Anexo

Número: IF-2022-45687000-GCABA-SECITD

Buenos Aires, Martes 6 de Diciembre de 2022

Referencia: Anexo I - Sistema de Interoperabilidad del Gobierno de la Ciudad Autónoma de Buenos Aires

---

ANEXO I
SECCIÓN I
DISPOSICIONES GENERALES

1. Definiciones:

1.1 Autoridad de Certificación: entidad de confianza responsable de emitir o revocar Certificados de Autenticación.

1.2 Autoridad de Sellado de Tiempo (TSA): prestador del servicio de sellado de tiempo, definida por los estándares de la Agencia de Sistemas de Información conforme la Ley N° 2.689. Constituye una tercera parte de confianza, no involucrada en ninguna transacción digital.

1.3 Caso de Uso: trámites o procesos administrativos que involucran a dos o más Organizaciones Miembro, que comparten e intercambian datos, procesos y servicios digitales a través del Sistema de Interoperabilidad.

1.4 Catálogo de Servicios: listado de servicios web disponibles para las Organizaciones Miembro del Sistema de Interoperabilidad, por parte de las Fuentes Auténticas.

1.5 Certificado de Autenticación: certificado digital, emitido por la Autoridad de Certificación, que permite, en una comunicación electrónica, validar la identidad del portador.

1.6 Certificado de Firma: certificación emitida por la Autoridad de Certificación con el objeto de validar la identidad del emisor del mensaje y asegurar la trazabilidad e inalterabilidad del mensaje enviado y recibido.

1.7 Datos informatizados: datos sometidos al tratamiento o procesamiento electrónico.

1.8 Fuente Auténtica: Organización Miembro del Sistema de Interoperabilidad que, en el marco de sus misiones y funciones, es responsable exclusivo de registrar, resguardar, mantener y proveer digitalmente un dato al resto de las Organizaciones Miembro.

1.9 Gobernanza de Datos: establecimiento de procesos, coherentes y ordenados, abarcando todo el ciclo de vida del dato, el cual contiene las instancias de planeación, captura, producción, organización, administración, difusión, promoción y uso.

1.10 Interoperabilidad: capacidad de dos o más sistemas o componentes para intercambiar información, por medio de una instancia común de software de datos, logrando una eficaz utilización de los mismos.

1.11 Modelo de Operación: estándares que organizan y controlan los procesos, para que interactúen de manera articulada, ordenada y eficiente.

1.12 Nodo de Seguridad: punto de interacción de cada Organización Miembro con el resto del Sistema de Interoperabilidad. Es utilizado para proveer y/o consumir servicios.

1.13 Operador del Sistema de Interoperabilidad: es el responsable primario, en la operación del Sistema de Interoperabilidad, de la definición de políticas y protocolos de gobernanza de datos.

1.14 Organización Miembro: organización perteneciente al Sistema de Interoperabilidad. Interopera a través de un Nodo de Seguridad, poniendo a disponibilidad la información que produce o consumiendo servicios brindados por otras Organizaciones Miembro en el Catálogo de Servicios.

1.15 *Peer to Peer* (p2p): red de sistemas o nodos que se comunican directamente entre sí, comportándose como iguales, sin la necesidad de la intervención de un Servidor Central.

1.16 PKI (Infraestructura de Clave Pública): conjunto de políticas, procesos y tecnologías que permiten emitir certificados digitales encriptados que autentifican personas, dispositivos o servicios.

1.17 Red de Confianza: entorno por el cual la interoperabilidad de sistemas de distintas organizaciones que, a través de 1) *timestamp* de una Autoridad de Sellado de Tiempo (TSA) y 2) certificados de firma digital y autenticación provistos por una Autoridad de Certificación (CA) confiable, aseguran el intercambio de información identificada y verificada.

1.18 Responsable de Archivo, Registro, Base o Banco de Datos Informatizados: persona humana o jurídica pública o privada, que es titular de un archivo, registro, base o banco de datos informatizados.

1.19 Sellado de Tiempo (*timestamp*): mecanismo que permite asociar un documento o transacción con una fecha y hora determinada, demostrando que no ha sufrido alteración alguna desde que la Autoridad de Sellado de Tiempo (TSA) lo ha proporcionado, como tercer parte de confianza.

