

Gobernanza de Datos

Proceso de **Gestión de Acceso a Datos**

SECRETARÍA DE INNOVACIÓN Y TRANSFORMACIÓN DIGITAL

SUBSECRETARÍA DE POLÍTICAS PÚBLICAS BASADAS EN EVIDENCIA



Jefe de Gobierno

Horacio Rodríguez Larreta

Jefe de Gabinete

Felipe Miguel

Secretario de Innovación y Transformación Digital

Diego Fernández

Subsecretaria de Políticas Públicas Basadas en Evidencia

Melisa Breda

Índice

1. Introducción	3
2. Objetivo del Proceso de Gestión de Alta de Acceso a Datos	5
2.1. Objetivo del Proceso de Gestión de Alta de Acceso a Datos	5
2.2. Alcance del proceso de gestión de alta de acceso a datos	5
2.3. Entrada del proceso de gestión de alta de acceso a datos	6
2.4. Propietario del proceso de gestión de alta de acceso a datos	6
2.5. Salida del proceso de gestión de alta de acceso a datos	6
1. 2.6. Flujo del Proceso de Gestión de Alta de Acceso a Datos	7
2.6.1. Ingresar solicitud de acceso	7
2.6.2. Analizar solicitud de acceso a datos	7
2.6.3. Gestionar acceso a datos	8
2.6.4. Comunicar rechazo	8
2.7. Subproceso analizar solicitud de acceso a datos	8
2.7.1. Objetivo del subproceso analizar solicitud de acceso a datos	9
2.7.2. Alcance del subproceso analizar solicitud de acceso a datos	9
2.7.3. Entradas del subproceso analizar solicitud de acceso a datos	9
2.7.4. Propietario del subproceso analizar solicitud de acceso a datos	10
2.7.5. Salida del subproceso analizar solicitud de acceso a datos	10
2. 2.7.6. Flujo del subproceso analizar solicitud de acceso a datos	11
2.7.6.1. Verificar alcance de la solicitud (Aplicar guía de clasificación)	12
2.7.6.2. Rectificar Solicitud	12
2.7.6.3. Derivar solicitud	12
2.7.6.4. Validar y aplicar guía de clasificación	12
2.7.6.5. Arbitrar solicitud de acceso	13
2.8. Subproceso gestionar acceso a datos	13
2.8.1. Objetivo del subproceso gestionar acceso a datos	14
2.8.2. Alcance del subproceso gestionar acceso a datos	14
2.8.3. Entrada del subproceso gestionar acceso a datos	14
2.8.4. Propietario del subproceso gestionar acceso a datos	14
2.8.5. Salidas del subproceso gestionar acceso a datos	14
3. 2.8.6. Flujo del subproceso gestionar acceso a datos	15
4. 2.8.6.1.1. Especificar y desarrollar	15
5. 2.8.6.1.2. Otorgar acceso a fuente/repositorio	15
3. Proceso de gestión de baja de acceso a datos	16
3.1. Objetivo del proceso de gestión de baja de acceso a datos	16

3.2. Alcance del proceso de gestión de baja de acceso a datos	16
3.3. Entrada del proceso de gestión de baja de acceso a datos	16
3.3.1. Ingreso de solicitud de baja de acceso	17
3.3.2. Auditoría de accesos	17
3.4. Propietario del proceso de gestión de baja de acceso a datos	17
3.5. Salida del proceso de gestión de baja de acceso a datos	17
3.6. Flujo del proceso de gestión de baja de acceso a datos	18
3.6.1. Ingresar Solicitud de Baja de Acceso	18
3.6.2. Analizar Alcance de la Solicitud de Baja	18
3.6.3. Auditoría de Accesos	19
3.6.4. Solicitar Revocación con Plazo Vencido	19
3.6.5. Revocar Acceso	19
Anexo	21
C. Contacto	21



En la era digital, los datos se han convertido en uno de los activos más valiosos para las organizaciones ya que desempeñan un rol fundamental en la gestión de procesos y toma de decisiones.

Reconociendo su importancia, el Gobierno de la Ciudad Autónoma de Buenos Aires (GCABA), a través de la Secretaría de Innovación y Transformación Digital (SECITD), ha adoptado una política de datos que busca fortalecer los procesos de obtención, integración y almacenamiento, con el objetivo de tomar decisiones basadas en evidencia y mejorar la vida de los vecinos que viven y transitan por la Ciudad.

Para lograr este propósito, el GCABA ha establecido una política de interoperabilidad como parte de su enfoque de gobernanza de datos. Estos lineamientos, basados en las mejores prácticas internacionales y el modelo DAMA-DMBOK, definen un marco común de gobernanza de datos que abarca todas las etapas del ciclo de vida de los mismos.

Con el objetivo de integrar y disponibilizar todos los datos del GCABA, en 2021 se implementó la Plataforma Inteligente de Buenos Aires (PIBA), a través de un data lake, que consiste en una herramienta de inteligencia aumentada.

En tanto, en 2022 se creó el Sistema de Interoperabilidad de la Ciudad de Buenos Aires (SI) con la intención de eficientizar los procesos y servicios de cara al ciudadano.

A continuación, se transmiten los lineamientos que rigen el data lake y que determinan los estándares que deben aplicarse en el ciclo de vida de gestión de datos. Los mismos establecen procesos claros y universales sobre cómo GCABA clasifica, comparte, accede, gestiona y protege los datos.

1. Introducción

El objetivo de este proceso es **definir cómo en el GCABA se realiza la solicitud, análisis y otorgamiento de acceso a datos, teniendo en cuenta los criterios de clasificación y si son datos personales o sensibles. En función del contexto** en el que se realiza la solicitud, el **proyecto involucrado y los datos solicitados** se podrá obtener una mejor interpretación del **alcance del acceso** solicitado.

El proceso el proceso aborda preguntas como: ¿Quién es el responsable del dato? ¿Para qué se utilizará? ¿Con qué objetivo? ¿Por cuánto tiempo? ¿Qué datos solicita? ¿Qué nivel de confidencialidad o sensibilidad tienen los datos? ¿En qué contexto y qué otros datos se van a utilizar? Y con ello poner el marco de usabilidad correspondiente para el acceso, avalados por los parámetros mencionados en la *Guía de Clasificación de Datos*, donde se detalla la normativa vigente en materia de protección de datos, criterios de clasificación de datos personales y sensibles, etc. Los datos públicos o de acceso irrestricto (ver *Guía de Clasificación*) no necesitan pasar por este proceso de autorización de acceso por parte de la Persona Dueña.

