Gobierno de la Ciudad Autónoma de Buenos Aires

"2022 - Año del 40° Aniversario de la Guerra de Malvinas.
En homenaje a los veteranos y caídos en la defensa de las Islas Malvinas y el Atlántico Sur"

DECRETO N.º 118/22

Buenos Aires, 1 de abril de 2022

VISTO: La Ley N° 3.304 y 6.292 (textos consolidados por Ley N° 6.347), el Decreto N° 463/19 y sus modificatorios, el Expediente Electrónico EX-2022-12284341-GCABA-DGEADM, y

CONSIDERANDO:

Que la Ley N° 3.304 estableció el "Plan de Modernización de la Administración Pública del Gobierno de la Ciudad Autónoma de Buenos Aires" a fin de encarar un proceso de modernización administrativa;
Que el artículo 3° de la mencionada Ley determina que la Jefatura de Gabinete de Ministros es la autoridad de aplicación;
Que el artículo 2° del Título I del Anexo de la Ley N° 3.304 establece entre sus objetivos específicos, el de orientar la Administración al servicio de los ciudadanos, a través de una gestión transparente y de canales efectivos de participación y control ciudadano y promover e introducir el uso de las nuevas Tecnologías de Información y Comunicación, de manera de responder con mayor celeridad y efectividad a las demandas de la sociedad, entre otros;
Que por la Ley N° 6.292 se sancionó la Ley de Ministerios del Gobierno de la Ciudad Autónoma de Buenos Aires contemplando a la Jefatura de Gabinete de Ministros;
Que por el Decreto N° 463/19, y sus modificatorios, se aprobó la estructura orgánico funcional del Poder Ejecutivo de la Ciudad Autónoma de Buenos Aires, contemplando a la Secretaria de Innovacion y Transformacion Digital dependiente de la Jefatura de Gabinete de Ministros;
Que el mencionado decreto establece, entre las responsabilidades primarias de la mencionada Secretaria de Innovacion y Transformacion Digital, las de fomentar el diseño ágil de procesos, la digitalización y la coordinación de las políticas de transformación de la gestión administrativa dentro del Gobierno de la Ciudad Autónoma de Buenos Aires, incentivando la incorporación de nuevas metodologías de trabajo, el uso de herramientas y sistemas digitales y la optimización de los procesos; intervenir en el diseño y coordinación de las políticas de transformación y modernización en las distintas áreas de gobierno y la propuesta de las normas en la materia; supervisar el diseño de procesos y asistir en esta materia a todas las áreas del Gobierno de la Ciudad Autónoma de Buenos Aires que lo requieran y supervisar la implementación de las iniciativas de modernización, relativas a la gestión y modernización administrativa y tecnológica, procesos y servicios al ciudadano;
Que los objetivos mencionados tienen como principal destinatario al ciudadano, por tratarse del diseño de procesos que agilizan sus gestiones y evitan el dispendio de tiempo y costos, a fin de mejorar la calidad de vida de los ciudadanos;
Que desde el dictado de dicha norma hasta la actualidad se generó un conjunto de canales de vinculación directa entre el ciudadano y las diversas áreas de gobierno, conocido como ecosistema de gobierno abierto;
Que, a su vez, uno de los pilares de este proceso de modernización ha sido el desarrollo de un gobierno electrónico y la consiguiente evolución a un gobierno digital,

lo que no implica únicamente automatizar los procedimientos sino eliminar o reformular los procesos del gobierno de acuerdo a sus lineamientos estratégicos;
Que los pilares fundamentales para un gobierno digital son la gobernanza de datos, la interoperabilidad y la mejora regulatoria constante;
Que el Modelo de Gobernanza de los Datos Públicos, incluye el ordenamiento de datos como proceso de reorganización de registros en un orden o secuencia específica, configura un elemento esencial para la óptima utilización y acceso a la información;
Que tal ordenamiento, a su vez, constituye un hito fundamental y necesario para la interoperabilidad de los mismos;
Que, por su parte, la interoperabilidad de los datos constituye la capacidad de varios sistemas o componentes para intercambiarlos y entender estos datos para su más eficaz utilización;
Que es indispensable contar con una estrategia sistémica e integral que establezca como premisa básica la referida mejora regulatoria como una labor continua del sector público en beneficio de la sociedad que incluya la reducción de las cargas administrativas, la simplificación de procesos y la elaboración de normas vinculadas a dichos trámites, de manera tal de construir un Estado eficiente, organizado, predecible y capaz de brindar una respuesta rápida y transparente a los ciudadanos que realicen gestiones ante sus organismos;
Que, conforme lo expresado, resulta necesario dictar el acto administrativo pertinente.
Por ello, y en uso de las atribuciones conferidas por los artículos 102 y 104 inciso 9) de la Constitución de la Ciudad Autónoma de Buenos Aires,

EL JEFE DE GOBIERNO
DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES
DECRETA;

Artículo 1°.- Establécese un Modelo de Gobernanza de los Datos, entendiendo por tal al 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.
Artículo 2°.- Establécese un Sistema de Interoperabilidad del Gobierno de la Ciudad Autónoma de Buenos Aires que interconecte los sistemas de información de todas las áreas de gobierno, para garantizar el intercambio de datos de manera segura, transparente y confidencial.
Artículo 3°.- Establécese que el sistema previsto en el artículo 2° del presente será implementado por la Jefatura de Gabinete de Ministros, a través de la Secretaría de Innovación y Transformación Digital, que brindará las herramientas tecnológicas que permitan que el intercambio de información se realice de manera eficiente y segura y dictará los principios, protocolos de intercambio, pautas de interoperabilidad, normas complementarias y operativas necesarias. Asimismo, definirá en coordinación con las áreas del gobierno involucradas, los plazos a partir del cual cada una de ellas deberá implementar las herramientas tecnológicas y protocolos que se determinen.
Artículo 4°.- El presente Decreto será de aplicación para las entidades y jurisdicciones comprendidas en el artículo 4° de la Ley N° 70 (texto consolidado por Ley N° 6347), quienes deberán:
a) Poner a disposición de la Secretaría de Innovación y Transformación Digital de la

Jefatura de Gabinete de Ministros, o al organismo que en un futuro la reemplace, el conjunto de datos, los servicios web y/o aplicaciones correspondientes a sus sistemas de gestión con el objetivo de asegurarlos y crear interoperabilidad entre los mismos.
b) Intercambiar la información pública que produzcan, obtengan, obre en su poder o se encuentre bajo su control, con cualquier otro organismo público que así se lo solicite.
Los incisos anteriores se aplicarán bajo las condiciones establecidas en la Ley de Acceso a la Información Pública y la Ley de Protección de Datos Personales y de acuerdo con el procedimiento que establezca la Secretaría de Innovación y Transformación Digital.
Artículo 5°.- El Gobierno de la Ciudad Autónoma de Buenos Aires podrá utilizar la tecnología que implemente para el intercambio de información con el sector privado, u otros gobiernos, bajo las obligaciones establecidas en la Ley de Acceso a la Información Pública y la Ley de Protección de Datos Personales. A dichos efectos, la Secretaría de Innovación y Transformación Digital podrá suscribir los convenios respectivos.
Articulo 6°.- Establécese que ningún área del Gobierno de la Ciudad Autónoma de Buenos Aires podrá obligar al ciudadano a brindar información, datos, documentos o certificados que emita otra entidad o jurisdicción de este Gobierno.
Articulo 7°.- Créase el Inventario Único de Trámites (IUT), dentro del Módulo Registro de Legajo Multipropósito (RLM) del Sistema de Administración de Documentos Electrónicos (SADE).
Articulo 8°.-. Establécese que el Inventario Único de Trámites (IUT) será implementado y organizado por la Secretaría de Innovación y Transformación Digital de la Jefatura de Gabinete de Ministros, o el organismo que en el futuro la reemplace, y estará integrado por los trámites que las áreas de Gobierno deberán informar en las formas, plazos y condiciones que determine dicha Secretaría para asegurar su vigencia.
Artículo 9°.- Establécese que sobre los trámites incluidos en el Inventario Único de Trámites (IUT) se realizará un trabajo de eliminación, simplificación normativa y procedimental, y de digitalización tomando como principio la mejora regulatoria, con las áreas competentes y con la Unidad de Proyectos Especiales Simplificación Productiva y la Secretaría Legal y Técnica, cuando correspondiere.
Articulo 10.- El presente Decreto es refrendado por el señor Jefe de Gabinete de Ministros.
Artículo 11.- Publíquese en el Boletín Oficial de la Ciudad de Buenos Aires. Comuníquese a todos los Ministerios y Secretarías del Poder Ejecutivo, Entes Descentralizados y a los Organismos Fuera de Nivel, a la Sindicatura General de la Ciudad de Buenos Aires y, para su conocimiento y demás efectos, remítase a las Secretarías de Innovación y Transformación Digital y de Atención Ciudadana y Gestión Comunal, ambas dependientes de la Jefatura de Gabinete de Ministros y a la Subsecretaría de Desarrollo Económico del Ministerio de Desarrollo Económico y Producción. Cumplido, archívese. **RODRÍGUEZ LARRETA - Miguel**