1.20 Servidor Central: sistema único que contiene y ejecuta la política de seguridad del Sistema de Interoperabilidad, del registro de autoridades certificantes disponibles tanto de firma de mensajes como de sellado de tiempo y sus respectivos Nodos de Seguridad.

1.21 Sistema de Información: conjunto de componentes que interactúan entre sí con el objeto de administrar, recolectar, recuperar, procesar, almacenar y distribuir información.

1.22 Sistema de Interoperabilidad: Instancia común de un software utilizado para producir y consumir servicios de datos entre sistemas de información.

1.23 Titular de los Datos: toda persona humana o jurídica pública o privada cuyos datos sean objeto de tratamiento a través del Sistema de Interoperabilidad.

1.24 Usuario de Datos: toda persona humana y/o jurídica pública o privada que realice a su arbitrio el uso de datos.

2. Principios Rectores:

Las políticas, protocolos, acciones y casos de uso enmarcados dentro del Sistema de Interoperabilidad del GCABA deberán cumplir, teniendo en cuenta su naturaleza y los derechos involucrados, la aplicación de los siguientes principios de interoperabilidad:

2.1 Confidencialidad: Serán aplicables al presente todas las disposiciones establecidas en la Ley Nacional N° 25.326 y la Ley local N° 1.845 ambas de Protección de los Datos Personales, sus normas reglamentarias, complementarias y demás normativa vigente en la materia.

2.2 Interoperabilidad Digital: Los procesos administrativos que constituyan un trámite deberán ser digitales.

2.3 No repudio: Garantía de seguridad e inalterabilidad, a través del sellado de tiempo y firma digital con certificado PKI GCABA, en las transacciones que se realizan en el Sistema de Interoperabilidad.

2.4 Principio de única vez: Tanto ciudadanos como entidades del sector productivo presentarán por única vez sus datos a la Administración Pública, y éstas deberán compartir y reutilizar los datos, en cumplimiento con la normativa vigente.

2.5 Seguridad, Preservación y Protección de la Información: Todo intercambio de datos deberá preservarse y realizarse mediante protocolos de seguridad informática definidos por los estándares de la Agencia de Sistemas de la Información del Gobierno de la Ciudad Autónoma de Buenos Aires conforme lo establecido en la Ley Nº 2.689.

2.6 Simplificación Normativa y Procedimental: Las normas y regulaciones que se dicten deberán ser simples, claras, precisas y de fácil comprensión.

2.7 Transparencia: La Agencia de Sistemas de la Información deberá poner a disposición de los ciudadanos y las dependencias de la Administración Pública del Gobierno de la Ciudad Autónoma de Buenos Aires, los registros de las transacciones de manera completa, comprensible y oportuna.

2.8 Trazabilidad: Todo acceso e intercambio de información y gestión de servicios, trámites, avisos, comunicaciones, notificaciones y demás actuaciones deberán registrarse.

SECCIÓN II

MARCO TÉCNICO DEL SISTEMA DE INTEROPERABILIDAD

1. Fundamentos Tecnológicos del Sistema de Interoperabilidad de GCABA

La arquitectura a implementar asegura un conjunto de funciones estándar para respaldar y facilitar el intercambio de datos, su confidencialidad, integridad e interoperabilidad entre las entidades y jurisdicciones comprendidas en el artículo 4° de la Ley N° 70 (Texto consolidado por la Ley N° 6.347), constituida por los siguientes componentes:

- Gestión de direcciones y enrutamiento de mensajes, mediante las cuales se administran las direcciones de cada nodo de seguridad integrante de la plataforma, dentro del registro de Organizaciones Miembro del Servidor Central.Gestión de Derechos de Acceso (control de acceso) mediante el cual se pueden habilitar o deshabilitar servicios disponibles por la Organización Miembro en el Catálogo de Servicios. Autenticación a nivel de organización mediante los nodos de seguridad.
- Encriptado de mensajes (nodos de seguridad envían mensajes por canal seguro).
- Sellado de tiempo provisto por la Autoridad de Sellado, siendo la Agencia de Sistemas de

Información conforme la Ley N° 2.689, la responsable de definirla y registrarla en el Servidor Central.
- Firma digital de mensajes con certificados de la PKI de GCABA.
- Manejo de errores (auditoría y monitoreo).