La gestión de accesos se divide en dos procesos: *Gestión de Alta de Acceso a Datos* y *Gestión de Baja de Acceso a Datos*. A su vez los procesos se descomponen en subprocesos, que en el futuro se relacionarán con procedimientos y herramientas para llevar a cabo las gestiones, aunque esto último está fuera del alcance de este documento.

Los roles de los actores involucrados en el proceso y subprocesos de gestión de acceso a Datos, son los mismos que fueron descritos detalladamente, con sus alcances y responsabilidades en la *Guía de Roles de Gobernanza de Datos*.

Cabe aclarar que este documento no define procedimientos de otorgamiento de permisos a bases de datos, repositorios o herramientas, toda vez que estos ya estén definidos y en funcionamiento por la Agencia de Sistemas de Información (ASI). **Lo que hace este documento es definir quiénes y de qué manera autorizan el otorgamiento de esos permisos**, es decir, quiénes son los responsables funcionales de los datos y por lo tanto quienes deben otorgar o denegar permisos, y cuál es el proceso que deben seguir para hacerlo.

En el caso que la Persona Dueña de los datos sea un actor externo a GCABA, quien puede administrar el acceso a esos datos es el área que gestiona los mismos dentro del convenio establecido entre las partes y el marco legal que brinda la *Guía de Clasificación de Datos* debiendo realizarse la anonimización de los mismos de ser posible.

Por otro lado, una buena práctica al trabajar con proveedores externos, es incluir en los pliegos de licitación o convenios firmados, un estándar o normativa para que dichos proveedores tengan la responsabilidad de brindar el acceso a los datos de los que el GCABA es dueño.



Como se mencionó en la *Guía de Roles de Gobernanza de Datos*, el DMBOK2 (Data Management Body of Knowledge) del framework de **DAMA** define una rueda que incluye **las áreas de conocimiento de Gestión de Datos en donde se sitúa la Gobernanza de Datos en el centro de las actividades de gestión** ya que se requiere gobernanza **para mantener la coherencia y el equilibrio entre las diferentes funciones**. Todas esas áreas de conocimiento se equilibran alrededor de la rueda y son necesarias para una administración de datos madura, pero no necesariamente deben implementarse en el mismo momento ya que unas dependen de la madurez de las otras y es una buena práctica ir evolucionando y escalando las mismas en el tiempo dado que **la gobernanza de datos es un proceso continuo**.

En este contexto, dentro de la **estrategia global de Gobernanza de Datos** se definen diferentes procesos y guías entre los cuales se encuentra el **Proceso de Gestión de Acceso a Datos** como una de las áreas de conocimiento involucradas en la Gestión de Datos. Este proceso se corresponde con el área de conocimiento de la rueda de DAMA que trata de la **Seguridad de los datos**.



DAMA-DMBOK Data Management Framework

Imagen 1. Rueda de procesos vinculados a la Gobernanza de Datos

Fuente: DAMA-DMBOK2 Data Management Framework. Copyright © 2017 - DAMA International

A continuación, se detallan los procesos y subprocesos que comprenden el Proceso de Gestión de Acceso a Datos.

2. Objetivo del Proceso de Gestión de Alta de Acceso a Datos

Partiendo de los roles definidos en la *Guía de Roles de Gobernanza de Datos* (cuya previa lectura es requisito fundamental para poder comprender los procesos definidos en este documento) se describen los pasos necesarios para que cualquier Persona Usuaria de Datos que pertenezca activamente al Gobierno de la Ciudad Autónoma de Buenos Aires o esté prestando determinado servicio al mismo, obtenga las autorizaciones necesarias para acceder a los datos. Estos pasos conllevan una secuencia de tareas que se deberán llevar a cabo por distintos roles para otorgar o denegar una solicitud de acceso a datos.

Comienza con la solicitud de acceso a datos y finaliza con el otorgamiento del acceso o con el rechazo de la solicitud. El proceso contempla que la aprobación o rechazo de una solicitud de acceso se realice dentro del marco de gestión de la privacidad y protección del activo, definido en la *Guía de Clasificación de Datos*.

2.1. Objetivo del Proceso de Gestión de Alta de Acceso a Datos

El objetivo de este proceso es gestionar y controlar los accesos de cualquier Persona Usuaria de Datos a los repositorios de datos, tener visibilidad de la trazabilidad de la gestión de solicitud de acceso y finalmente la disponibilización de los datos, todo esto dentro del marco de regulaciones y lineamientos previamente definidos en la Guía de Clasificación de Datos.

Este proceso será el mecanismo transparente que conecte a las Personas Dueñas de Negocio (dueña de los datos) y Personas Usuarias de Datos, logrando que los primeros compartan los datos y los segundos se encarguen de su tratamiento oportuno y ético.

En toda la gestión intervienen los roles de “Persona Dueña” de los programas, proyectos, prestaciones, servicios y políticas públicas de gobierno, así como los Data Champions quienes facilitan o limitan de manera justificada los accesos, como parte del camino hacia un gran cambio cultural de apertura, colaboración y transparencia en el manejo de la información.

2.2. Alcance del proceso de gestión de alta de acceso a datos

El alcance de este proceso abarca:

- La solicitud de acceso a los datos por parte de la Persona Usuaria, para consultarlos y/o explotarlos como se encuentran en el sistema fuente.
- Las solicitudes de datos que previamente requieran pasar por un proceso de integración y transformación que se incluye dentro del *proceso de desarrollo*.

Para todas las solicitudes de acceso a los datos, los otorgamientos o denegaciones deben sustentarse en los lineamientos definidos en la *guía de clasificación de datos*, y en el consentimiento previo de todos los roles responsables involucrados en el proceso.

2.3. Entrada del proceso de gestión de alta de acceso a datos

Este evento disparador (ingreso de una solicitud de acceso) es provocado por el rol de la Persona Usuaría de Datos, quién puede solicitar acceso a los datos propiamente dichos desde el sistema en origen, o a datos que requieran previa transformación e integración.