G O B I E R N O DE LA C I U D A D DE B U E N O S A I R E S

"2022 - Año del 40° Aniversario de la Guerra de Malvinas. En homenaje a los veteranos y caídos en la defensa de las Islas Malvinas y el Atlántico Sur"

Resolución

Número: RESOL-2022-303-GCABA-SECITD

Buenos Aires, Martes 6 de Diciembre de 2022

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

---

VISTO: Las Leyes Nros. 3.304 y 6.292 (textos consolidados por Ley N° 6.347), los Decretos Nros. 463/19, y sus modificatorios, y 118/22, el Expediente Electrónico N° EX-2022-45661538- -GCABA-DGEADM, y

CONSIDERANDO:

Que la Ley N° 3.304 estableció el "Plan de Modernización de la Administración Pública del Gobierno de la Ciudad Autónoma de Buenos Aires" a fin de encarar un proceso de modernización administrativa;

Que el artículo 2° del Anexo A de la mencionada Ley estableció entre sus objetivos específicos, el de orientar a la Administración al servicio de los ciudadanos, a través de una gestión transparente y de canales efectivos de participación y control ciudadano y promover e introducir el uso de las nuevas Tecnologías de Información y Comunicación, de manera de responder con mayor celeridad y efectividad a las demandas de la sociedad;

Que el artículo 3° de la misma norma estableció a la Jefatura de Gabinete de Ministros como autoridad de aplicación;

Que a través del Decreto N° 118/22 se estableció un Modelo de Gobernanza de los Datos, entendiendo por tal al 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;

Que el artículo 2° del mencionado Decreto Nº 118/22 estableció un Sistema de Interoperabilidad del Gobierno de la Ciudad Autónoma de Buenos Aires que interconecte los sistemas de información de todas las áreas de gobierno, para garantizar el intercambio de datos de manera segura, transparente y confidencial;

Que asimismo, la mencionada norma estableció que el Sistema de Interoperabilidad será implementado por la Jefatura de Gabinete de Ministros, a través de la Secretaría de Innovación y Transformación Digital, que brindará las herramientas tecnológicas que permitan que el intercambio de información se realice de manera eficiente y segura, dictando los principios, protocolos de intercambio, pautas de interoperabilidad, normas complementarias y operativas necesarias;

Que por la Ley N° 6.292 se sancionó la Ley de Ministerios del Gobierno de la Ciudad Autónoma de

Buenos Aires contemplándose entre los Ministerios del Poder Ejecutivo a la Jefatura de Gabinete de Ministros;

Que por el Decreto N°463/19, y sus modificatorios, se aprobó la estructura orgánico funcional del Poder Ejecutivo de la Ciudad Autónoma de Buenos Aires, contemplando a la Secretaría de Innovación y Transformación Digital bajo la órbita de la Jefatura de Gabinete de Ministros;

Que dentro de las responsabilidades primarias de la mencionada Secretaría de Innovación y Transformación Digital se encuentran las de coordinar las acciones necesarias para promover la innovación pública, la implementación de una política de datos y el gobierno digital, diseñar y ejecutar políticas de innovación orientadas al desarrollo tecnológico y sustentable de la Ciudad Autónoma de Buenos Aires, promover la vinculación entre los organismos públicos y el sector privado a fin de fomentar la participación en la producción de innovación y desarrollo de tecnologías disruptivas, transfiriendo al sistema productivo y a la sociedad en general, para mejorar la competitividad de la economía y la calidad de vida del ciudadano, entre otras;

Que resulta necesario desarrollar un Sistema de Interoperabilidad del Gobierno de la Ciudad Autónoma de Buenos Aires, cuya implementación incluya las etapas de diseño y puesta en funcionamiento de la arquitectura tecnológica del mencionado Sistema;

Que en virtud de ello, resulta necesario implementar el Sistema de Interoperabilidad del Gobierno de la Ciudad Autónoma de Buenos Aires, así como también, establecer los criterios técnicos y procedimentales de la interoperabilidad;

Que en atención a lo expuesto, corresponde dictar la norma legal pertinente.

Por ello, y en uso de las facultades otorgadas por los Decretos N° 463/19 y sus modificatorios y 118/22,

EL SECRETARIO DE INNOVACIÓN Y TRANSFORMACIÓN DIGITAL

RESUELVE:

Artículo 1°. - Implementar el Sistema de Interoperabilidad del Gobierno de la Ciudad Autónoma de Buenos Aires, conforme lo establecido en el artículo 3° del Decreto Nº 118/2022, que se regirá por las disposiciones, lineamientos, estándares establecidos en la presente Resolución.

Artículo 2°. - Aprobar el Anexo I (IF-2022-45687000-GCABA-SECITD), que forma parte integrante de la presente Resolución.

Artículo 3º.- Encomendar a la Dirección General de Eficiencia Administrativa, o la que en su futuro la reemplace, la coordinación y seguimiento de todas las acciones necesarias para dar cumplimiento a lo previsto en el artículo 1° de la presente Resolución.

Artículo 4°. - Establecer que el Sistema de Interoperabilidad del Gobierno de la Ciudad Autónoma de Buenos Aires se regirá bajo los estándares y lineamientos establecidos por la Agencia de Sistemas de Información conforme la Ley N° 2.689.

Artículo 5° - Encomendar a la Subsecretaría de Políticas Públicas Basadas en Evidencia, o el organismo que en el futuro la reemplace, la elaboración de los lineamientos, protocolos y procedimientos en materia de gobernanza de datos.

Artículo 6°. - Publíquese en el Boletín Oficial de la Ciudad de Buenos Aires. Comuníquese a todos los Ministerios y Secretarías del Poder Ejecutivo, Entes Descentralizados y a los Organismos Fuera de Nivel, a

la Sindicatura General de la Ciudad de Buenos Aires y para su conocimiento y demás efectos, remítase a la Dirección General de Eficiencia Administrativa y a la Subsecretaría de Políticas Públicas Basadas en Evidencia. Cumplido, archívese.

Digitally signed by Diego Fernandez
Date: 2022.12.06 17:29:58 ART
Location: Ciudad Autónoma de Buenos Aires

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 17:30:03 -03'00'

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:

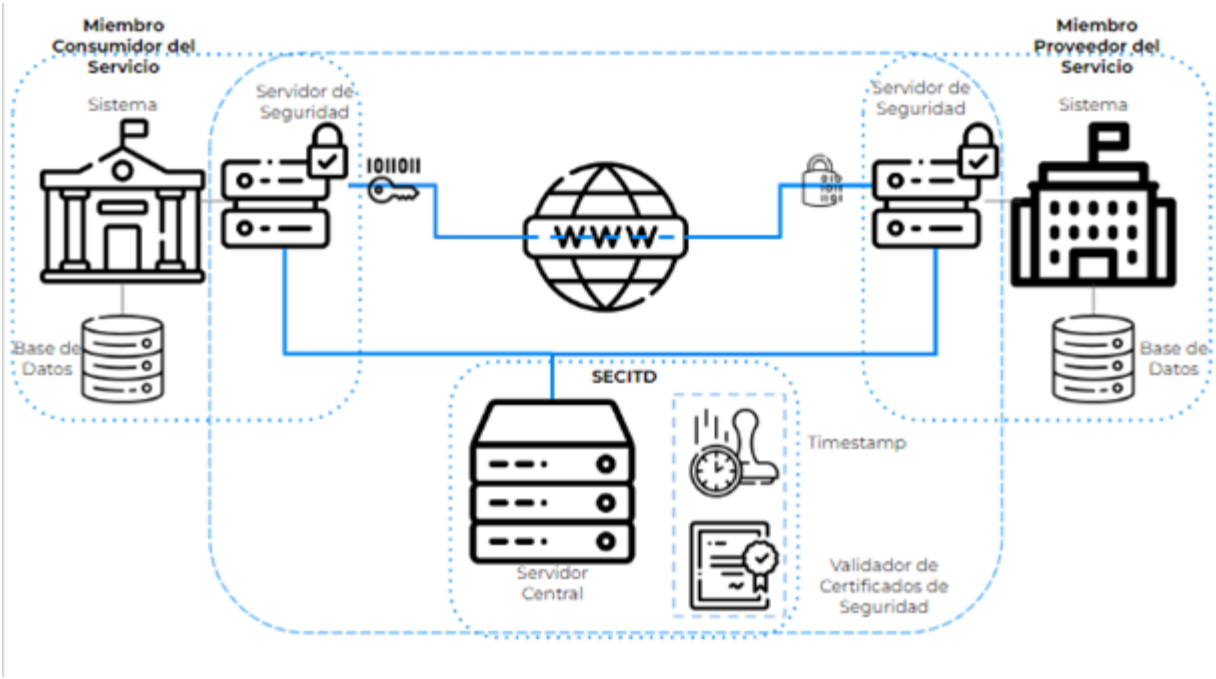
- Las políticas de seguridad globales compartidas por todos los Nodos de Seguridad.
- La lista de Autoridades Certificantes confiables que incluyen la PKI de GCABA.
- La lista de autoridades de sellado de tiempo permitidas incluye la TSA (Timestamp authority) utilizada en GCABA.