2. Arquitectura del Sistema de interoperabilidad

La arquitectura del Sistema de Interoperabilidad debe permitir que los Sistemas de Información puedan interoperar directamente, a través de un Nodo de Seguridad.

Dicho Nodo de Seguridad, actúa como una puerta de seguridad, proporcionando una forma estandarizada, segura de producir y consumir servicios, permitiendo la gestión en el intercambio de su información de manera confidencial, segura y auditable. El intercambio es acompañado con una firma digital y un sellado en el tiempo, garantizando el no repudio entre las partes.

Para hacer posible el intercambio de información entre un proveedor y consumidor de servicios, previamente se debe haber realizado el proceso de registración como Organización Miembro en el Sistema de Interoperabilidad.

El Servidor Central contendrá los registros de Organizaciones Miembros y Nodos de Seguridad de todo el Sistema de Interoperabilidad y además definirá:

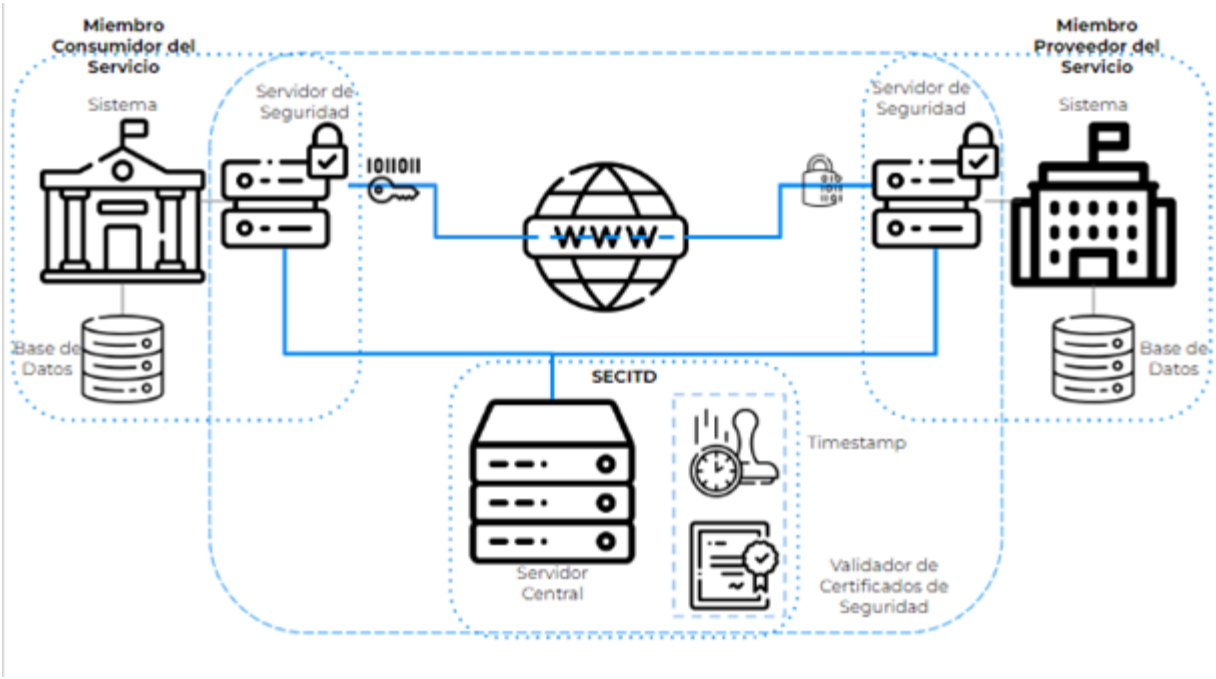
- Las políticas de seguridad globales compartidas por todos los Nodos de Seguridad.
- La lista de Autoridades Certificantes confiables que incluyen la PKI de GCABA.
- La lista de autoridades de sellado de tiempo permitidas incluye la TSA (Timestamp authority) utilizada en GCABA.

Este tipo de arquitectura cuenta con las siguientes características:

- Comunicación segura y confidencial entre pares (*Peer to Peer*).
- Cada Organización Miembro mantiene el total control sobre el acceso a sus datos.
- Todos los intercambios son auditables.

