PLIEGO DE PRESCRIPCIONES TÉCNICAS

QUE DEBE REGIR EL ACUERDO MARCO RELATIVO AL "SERVICIO DE DESARROLLO DE SISTEMAS DE INFORMACIÓN (SI) DEL ÁREA del DATO DE AIGÜES DE BARCELONA"

Nº EXP.: AB/2026/060

Aigües de Barcelona

Índice

1. Objeto

El presente Pliego de Prescripción Técnicas (en adelante, PPT) establece las prescripciones técnicas que rigen el procedimiento de contratación para la creación del "Acuerdo Marco relativo al Servicio de desarrollo de sistemas de información (SI) del ÁREA del DATO", promovido por **Aigües de Barcelona, Empresa Metropolitana de Gestió del Cicle Integral de l'Aigua, S.A.** (en adelante, "Aigües de Barcelona"), así como la ejecución del mismo.

2. Alcance

El ámbito del presente procedimiento comprende la ejecución de proyectos de desarrollo e implementación de nuevos casos de uso en el área del Dato de Aigües de Barcelona, abarcando tanto la evolución de las soluciones existentes como la incorporación de nuevas funcionalidades. Asimismo, algunas iniciativas podrán implicar transformaciones tecnológicas orientadas a la modernización y retirada de sistemas legacy, con el objetivo de migrar hacia las plataformas y arquitecturas más avanzadas.

Los proyectos podrán abarcar, entre otros, las siguientes áreas: Business Intelligence (BI), Big Data, Analytics avanzado y Data Governance.

En todos los casos, los proyectos estarán orientados a potenciar el soporte decisional basado en datos en Aigües de Barcelona.

Las plataformas, arquitecturas y tecnologías sobre las que se trabajará se describen en el apartado 3 del presente pliego.

Para dar cobertura a la diversidad y complejidad de los proyectos descritos, el adjudicatario deberá disponer de equipos multidisciplinares con competencias en las distintas disciplinas del área del dato. Los perfiles profesionales de referencia, sus competencias requeridas y las condiciones de prestación del servicio se detallan en el apartado 5 del presente pliego.

El volumen de horas a demandar dependerá del volumen de proyectos aprobados para su ejecución. Como número orientativo y sin ningún tipo de compromiso por parte de Aigües de Barcelona, puede considerarse una línea base de alrededor de 12.700 horas al año para el conjunto de los perfiles durante la vigencia del acuerdo marco. Al tratarse de un acuerdo marco con múltiples proveedores, este volumen estimado no se asignará previsiblemente a un solo adjudicatario, sino que se repartirá entre los proveedores seleccionados en función de las adjudicaciones que se deriven de cada proyecto o encargo concreto a lo largo de la vigencia del acuerdo.

Para la correcta ejecución de los proyectos descritos, se han identificado seis perfiles profesionales clave que conformarán los equipos de trabajo. A continuación se presenta el cuadro resumen con las responsabilidades, tarifas horarias estimadas y la distribución orientativa de horas para el primer año.

La descripción completa de cada perfil, sus competencias requeridas y las condiciones de prestación del servicio se detallan en el apartado 5 del presente pliego.

Nota: Las cantidades de horas indicadas tienen carácter meramente orientativo y no vinculante. El volumen real de horas y la distribución por perfiles dependerá de las necesidades específicas de cada proyecto aprobado durante la vigencia del Acuerdo Marco.

Cuadro de Perfiles de Referencia y Tarificación Estimada Anual

Perfil Profesional	Responsabilidad principal en la plataforma	Tarifa (€/h)	Horas/año	Importe/año
PERFIL 1 — Ingeniero de Datos / Data Engineer	Diseño, desarrollo y mantenimiento de pipelines de datos y flujos de información (Kafka, dbt, Airflow)	65,00 €/h	4.308 h	280.000,00 €
PERFIL 2 — Arquitecto de Datos / Data Architect	Diseño, escalabilidad y rendimiento de la arquitectura de datos (Snowflake, Data Vault, Data Lakehouse)	75,00 €/h	1067 h	80.000,00 €
PERFIL 3 — Ingeniero DevSecOps / Platform Engineer	Automatización de infraestructuras, despliegue continuo (CI/CD) y seguridad en entornos cloud (Terraform, Kubernetes)	75,00 €/h	853 h	64.000,00 €
PERFIL 4 — Analista de Gobierno del Dato / Data Governance Analyst	Definición de políticas, calidad, trazabilidad (linaje) y cumplimiento normativo (GDPR) de los activos de información	55,00 €/h	1018 h	56.000,00 €
PERFIL 5 — Jefe de Proyecto / Project Manager	Planificación ágil, seguimiento, control de entregas y actuación como interlocutor principal técnico-negocio	75,00 €/h	1067 h	80.000,00 €
PERFIL 6 — Desarrollador de Reporting / Visualización	Creación de cuadros de mando, informes y explotación analítica priorizando Power BI y soportando MicroStrategy	55,00 €/h	4.364 h	240.000,00 €
TOTAL ESTIMADO			12.677 h	800.000,00 €

3. Especificaciones del entorno y descripción técnica

3.1 Breve introducción a la arquitectura actual

La arquitectura de datos de Aigües de Barcelona representa el núcleo tecnológico que sustenta nuestras operaciones, toma de decisiones y servicios al cliente. Esta infraestructura integral combina soluciones en la nube y on-premise, diseñadas para gestionar, procesar y analizar grandes volúmenes de datos de manera eficiente y segura.

En las siguientes secciones, se detalla la estructura actual de nuestra arquitectura, tanto en su vertiente en la nube como on-premise, así como las iniciativas en curso para su continua evolución y mejora. Esta visión general servirá como base para comprender el alcance, la complejidad y los requisitos del servicio que se solicita en este pliego.