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'

G O B I E R N O DE LA C I U D A D DE B U E N O S A I R E S
"1983-2023. 40 Años de Democracia"

Resolución

Número: RESOL-2023-236-GCABA-SECITD

Buenos Aires, Viernes 10 de Noviembre de 2023

Referencia: S/ Resolucion Modifica Resolución N° 303-SECITD/22 - EX-2023-41723034- -GCABA-DGEADM

VISTO: Las Leyes Nros. 3.304 y 6.292 (textos consolidados por Ley N° 6.588), los Decretos Nros. 463/19, y sus modificatorios, y 118/22, las Resoluciones Nros. 70-SECITD/22 y 303-SECITD/22, el Expediente Electrónico N° 41723034-GCABA-DGEADM/23, y

CONSIDERANDO:

Que la Ley N° 3.304 estableció el "Plan de Modernización de la Administración Pública del Gobierno de la Ciudad Autónoma de Buenos Aires" a fin de encarar un proceso de modernización administrativa;

Que el artículo 2° del Título I del Anexo de la mencionada Ley establece entre sus objetivos específicos, el de orientar a la Administración al servicio de los ciudadanos, a través de una gestión transparente y de canales efectivos de participación y control ciudadano y promover e introducir el uso de las nuevas Tecnologías de Información y Comunicación, de manera de responder con mayor celeridad y efectividad a las demandas de la sociedad, entre otros;

Que el artículo 3° de la misma norma estableció a la Jefatura de Gabinete de Ministros como autoridad de aplicación; Que en el marco del Plan de Modernización de la Administración Pública del Gobierno de la Ciudad Autónoma de Buenos Aires se dictó el Decreto N° 118/2022 que establece un Modelo de Gobernanza de los Datos y un Sistema de Interoperabilidad del Gobierno de la Ciudad de Buenos Aires;

Que, asimismo mediante dicho Decreto, se estableció que el Sistema de Interoperabilidad será implementado por la Jefatura de Gabinete de Ministros, a través de la Secretaría de Innovación y Transformación Digital, que brindará las herramientas tecnológicas que permitan que el intercambio de información se realice de manera eficiente y segura y dictará los principios, protocolos de intercambio, pautas de interoperabilidad, normas complementarias y operativas necesarias;

Que, a su vez, el artículo 4° del mencionado Decreto establece que las entidades y jurisdicciones comprendidas en el artículo 4° de la Ley N° 70, deberán intercambiar la información pública que produzcan, obtengan, obre en su poder o se encuentre bajo su control, con cualquier otro organismo público que así se lo solicite, bajo las condiciones establecidas en la Ley de Acceso a la Información Pública y la Ley de Protección de Datos Personales y de acuerdo con el procedimiento que establezca la Secretaría de Innovación y Transformación Digital;

Que, además, el artículo 6° del mentado Decreto establece que ningún área del Gobierno de la Ciudad Autónoma de Buenos Aires podrá obligar al ciudadano a brindar información, datos, documentos o certificados que emita otra entidad o jurisdicción de este Gobierno;

Que, en ese orden, la Resolución N° 70-SECITD/22 aprueba el Reglamento Operativo del Inventario Único de Trámites, estableciendo la aplicación de los principios de buenas prácticas regulatorias, entre los que se encuentran, el principio de "única vez" mediante el cual tanto ciudadanos como entidades del sector productivo sólo deberán presentar por única vez sus datos a la Administración Pública, y éstas compartirán y reutilizarán los datos;

Que mediante la Resolución N° 303-SECITD/22, se implementa el Sistema de Interoperabilidad del Gobierno de la Ciudad Autónoma de Buenos Aires, estableciendo los criterios técnicos y procedimentales del mismo;

Que, deviene necesario y oportuno denominar al Sistema establecido por la Resolución precitada, en lo sucesivo, "X-BA";

Que, teniendo en consideración la instancia de implementación y funcionamiento del Sistema de Interoperabilidad, resulta oportuno realizar modificaciones y actualizaciones sobre la implementación del Sistema de Interoperabilidad del Gobierno de la Ciudad Autónoma de Buenos Aires, aprobado por Resolución Nº 303-SECITD/22;

Que asimismo, resulta necesario crear un Portal de Gestión de Servicios de Interoperabilidad que permitirá gestionar y registrar todas las solicitudes de consumo de servicios de interoperabilidad entre las Organizaciones Miembro pertenecientes al mencionado Sistema;

Que el mencionado Portal actuará como un canal de comunicación formal entre las Organizaciones Miembro del Sistema, facilitando la interoperabilidad entre las mismas, y posibilitando una respuesta rápida y segura, en un marco de seguridad y confianza;

Que por la Ley N° 6.292 se sancionó la Ley de Ministerios del Gobierno de la Ciudad Autónoma de Buenos Aires contemplando entre los Ministerios del Poder Ejecutivo a la Jefatura de Gabinete de Ministros;

Que por el Decreto N°463/19, y sus modificatorios, se aprobó la estructura orgánico funcional del Poder Ejecutivo de la Ciudad Autónoma de Buenos Aires, contemplando a la Secretaría de Innovación y Transformación Digital bajo la órbita de la Jefatura de Gabinete de Ministros;

Que el mencionado Decreto establece entre las responsabilidades primarias de la mencionada Secretaría de Innovación y Transformación Digital, las de coordinar las acciones necesarias para promover la innovación pública, la implementación de una política de datos y el gobierno digital, diseñar y ejecutar políticas de innovación orientadas al desarrollo tecnológico y sustentable de la Ciudad Autónoma de Buenos Aires, promover la vinculación entre los organismos públicos y el sector privado a fin de fomentar la participación en la producción de innovación y desarrollo de tecnologías disruptivas, transfiriendo al sistema productivo y a la sociedad en general, para mejorar la competitividad de la economía y la calidad de vida del ciudadano;

Que, asimismo, el mencionado Decreto dispuso que la Dirección General de Eficiencia Administrativa, dependiente de la Secretaría de Innovación y Transformación Digital, tiene entre sus responsabilidades primarias la de coordinar las acciones necesarias para implementar y mantener el Sistema de Interoperabilidad del Gobierno de la Ciudad Autónoma de Buenos Aires, promoviendo el intercambio seguro de información entre distintas dependencias del Gobierno de la Ciudad Autónoma de Buenos Aires, en el marco de sus competencias.

Que en atención a lo expuesto, corresponde dictar la norma legal pertinente.

Por ello, y en uso de las facultades otorgadas por los Decretos Nros. 463/19 y sus modificatorios y 118/22,

EL SECRETARIO DE INNOVACIÓN Y TRANSFORMACIÓN DIGITAL

RESUELVE:

Artículo 1°.- Modificar el artículo 1° de la Resolución N° 303-SECITD/22, el que quedará redactado de la siguiente manera:

"Artículo 1°.- Implementar "X-BA", el Sistema de Interoperabilidad del Gobierno de la Ciudad Autónoma de Buenos Aires, conforme lo establecido en el artículo 3° del Decreto Nº 118/2022, que se regirá por las disposiciones, lineamientos, estándares establecidos en la presente Resolución."

Artículo 2°.- Sustituir el Anexo I (IF-2022-45687000-GCABA-SECITD) de la Resolución N° 303-SECITD/22 por el Anexo I (IF-2023-41754734-GCABA-DGEADM), que forma parte integrante de la presente Resolución.

Artículo 3°.- Crear el Portal de Gestión de Servicios de Interoperabilidad como herramienta de gestión de solicitudes de consumo de servicios entre las Organizaciones Miembro del Sistema de Interoperabilidad del Gobierno de la Ciudad Autónoma de Buenos Aires "X-BA".

Artículo 4°.- Aprobar el Reglamento de Uso del Portal de Gestión de Servicios de Interoperabilidad que como Anexo II (IF-2023-41754764-GCABA-DGEADM) forma parte de la presente Resolución.

Artículo 5°.- Aprobar la Gobernanza del Sistema de Interoperabilidad que como Anexo III (IF-2023-41754793-GCABA-DGEADM) forma parte de la presente Resolución.

Artículo 6°- Designar a la Dirección General de Eficiencia Administrativa, o al organismo que en el futuro la reemplace, como administradora del Portal de Gestión de Servicios de Interoperabilidad.