- El número de Organizaciones Miembros puede crecer en forma ilimitada.
- No existe un punto único de falla, es decir, al ser un modelo distribuido, puede fallar alguno de los puntos de la arquitectura. No obstante, no ocasionará una falla global.

La arquitectura del Sistema de Interoperabilidad sigue el siguiente esquema:



3. Modelo del Sistema de Interoperabilidad

El Sistema de Interoperabilidad está integrado por tres tipos de actores: un Operador, Proveedores de servicios de confianza y Organizaciones Miembro que se conecten al Sistema de Interoperabilidad.

3.1 Operador del Sistema de Interoperabilidad

El Operador es el responsable de todos los aspectos operacionales.

Dentro de las responsabilidades se encuentran:

- Definir regulaciones y prácticas.
- Verificar la aplicación de las mismas.
- Definir y aplicar parámetros y configuraciones globales tendientes al mejor uso y estabilidad del Servidor Central y componentes del Sistema de Interoperabilidad.
- Publicar los estándares aceptables a ser cumplidos por las Organizaciones Miembro.
- Gestionar las solicitudes de ingreso de las nuevas Organizaciones Miembro.
- Brindar apoyo y operar los servicios centrales de dicho Sistema.

La Secretaría de Innovación y Transformación Digital (en adelante “SECITD”), como Operador del Sistema de Interoperabilidad del GCABA, coordinará con las áreas de gobierno según su competencia.

3.2 Proveedor/es de Servicios de Confianza:

3.2.1 Autoridad de Servicio de Sellado de Tiempo (TSA):

A todos los mensajes intercambiados a través del Sistema de Interoperabilidad se les aplica una marca de tiempo y son registrados por los servidores de nodos de seguridad intervinientes. En el caso de GCABA se utiliza la provista por *tsa.buenosaires.gob.ar.*

El Sistema de Interoperabilidad permite incorporar nuevas autoridades de sellado de tiempo o incluso reemplazar la actual en función de la demanda y crecimiento de este.

3.2.2 Autoridad de Certificación (CA)

Todos los Nodos de Seguridad del Sistema de Interoperabilidad 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 de Interoperabilidad.
- 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. En este caso el certificado es provisto por la PKI del GCABA.

3.3 Organizaciones Miembro

Las Organizaciones Miembro del Sistema de Interoperabilidad son organizaciones con derecho a producir y/o consumir servicios con otros Miembros. Una Organización Miembro puede ser un proveedor de servicios, un consumidor de servicios o ambos. Estas Organizaciones Miembro pueden ser de gestión pública, pertenecientes al GCABA u otras jurisdicciones, o de gestión privada.

Todas las Organizaciones Miembro deben implementar al menos un Nodo de Seguridad que les permita proveer o consumir servicios digitales con sus sistemas de información con otros miembros y deben acceder a los servicios de confianza TSA(s) y CA(s) para desencriptar y verificar la autoría de los mensajes.

3.3.1. Nodo de Seguridad

La Organización Miembro gestiona para cada Nodo de Seguridad ante la PKI de GCABA dos tipos de certificados los que fueron descriptos en el punto 3.2.2 de la presente Sección. Los certificados emitidos por otras Autoridades de Certificación se consideran inválidos a menos que sean autorizados para su uso por el Operador del Sistema de Interoperabilidad del GCABA.

Un único Nodo de Seguridad puede alojar varias Organizaciones Miembro (multicliente).

La Organización Miembro que administra el Nodo de Seguridad es la propietaria del mismo y las organizaciones alojadas son clientes de dicho nodo, pudiendo en un futuro, alguna organización cliente, crear su propio nodo mediante el registro de nuevas Organizaciones Miembro y convertirse en propietaria de este.

3.3.2 Sistemas de Información

Los Sistemas de Información de las Organizaciones Miembro del Sistema de Interoperabilidad son los que producen y/o consumen servicios a través de los Nodos de Seguridad, mediante el uso de APIs o Web Services.

Para un consumidor de servicios de un Sistema de Información, el Nodo de Seguridad, actúa como un punto de entrada a todos los servicios del Sistema de Interoperabilidad. El consumidor puede encontrar servicios de Organizaciones Miembros registradas en el Catálogo de Servicios alojado en el Servidor Central.