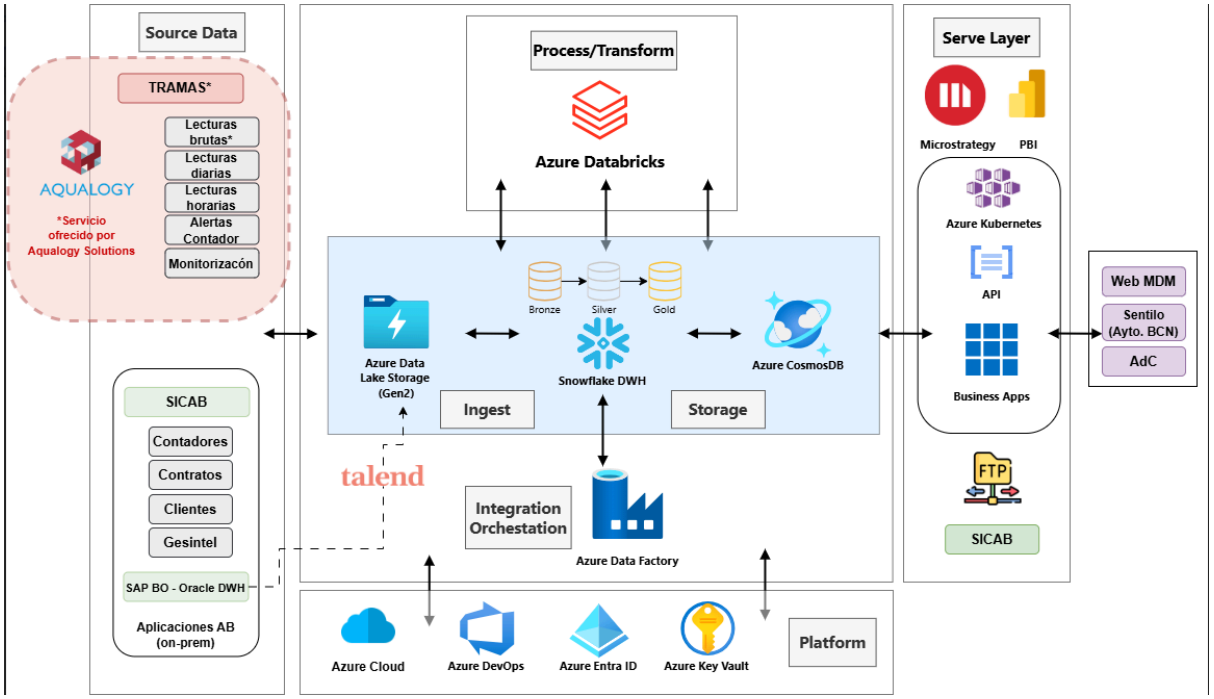
Es importante destacar que los proyectos a desarrollar podrán implementarse sobre las diferentes plataformas del área del Dato de Aigües de Barcelona, descritas a continuación. Entre ellas, DataHub (3.7) tendrá un papel predominante en los próximos años, siendo la plataforma sobre la que se concentrará la mayor parte de los nuevos desarrollos. El adjudicatario deberá acreditar el conocimiento y capacidad de trabajo sobre dichas plataformas, dimensionando adecuadamente el equipo técnico en función de las tecnologías específicas requeridas en cada proyecto, de acuerdo con la descripción arquitectónica detallada.

3.2 Arquitectura Cloud Aigües de Barcelona

En este capítulo se describe técnicamente la arquitectura de datos actual (AS-IS) principalmente desplegada en Azure, que proporciona una introducción y visión resumida de los componentes, herramientas y procesos que actualmente componen la infraestructura de datos de la organización.

3.2.1 Diagrama de Arquitectura

En el siguiente diagrama se observa que la plataforma de datos sigue un modelo de arquitectura en capas. A continuación, se ofrece un resumen de los principales componentes asociados a cada una de estas capas clave en la plataforma:



3.2.2 Capas de la arquitectura

a) Orígenes de datos

En esta capa se encuentran los sistemas externos que proporcionan los datos que serán incorporados a la plataforma. Actualmente se integran diferentes fuentes de información mediante archivos (txt/csv/parquet) y consultas SQL a base de datos. Además, contamos con un ADF de ingestas que centraliza la captura de datos procedentes del Datahub, SAP y otros orígenes, actuando como punto de convergencia de múltiples fuentes.

- ➔ SICAB (Sistema Comercial de Aguas de Barcelona): Consulta SQL directa al clon de SICAB (instantánea del día anterior).
- ➔ Tramas: Carga horaria de archivos snappy.parquet enviados por un proveedor externo
- ➔ DWH Oracle: Carga diaria vía Talend en formato CSV.

b) Orquestación de la ingesta

En esta capa encontramos los procesos encargados de conectarse a las fuentes de datos o acceder a los repositorios donde estos depositan los datos según la frecuencia que determinen los requisitos del negocio. Azure Data Factory (ADF) es el componente principal en esta capa, realizando operaciones fundamentales de integración tales como actividades de copia de datos (Copy Data), movimiento de ficheros entre repositorios y escritura en almacenamientos de destino. Es importante destacar que ADF se limita a operaciones de ingesta y orquestación, sin realizar transformaciones complejas de datos en esta fase. Los datos se extraen desde diversas fuentes, tanto internas como externas, y se cargan en la plataforma de almacenamiento en formato crudo, sin ningún tipo de transformación o modificación, preservando así la integridad de los datos originales en la capa de almacenamiento (Data Lake). Las capacidades principales de esta capa incluyen:

- ➔ Extracción de datos programados (batch)
- ➔ Operaciones básicas de movimiento y copia de datos
- ➔ Automatización de flujos de trabajo.
- ➔ Integración con otros servicios.

c) Almacenamiento

Su objetivo es depositar los datos para su procesamiento o explotación posterior. En un entorno de Big Data, los almacenes de datos deben ser capaces de manejar volúmenes muy grandes y entregarlos en el menor tiempo posible. La plataforma actual cuenta con diferentes tipos de almacenamiento basándose en la funcionalidad y casos de uso:

- ➔ Almacenamiento de Azure Data Lake para datos crudos y procesados (véase 3.2.3)
- ➔ Azure Cosmos DB para el consumo de aplicaciones de baja latencia.
- ➔ Snowflake Data Lakehouse

d) Procesamiento y/o Transformación

Esta capa permite desarrollar y desplegar modelos de analítica avanzada y predictiva. Pone a disposición de los desarrolladores las herramientas, bibliotecas y marcos de trabajo para, a partir de un gran volumen de datos, poder dar respuesta a problemas de negocio que las herramientas analíticas tradicionales no son capaces de calcular. Databricks (basado en Apache Spark) permite realizar transformaciones complejas y procesar grandes volúmenes de datos mediante procesamiento distribuido. Complementariamente, una parte significativa de las transformaciones de datos se ejecuta mediante Stored Procedures en SQL, orquestadas a través de Azure Data Factory y ejecutadas directamente en Snowflake, lo que permite aprovechar la capacidad de procesamiento nativo de la plataforma de almacenamiento. Los datos procesados tanto en Databricks como en Snowflake se integran con Cosmos DB para su almacenamiento y análisis adicional, proporcionando así múltiples opciones de persistencia según los requisitos específicos de cada caso de uso analítico.

e) Consumo:

La capa de consumo está diseñada para proporcionar acceso a los datos procesados y refinamientos a través de herramientas de visualización, interfaces de usuario y aplicaciones específicas que requieren información.

Actualmente, la organización cuenta con una solución de Inteligencia de Negocios (BI) basada en MicroStrategy. Es importante destacar que esta plataforma está implementada y operativa en la infraestructura nativa de la nube de MicroStrategy, lo que se conoce como 'MicroStrategy Cloud Environment' (MCE).

Dada esta configuración, el proveedor del Servicio del Dato que resulte adjudicatario no será responsable de la administración, mantenimiento o gestión de la infraestructura de MicroStrategy. La plataforma es gestionada directamente por MicroStrategy como parte de su oferta de servicios en la nube.

El alcance del servicio requerido se centrará en el desarrollo, optimización y soporte de soluciones analíticas, independientemente de si los datamart están ubicados en las instalaciones o en la nube, sin incluir tareas de administración de la plataforma base o su infraestructura subyacente. (ver también sección 3.3 Arquitectura On premise)

Además de la visualización en MicroStrategy, esta capa sirve a otras aplicaciones y áreas operativas que requieren acceso a datos específicos. Por ejemplo, el área de clientes y el sitio web de telelectura obtienen datos desde la Cosmos DB a través de API, proporcionando actualizaciones constantes y precisas en sus respectivos entornos. Esta capacidad de consumo multicanal permite que los datos procesados en la plataforma lleguen a diferentes partes de la organización, facilitando tanto el análisis estratégico como la operativa diaria.

Es importante, comentar que existe un proyecto de intercambio de información del consumo de agua diario/horario que compartirá información de manera segura con grandes clientes o clientes estratégicos.

f) Plataforma y desarrollo

Esta capa integra todas las herramientas y procesos necesarios para administrar el monitoreo, mantenimiento y funcionamiento automatizado de la plataforma de datos en los entornos de desarrollo (Dev), preproducción (Pre) y producción (Pro).

Esta capa facilita el ciclo de vida del desarrollo y despliegue, asegurando la continuidad de la operación y habilitando una gestión eficiente del flujo de datos en toda la plataforma. Actualmente, la plataforma sigue los principios de DevOps y utiliza metodologías CI/CD (Integración y Despliegue Continuo) para facilitar la agilidad y el control de cambios de los diferentes componentes.

Las herramientas corporativas en este ámbito son Azure DevOps para el control de versiones y el despliegue continuo. Debido a incompatibilidades de ciertos componentes desplegados y en uso en la plataforma con soluciones de código abierto, no es posible utilizar alternativas como GitLab o Jenkins, por lo que se ha adoptado Azure DevOps como solución principal para la orquestación de los procesos de integración y despliegue continuo.

La integración y el control de acceso a la plataforma se gestionan principalmente a través de Azure Active Directory (Azure AD), con un uso importante de Entra ID para la autenticación y autorización de los usuarios. Actualmente, la plataforma no dispone de una herramienta específica para la gobernanza de datos. Como se ha comentado anteriormente, se abordará en otra iniciativa.

Gestión de Secretos con Azure Key Vault: Para garantizar la seguridad y privacidad de las credenciales, contraseñas y otros secretos, la plataforma utiliza Azure Key Vault.

3.3 Plataforma y Arquitectura DataHub Veolia

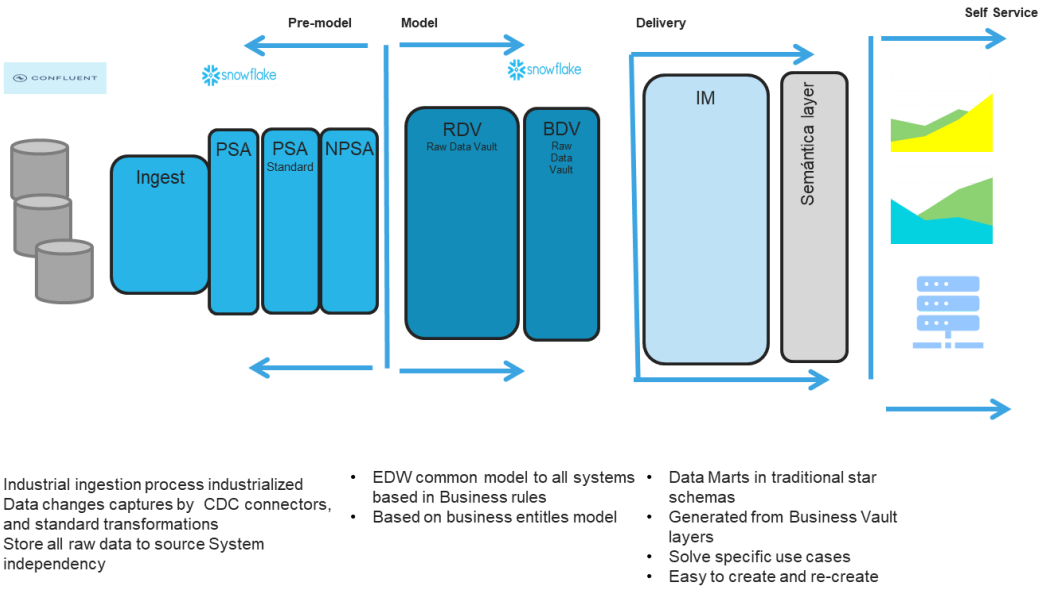
Desde 2023, se encuentra en operación el nuevo datalake corporativo que implementa un moderno Data Stack basado en una arquitectura "medallion" totalmente flexible en cloud que nos permite tener un modelo Enterprise con los datos de negocio historificados relevantes.