Artículo 7°. - Publíquese en el Boletín Oficial de la Ciudad de Buenos Aires. Comuníquese a todos los Ministerios y Secretarías del Poder Ejecutivo, Entes Descentralizados y a los Organismos Fuera de Nivel, a la Sindicatura General de la Ciudad de Buenos Aires y para su conocimiento y demás efectos, remítase a la Dirección General de Eficiencia Administrativa y a la Subsecretaría de Políticas Públicas Basadas en Evidencia. Cumplido, archívese.

Digitally signed by Diego Fernandez
Date: 2023.11.10 18:06:42 ART
Location: Ciudad Autónoma de Buenos Aires

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

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2023.11.10 18:06:46 -03'00'

Anexo

Número: IF-2023-41754734-GCABA-DGEADM

Buenos Aires, Miércoles 8 de Noviembre de 2023

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): Procedimiento que vincula una marca de tiempo fidedigna a un conjunto de datos, validando su existencia e inmutabilidad en un momento determinado.

1.3 Caso de Uso: trámites o procesos administrativos que involucran a dos o más Organizaciones Miembro, que interoperan 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 Comunicación segura y confidencial entre pares (Peer to Peer): red de sistemas o nodos que se comunican directamente entre sí, comportándose como iguales, sin la necesidad de la intervención de un Servidor Central.

1.8 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 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.

1.12 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.

1.13 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.

1.14 PKI (Infraestructura de Clave Pública): combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías, de operaciones como el cifrado, la firma digital o el no repudio de transacciones electrónicas. Una PKI debe permitir: autenticidad, confidencialidad, integridad y no repudio.

1.15 Red de Confianza: entorno por el cual la interoperabilidad de sistemas de distintas organizaciones asegura la interoperabilidad identificada y verificada, 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.

1.16 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 tercera parte de confianza.

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

1.18 Servidor de Seguridad: componente del Sistema de Interoperabilidad que se encarga de gestionar la seguridad y el acceso de los datos y servicios en la red.

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

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

1.21 Subsistema: entidad o sistema individual que se registra en cada Servidor de Seguridad, que permite una gestión y autorización precisa para el intercambio de datos entre sistemas de información.

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

1.23 X-BA: denominación que se le da al Sistema de Interoperabilidad del Gobierno de la Ciudad Autónoma de Buenos Aires.

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 Alta disponibilidad: El sistema y los servicios ofrecidos mediante el mismo deberán satisfacer alta demanda de consumo y alto rendimiento.

2.2 Confidencialidad: Serán aplicables al presente todas las disposiciones establecidas en las Leyes Nacionales N° 25.326 y N° 26.061 y la Ley N° 1.845 de Protección de los Datos Personales, sus normas reglamentarias, complementarias y demás normativa vigente en la materia.

2.3 Cooperación: el Sistema de Interoperabilidad tiene como objetivo promover la interoperabilidad de datos entre Organizaciones Miembro. Para ello, las Organizaciones procurarán facilitar la consulta de los datos que cada una de ellas administra de conformidad a sus competencias, en caso de que otro Organismo así lo requiera y que el tratamiento de tal información se encuentre dentro de la órbita de sus competencias. La negativa de la Organización proveedora del servicio de Interoperabilidad deberá ser siempre justificada.

2.4 Descentralización: Las Organizaciones Miembro deberán ofrecer y operar los Servicios de Interoperabilidad de forma directa entre ellos.

2.5 Estabilidad: Las Organizaciones Miembro deberán asegurar la continuidad, administración, desarrollo y funcionamiento seguro e ininterrumpido de su sistema de información.

2.6 Gratuidad: El uso del Sistema de Interoperabilidad para las Organizaciones Miembros no implica erogación presupuestaria.

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

2.8 No repudio: Garantía de seguridad e inalterabilidad, a través del sellado de tiempo y firma digital otorgado por el certificado aprobado por el operador del Sistema, en las transacciones que se realizan en el Sistema de Interoperabilidad.

2.9 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.

2.10 Seguridad, Preservación y Protección de la Información: Toda interoperabilidad 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 N° 2.689.

2.11 Transparencia: La Agencia de Sistemas de la Información deberá poner a disposición de los ciudadanos y ciudadanas 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.

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

2.13 Uso limitado de los Datos: Los datos interoperados deberán ser tratados únicamente con el fin para los cuales fue autorizado su consumo. El registro que se obtuvo de la consulta no deberá reutilizarse para la validación de un dato en un proceso posterior. Los datos obtenidos por la interoperabilidad no podrán cederse a terceros.

2.14 Veracidad: Se presume que la información proveniente de la fuente auténtica de las Organizaciones Miembro es cierta, completa y fiable. Se considera que la misma podrá ser utilizada como hecho y antecedente que sirva de causa para la formación de Actos Administrativos válidos.

SECCIÓN II

MARCO TÉCNICO DEL SISTEMA DE INTEROPERABILIDAD

1. Arquitectura del Sistema de Interoperabilidad del GCABA

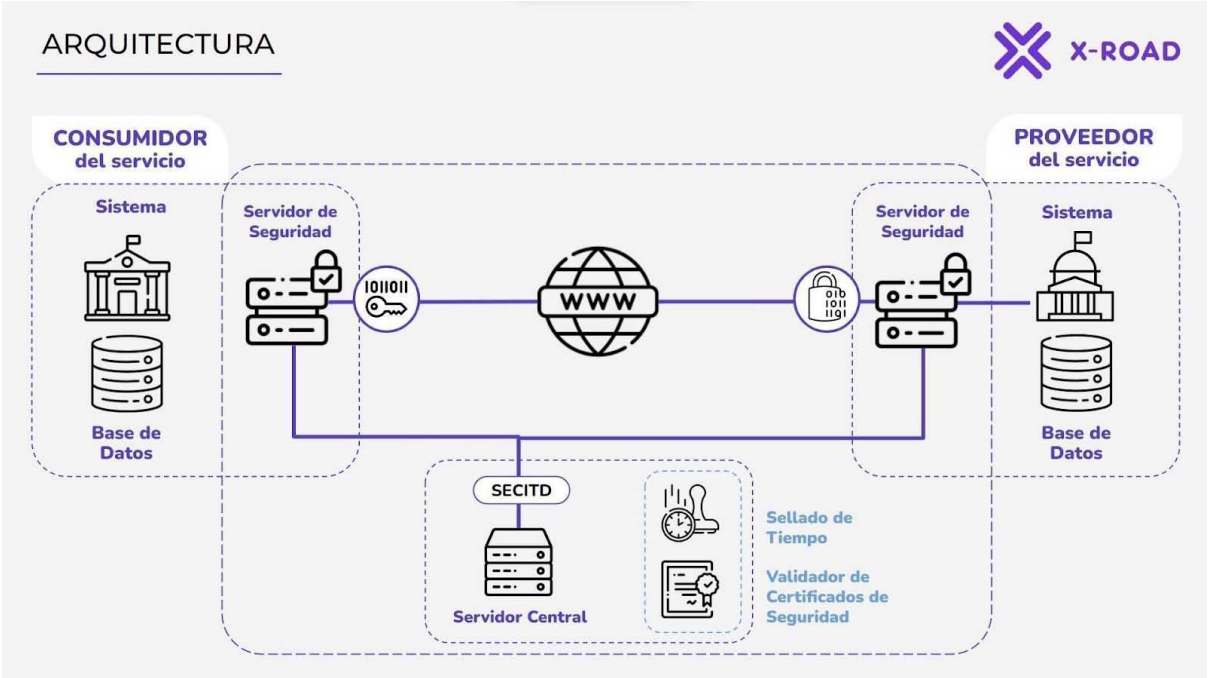
La arquitectura a implementar asegura un conjunto de funciones estándar para respaldar y facilitar el intercambio de datos dentro de una red de confianza, garantizando su integridad e interoperabilidad entre las Organizaciones Miembro del Sistema de Interoperabilidad mediante sus componentes.

1.1 Componentes y sus principales funcionalidades

- Servidor Central: Coordina el funcionamiento de la red de interoperabilidad. Es único y administra el registro de organizaciones miembro, servidores de seguridad, contiene la política de seguridad y las listas de autoridades certificantes y de sellado de tiempo.
- Servidor de Seguridad: Gestiona la creación de subsistemas, la disponibilización de servicios web y su control de acceso. Cada Organización Miembro gestionará a través de un Servidor de Seguridad y este debe contener al menos un Nodo de Seguridad, el cuál actúa como una puerta de seguridad para producir y consumir servicios.
- Sistemas de Información: Utiliza y/o proporciona servicios a través de cada servidor de seguridad.
- Sellado de Tiempo: Certifica la existencia de elementos de datos en el momento de la consulta al servicio web.
- Certificación Digital: Auténtica y verifica la identidad de los participantes de cada transacción.