3.3.3 Modelo de operación del Sistema de Interoperabilidad

El modelo de operación del Sistema de Interoperabilidad resuelve la interacción entre los sistemas de las distintas organizaciones miembros, permitiendo que los mismos puedan acceder y usar datos de otras fuentes con seguridad y confidencialidad.

Para este fin la operación cumple con cinco pilares fundamentales:

- Identidad Digital de Sistemas: mediante certificados de firma digital.

Seguridad del Intercambio: canales encriptados con certificados de autenticación.
- Interoperabilidad: soportando los estándares abiertos como SOAP y REST.
- Responsabilidad: cada organización mantiene el control de acceso a sus datos.
- Verificabilidad: los intercambios quedan registrados en forma inmutable para su auditoría.

3.3.4 Registro de nuevas Organizaciones Miembro

3.3.4.1 Solicitud de ingreso para entidades, jurisdicciones y otros Gobiernos con acceso al Sistema de Administración de Documentos Electrónicos (en adelante "SADE"):

Para iniciar la solicitud de ingreso como Organización Miembro del Sistema de Interoperabilidad, deberán enviar una Comunicación Oficial (en adelante "CCOO") a través de SADE, a la Secretaría de Innovación y Transformación Digital (en adelante "SECITD"), firmada por la máxima autoridad de la repartición, conforme el modelo que oportunamente se apruebe.

En caso de corresponder y conforme lo establecido en el artículo 5° del Decreto Nº 118/22 se suscribirán los Convenios correspondientes.

3.3.4.2 Solicitud de ingreso para el Sector Privado, otras entidades y jurisdicciones; y otros Gobiernos sin acceso a SADE:

Para dar inicio a la solicitud de ingreso como Organización Miembro del Sistema de Interoperabilidad, previamente, las partes interesadas, deberán suscribir un Convenio, conforme lo establecido en el artículo 5° del Decreto Nº 118/22.

Suscripto el mismo, iniciarán la solicitud al Sistema mencionado precedentemente, a través de la Plataforma de Trámites a Distancia (en adelante "TAD"). Dicho trámite deberá ser gestionado por la autoridad firmante del Convenio mencionado en el párrafo anterior, con facultades suficientes.

3.3.5 Otras Consideraciones:

La SECITD y/o el área que oportunamente ésta designe, evaluará el registro de nuevas Organizaciones Miembro, y gestionará su aceptación o rechazo de acuerdo a los estándares mencionados y el cumplimiento de la presente Resolución.

La SECITD siempre mantendrá el derecho de realizar revisiones periódicas sin previo aviso, con el fin de verificar el fiel cumplimiento de la presente Resolución, los estándares y sus modificatorias como también de los servicios ofrecidos por los Nodos de Seguridad. Asimismo, podrá decidir la suspensión temporal o definitiva de la pertenencia de la Organización Miembro al Sistema de Interoperabilidad, conforme lo establecido en los Convenios suscriptos y los principios rectores de esta Resolución.

Respecto a las Organizaciones Miembro mencionadas en el punto 3.3.4.2 de la presente Sección, las notificaciones se realizarán por medio de una CCOO por SADE, a la máxima autoridad de la repartición.

En el caso de las Organizaciones Miembro mencionadas en el punto 3.3.4.3 de la presente Sección, las notificaciones se realizarán por medio de TAD dirigidas a la máxima autoridad solicitante.

Una vez aceptada la solicitud, la identidad de cada Organización Miembro y punto de acceso técnico es verificado por la Agencia de Sistemas de Información conforme lo establecido en la Ley N°2.689, mediante certificados emitidos por una Autoridad de Certificación (CA).

3.3.6 Causas de rechazo, suspensión y expulsión:

Todas las Organizaciones Miembro deberán cumplir las normas de privacidad, uso de datos y propiedad intelectual, estipuladas por la Fuente Auténtica, y las disposiciones generales de la presente Resolución.