La plataforma de datos tiene como principales características:

- ➔ Una arquitectura de ingesta y modelado de datos centralizada, con apoyo de los procesos en tiempo real y que se adapta automáticamente a los cambios en las fuentes origen de datos.
- ➔ Un modelo de datos común a todo el negocio, basado en estándares de la industria y adaptado a las necesidades de Aigües de Barcelona.
- ➔ Apoyo a metodologías CI/CD y Devops que permiten el desarrollo de casos de uso con equipos mixtos de técnicos y de negocio trabajando simultáneamente.

Técnicamente se compone de la zona común multi-tenant y el entorno dedicado a Aigües de Barcelona donde se almacenan los datos y que incluyen:

- ➔ Lakehouse basado en *Snowflake* que aloja:
  - ◆ Un área de *Staging (Bronce)* dividido en *"layers"; Persistente Storage Area, Persistente Standardized Area* y *Non Persistent Storage Area.*
  - ◆ Un área modelada *Data Vault 2.0* (Silver) dividido en *Raw Data Vault* y *Business DataVault.*
  - ◆ Un área compuesta de diferentes *DataMarts* específicos (Gold).

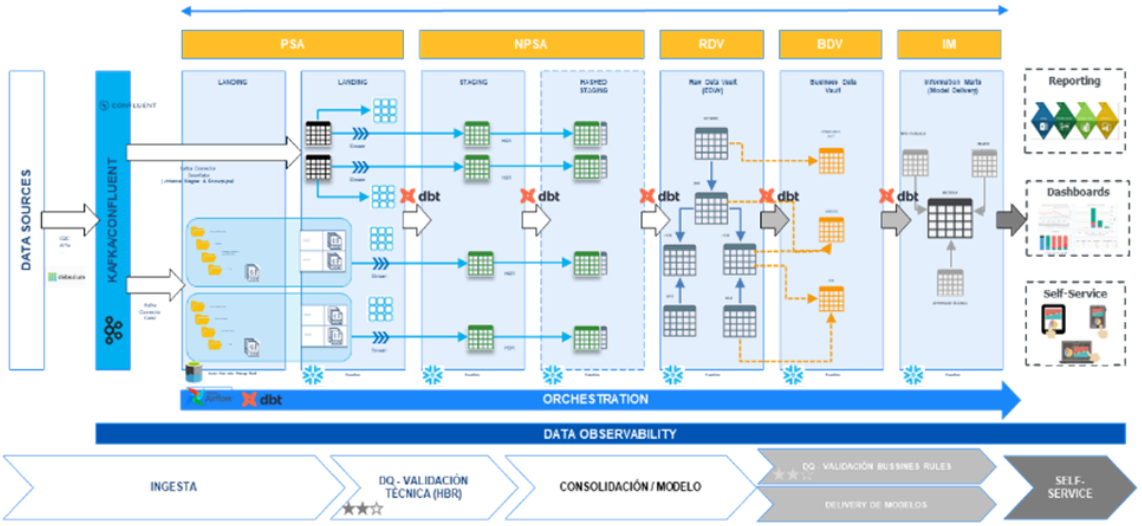


- ➔ Motor de Ingesta basado en:
  - ◆ Sistema CDC *(changes data captures)* basado en Kafka desplegado en el servicio *Confluente Cloud,* que incluye los nodos de transporte, *Kafka Connect* y apoyo para *Data Streaming.*
  - ◆ Transformaciones de datos basadas en desarrollos en *DBT* y gestionadas por Airflow.

El despliegue del sistema está completamente basado en clusters de Kubernetes desplegados en Azure (AKS) y la base de datos analítica en Snowflake que nos proporciona tanto el storage como lo compute necesario para acceder a los datos.

- ➔ Componentes Azure
  - ◆ AKS para la ejecución de:
    - Conectores Kafka
    - Ejecución de DAGS DBT
    - Sistema *airflow* para la orquestación de actividades
    - Apoyo a desarrollos y flujos MLOPS
  - ◆ APIO Manager para la publicación de APIO RISTRE
- ➔ Conectores a los diferentes orígenes de datos
- ➔ Sistema de CI/CD para la gestión de la infraestructura y sus configuraciones.
- ➔ Sistema de monitorización y observabilidad basado en Graphana.

Abajo un diagrama de la plataforma:



1. La gestión centralizada de todos los datos de la empresa en un único punto

El sistema se basa en la ingesta en tiempo real del mayor número de datos posible a través de sistemas no intrusivos como conectores CDC (*Change Data Capture*) sobre las bases de datos de IT y el bus OPC para SCADA. Adicionalmente soporta acceso vía API y carga de ficheros externos.

Estos sistemas permiten la obtención rápida con muy poco desarrollo de los datos en las primeras fases de desarrollo permitiendo a los equipos especialistas el trabajo de transformación con datos reales.