2.4. Propietario del proceso de gestión de alta de acceso a datos

El Data Champion, en su carácter de principal promotor de la cultura y apertura de datos en su área, es el responsable del proceso y de la correcta gestión de acceso a los datos. Debe velar por que se respeten y cumplan todas las instancias de validación y aprobación de acceso, interviniendo directamente en los casos donde haya que mediar entre las Personas Usuarías que solicitan acceso y las Personas Dueñas de Negocio. Sus decisiones y acciones, tanto para aprobar el otorgamiento de acceso, como para denegarlo, están enmarcadas en la *guía de clasificación de datos*.

2.5. Salida del proceso de gestión de alta de acceso a datos

Como salida del proceso, se puede esperar el otorgamiento o denegación del acceso:

- **Otorgamiento de acceso:** permite acceder a los datos finales, con o sin transformación e integración previa. Cuando los datos solicitados requieran alguna transformación, ésta se dará en el marco del *proceso de desarrollo*.
- **Denegación de acceso:** el mismo deberá estar sustentado y documentado debidamente por el Data Champion, velando que la Persona Usuaría de Datos esté debidamente notificada a través de la herramienta formal que corresponda, según el procedimiento asociado a este proceso.

1. 2.6. Flujo del Proceso de Gestión de Alta de Acceso a Datos

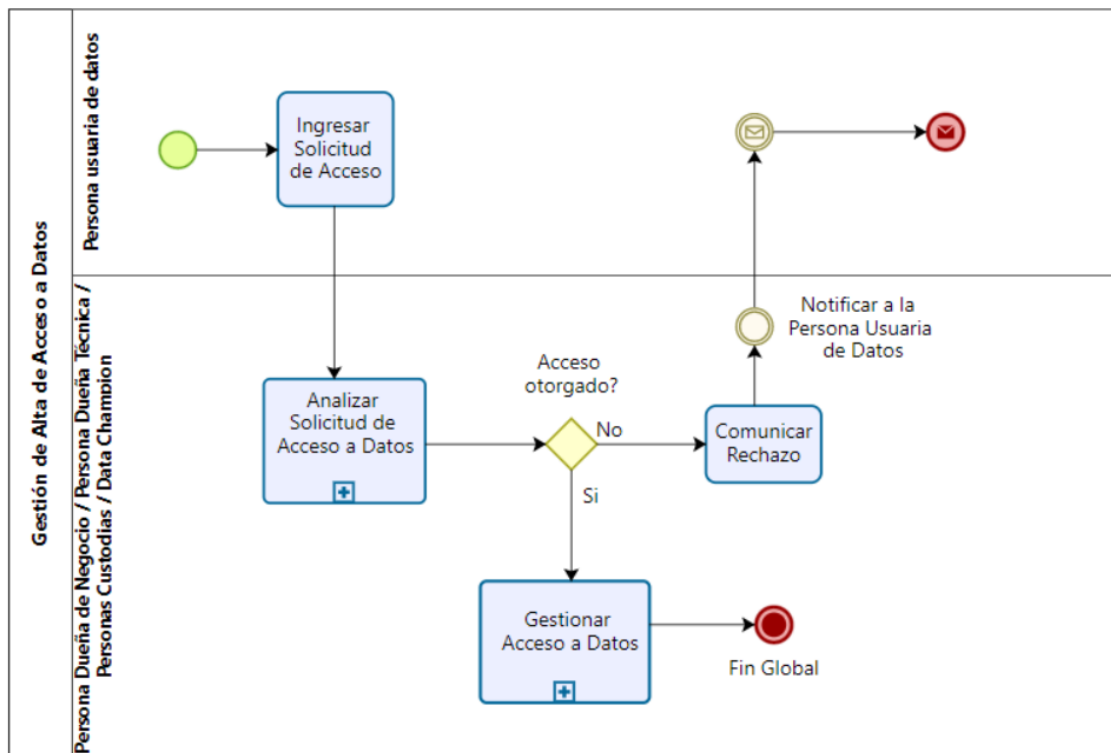


Imagen 2. Flujo del Proceso de Gestión de Alta de Acceso a Datos

Fuente: Elaboración propia.

2.6.1. Ingresar solicitud de acceso

Una Persona Usuaria ingresa una solicitud de acceso a datos para analizarlos y/o explotarlos. Dicha solicitud debe contemplar, para un correcto análisis del alcance de la misma, toda la información necesaria que se requiera para un correcto análisis del tipo de acceso solicitado, duración del mismo, detalle de la información solicitada y otros requisitos definidos previamente. Esta solicitud solamente será requerida para los datos que no sean de libre acceso.

R/A: Persona Usuaria de Datos

C: Data Champion

I: Persona Dueña de Negocio

2.6.2. Analizar solicitud de acceso a datos

Es un subproceso que recibe y analiza todas las solicitudes de acceso a datos. La salida de este subproceso es la aprobación o denegación de la solicitud de acceso.

R : Persona Dueña de Negocio

C/A: Data Champion
I: Persona Usuaria de Datos

2.6.3. Gestionar acceso a datos

Es un subproceso que gestiona las solicitudes de acceso a datos, en el caso de que una solicitud haya sido aprobada. La salida de este subproceso es la disponibilización de los datos a la Persona Usuaria.

R: Persona Dueña Técnica / Persona Custodia Técnica
A: Persona Dueña de Negocio
C/I: Persona Usuaria de Datos

2.6.4. Comunicar rechazo

Esta tarea es disparada por el Data Champion en el caso de que una solicitud de acceso a los datos sea rechazada. Se debe notificar a la Persona Usuaria tal rechazo, y se debe documentar pertinentemente los motivos de la negativa. Un rechazo debe estar avalado por los lineamientos definidos en la *guía de clasificación de datos*.

R/A: Data Champion
I: Persona Usuaria de Datos

2.7. Subproceso analizar solicitud de acceso a datos

Este subproceso describe la secuencia de tareas por la que transcurre una solicitud de acceso de datos, desde que es ingresada hasta que se determina si se autoriza o niega el acceso. Los lineamientos definidos en la *guía de clasificación de datos* son tomados en cuenta al momento de analizar las solicitudes de acceso. Si una solicitud no es del todo clara, puede iterar entre el usuario solicitante y la dueña del dato (Persona Dueña de Negocio) hasta que se aclaren todas las dudas.

El proceso contempla que la aprobación o rechazo de una solicitud de acceso se realice dentro del marco de gestión de la privacidad y protección del activo, definido en la *guía de clasificación de datos*.