Frente a la detección de incompatibilidades en alguno de los puntos mencionados en el párrafo precedente, durante el proceso de solicitud, incorporación y utilización del Sistema de Interoperabilidad, se decidirá lo siguiente:

Respecto a las Organizaciones Miembro mencionadas en el punto 3.3.4.2 de la presente Sección, las notificaciones que informen rechazo, suspensión y/o expulsión, se realizarán por medio de una CCOO por SADE, a la máxima autoridad de la repartición.

En el caso de las Organizaciones Miembro mencionadas en el punto 3.3.4.3 de la presente Sección, las notificaciones que informen rechazo, suspensión y/o expulsión, se realizarán por medio de TAD dirigidas a la máxima autoridad solicitante.

3.3.7 Solicitud de baja de una Organización Miembro:

Las Organizaciones Miembro, integradas por el Sector Privado u otros Gobiernos, podrán solicitar la baja al Sistema de Interoperabilidad del Gobierno de la Ciudad Autónoma de Buenos Aires, conforme el procedimiento establecido en el Convenio oportunamente suscripto por las partes.

3.3.8 Operación bajo Red de Confianza

Las identidades de las Organizaciones Miembro son registradas por la Agencia de Sistemas de Información en el Servidor Central. El intercambio de datos se hace directamente entre un consumidor de servicios y un proveedor de servicios sin pasar por el Servidor Central.

Todo Nodo de Seguridad del Sistema de Interoperabilidad comprueba que el Nodo emisor o receptor del mensaje es una Organización Miembro activa del Sistema de Interoperabilidad mediante el uso del protocolo de estado de certificados en línea (Online Certificate Status Protocol - OCSP).

Tanto el Servicio de Sellado de Tiempo como el Servicio de Certificados de Confianza del Sistema de Interoperabilidad están previamente definidos en el Servidor Central del Sistema de Interoperabilidad, por lo que solo se podrá hacer uso de esos servicios.

3.3.9 Control de Acceso

El Nodo de Seguridad implementa un modelo de autorización que cada Organización Miembro utiliza para otorgar derechos o permisos de acceso a sus servicios por parte de otras. Dichos Servicios son registrados en el Catálogo de Servicios.

Cuando una Organización Miembro, ya registrada, requiera utilizar un servicio que no produce, deberá solicitar a la Fuente Autentica que le otorgue los derechos de acceso.

Ante la decisión de discontinuar la provisión de un servicio ofrecido en el Catálogo de Servicios por un Nodo de Seguridad, la Fuente Auténtica deberá informar a las áreas consumidoras en un plazo de seis (6) meses, para permitir e implementar un rediseño funcional adecuado.

4. Auditoría y Monitoreo

Todos los intercambios de datos se registran localmente en los Nodos de Seguridad de las Organizaciones Miembro involucrados (proveedor/consumidor) y ningún tercero tiene acceso a los mismos.

Los registros de auditoría de cada Nodo de Seguridad pueden ser utilizados como prueba en caso de requerimiento judicial.

Los registros detallados de los intercambios, sin incluir el contenido de los mensajes, permiten realizar el seguimiento y monitoreo de la actividad tanto local de cada Nodo de Seguridad como de la actividad de todo el Sistema de Interoperabilidad. Esto permite medir el uso de servicios individuales, comprender las dependencias y las relaciones entre los diferentes sistemas y servicios de información, monitorear el estado del servicio y evaluar estrategias de expansión del Sistema de Interoperabilidad.

SECCIÓN III

IMPLEMENTACIÓN DE CASOS DE USO

Una vez creado e instalado el Sistema de Interoperabilidad, su aplicación efectiva se realizará a través de la implementación de nuevos Casos de Uso que podrán ser propuestos por la SECITD, la Agencia de Sistemas de la Información conforme Ley N°2.689, o una Organización Miembro.

Un Caso de Uso requiere de una Organización Miembro que ofrezca un servicio a través del catálogo de servicios y que otra Organización Miembro consuma dicho servicio cumpliendo con los estándares del Sistema de Interoperabilidad.

Para implementar un Caso de Uso entre Organizaciones Miembro, las mismas deberán estar registradas en el Sistema de Interoperabilidad siguiendo el procedimiento establecido en el punto 3.3.4 de la Sección II, del Anexo I de la presente Resolución.