La ingesta de datos al mismo tiempo realiza la ingesta y modelización de los metadatos asociada al dato que dirigirá todas las etapas de modelado e identificación de datos fuente. Cada cambio en los metadatos de ingesta se notificará a los administradores para que tomen las acciones oportunas en la identificación de los

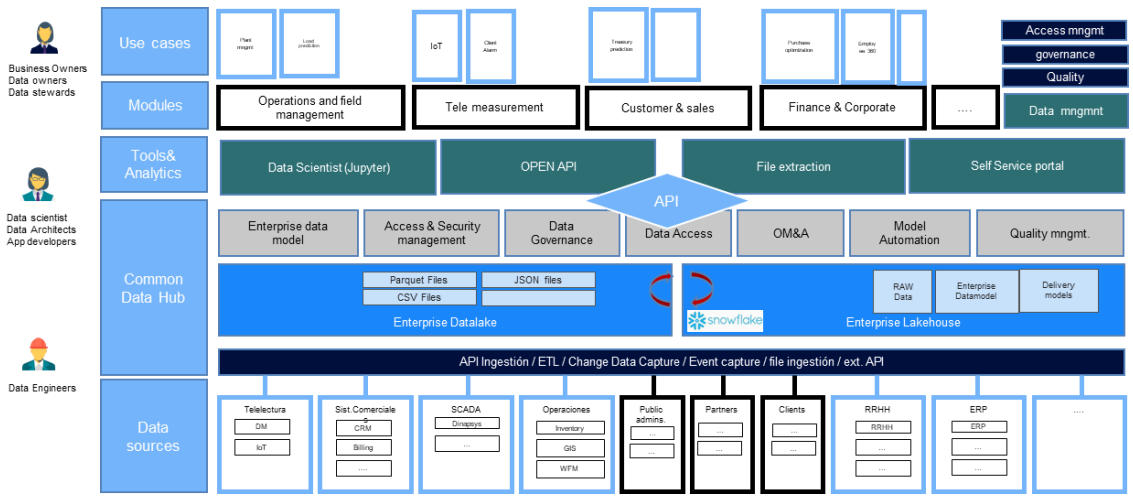
cambios, modificación de las especificaciones de seguridad, privacidad de los datos y refactorización de los procesos de modelado y control de calidad de los datos.

A la vez que se realizan los procesos de transformación de los datos se validan las reglas identificadas de calidad que permiten tener control en todo momento de los datos y alertar a los administradores ante cambios en los datos recibidos.

Todos los procesos y actividades en la plataforma dejan el rastro en el sistema unificado de observabilidad donde se centraliza la monitorización de la plataforma, la calidad de los datos y los registros de actividad para el control financiero y de consumos.

2. Arquitectura y modelo de datos unificado para todos los modelos analíticos

Las arquitecturas de EDW pueden requerir una lenta construcción y requerir grandes esfuerzos de gobernanza. Por esta razón la plataforma analítica está diseñada para crear modelos corporativos que puedan crecer de forma integrada y progresiva y soportar el concepto *de Agile DW,* adaptarse al cambio y ofrecer una visión de los datos del negocio en constante evolución.



La arquitectura se basa en la adopción de dos paradigmas. En primer lugar, el nuevo paradigma *Data Vault 2.0 (DV)* que representa la tendencia más innovadora y actualmente con más auge; son bien conocidos los beneficios que puede aportar, básicamente trazabilidad/auditoría, resiliencia, agilidad, automatización y reducción del tiempo requerido para que nuevas fuentes lleguen a las diferentes audiencias. Y, en segundo lugar, el paradigma tradicional basado en una arquitectura en bus del EDW, al estilo *Kimball*, en la cual los datos son dimensionales, atómicos y centrados en el proceso.

Data Vault 2.0

El modelo *Data Vault* (de ahora en adelante, "DV.") está basado en convenciones, lo que facilita la realización de tareas comunes de diseño como agregar atributos, refactorizar las relaciones entre entidades, incorporar

nuevas fuentes y eliminar las antiguas. Todas estas tareas se convierten en tareas aditivas de estructuras estandarizadas y conceptualmente simples, pero en ningún caso requiere propagar cambios sobre ellas.

Un modelo DV también mantiene una nítida separación entre los datos "sin procesar" organizado por fuente y los datos que son datos integrados a que se les aplica reglas de negocio, homogeneización y calidad. Esta abstracción facilita muchas decisiones de modelización, ya que la estructura de los nuevos datos se deriva en gran manera del sistema de origen y de los convenios adoptados:

1. Agilidad en los cambios

   Permite una interacción mayor y experimentación, ya que permite realizar cambios en entidades y relaciones sin que estos se tengan que propagar en cascada como sucede con la modelización tradicional. Además, la no necesidad de refactorizar relaciones (es decir, reclasificar claves en mesas de hechos) abre las puertas a los ciclos de desarrollo ágil con iteraciones francamente cortas y nunca vistas.

2. Auditoría, cumplimiento y automatización

   Además de la flexibilidad y agilidad en el diseño, el modelado DV también ofrece soluciones a problemas prácticos como la auditoría, el registro de la procedencia o el linaje y la velocidad de carga.

   Este enfoque incorpora las fuentes de datos en diferentes mesas de tipo entidad, relación y atributo (hubes, links y satélites), lo cual le permite rastrear de donde proviene cada dato, y la naturaleza aditiva del modelo permite recuperar el estado de sus datos tal como estaban en cualquier momento pasado.

   La información de auditoría forma parte del diseño de cada elemento, eso permite analizar de forma exhaustiva la carga de los datos, p. ej. incidencias producidas, hora, duración e, incluso, recursos utilizados.

3. Arquitectura a tres capas

   Los datos se estructuran en tres capas que permiten una separación nítida de los datos y una trazabilidad exhaustiva. Los datos “sin procesar”, o RAW DATA VAULT, los datos de “negocio”, o BUSINESS DATA VAULT. Estos conceptos, nuevos para el público más tradicional de modelado, permiten dar cobertura funcional end-to-end desde que se ingesta el dato hasta que se consume de forma segura.

4. Capa de consumo

   Es importante remarcar que, aunque el modelo DV pueda ofrecer servicios para el consumo en ciertas audiencias, incluso baja latencia, no es un modelo de consumo sino de integración y requiere un modelo de consumo que permita ofrecer autoservicio, que denominamos Information Mart o Data Mart

   Estas capas de consumo siguen un modelado dimensional, al estilo Kimball, en la que los datos son dimensionales, atómicos, centrados en el proceso y se ajustan a la arquitectura en bus del EDW.

5. Metadatos y automatización

El VI. dispone de un modelo de metadatos que permite identificar y relacionar de forma lógica y funcional los diferentes conceptos de negocio, vincularles con los componentes del VI. que los contienen, determinar cómo se relacionan y de qué atributos están constituidos.