Durante el flujo intervienen distintos roles que participan verificando que el alcance de la solicitud sea claro, constatando si es necesario con el **procedimiento para la cesión de datos entre organismos públicos**. Por ejemplo, el Data Champion del área a la que le llega la solicitud de acceso analiza la solicitud y puede solicitar al Chief Data Officer del GCABA que intervenga en casos de conflictos y brinde un entendimiento claro sobre la situación, para finalmente llegar hasta el otorgamiento o denegación de la autorización de acceso a los datos.

Roles

R: Persona Dueña de Negocio

A: Data Champion

C: Responsable de la Gestión de Datos

I: Persona Usuaria de Datos / Persona Dueña Técnica / Persona Custodia Técnica

2.7.1. Objetivo del subproceso analizar solicitud de acceso a datos

El objetivo tangible de este subproceso es realizar una revisión minuciosa del contenido de una *solicitud de acceso* (ver ANEXO): detalle del tipo de dato a acceder, periodo y frecuencia de acceso, Personas Usuarias de Datos, objetivo del requerimiento, destinatarios, entre otros. Todos estos requerimientos deberán estar enmarcados en la *guía de clasificación de datos* para que la autorización se haga efectiva, transparente y trazable.

Este subproceso también permite la intervención de distintos roles, como puede ser un Data Champion o un Chief Data Officer para dar transparencia, visibilidad y legitimidad a la solicitud, finalizando en una posterior autorización o denegación de acceso con respuesta formal por parte del responsable del dato.

2.7.2. Alcance del subproceso analizar solicitud de acceso a datos

El alcance de este subproceso abarca: la revisión detallada de la solicitud de acceso a los datos por parte del Persona Dueña de Negocio, aclaración de dudas si las hubiere entre la Persona Usuaria de Datos y la Persona Dueña de Negocio, intervención del Data Champion del área de negocio de los datos solicitados y de ser necesario, intervención del Chief Data Officer del GCABA que vele por el correcto cumplimiento de los lineamientos definidos en la *Guía de Clasificación de Datos*.

2.7.3. Entradas del subproceso analizar solicitud de acceso a datos

La entrada de este subproceso puede ser disparada por la Persona Usuaria de Datos hacia quien recibe la solicitud de acceso a datos, que puede ser una Persona Dueña de Negocio, Persona Dueña Técnica, Custodia Técnica o Persona Custodia de Negocio. Si bien los últimos roles no son los dueños de datos que pueden autorizar un acceso, pueden redireccionar y derivar correctamente la solicitud a la respectiva Persona Dueña de Negocio.

Esos disparadores de eventos son provocados por **actores** que están definidos en la *guía de roles de gobernanza de datos*.

Este subproceso cuenta con dos disparadores:

- Verificación del alcance de la solicitud de acceso a datos

Evento iniciado por la Persona Usuaria de Datos hacia la Persona Dueña de Negocio, ante la necesidad de acceder a los datos requeridos para su gestión.

- **Derivación de la solicitud de acceso a datos**

Ocurre cuando la Persona Usuaria desconoce a quién solicitar el acceso a datos, o cuando requiere un dato bajo tratamiento de la Persona Dueña Técnica, Custodia Técnica o Custodia de Negocio.

2.7.4. Propietario del subproceso analizar solicitud de acceso a datos

El responsable de este subproceso es el Data Champion, por ser el principal promotor de la cultura de datos en su área y de la apertura de los mismos hacia el resto de la organización.

2.7.5. Salida del subproceso analizar solicitud de acceso a datos

El subproceso tiene como resultado el otorgamiento de acceso o el rechazo del mismo.