1. Mapeo y Diagnóstico:

Se llevará a cabo un relevamiento y mapeo de los documentos, datos e integraciones (MIDD), de dicho Sistema, del que se obtendrá como resultado el detalle de los procesos, haciendo foco en los requisitos de cada uno de los trámites.

El relevamiento sobre los procesos, alimentará el Inventario Único de Trámites (IUT), completando la caracterización de los mismos, entendiendo los requisitos, la necesidad de validación, documentos y datos necesarios, el volumen del trámite, las áreas que lo requieren, dónde se almacena y el impacto del mismo, tanto para el ciudadano como para los organismos del Sistema de Interoperabilidad.

Durante esta etapa, y de manera continua, se realizará la identificación de Caso de Uso ya sea por la detección durante el MIDD, por la incorporación de nuevos procesos o modificaciones al IUT, por la Ventanilla Única (en adelante “VU”) de la SECITD, o bien por una instancia primaria de contacto, en la que se identifica un Caso de Uso y luego se formaliza el requerimiento por los canales preestablecidos anteriormente.

2. Priorización de Caso de Uso:

La implementación de los Casos de Uso se realizará de manera progresiva, siguiendo los Principios Rectores definidos en el punto 2 de la Sección I del Anexo I de la presente Resolución, según los siguientes criterios de priorización:

- **Normativa Vigente:** requiere de verificar que en el proceso a implementar se resguarden los principios rectores del Sistema de Interoperabilidad, y se opere dentro del alcance de las misiones y funciones de las Organizaciones Miembro intervinientes.
- **Impacto Ciudadano y/o Productivo:** trámites y procesos con mayor volumen de gestión por parte

de los ciudadanos y sectores productivos, personas humanas como personas jurídicas.

- **Eficiencia Administrativa:** la documentación y/o los registros expedidos por un organismo del GCABA que son requeridos por otras reparticiones del GACBA para la gestión de trámites.
- **Madurez Técnica:** los organismos involucrados en el Caso de Uso cuentan con las capacidades técnicas para operar de manera segura y transparente en el Sistema de Interoperabilidad.
- **Calidad del Dato**: la información involucrada en el Caso de Uso cumple con los estándares, lineamientos y protocolos en materia de Gobernanza de Datos conforme lo establecido en el Decreto Nº 118/2022.
- **Seguridad:** proveer un mayor nivel de resguardo en transacciones de datos privados.

3. Diseño del Caso de Uso:

Seleccionado el Caso de Uso, se procederá al diseño de la solución del mismo a través del Sistema de Interoperabilidad, en razón dos (2) aspectos:

3.1 Aspecto Tecnológico

Incluye la disponibilización de la infraestructura para un Nodo de Seguridad, la instalación y configuración del mismo en cumplimiento de la arquitectura y los estándares técnicos del Sistema de Interoperabilidad, y capacitación al personal de la Organización miembro en la gestión y administración del Servidor.

También abarca la creación, modificación o configuración de APIs y servicios web por parte de una organización miembro para ofrecer o consumir servicios de otra organización miembro.

3.2 Aspecto Funcional

Involucra la modificación, el rediseño y/o la reingeniería de los procesos y/o sistemas de una organización miembro para poder consumir un servicio de otra organización miembro con vistas de simplificar y eficientizar los procesos administrativos, procurando tener el mayor impacto positivo posible en el ciudadano.

4. Registro en el Catálogo de Servicios:

Una vez disponibilizado el servicio, el mismo deberá ser registrado en el Catálogo de Servicios, siguiendo los lineamientos establecidos en el inciso 3.3.8 de la Sección II del Anexo I, de la presente Resolución.

Una vez registrado el servicio, otras Organizaciones Miembro podrán solicitar permisos para consumir los servicios publicados en el mencionado Catálogo de Servicios.

5. Implementación del Caso de Uso:

El Caso de Uso estará implementado una vez que, finalizados los desarrollos correspondientes a los Aspectos Tecnológicos y Funcionales, dos sistemas intercambien información para impactar en un trámite o procedimiento administrativo digital.

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2022.12.06 17:22:56 -03'00'

Diego Fernandez
Secretario
SECRETARIA INNOVACION Y TRANSFORMACION DIGITAL
MINISTERIO JEFATURA DE GABINETE

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2022.12.06 17:22:57 -03'00'