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'