2. 2.7.6. Flujo del subproceso analizar solicitud de acceso a datos

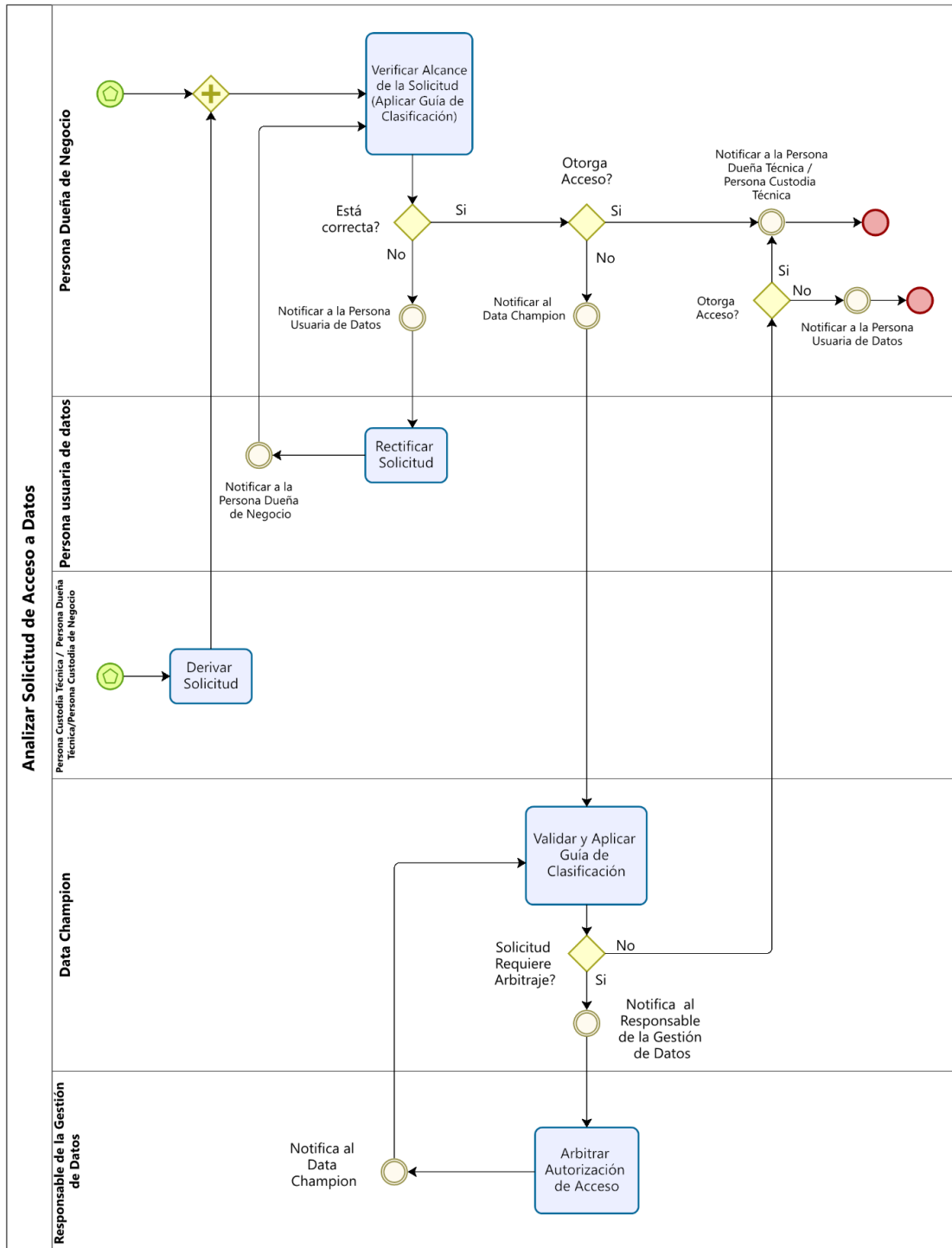


Imagen 3. Flujo del subproceso analizar solicitud de acceso a datos

Fuente: Elaboración propia.

2.7.6.1. Verificar alcance de la solicitud (Aplicar guía de clasificación)

Esta tarea le corresponde en primera instancia a la persona dueña del dato (Persona Dueña de Negocio) quien, Una vez que reciba la solicitud, deberá validar tanto su completitud como su alcance y objetivo de solicitud de acceso. Para un correcto análisis de la solicitud, en cuanto al tipo de datos que requiere la Persona Usuaría, los que se pueden compartir y los que no, la Persona Dueña de Negocio deberá apoyarse en los lineamientos definidos en la *guía de clasificación de datos*. Si la solicitud cumple con todos los requisitos, la Persona Dueña de Negocio podrá dar su aprobación. Si la solicitud no cumple con todos los requisitos, o se presentan dudas al momento del análisis, se podrá solicitar la subsanación y rectificación de la solicitud inicial.

A/R: Persona Dueña de Negocio

I/C: Persona Usuaría de Datos.

2.7.6.2. Rectificar Solicitud

Si durante la revisión del alcance de una solicitud, la Persona Dueña de Negocio tiene dudas respecto a lo solicitado, debe realizar un pedido de subsanación a la Persona Usuaría, quien debe aclarar todos los puntos que son consultados. Una vez rectificada la solicitud, se la vuelve a derivar a la Persona Dueña de Negocio para que prosiga con su análisis.

A/R: Persona Usuaría de Datos

I/C: Persona Dueña de Negocio

2.7.6.3. Derivar solicitud

Esta tarea se dispara cuando una solicitud de acceso a datos no es dirigida directamente a la Persona Dueña de Negocio, sino que la Persona Usuaría de Datos se la genera a una Persona Dueña Técnica, Custodia Técnico o Persona Custodia de Negocio. Si la persona que recibe la solicitud no es la dueña funcional de los datos, debe derivar la misma a la dueña del dato (Persona Dueña de Negocio) para que realice el correspondiente análisis y revisión de la solicitud.

A/R: Persona Dueña Técnica / Persona Custodia Técnica / Persona Custodia de Negocio

I/C: Persona Dueña de Negocio

2.7.6.4. Validar y aplicar guía de clasificación

Esta tarea es ejecutada por el Data Champion perteneciente al área de la Persona Dueña de Negocio, toda vez que este último solicite su intervención en el análisis de una solicitud de acceso. El data Champion, en su rol de autoridad competente en el tema y apoyándose en los lineamientos definidos en la *guía de clasificación de datos*, analiza la solicitud para tomar una decisión consensuada con la Persona Dueña de Negocio sobre si se debe



autorizar o no el acceso.

Si al Data Champion se le presentan dudas acerca de la competencia de la solicitud, puede dar intervención al Chief Data Officer, para consultar, evaluar y validar los criterios a aplicar.

El resultado final del análisis de la solicitud puede ser la aprobación o denegación de la solicitud de acceso al dato. En caso de aprobación, la Persona Dueña de Negocio notifica su decisión a la Persona Dueña Técnica y/o Custodia Técnica para que prosigan con la solicitud. En caso de denegación, el rechazo de la solicitud es notificado a la Persona Usuaria de Datos con su debida justificación.

R/A: Data Champion

C: Responsable de la Gestión de Datos

I: Persona Dueña Técnica / Persona Custodia Técnica / Persona Usuaria de Datos / Persona Dueña de Negocio.

2.7.6.5. Arbitrar solicitud de acceso

Esta tarea es activada por el Data Champion de un área si no puede resolver la autorización ya que se presenta un conflicto que excede a sus funciones. En este caso, hace intervenir al Chief Data Officer de GCABA para que arbitre en la situación y active los mecanismos con los que cuenta para la resolución final de la situación. Su intervención puede iterar con el Data Champion hasta clarificar y resolver la situación.

R/A: Responsable de la Gestión de Datos

C: Data Champion

I: Persona Dueña de Negocio.

2.8. Subproceso gestionar acceso a datos

Este subproceso se activa una vez que la autorización de acceso a los datos es otorgada. Se inicia con la invocación del subproceso de desarrollo, siempre y cuando la solicitud de acceso lo requiera. El alcance detallado de dicho subproceso no será desarrollado en este documento. La efectivización del acceso puede consistir solo en brindar credenciales de acceso a la Persona Usuaria de Datos, o puede requerir un desarrollo previo por parte de la Persona Dueña o Custodia Técnica.

Durante el flujo pueden intervenir los distintos roles hasta que finalmente se disponibilicen los datos al Persona Usuaria.

Roles

R: Persona Dueña Técnica / Persona Custodia Técnica

A/ C: Persona Dueña de Negocio

I: Persona Usuaria de Datos.

2.8.1. Objetivo del subproceso gestionar acceso a datos

El objetivo de este subproceso es publicar y compartir los datos a la Persona Usuaria de Datos, de acuerdo a los criterios y lineamientos enmarcados en la *guía de clasificación de datos*.

2.8.2. Alcance del subproceso gestionar acceso a datos

El alcance de este subproceso abarca desde la autorización efectiva de acceso a los datos por parte de la Persona Dueña de Negocio, hasta la efectivización de la misma con el envío de credenciales de acceso y detalle de los datos a los que podrá acceder la Persona Usuaria.

