMoroso	xroad-mjysgc.buenosaires.gob.ar

A continuación, se muestra cómo quedaría la URL para consultar el ServicioWeb de DeudorMoroso del Ministerio de Justicia y Seguridad, desde diferentes consumidores:

SS CONSUMER	API	VALUE HEADER
Innovación	https://xroad-innovacion.buenosaires.gob.ar/r1/edicaba/GOB/020/Prov-RDAM-Prd/DeudorMoroso	edicaba/GOB/002/Cons-TAD-Prd
Educación	https://xroad-educacion.buenosaires.gob.ar/r1/edicaba/GOB/020/Prov-RDAM-Prd/DeudorMoroso	edicaba/GOB/006/Cons-TAD-Prd

Servicio SOAP

El consumo de servicios SOAP, se realiza de una manera diferente, ya que los datos de los servidores, subsistemas y servicios no se cargan en la URL, sino que se arman en el body.

Para poder consumir los servicios SOAP, como URL únicamente se utiliza el DNS del servidor consumidor del servicio:

Ej. https://xroad-innovacion.buenosaires.gob.ar

En el Body para la consulta deben enviarse los datos del subsistema consumidor, el subsistema proveedor y el código del servicio:

Body:

```
<SOAP-ENV:Header>
  <xrd:client iden:objectType="SUBSYSTEM">
      <iden:xRoadInstance>[Ecosistema]</iden:xRoadInstance>
      <iden:memberClass>[MemberClass]</iden:memberClass>
      <iden:memberCode>[MemberCode Cons]</iden:memberCode>
      <iden:subsystemCode>[SubsystemCode Cons]</iden:subsystemCode>
  </xrd:client>
  <xrd:service iden:objectType="SERVICE">
      <iden:xRoadInstance>[Ecosistema]</iden:xRoadInstance>
      <iden:memberClass>[MemberClass]</iden:memberClass>
      <iden:memberCode>[MemberCode Prov]</iden:memberCode>
      <iden:subsystemCode>[SubsystemCode Prov]</iden:subsystemCode>
      <iden:serviceCode>[ServiceCode]</iden:serviceCode>
  </xrd:service>
  <xrd:userId>tuser</xrd:userId>
  <xrd:id>ID11234</xrd:id>
  <xrd:protocolVersion>4.0</xrd:protocolVersion>
</SOAP-ENV:Header>
```

Luego de este body, debajo se deberá agregar el body específico del servicio que se quiere consumir.

D. Buenas prácticas y Recomendaciones

Funcionales

Uso Ético de Datos

La Organización Miembro dueña del servicio, debe analizar las solicitudes que recibe de otras Organizaciones Miembro, y cumplir con las leyes de protección de datos personales al habilitar cualquier acceso. También puede establecer condiciones de uso de los datos para cada integración. 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 web, 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

Uno de los principios fundamentales para mejorar la experiencia del vecino al realizar un trámite es minimizar la cantidad de información requerida. Esto 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, 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**
  Implemente un manejo de errores robusto que proporcione 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**
  Proporcione varios endpoints que permitan a los usuarios realizar diferentes acciones. Utilice parámetros claros y específicos para cada endpoint, facilitando así las consultas y operaciones.
- **Limitar la información exponencial**
  Evite exponer demasiada información en las respuestas. Diseñe la API para que los usuarios puedan obtener solo la información necesaria. Use opciones como filtros y campos de selección para controlar los datos devueltos.
- **Utilización de metadatos**
  En lugar de devolver documentos completos, como archivos PDF o HTML, proporcione 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 a través de X-BA, las nuevas URL y el header a agregar. La documentación debe ser comprensible para que los desarrolladores puedan integrar fácilmente la API en sus aplicaciones. Se adjunta modelo de documentación: Modelo Documentación.
  Es importante que no se agreguen en la documentación las URL originales que no incluyen la capa de seguridad de X-BA.

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.

Criterios de Publicación de Servicios Web en X-BA
Solicitar documento a equipo XBA a: interoperabilidad@buenosaire.gob.ar

Mantenimiento y Soporte
El mantenimiento y soporte de cada servicio que se provee es responsabilidad de la Organización Miembro proveedora 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 de X-BA.

- **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 web.

- **Monitoreo y resolución de problemas**
  Realizar un monitoreo constante de sus servicios para detectar posibles problemas en tiempo real. Además, se espera que 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 con el fin de asegurar la efectividad y la comunicación constante en el entorno de X-BA. Estos referentes brindan a los usuarios una clara dirección sobre a quién recurrir en caso de requerir apoyo técnico y/o asesoramiento. Asimismo, se establecen como un canal directo para resolver problemas y facilitan la coordinación entre diferentes entidades dentro del sistema.

SUSPENSIÓN Y EXCLUSIÓN DEL SISTEMA X-BA

Es esencial para el Gobierno de la Ciudad Autónoma de Buenos Aires garantizar el cumplimiento de los principios rectores del Sistema de Interoperabilidad y de las demás obligaciones establecidas en la normativa vigente para mantener la integridad y la eficacia del sistema.

La Dirección General de Eficiencia Administrativa, dependiente de la Secretaría de Innovación y Transformación Digital, siempre mantendrá el derecho de realizar revisiones periódicas sin previo aviso, con el fin de verificar el fiel cumplimiento de las normas de privacidad, uso de datos y propiedad intelectual, estipuladas por la Fuente Auténtica, y los principios rectores estipulados en la Resolución N° 303/22/SECITD y su modificatoria N°236/23/SECITD, como lo son la confidencialidad, no repudio, seguridad, preservación y protección de la información. En caso de incumplimiento de dichas obligaciones, se establecen diversas sanciones con el fin de mantener la coherencia y la calidad de los servicios ofrecidos.

Frente a la detección de incompatibilidades o incumplimientos en alguno de los puntos mencionados, la Secretaría de Innovación y Transformación Digital tiene la facultad de decidir rechazar, suspender o expulsar a la Organización Miembro del Sistema de Interoperabilidad.

Con respecto a las Organizaciones Miembro comprendidas dentro de la estructura del GCBA, cualquier notificación que informe sobre una decisión de rechazo, suspensión o expulsión se llevará a cabo a través de una Comunicación Oficial por el Sistema de Administración Documental Electrónica (SADE) y se dirigirá a la máxima autoridad de la respectiva entidad.

En lo que concierne a las Organizaciones Miembro de tipo privado, las notificaciones se efectuarán mediante notificaciones electrónicas fehacientes a través de la plataforma TAD (Trámite a Distancia) y estarán dirigidas a los representantes legales de la Organización y/o los apoderados que designen para tal efecto.