1.2 Esquema de Arquitectura

La arquitectura del Sistema de Interoperabilidad sigue el siguiente esquema:



El esquema representa una instancia básica del Sistema de Interoperabilidad entre dos Organizaciones Miembro con servidores de seguridad que funcionan con nodos únicos.

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 utilizarán la configuración necesaria para garantizar el principio de Alta Disponibilidad.

2. Utilización y Funcionamiento

El Sistema de Interoperabilidad es una instancia de acceso regulada por el Operador del Sistema. Para interoperar datos a través del mismo, los proveedores y consumidores de servicios, previamente deberán registrarse como Organización Miembro en el Sistema de Interoperabilidad, conforme al Anexo III de la presente Resolución.

Para ser miembros activos, deberán instalar, configurar, y registrar en el Servidor Central, un Servidor de Seguridad de la Organización de acuerdo a los estándares establecidos por la ASINF, conforme la Ley N° 2.689.

Una vez aprobada dicha solicitud, se deberán gestionar los accesos correspondientes mediante el Portal de Gestión de Servicios de Interoperabilidad (en adelante “PGSI”).

La arquitectura del Sistema de Interoperabilidad permite un modelo de interoperabilidad descentralizado, en el cual las Organizaciones Miembro pueden interoperar datos a través de sus Servidores de Seguridad.

El Servidor de Seguridad propicia una capa de seguridad, proporcionando una forma estandarizada y segura de producir y consumir servicios, permitiendo la gestión en el intercambio de manera confidencial, segura y auditable.

El intercambio se realiza mediante firmas digitales con certificados emitidos por fuentes autorizadas por el Servidor Central, por lo que solo se podrá hacer uso de estos. Las transacciones están resguardadas por un sellado de tiempo centralizado, garantizando el no repudio entre las partes.

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

El Servidor 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, accesible a través del PGSI.

Cuando una Organización Miembro, ya registrada, requiera utilizar un servicio que no produce, deberá solicitar a la Fuente Auténtica que le otorgue los derechos de acceso mediante el PGSI, conforme el procedimiento que se establece en el Anexo II.

3. Beneficios

Este tipo de arquitectura cuenta con los siguientes beneficios:

- 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.
- Escalabilidad, tanto en el número de Organizaciones Miembros como en la frecuencia de uso.

- No existe un punto único de falla, es decir, al ser un modelo distribuido, puede fallar alguno de los servidores de seguridad sin ocasionar una falla global del sistema.

4. Federación

La arquitectura del Sistema de Interoperabilidad permite extender la Interoperabilidad a un modelode Federación, en el que múltiples sistemas de interoperabilidad se unen para formar una red colaborativa y segura de intercambio de datos y servicios.

Bajo este escenario, cada Sistema mantiene su propia infraestructura local, que incluye sus servicios y datos. Al unirse a la federación, conforme se encuentra establecido en el punto 5. de la Sección II del Anexo III del presente, estas entidades se conectan entre sí a través de un conjunto común de estándares y protocolos, para permitir la comunicación y el intercambio de información de manera confiable.

5. Auditoría y Monitoreo

Todos los intercambios de datos se registran localmente en los Servidores de Seguridad de las Organizaciones Miembro involucradas (proveedor/consumidor). Ningún tercero tiene acceso a los mismos.

Los registros de auditoría de cada Servidor 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 Servidor 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.

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2023.11.08 17:50:08 -03'00'

AXEL MC CALLUM
Director General
D.G. EFICIENCIA ADMINISTRATIVA
MINISTERIO JEFATURA DE GABINETE

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2023.11.08 17:50:08 -03'00'

Anexo

Número: IF-2023-41754764-GCABA-DGEADM

Buenos Aires, Miércoles 8 de Noviembre de 2023

Referencia: ANEXO II REGLAMENTO DE USO DEL PORTAL DE GESTIÓN DE SERVICIOS DE INTEROPERABILIDAD

ANEXO II

REGLAMENTO DE USO DEL PORTAL DE GESTIÓN DE SERVICIOS DE INTEROPERABILIDAD

SECCIÓN I

INTRODUCCIÓN

1. Objeto

El Portal de Gestión de Servicios de Interoperabilidad (en adelante "PGSI") es una plataforma digital que proporciona un canal seguro para que las Organizaciones Miembro gestionen servicios y solicitudes de consumo de servicios en el Sistema de Interoperabilidad del Gobierno de la Ciudad Autónoma de Buenos Aires "X-BA".

Su objetivo principal es facilitar estas operaciones de manera controlada y confiable, mejorando la eficiencia y la seguridad en la colaboración entre las organizaciones que forman parte del sistema.

Para resguardar la seguridad, el acceso al PGSI brinda una gestión centralizada de permisos de acceso, restringiendo su uso a usuarios autorizados por las Organizaciones Miembro con autoridad para disponer, solicitar y autorizar el consumo de servicios de la Organización.

Asimismo, el PGSI registra los servicios disponibles en el Sistema de Interoperabilidad, como también lleva un registro de las solicitudes y la gestión de las mismas por parte de las Organizaciones Miembro.

2. Alcance

Las Organizaciones Miembros deberán usar el PGSI para disponibilizar sus servicios en el Sistema de Interoperabilidad, gestionar las solicitudes referidas a los mismos, administrar los usuarios para el uso de la plataforma y el monitoreo de los servicios.

Cada Organización Miembro del Sistema de Interoperabilidad deberá designar a un referente técnico, quién será el representante de la organización en el Sistema, asumiendo el rol de Administrador de Usuarios, detallado en la Sección III del presente Anexo.

SECCIÓN II

COMPONENTES DEL PORTAL

El Portal de Gestión del Sistema de Interoperabilidad estará integrado por diversos componentes:

1. Catálogo de Servicios (CAS): listado de servicios web disponibles en el Sistema de Interoperabilidad del GCABA para que las Organizaciones Miembro puedan utilizarlos en sus sistemas de información.

2. Catálogo de Organizaciones Miembro (COM): listado de Organizaciones ya registradas como Miembros del Sistema de Interoperabilidad del GCABA.

3. Gestor de Usuarios y Permisos (GEUP): componente del Portal para la designación de usuarios y asignación de permisos para gestionar diversas acciones dentro del mismo.

4. Gestor de Solicitudes (GES): componente del Portal destinado a realizar la gestión y el seguimiento de todas las solicitudes de acceso al mismo.

5. Centro de Monitoreo (CEM): componente del Portal en el cual se puede monitorear el funcionamiento de los nodos de seguridad y los servicios gestionados a través del Servidor de Seguridad.

SECCIÓN III

ROLES DEL PORTAL

El PGSI cuenta con tres roles a fin de garantizar un control adecuado y seguro para la interoperabilidad y el acceso a los datos y servicios.

1. Administrador del Portal: responsable de la gestión general del PGSI. Sus responsabilidades incluyen la asignación de los administradores de usuarios de cada Organización Miembro, en función de la definición tomada por las autoridades correspondientes, el monitoreo del funcionamiento de servicios y servidores de seguridad del Sistema de Interoperabilidad, y la supervisión y administración del funcionamiento global del portal.

El Portal de Gestión de Servicios de Interoperabilidad.es administrado por la Dirección General de Eficiencia Administrativa dependiente de la Secretaría de Innovación y Transformación Digital, o el organismo que en un futuro la reemplace (en adelante “DGEADM”).

2. Administrador de usuarios de la Organización Miembro: única persona designada por cada Organización Miembro cuya responsabilidad es gestionar los usuarios que actuarán como gestores del servidor de seguridad dentro de cada Organización Miembro. Su principal responsabilidad es asegurar que los usuarios designados cuenten con los permisos y accesos adecuados en el servidor de seguridad.

Deberá garantizar, además, la actualización y veracidad de la información de sus usuarios gestores, como así también revocar los permisos en caso de cese de sus funciones.

Asimismo, es responsable del monitoreo del estado de los servidores de seguridad de la Organización Miembro, y tiene acceso al monitoreo de los servicios disponibles y consumidos por el servidor de seguridad.

La autoridad máxima de cada Organización Miembro es quien definirá al administrador de usuarios, mediante una Comunicación Oficial para el supuesto de las organizaciones mencionadas en el punto 1.1 de la Sección II del Anexo III de la presente Resolución, y mediante el trámite de “Solicitud de Alta como Organización Miembro - Sistema de Interoperabilidad GCABA” de la plataforma de Trámites a Distancia (TAD), para las organizaciones mencionadas en el punto 1.2 de la Sección II del Anexo III.

3. Gestor del Servidor de Seguridad: responsable del registro y administración de subsistemas dentro del

servidor de seguridad y de la publicación de nuevos servicios web. Debe solicitar y gestionar los permisos de accesos de los mismos a otras Organizaciones Miembro por medio del PGSI, y monitorear el estado de los servicios que gestiona.

Será designado un Gestor del Servidor de Seguridad por el Administrador de Usuarios de la Organización Miembro.