Para determinar el nivel de acceso, en esta instancia ya fueron aplicados todos los criterios y lineamientos definidos en la *guía de clasificación de datos*, estando de esta manera alineados en este sentido, tanto la Persona Usuaria y Dueña de Datos como el Data Champion, Responsable de Gestión de Datos si se lo requiere y todos los demás roles intervinientes necesarios.

2.8.3. Entrada del subproceso gestionar acceso a datos

La entrada del subproceso es disparada por la Persona Dueña de Negocio una vez que le otorgó la autorización de acceso a la Persona Usuaria de Datos.

2.8.4. Propietario del subproceso gestionar acceso a datos

El responsable de hacer que este subproceso se cumpla es el Data Champion de cada área de gobierno, quien vela por la seguridad y privacidad de los activos de su ámbito como máximo responsable de datos en su sector.

2.8.5. Salidas del subproceso gestionar acceso a datos

La salida de este subproceso es el otorgamiento de acceso a los datos por parte de las Personas Dueñas o Custodias Técnicas, comunicando las respectivas credenciales de acceso y detallando el alcance de las mismas.

3. 2.8.6. Flujo del subproceso gestionar acceso a datos

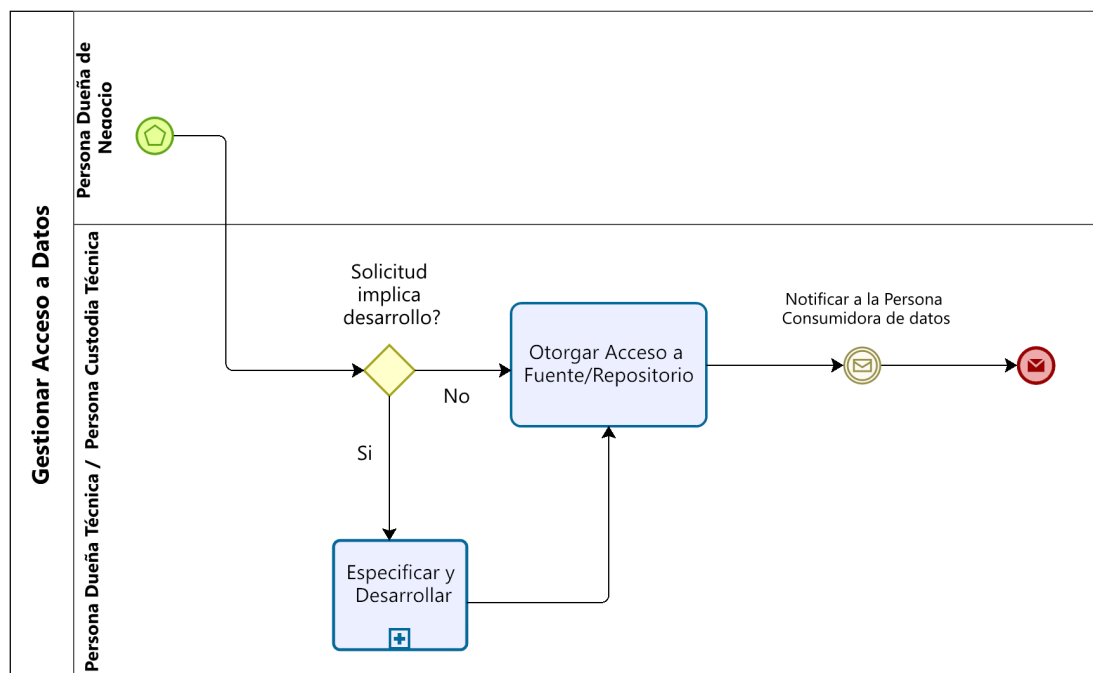


Imagen 4. Flujo del subproceso gestionar acceso a datos

Fuente: Elaboración propia.

4. 2.8.6.1.1. Especificar y desarrollar

Se trata del *proceso de desarrollo* que siguen los requerimientos. Este subproceso es activado por la Persona Dueña de Negocio una vez que se concedió la autorización de acceso a los datos. Dependiendo del tipo de activo solicitado y el detalle especificado en la solicitud de acceso inicial, puede ser necesario que se realice un desarrollo previo a su publicación.

R/A: Persona Dueña Técnica / Persona Custodia Técnica

C: Persona Usuaria de Datos / Persona Dueña de Negocio

I: Data Champion.

5. 2.8.6.1.2. Otorgar acceso a fuente/repositorio

Esta tarea es disparada por la Persona Dueña Técnica o Custodia Técnica. Consiste en notificar a la Persona Usuaria las credenciales de acceso a los datos, ya sea para acceder a las fuentes de datos originales, o a un repositorio de donde podrá extraer los datos para su utilización según lo especificado en la solicitud de acceso inicial.

La manera de compartir esas credenciales escapa al nivel de abstracción de este proceso y se detallarán en el anexo con el procedimiento asociado al mismo.

R/A: Persona Dueña Técnica / Persona Custodia Técnica

C: Persona Dueña de Negocio
I: Persona Usuaria de Datos.

3. Proceso de gestión de baja de acceso a datos

Este proceso recibe, analiza, procesa y notifica todas las solicitudes de baja de acceso a los datos, ya sean solicitadas por una Persona Usuaria de Datos, Dueña o Custodia de Negocio; o detectadas en un proceso automático de auditoría de accesos.

En el caso de que el vencimiento de la credencial de acceso lo detecte la auditoría, previo a su ejecución se da aviso a la Persona Usuaria de Datos.

Roles

A/C: Persona Dueña de Negocio
R: Persona Dueña Técnica / Persona Custodia Técnica
I: Persona Usuaria de Datos.

3.1. Objetivo del proceso de gestión de baja de acceso a datos

El objetivo de este proceso es efectivizar la baja de acceso a los datos de las Personas Usuarias. En los casos en donde un proceso de auditoría de accesos detecte que la credencial está próxima a vencer, se le dará aviso anticipado a la Persona Usuaria.