Esta es la base en que se sustenta la automatización del EDW (DataOps) y la capacidad de generación de código para asegurar la trazabilidad, observabilidad y el movimiento y transformación de datos capas de la arquitectura. En la actualidad la capa de automatización no cubre la capa de consumo.

La flexibilidad de los modelos Data Vault tienen un coste que es el número de objetos que genera y que tendrá que gestionar, el modelo de metadatos asociado y el nivel de automatización que ofrece DataOps permiten superar totalmente el mencionado coste.

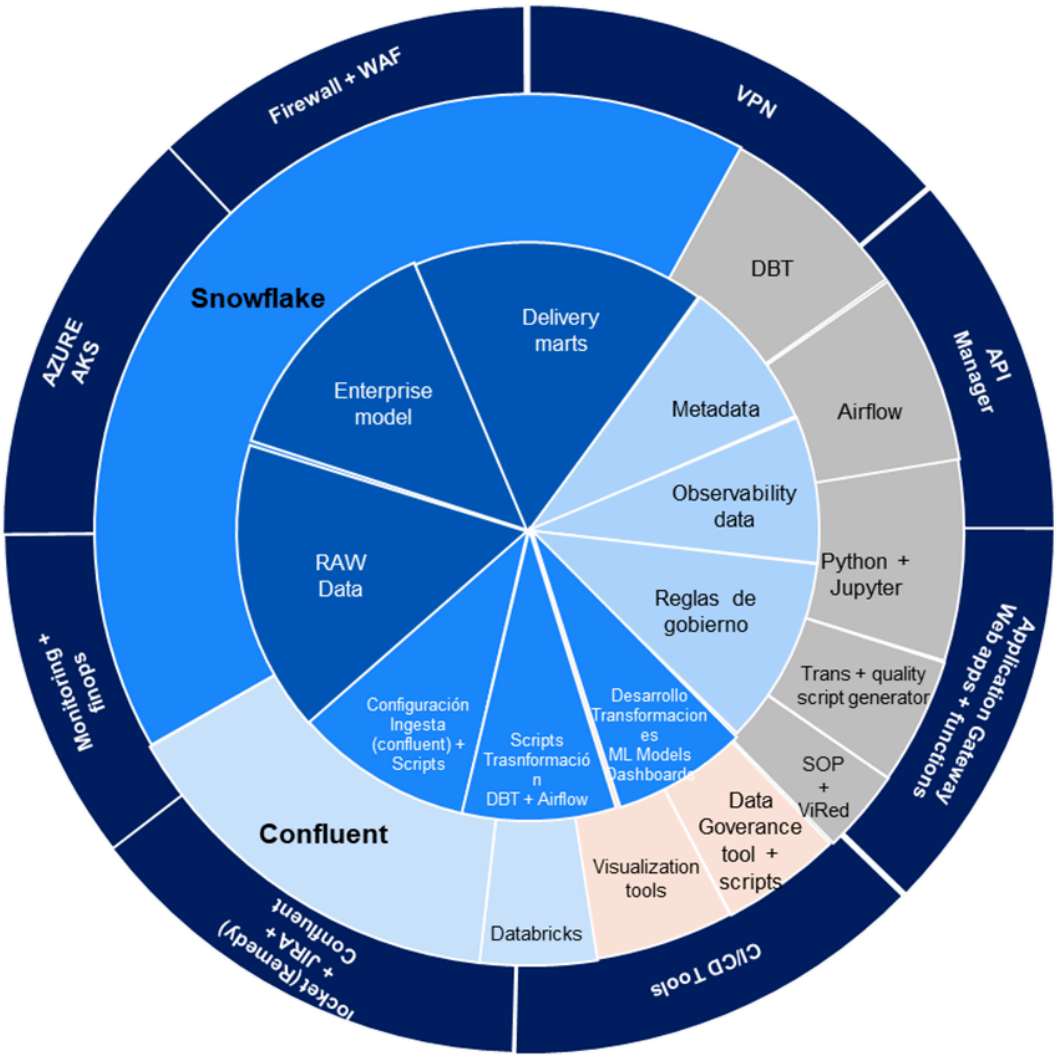
6. Enterprise Data Model (EDM)

   La arquitectura de datos propuesta permite integrar el modelado de datos con los dominios de datos existentes. El modelo de datos constituye una representación integrada que crece de forma progresiva incorporando nuevos contenidos no sujetos a compartición/segmentación por criterios de caso de uso u organización. Esta orientación, alcanzar la transversalidad de los datos e indicadores, permite que la aportación de valor de los activos de información crezca exponencialmente.

7. Gobierno del dato centralizado

   El sistema incorpora un catálogo centralizado de todos los datos en un modelo único facilitando las tareas de catalogación, linaje, gestión de la privacidad y control de las reglas GDPR proporcionando un punto único de acceso a los datos, tanto para el acceso desde las herramientas de visualización como a través de accesos automáticos.

3. Los Componentes de la Plataforma



La plataforma actual está construida utilizando como core componentes SaaS líderes de Mercado que cubren las principales funciones del sistema que son complementados con componentes desplegados en el *Cloud* de Azure para las tareas más especializadas y para proporcionar los perímetros de gestión y seguridad requeridos.

3.4 Arquitectura On Premise legacy

La arquitectura local actual fue la plataforma principal de datos de Aigües de Barcelona antes del desarrollo de la plataforma en la nube de Big Data; se basa en un enfoque ampliamente utilizado en el mercado. Aprovechando las mejores prácticas en arquitectura de datos empresariales, se desarrolló una solución que incluye desde la ingesta de datos hasta la presentación de informes, garantizando una gestión eficiente del ciclo de vida completo de los datos y que resulta adecuada cuando no se necesita manejar un gran volumen de datos o la flexibilidad de escalar en un entorno en la nube.

Extracción, Transformación y Carga (ETL):

La plataforma Talend ha sido seleccionada como ETL, gracias a que ofrece capacidades avanzadas de integración de datos, permitiendo flujos de trabajo complejos y gestión de grandes volúmenes de información con alta eficiencia. Talend facilita la orquestación de datos desde múltiples fuentes, asegurando la integridad y consistencia a lo largo del pipeline de datos.