SECCIÓN IV

FUNCIONALIDADES

1. Catálogo de Servicios

1.1. Publicación de Servicios Web

Cualquier nuevo servicio web que se disponibilice en el Sistema de interoperabilidad, deberá ser publicado por un Gestor del Servidor de Seguridad en el catálogo de servicios con la información y documentación pertinente que permita comprender su uso y alcance.

1.2 Actualización del Catálogo de Servicios

Las Organizaciones Miembro, a través de los Gestores del Servidor de Seguridad, deberán mantener actualizada la información y documentación de los servicios del catálogo, incluyendo descripciones, características y cualquier cambio relevante que se realice.

1.3 Solicitudes de acceso a servicios

Cada Organización Miembro podrá solicitar acceso a los servicios disponibles en el catálogo de servicios, debiendo fundamentar el pedido de acuerdo a las necesidades de uso del mismo, y las competencias de la organización.

La Organización Miembro que sea fuente auténtica de un servicio, a través del Gestor del Servidor de Seguridad, podrá aceptar o rechazar las solicitudes de consumo de sus servicios. En cumplimiento del principio de cooperación, los rechazos deberán ser debidamente fundamentados.

2. Gestión de usuarios y organizaciones miembro

2.1 Organizaciones Miembro

Es obligación de las Organizaciones Miembro, a través del Administrador de Usuarios, mantener actualizada la información y datos de contacto requeridos en el Catálogo de Organizaciones Miembro.

2.2 Asignación de usuarios y permisos

El alta, baja o modificación de usuarios y permisos deberá ser gestionado por el Administrador de Usuarios a través del PGSI.

3. Monitoreo de nodos y servicios

Cada Organización Miembro podrá monitorear el estado de los Nodos de Seguridad que opera, de los servicios que provee y los servicios que consume de otras Organizaciones Miembro.

Los registros de auditoría de cada Servidor de Seguridad pueden ser utilizados como prueba en caso de requerimiento judicial a la Organización Miembro, quien será la responsable de brindar dicha información,

SECCIÓN V

OBLIGACIONES DE LOS USUARIOS

1. Administrador del Portal

Son obligaciones del Administrador del Portal:

1. Supervisar el correcto funcionamiento del sistema y solicitar las acciones necesarias a las Organizaciones Miembro, para garantizar su disponibilidad y rendimiento.

2. Solicitar auditorías técnicas a las Organizaciones Miembros del Sistema de Interoperabilidad, para verificar el cumplimiento de las normas y asegurar la integridad y seguridad de los datos.

3. Mantener actualizado el catálogo de Organizaciones Miembro

4. Proporcionar soporte técnico y capacitación a los administradores de usuarios y gestores de servidores de seguridad de las organizaciones miembro que así lo requieran.

5. Monitorear el correcto funcionamiento de los nodos y servicios del Sistema de Interoperabilidad, contactando a las Organizaciones Miembro correspondientes en caso de incidentes.

6. Administrador de Usuarios de las Organizaciones Miembro

Son obligaciones del Administrador de Usuarios de las Organizaciones Miembro:

1. Asignar roles y permisos adecuados a los usuarios de su organización para acceder a los servicios y datos necesarios.

2. Mantener actualizada la información de los usuarios y garantizar que solo el personal autorizado tenga acceso a la plataforma.

3. Cumplir con las políticas de seguridad y las directrices establecidas por el administrador del sistema.

4. Serán responsables de las acciones de los gestores del servidor de seguridad que hayan designado.

5. Monitorear el correcto funcionamiento del nodo de seguridad y los servicios que utiliza la Organización Miembro dentro del Sistema de Interoperabilidad, notificando al ecosistema en caso de incidentes.

6. Gestor del Servidor de Seguridad

Son obligaciones del Gestor del Servidor de Seguridad:

1. Brindar información detallada, a pedido de parte y actualizar los datos brindados en el catálogo de servicios.

2. Brindar datos correctos y completos sobre los servicios bajo su gestión.

3. Ante la decisión de discontinuar la provisión de un servicio ofrecido en el Catálogo de Servicios por un servidor de seguridad, deberá informar a las áreas consumidoras en un plazo previo de tres (3) meses, para permitir e implementar un rediseño funcional adecuado.

4. Ante la realización de tareas de mantenimiento que afecten la operativa y disponibilidad de los servicios, deberán comunicar a las Organizaciones Miembro consumidoras de los mismos, con al menos tres (3) días hábiles de anticipación.

5. Rechazar una solicitud de consumo de servicio, conforme lo detallado en el punto 1.1 de la Sección VI del presente Anexo.

6. Suspender el acceso de su servicio, conforme lo detallado en el punto 1.1 de la Sección VI del presente Anexo.

7. Notificar al Operador del Sistema de Interoperabilidad ante cualquier suspensión realizada.

8. Notificar a las Organizaciones Miembro consumidoras de sus servicios en un plazo de tres (3) meses frente a cualquier modificación de los servicios provistos para permitir adecuar el consumo de los mismos.

9. Notificar de manera inmediata al Operador del Sistema de Interoperabilidad ante cualquier vulnerabilidad de seguridad en los sistemas proveedores o consumidores de servicios bajo su gestión.

10. Monitorear el correcto funcionamiento de los servicios provistos y consumidos por la Organización Miembro, dando aviso a las contrapartes frente a cualquier incidencia.

SECCIÓN VI

RECHAZO, SUSPENSIÓN Y EXPULSIÓN

El incumplimiento de las obligaciones establecidas podrá dar lugar a la aplicación de las siguientes sanciones:

1. Servicios

1.1. Rechazo

El Gestor del Servidor de Seguridad de la organización proveedora de un servicio, podrá rechazar un pedido de consumo del mismo, si entiende que la organización solicitante no tiene competencias y/o facultades para el consumo de ese dato, y/o entiende que el caso de uso propuesto no cumpliría con los principios establecidos en el Sistema de Interoperabilidad.

1.2 Suspensión y Revocación

La fuente auténtica de un servicio podrá suspender o revocar el acceso al mismo, si entiende que la organización no hizo un uso correcto de éste o vulneró alguno de los principios del marco normativo del Sistema de Interoperabilidad.

2. Usuarios

2.1 Administrador del portal

El administrador del portal, podrá solicitar auditorías técnicas a las Organizaciones Miembro , para verificar el cumplimiento de las normas y asegurar la integridad y seguridad de los datos.

En caso de incumplimiento o detección de irregularidades, el administrador del portal tomará las medidas necesarias, que pueden incluir la suspensión o revocación de permisos y la aplicación de sanciones según lo establecido en las normativas vigentes.

El administrador del portal puede suspender o expulsar al administrador de usuarios y deberá notificar fehacientemente la decisión justificada a la Organización Miembro.

2.2 Organizaciones Miembro

El Administrador de Usuarios puede rechazar un pedido de usuario gestor del servidor de seguridad si considera que éste no cumple con las competencias para ejecutar ese rol.

El Administrador de Usuarios puede suspender o expulsar usuarios gestores del servidor de seguridad ante la detección de incumplimiento de sus obligaciones.

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2023.11.08 17:50:24 -03'00'

AXEL MC CALLUM
Director General
D.G. EFICIENCIA ADMINISTRATIVA
MINISTERIO JEFATURA DE GABINETE

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2023.11.08 17:50:24 -03'00'

Anexo

Número: IF-2023-41754793-GCABA-DGEADM

Buenos Aires, Miércoles 8 de Noviembre de 2023

Referencia: ANEXO III - GOBERNANZA DEL SISTEMA DE INTEROPERABILIDAD

ANEXO III

GOBERNANZA DEL SISTEMA DE INTEROPERABILIDAD

1. Objeto:

El presente Anexo tiene por objeto definir la Gobernanza aplicable al Sistema de Interoperabilidad del GCABA "X-BA", descripto en la Sección II del Anexo I, los actores participantes y losprocesos involucrados.

Todos los preceptos detallados en el presente revisten el carácter de obligatorio para la Interoperabilidad entre las Organizaciones Miembro del Sistema, sean de carácter público o privado, y deberán aplicarse para garantizar la exactitud, calidad y seguridad de los datos.

Para el supuesto de las Organizaciones Miembro mencionadas en el punto 1.1, Sección II del presente Anexo, las mismas deberán adecuar sus trámites e integraciones a fin de migrar la disponibilización y consumo de servicios al Sistema de Interoperabilidad.

Se deberá tender a la interoperabilidad a través del Sistema de Interoperabilidad con otros gobiernos.

SECCIÓN I

ROLES DENTRO DEL SISTEMA DE INTEROPERABILIDAD

1. Roles

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 mismo.