3.2. Alcance del proceso de gestión de baja de acceso a datos

El alcance de este proceso abarca a todos los usuarios que pertenezcan al GCABA o estén prestando servicio al mismo y tengan acceso a datos, ya sea con fecha de vencimiento de acceso asociado o no. La baja de usuarios que no deberían tener más acceso a los datos, ya sea porque no pertenecen más a la organización o por razones justificadas como cambio de área o vencimiento del plazo de acceso otorgado, puede ser solicitada por otra Persona Usuaria de Datos responsable, por la Persona Dueña de Negocio o por la Persona Custodia Técnica.

La persona Custodia Técnica y la Dueña Técnica del área también pueden detectar situaciones para solicitar la baja del acceso. En ocasiones, lo detectará un proceso automático, que con periodicidad procesa y levanta todas las credenciales de acceso próximas a vencer. En estos casos las bajas serán efectivizadas, pero previamente se notificará a la Persona Usuaria de Datos para que esté en conocimiento y, si persiste su necesidad de acceso, genere una nueva solicitud.

3.3. Entrada del proceso de gestión de baja de acceso a datos

El proceso de baja de acceso a datos cuenta con los siguientes disparadores:

3.3.1. Ingreso de solicitud de baja de acceso

Este evento puede ser disparado por la Persona Usuaria de Datos, la Persona Dueña o Custodia de Negocio. Las solicitudes deben contener toda la información necesaria para revocar el acceso a la Persona Usuaria de Datos correctamente.

3.3.2. Auditoría de accesos

Este evento puede ser disparado por un proceso automático que revisa el periodo de acceso a los datos otorgado a la Persona Usuaria y si detecta un próximo vencimiento. La información recolectada será input para dar aviso a la Persona Usuaria de Datos de que se le revocará el acceso, y después se utilizará esa información para ejecutar la revocación. La Persona Dueña o Custodia Técnica también puede disparar este evento al detectar un vencimiento.

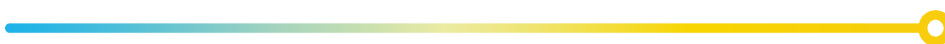
3.4. Propietario del proceso de gestión de baja de acceso a datos

El responsable de hacer que este proceso se cumpla es la Persona Dueña de Negocio, como dueña de los datos. Si un acceso se otorgó por un período determinado, debe garantizar que el mismo se cumpla. Si la baja es solicitada antes del vencimiento del período otorgado por parte de la Persona Usuaria de Datos, debe garantizar que se efectivice.

3.5. Salida del proceso de gestión de baja de acceso a datos

La salida del proceso es el aviso a la Persona Usuaria de Datos de que se efectivizó la revocación de acceso, ya sea porque sus credenciales han vencido según el tiempo estipulado inicialmente, o porque alguien autorizado ha solicitado la baja.

Otra salida también se dará en el caso de que un proceso automático de auditoría detecte su próximo vencimiento, y dispare un aviso de esta situación a la Persona Usuaria de Datos.



3.6. Flujo del proceso de gestión de baja de acceso a datos

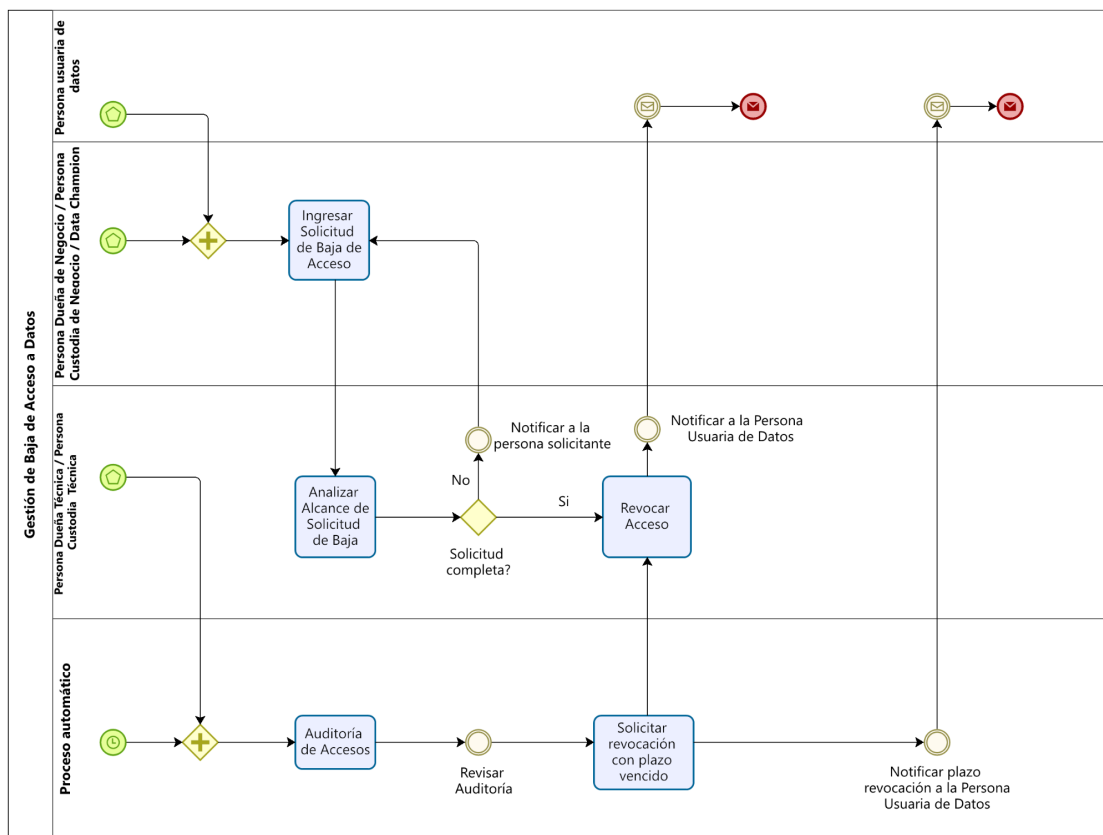


Imagen 5. Flujo del proceso de gestión de baja de acceso a datos

Fuente: Elaboración propia.

3.6.1. Ingresar Solicitud de Baja de Acceso

Los roles disparadores de la tarea pueden ser tanto la Persona Usuaria de Datos, la Persona Dueña o Custodia de Negocio o el Data Champion; este último en su rol de responsable y representante de su área, son quienes solicitan Persona Dueña o Custodia Técnica que analice la revocación de acceso a los datos otorgados oportunamente.