El número de trabajos de Talend actualmente operativos es de aproximadamente 80.

3.4.1 Almacenamiento y modelado de datos

El núcleo del Data Warehouse (DWH) se basa en un esquema de base de datos Oracle 11g, una plataforma robusta y altamente escalable. En este entorno se pueden definir y desarrollar nuevas estructuras de datos, implementando modelos dimensionales y esquemas en estrella o copo de nieve según las necesidades analíticas. La arquitectura del DWH está diseñada para optimizar las consultas complejas y el rendimiento de las cargas de trabajo analíticas.

3.4.2 Capa de Presentación i Anàlisis

Como ya especificado en la descripción de la capa de consumo del arquitectura Cloud, actualmente la organización cuenta con una solución de reporting basada en MicroStrategy. Es importante destacar que esta plataforma está implementada y operativa en la infraestructura cloud nativa de MicroStrategy.

Microstrategy ofrece capacidades avanzadas de visualización y exploración de datos: se aprovecha al máximo su funcionalidad de acceso a informes, visualizaciones interactivas, navegación intuitiva y capacidades de drill-down. Además, se explotan las características más innovadoras de esta versión, como dossiers, servicios de transacción o formularios libres.

- Gobierno del dato: Se ha establecido un marco integral de gobierno que contempla tres pilares fundamentales: un glosario empresarial unificado, trazabilidad del linaje de datos y estándares de calidad. El proveedor deberá colaborar activamente en la implementación y evolución de este modelo,

promoviendo su adopción dentro de su ámbito de competencia, con el objetivo de garantizar una gestión eficiente y consistente de los datos en toda la organización.

3.5 Tecnologías de reporting: Power BI

En el ámbito del reporting y la visualización de datos, Power BI será la herramienta de referencia para los nuevos proyectos, si bien en determinados casos podrá mantenerse el uso de MicroStrategy para dar continuidad a soluciones existentes. En consecuencia, el adjudicatario deberá acreditar competencia y experiencia comprobable en ambas herramientas, siendo el dominio de Power BI un requisito prioritario de cara a los desarrollos futuros.

El adjudicatario deberá estar en condiciones de asesorar, implementar y gestionar soluciones basadas en Power BI, garantizando una adopción eficiente de la herramienta y contribuyendo a la evolución y optimización continua de las capacidades de reporting y análisis de datos de Aigües de Barcelona

3.6 Entornos Infraestructura BI

La infraestructura actual dispone de tres entornos diferenciados de desarrollo, preproducción y producción fundamentales para garantizar la calidad, estabilidad y eficiencia de las aplicaciones y sistemas que se implementan:

- **Desarrollo**: Este entorno está donde los desarrolladores trabajan en la creación y mejora de aplicaciones y sistemas. Aquí, se pueden probar nuevas funcionalidades, corregir errores y realizar integraciones de código. Al mantener un entorno de desarrollo separado, se asegura que los cambios en curso no afecten al funcionamiento de los sistemas en producción.

- **Preproducción**: Este entorno actúa como un puente entre el desarrollo y la producción. Se utiliza para validar y verificar que las aplicaciones y sistemas funcionan correctamente antes de ser lanzados en el entorno de producción. La preproducción permite realizar pruebas de integración, pruebas de rendimiento y pruebas de seguridad, entre otros, para garantizar que todo funciona según lo previsto y se han solucionado los problemas potenciales.

- **Producción**: Este es el entorno en el cual las aplicaciones y sistemas están activos y disponibles para los usuarios finales. Es fundamental que el entorno de producción sea estable y confiable, ya que cualquier problema en este entorno puede afectar directamente a los usuarios y el negocio en general.

Mantener estos tres entornos separados permite a los equipos de desarrollo, operaciones y QA colaborar de manera más efectiva, mientras reduce los riesgos asociados con la implementación de cambios en la producción. También permite una mejor gestión del ciclo de vida de las aplicaciones, asegurando que las nuevas características y mejoras se lleven a cabo de manera controlada y segura.

3.7 Ciclo de vida del desarrollo (CI/CD)

3.7.1 Enfoque general

Esta documentación se centra exclusivamente en los componentes cloud donde hay un proceso de CI/CD actualmente implementado, garantizando que los cambios sean gestionados de manera eficiente y alineados con las mejores prácticas de DevOps. Se basa en una combinación de herramientas:

- Azure Data Factory para la orquestación de procesos ETL.
- Databricks para la transformación y modelado avanzado de datos.
- Snowflake como plataforma de almacenamiento y procesamiento de los datos.
- Azure DevOps, como plataforma colaborativa para el desarrollo de software y gestión de proyectos y despliegues.

Es importante remarcar que cualquier otro componente que no esté listado en este apartado no está sujeto a un procedimiento de desarrollo supervisado actualmente por Aigües de Barcelona y, por lo tanto, no debe considerarse dentro de este marco de trabajo. No obstante, esto no limita la posibilidad de identificar oportunidades de mejora o automatización.

La plataforma de datos de Aigües de Barcelona se ha dividido en dominios funcionales con recursos independientes, por lo que los cambios y mejoras pueden implementarse más rápidamente dentro de un dominio específico sin afectar a toda la plataforma, lo que permite una respuesta más ágil a las necesidades del negocio, optimizando la coordinación y resolución de conflictos entre proyectos.

Para facilitar el proceso de despliegue siguiendo un modelo ágil y automatizado, se utiliza un pool de agentes (self-hosted) de Azure DevOps desplegado sobre Azure Kubernetes Service (AKS) que pre-configurado con todas las dependencias y librerías necesarias como (Python, Databricks CLI, PowerShell, Liquibase, etc) interactúa de forma privada y segura con los diferentes entornos de Snowflake, Databricks y Azure Data Factory.

Esto también asegura que las credenciales y configuraciones sensibles se mantengan protegidas, permitiendo que las implementaciones se realicen sin comprometer la seguridad de los datos.