1.1. Operador del Sistema de Interoperabilidad

Dentro de las responsabilidades se encuentran:

- Definir regulaciones y prácticas.
- 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 o el organismo que en un futuro la reemplace (en adelante "SECITD") a través de las Direcciones a su cargo y de la Agencia de Sistemas de Información (ASINF), como Operador del Sistema de Interoperabilidad del GCABA, coordinará con las áreas de Gobierno según su competencia.

1.2. Proveedor/es de Servicios de Confianza:

1.2.1. Autoridad de Servicio de Sellado de Tiempo (TSA):

A todos los mensajes intercambiados a través del Sistema de Interoperabilidad se les aplica un sellado de tiempo y son registrados por los servidores 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.

1.2.2. Autoridad de Certificación (CA)

Todos los Servidores 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 Servidores de Seguridad dentro del Sistema de Interoperabilidad.

- Certificado de Firma: todo mensaje que se comparte entre Servidores 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 GCABA para la provisión de certificados. A futuro el Operador del Sistema podrá autorizar autoridades de certificación provistas por otras organizaciones.

1.3. 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 gestionar a través de un Servidor de Seguridad que les permita proveer y/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.

1.3.1. Servidor de Seguridad

La Organización Miembro gestiona para cada Servidor de Seguridad, ante la PKI de GCABA, dos tipos de certificados los que fueron descriptos en el punto 1.2.2 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 Servidor de Seguridad puede alojar varias Organizaciones Miembro (multicliente).

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

1.3.2. 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 Servidores de Seguridad, mediante el uso de APIs o Servicios Web.

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

SECCIÓN II

INGRESO AL SISTEMA DE INTEROPERABILIDAD

1. Solicitud de ingreso de Organización Miembro

1.1. Solicitud de ingreso para las entidades y jurisdicciones comprendidas en el artículo 4° de la Ley N° 70 (texto consolidado por Ley N° 6.588):

Para iniciar la solicitud de ingreso como Organización Miembro del Sistema de Interoperabilidad, las entidades y jurisdicciones comprendidas en el artículo 4° de la Ley N° 70 (texto consolidado por Ley N° 6.588), deberán enviar una Comunicación Oficial (en adelante "CCOO") a través del Sistema de Administración de Documentos Electrónico (en adelante, SADE), dirigida a la SECITD, firmada por la máxima autoridad de la repartición, designando en la misma una persona como responsable de la Organización ante el Sistema de Interoperabilidad conforme el modelo que oportunamente apruebe la Dirección General de Eficiencia Administrativa, o el organismo que en un futuro la reemplace.

La persona designada como responsable de la Organización Miembro será definida como Administradora del Servidor de Seguridad y como Administrador de Usuarios del Portal de Gestión de Servicios de Interoperabilidad.

1.2. Solicitud de ingreso para el Sector Privado y otras entidades

Para dar inicio a la solicitud de ingreso como Organización Miembro del Sistema de Interoperabilidad, el interesado deberá iniciar el trámite "Solicitud de Alta como Organización Miembro - Sistema de Interoperabilidad GCBA", a través de la Plataforma de Trámites a Distancia (TAD), debiendo cumplir con los requisitos allí solicitados e informar en el mismo al responsable de la Organización ante el Sistema de Interoperabilidad y el administrador de usuarios de la Organización Miembro. Dicho trámite deberá ser gestionado por la autoridad que firmará el Convenio, con facultades suficientes.

Una vez aprobada la solicitud del trámite iniciado en TAD, se suscribirá el Convenio correspondiente, conforme lo establecido en el artículo 5° del Decreto N° 118/22, previo análisis de los antecedentes de hecho y de derecho que sustenten el proyecto.

1.3. Solicitud de ingreso para otras jurisdicciones y Gobiernos

Conforme lo establecido en el artículo 5° del Decreto N° 118/22 se suscribirán los Convenios correspondientes, previo análisis de los antecedentes de hecho y de derecho que sustenten el proyecto de Convenio.

2. Evaluación de solicitudes de ingreso al Sistema de Interoperabilidad

La Dirección General de Eficiencia Administrativa dependiente de la Secretaría de Innovación y Transformación Digital o el organismo que en un futuro la reemplace, (en adelante DGEADM), evaluará el registro de nuevas Organizaciones Miembro, y recomendará su aceptación o rechazo de acuerdo a los estándares mencionados y el cumplimiento de la presente Resolución.

La SECITD podrá negarse a celebrar el Convenio de suscripción y rechazar la solicitud de ingreso como Organización Miembro del Sistema de Interoperabilidad si:

1. la Autoridad no ha presentado los documentos requeridos para verificar el derecho de representación solicitado o la persona respectiva no tiene el derecho de representación para representar a la Autoridad en cuestión;

2. los datos proporcionados son incorrectos;

3. el interesado o su sistema de información no cumple con los lineamientos establecidos en el presente Anexo

La DGEADM 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.

Asimismo, podrá controlar el uso del Sistema de Interoperabilidad con fines estadísticos y para garantizar la calidad del mismo.

También, podrá recomendar a la SECITD 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 1.1 de la presente Sección, las notificaciones se realizarán por medio de una Comunicación Oficial por SADE, a la máxima autoridad de la repartición.

En el caso de las Organizaciones Miembro mencionadas en el punto 1.2 de la presente Sección, las notificaciones se realizarán por medio de TAD dirigidas a la máxima autoridad solicitante.

Por último, tratándose de las Organizaciones Miembro mencionadas en el punto 1.3 de la presente Sección, las notificaciones se deberán realizar mediante Comunicaciones Oficiales si la organización se encuentra dentro del ecosistema GDE, como repartición notificable (IOP), o en su defecto se realizará la notificación fehaciente al domicilio constituido.

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 (texto consolidado por Ley N° 6.588), mediante certificados emitidos por una Autoridad de Certificación (CA).

3. 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 y/o incumplimientos, durante, la incorporación y utilización del Sistema de Interoperabilidad, la DGEADM pondrá en conocimiento a la SECITD a fin de poder rechazar, suspender o expulsar a la Organización Miembro. Respecto a las Organizaciones Miembro mencionadas en el punto 1.1 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 1.2 de la presente Sección, las notificaciones se realizarán por medio de notificaciones electrónicas fehacientes a través de la plataforma TAD dirigidas a la máxima autoridad solicitante.

Por último, tratándose de las Organizaciones Miembro mencionadas en el punto 1.3 de la presente Sección, las notificaciones se deberán realizar mediante comunicaciones oficiales si la organización se encuentra dentro del ecosistema GDE, como repartición notificable (IOP), o en su defecto se realizará el de la notificación fehaciente al domicilio.

4. Solicitud de baja de una Organización Miembro

Las Organizaciones Miembro, integradas por el Sector Privado, otras jurisdicciones 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.

5. Federación del Sistema de Interoperabilidad

El Sistema de Interoperabilidad del Gobierno de la Ciudad de Buenos Aires podrá integrarse con otros sistemas de Interoperabilidad.

Para dar inicio a una federación se deberán suscribir los Convenios correspondientes, conforme a los requisitos específicos de cada país o entidad involucrada.

SECCIÓN III

TIPIFICACIÓN Y CALIDAD DE DATOS

1. Tipificación de Datos

En el marco de lo dispuesto por la Ley Nacional N° 25.326 y la Ley N° 1.845, ambas de Protección de los Datos Personales, se entiende por:

1.1. Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

1.2. Datos sensibles: Aquellos datos personales que revelan origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud o a la vida sexual o cualquier otro dato que pueda producir, por su naturaleza o su contexto, algún trato discriminatorio al titular de los datos.

2. Calidad

Dentro del Sistema de Interoperabilidad los datos deberán ser provistos por la fuente auténtica o en su excepción por la fuente secundaria con los accesos y permisos necesarios, cumpliendo con los deberes en materia de protección y calidad de datos impuestas por la normativa vigente, las cuales deberán cumplir y resguardar en todo el tratamiento, siendo responsables de velar por la exactitud y completitud de los mismos, comprendiendo con ello:

- Exactitud: los datos deberán cumplir las reglas de integridad explicitadas para cada campo en algún medio que las catalogue de forma unívoca y homogénea

- Completitud: todos los atributos del dato deben estar presentes en los registros

SECCIÓN IV

INTEROPERABILIDAD DE DATOS -CESIÓN- Y GOBERNANZA

1. Datos pasibles de ser interoperados

Cumpliendo con el marco normativo vigente y con los principios y condiciones establecidos para el Sistema de Interoperabilidad, los datos personales son pasibles de ser interoperados entre Organizaciones Miembros. En los casos que el marco normativo lo requiera se deberá solicitar el consentimiento libre, expreso e informado del titular del dato para consultar y compartir datos entre Organizaciones Miembro.

No será necesario el consentimiento cuando se trate de datos personales que se recaben para el ejercicio de funciones propias de los poderes de la Ciudad de Buenos Aires, o en virtud de una obligación legal o cuando los mismos se obtengan de fuentes de acceso público irrestricto, conforme lo dispuesto por la Ley N° 1845 (texto consolidado por Ley N° 6.588).