R: Persona Dueña de Negocio / Persona Custodia de Negocio / Data Champion

A: Data Champion

C: Persona Dueña Técnica / Persona Custodia Técnica.

3.6.2. Analizar Alcance de la Solicitud de Baja

Esta tarea le corresponde a la Persona Dueña Técnica o Custodia Técnica y son quienes deben analizar los datos de la solicitud de acceso recibida.

Deben verificar que posea toda la información correspondiente para gestionar la baja y en

caso de tener alguna duda, puede interactuar de manera cíclica con el remitente que la solicitó.

A/R: Persona Dueña Técnica / Persona Custodia Técnica

I/C: Persona Dueña de Negocio / Persona Custodia de Negocio / Persona Usuaría de Datos.

3.6.3. Auditoría de Accesos

Esta tarea la dispara la Persona Dueña Técnica o Custodia Técnica haciendo revisiones periódicas sobre accesos otorgados o un proceso automático y periódico que va recabando credenciales de acceso otorgadas próximas a vencer.

R: Proceso Automático / Persona Dueña Técnica / Persona Custodia Técnica

A: Data Champion

C: Persona Dueña de Negocio / Persona Custodia de Negocio

I: Persona Usuaría de Datos.

3.6.4. Solicitar Revocación con Plazo Vencido

Esta tarea es un mecanismo que se anticipa a los vencimientos y es input para dar aviso a las Personas Usuarías de Datos de que su acceso está próximo a caducar, así pueden iniciar una nueva solicitud de acceso a los datos. Las credenciales próximas a vencer solo se le notifican a la Persona Usuaría de Datos. Las credenciales vencidas son revocadas por la Persona Dueña Técnica y Custodia Técnica de manera inmediata, cuando sucede esto, el usuario ya fue notificado previamente.

A: Curador

R: Persona Dueña Técnica / Persona Custodia Técnica

I: Persona Usuaría de Datos

3.6.5. Revocar Acceso

Esta tarea la debe realizar la Persona Dueña Técnica o Custodia Técnica ante una solicitud de baja anticipadas que la pueden disparar una Persona Usuaría de Datos, la Persona Dueña o Custodia de Negocio o un Data Champion, haciendo efectiva la solicitud de baja a las fuentes de datos o repositorios habilitados para el acceso a datos.

La solicitud de revocación también puede ser recibida porque el acceso ha caducado. Este input puede ser generado por un proceso automático de auditoría o revisiones manuales realizadas por Personas Dueñas o Custodias Técnicas.

A/R: Persona Dueña Técnica / Persona Custodia Técnica.

I: Persona Dueña de Negocio / Persona Custodia de Negocio / Persona Usuaría de Datos.



Glosario

Persona Usuaria de Datos: Persona consumidora de los datos del GCABA.

Persona Custodia de Negocio: experto de negocio en su área. Responsable funcional del ciclo de vida del dato y sus transformaciones, desde que se origina hasta que es consumido. Define estándares y reglas sobre los Procesos de Negocio.

Persona Custodia Técnica: especialista con funciones de IT. Responsable técnico del ciclo de vida del dato y sus transformaciones, desde que se origina hasta que es consumido. Colabora con la Persona Custodia de Negocio en la confección de los metadatos desde el punto de vista técnico. Nutre el diccionario de datos en origen.

DAMA (International Data Management Association): DAMA International es una asociación global sin fines de lucro, independiente del proveedor, de profesionales técnicos y comerciales dedicada a promover los conceptos y prácticas de la gestión de información facilitando el desarrollo de la Cultura de la Gestión basada en Datos. Son referentes para organizaciones y profesionales en la Gestión de Datos, para encontrar y aportar recursos, información, formación, educación y conocimiento en la materia.

Data Champion: representante y responsable de la política de gestión de datos de las distintas áreas de gobierno, dentro del marco de las mesas de enlace de datos del GCABA que posteriormente formarán el Consejo de Gobernanza de Datos.

DMBOK2 (Data Management Body of Knowledge) del framework de

DAMA: contiene la recopilación de principios y mejores prácticas de la gestión de datos, siendo este último uno de sus principales objetivos, ser la fuente de acceso a ellas.

Persona Dueña de Negocio: responsable de los procesos de negocios y de los datos en origen. Es quien debe garantizar la calidad de los datos en origen. La publicación de datos (tanto dentro del gobierno como externamente) debe ser autorizada por él, en base a los parámetros mencionados en la “Guía de Clasificación de datos” en lo atinente a “cesión de datos entre áreas gubernamentales”.

Persona Dueña Técnica: responsable de las funciones de IT inherentes a los datos en origen. Es el responsable técnico de los repositorios y de los sistemas que generan los datos. Es quien debe garantizar la calidad de los datos desde el punto de vista técnico.

Gobernanza de Datos: Se define como el ejercicio de autoridad y control (planificación, monitoreo y ejecución) sobre la gestión de los activos de datos.

Negocio: la utilización de este término en el presente documento y dentro del ámbito

público se refiere a los programas, proyectos, prestaciones, servicios y políticas públicas de gobierno.

Responsable de la Gestión de Datos o Chief Data Officer (CDO): sponsor de la cultura de la gestión basada en datos y responsable de las políticas adecuadas para su implementación.

Anexo

A. Orden de lectura recomendada de las Guías que componen la Gobernanza de Datos

Para una mejor interpretación de los lineamientos, estos deben ser leídos de acuerdo al siguiente orden:

1. Guía de Clasificación de datos.
2. Guía de Roles de Gobernanza de Datos.
3. Proceso de Gestión de Acceso a Datos.

B. Formulario de Solicitud de Acceso (Alta / Baja)

Las credenciales de acceso deberán comunicarse a cada usuario vía correo electrónico, de modo de no comprometer la seguridad de los datos.

¿Cómo acceder y enviar las solicitudes?

Formulario de Solicitud de Acceso

- Disponible en Sistema SADE
- Módulo CCOO
- IFDAA: Solicitud de Alta de Acceso a Datos
- Solicitante Persona Usuaría de Datos
- Destinatario Persona Dueña de Negocio

Formulario de Baja de acceso

- Disponible en Sistema SADE
- Módulo CCOO
- IFDBA: Solicitud de Baja de Acceso a Datos
- Destinatario Persona Dueña de Negocio

C. Contacto

Ante cualquier duda o comentario sobre este documento podés contactarte a



datosgcba@buenosaires.gob.ar