Los datos sensibles podrán ser interoperados en la medida que se cumpla con lo dispuesto por la Ley N° 1845 (texto consolidado por Ley N° 6.588).

Conforme los principios rectores del Sistema, el uso de los datos interoperados debe ser delimitado, debiendo ser tratados únicamente con el fin para los cuales fue autorizado su consumo. El registro que se obtuvo de la consulta no deberá reutilizarse para la validación de un dato en un proceso posterior. Los datos obtenidos por la interoperabilidad no podrán cederse a terceros.

A modo de excepción, una Organización Miembro perteneciente al GCABA podrá solicitar disponibilizar un servicio como fuente secundaria en el Sistema de Interoperabilidad cuando la fuente auténtica sea un ente público de otra jurisdicción que no opere dentro del Sistema de Interoperabilidad.

En estos casos, la Organización Miembro que actuará como fuente secundaria deberá contar con los accesos y permisos necesarios de la fuente auténtica y estará sujeta a las mismas condiciones que una fuente auténtica.

A los efectos de la interoperabilidad de datos que se propicia se deberá atender siempre a los siguientes permisos y obligaciones:

- Para proveer un servicio:
    - Ser fuente auténtica del dato, o contar con los accesos y permisos que le permitan actuar como fuente secundaria del dato.
    - La Organización Miembro, por medio del responsable de datos, el responsable de negocio, o el responsable técnico, apruebe su uso, asignación de actores y roles enunciada precedentemente
- Para consumir un servicio:
    - Haber solicitado por el portal de gestión de servicios de interoperabilidad dicho consumo y contar con la autorización de la fuente auténtica;
    - Utilizar el dato para el Caso de Uso delimitado.
    - Contar con el consentimiento del titular del dato cuando así sea requerido conforme lo establecido en la Ley N° 1845 (texto consolidado por Ley N° 6.588).

2. Interoperabilidad de datos entre organizaciones miembro pertenecientes al GCABA

El uso del Sistema de Interoperabilidad es de carácter obligatorio para las reparticiones del GCABA, las cuales deberán migrar la disponibilización y consumo de servicios al sistema de interoperabilidad en un plazo máximo de dos (2) años.

La interoperabilidad de datos sensibles dentro del GCABA se regirá por lo dispuesto en la Ley N° 1.845 (texto consolidado por Ley N° 6.588).

3. Interoperabilidad de datos entre organizaciones de gestión pública y de gestión privada

Es factible interoperar datos entre Organizaciones Miembro de gestión pública y de gestión privada en el marco del sistema de Interoperabilidad ya que el mismo otorga transparencia y seguridad a los datos interoperados.

4. Interoperabilidad de datos entre Organizaciones Miembro pertenecientes al GCABA y otras jurisdicciones y Gobiernos

Se priorizará la interoperabilidad de datos a través del Sistema de Interoperabilidad. Un ente público externo al GCABA podrá interoperar con el Sistema de Interoperabilidad del GCABA ingresando como Organización Miembro o a través de la federación de sistemas.

Las partes deberán cumplir permisos y obligaciones definidos en el punto 3 de la presente Sección.

5. Responsabilidad

La Fuente Auténtica, 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 y responde por el contenido de la misma. La SECITD, o la autoridad de aplicación que en un futuro la reemplace, no será responsable por la exactitud, veracidad o completitud de la información brindada por la Organización cuando ésta sea publicada en el Portal de Gestión de Servicios de Interoperabilidad, tal como fue entregada.

El Gobierno de la Ciudad Autónoma de Buenos Aires no será responsable de las consecuencias que puedan resultar de las infracciones de una Organización Miembro que afecten los derechos de otra.

Toda Organización Miembro por intermedio del Gestor del Servidor de Seguridad, deberá notificar de manera inmediata al Operador del Sistema de Interoperabilidad ante cualquier vulnerabilidad de seguridad en los sistemas proveedores o consumidores de servicios bajo su gestión.

SECCIÓN V

IMPLEMENTACIÓN DE CASOS DE USO

La aplicación efectiva del Sistema de Interoperabilidad se efectúa a través de la implementación de Casos de Uso, los cuales 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 del Portal de Gestión de Servicios de Interoperabilidad, y que lo consuma otra Organización Miembro, con derechos de acceso a ese servicio, cumpliendo con los estándares del Sistema de Interoperabilidad, interoperando un dato o documento con el fin de simplificar, eficientizar o mejorar un trámite o proceso.

1. Identificación de Caso de Uso

Consiste en identificar un dato o documento que pueda ser interoperado entre dos Organizaciones Miembro con el fin de simplificar, eficientizar o mejorar un trámite o proceso.

1.1. Detección de Oportunidad

La detección de oportunidades puede realizarse desde cualquier Organización Miembro o actor interesado

en ser miembro del Sistema de Interoperabilidad.

1.1.1. Catálogo de Servicios

Contiene un listado de servicios web disponibles para las Organizaciones Miembro del Sistema de Interoperabilidad, por parte de las Fuentes Auténticas. El Catálogo es administrado por el Operador del Sistema y estará disponible para las Organizaciones Miembro en el Portal de Gestión de Servicios de Interoperabilidad. A través de él, las Organizaciones Miembro podrán explorar los servicios web disponibles en el Sistema, solicitar el consumo de un servicio existente o solicitar la creación de un servicio nuevo.

Con el objetivo de promover el crecimiento del Sistema de Interoperabilidad, la DGEADM mantendrá una versión pública del Catálogo de Servicios que será de acceso irrestricto. La versión pública del catálogo listará los servicios disponibles en el Sistema de Interoperabilidad, y las Fuentes Auténticas de los mismos, sin brindar la posibilidad de solicitar el consumo.

1.1.2. Mapeo de Integraciones, Datos y Documentos (MIDD)

Es una metodología estructurada utilizada para documentar los procesos y requisitos de los trámites de la Administración Pública, completando así el Inventario Único de Trámites (IUT). A través del mapeo se identifican oportunidades de interoperabilidad entre sistemas y aplicaciones gubernamentales, promoviendo el intercambio de información de manera más eficiente, optimizando procedimientos administrativos.

El MIDD releva: los requisitos de cada trámite, los documentos y datos solicitados para dar cumplimiento a dichos requisitos, la validación realizada sobre los datos y documentos, el proceso de gestión del trámite el volumen de las tramitaciones, las áreas involucradas, los sistemas utilizados y dónde se almacena la información.

1.2. Consideraciones

Al identificar un potencial Caso de Uso se deberán considerar los siguientes aspectos:

1.2.1. Consideraciones Generales

Normativa Vigente: 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.

Madurez Técnica: las organizaciones involucradas en el Caso de Uso deben contar con capacidad técnica para operar de manera segura y confiable en el Sistema de Interoperabilidad.

Calidad del Dato: la información involucrada en el Caso de Uso debe cumplir con los estándares, lineamientos y protocolos en materia de Gobernanza de Datos conforme lo establecido en el Decreto Nº 118/22.

Seguridad: proveer un mayor nivel de resguardo en transacciones de datos privados.

1.2.2. Consideraciones para el GCABA

Impacto Ciudadano y/o Productivo: priorizar trámites y procesos con mayor volumen de gestión por parte de los ciudadanos y sectores productivos, personas humanas como personas jurídicas.

Eficiencia Administrativa: priorizar la interoperabilidad de datos, documentación y/o los registros expedidos por un organismo del GCABA que son requeridos por otras reparticiones del GCABA para la

gestión de trámites.

2. Diseño del Caso de Uso

Identificada la oportunidad de interoperar, la Organización propiciante se contactará con la contraparte para diseñar en conjunto el Caso de Uso. El diseño de la solución a través del Sistema de Interoperabilidad, deberá contemplar tres (3) aspectos:

2.1. Normativo

Verificación del cumplimiento de los principios rectores del Sistema de Interoperabilidad y el marco normativo vigente. La solución diseñada deberá operar dentro del alcance de las misiones y funciones de las Organizaciones Miembro intervinientes.

2.2. Tecnológico

Disponibilización de la infraestructura para un Servidor 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 como también del PGSI.

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.

2.3. Funcional

Modificación, rediseño y/o 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.

3. Implementación del Caso de Uso

Finalizado el diseño en conjunto, la Organización Miembro consumidora solicitará a la Organización Miembro proveedora, a través del PGSI, el consumo del servicio necesario, fundamentando la solicitud y limitando su uso al Caso de Uso acordado. La Organización Miembro proveedora evaluará la solicitud y aceptará o rechazará según corresponda.

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

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2023.11.08 17:50:40 -03'00'

AXEL MC CALLUM
Director General
D.G. EFICIENCIA ADMINISTRATIVA
MINISTERIO JEFATURA DE GABINETE

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2023.11.08 17:50:41 -03'00'