3.7.2 Tareas de coordinación y rol del servicio en el ámbito DevOps

La coordinación entre los diferentes equipos es clave para la correcta implementación del proceso de ciclo de vida de desarrollo. En este contexto, (se detalla en el apartado 5 Perfiles Técnicos) las responsabilidades y funciones que se esperan del adjudicatario del servicio juegan un papel fundamental en la planificación, seguimiento, coordinación y validación de los despliegues, asegurando el cumplimiento de estándares y buenas prácticas DevOps/DataOps:

- Planificación y coordinación de releases: Definir el calendario de despliegues, priorizar cambios y gestionar dependencias entre equipos.

- Gestión de Cambios: Evaluar y aprobar cambios propuestos, asegurando que se alineen con los objetivos del negocio y la arquitectura de la plataforma.

- Control de calidad y validación de cambios: Garantizar que todas las modificaciones sean verificadas en los entornos previos antes de su promoción a producción.

- Supervisión del cumplimiento de estándares: El proceso de desarrollo y despliegue sigue una serie de normas de nomenclatura y buenas prácticas para garantizar la coherencia y mantenibilidad del código.

- Gestión de incidencias, riesgos y rollback: Definir estrategias de mitigación ante fallos en despliegues, asegurando la posibilidad de roll-back o vuelta atrás en caso de errores críticos.

- Coordinación con los diferentes equipos: Sobre la plataforma de datos de Aigües de Barcelona, se desarrollan casos de uso de diferentes ámbitos funcionales, cuyos despliegues pueden estar gestionados por diferentes equipos de proveedores que dan respuesta a las necesidades de diferentes áreas de negocio, por lo que hacer de enlace entre todas estas partes se antoja esencial dentro del servicio del adjudicatario.

- Supervisión de las ejecuciones: Asegurar que los procesos de integración y despliegue continúen operando sin interrupciones.

- Monitorización Post-Release: Supervisar el rendimiento y la estabilidad de la plataforma después de un release, asegurando que cualquier problema se aborde rápidamente con los diferentes integrantes del servicio del adjudicatario.

Asimismo, el equipo de Arquitectura y DevOps de Aigües de Barcelona, traspasar toda la documentación técnica relevante, como los procedimientos operativos, configuraciones de los pipelines, scripts de migración, y cualquier otro recurso necesario para que el proceso de CI/CD se ejecute sin contratiempos sobre el marco de responsabilidades del adjudicatario. El traspaso de esta documentación debe llevarse a cabo de manera organizada y detallada, garantizando que el equipo del adjudicatario tenga acceso a toda la información necesaria para ejecutar y gestionar correctamente los despliegues en los entornos de desarrollo, preproducción y producción, manteniendo siempre los estándares de calidad y seguridad definidos por Aigües de Barcelona.

A continuación, se explica, a modo resumen, cuál es el procedimiento de gestión de despliegues para cada uno de los componentes de la plataforma de datos de Aigües de Barcelona sobre el cloud de Azure:

3.7.3 Desarrollo y Control de Versiones

El desarrollo de nuevas funcionalidades o mejoras en la plataforma se realiza en un entorno de desarrollo, siguiendo una metodología basada en control de versiones con Git en Azure DevOps.

Cada desarrollador trabaja sobre ramas específicas feature/ derivadas de la rama principal (main), lo que permite una gestión eficiente y trazabilidad de los cambios.

Una vez completado el desarrollo, se realiza una solicitud de merge (Pull Request - PR) para su revisión y aprobación. Durante este proceso, se validan los cambios en base a las reglas de calidad y convenciones establecidas, asegurando la coherencia del código antes de su integración en la rama principal.

3.7.4 Snowflake con Liquibase

Para Snowflake, la gestión del ciclo de vida de objetos de base de datos como tablas, vistas o procedimientos almacenados se realiza con Liquibase. En este contexto, Liquibase juega un papel esencial, ya que habilita la automatización de la administración de esquemas y garantiza que los cambios se apliquen de forma consistente, controlada y auditada en los diferentes entornos de desarrollo, preproducción y producción, minimizando riesgos e incrementando la trazabilidad del proceso.

Este proceso comienza con el desarrollador proporcionando el script SQL que define este cambio o creación de objeto, que una vez subido al repositorio en la rama correspondiente, el siguiente paso es ejecutar el pipeline de CI/CD en Azure DevOps que automatiza todo el proceso de validación y despliegue en los diferentes entornos de preproducción y producción. Incluye:

- Validación en Desarrollo (DEV): Se realizan pruebas unitarias y de integración para asegurar la estabilidad y consistencia del cambio.

- Promoción a Preproducción (PRE): Una vez validados los nuevos desarrollos en el entorno de DEV, los cambios se despliegan en PRE para validaciones adicionales mediante el uso de PRs. Este proceso está completamente automatizado, lo que asegura una integración fluida y sin intervenciones manuales.

- Despliegue en Producción (PRO): Se realiza de forma controlada, asegurando la trazabilidad y auditabilidad de los cambios. Previa autorización y gestión del cambio, este proceso está completamente automatizado, lo que asegura una integración fluida en el entorno productivo.

Uno de los aspectos más importantes al trabajar con Liquibase es su capacidad para gestionar rollback de cambios, en caso de que surjan errores durante el proceso de despliegue. Si se detecta un fallo en cualquiera de los entornos, Liquibase permite revertir automáticamente los cambios mediante un archivo de rollback previamente definido. Esta funcionalidad asegura que el sistema pueda volver a un estado funcional sin afectar la integridad de la base de datos ni perder información crítica.

3.7.5 Azure Data Factory: Gestión de despliegues

En Azure Data Factory, la gestión del ciclo de vida sigue un enfoque basado en ARM templates y control de versiones en Azure DevOps. La orquestación de pipelines de CI/CD asegura la trazabilidad de los cambios en los diferentes entornos.

El proceso de CI/CD incluye:

- Validación en Desarrollo (DEV): Automatizado mediante ARM templates parametrizados, se realizan pruebas unitarias y de integración para asegurar la estabilidad y consistencia del cambio. Se crea una

rama /feature para el desarrollo de nuevas funcionalidades. Solo este entorno de desarrollo debe estar asociado con un repositorio Git. El resto de entornos no deben tener ningún repositorio Git asociado y solo deben actualizarse a través de los pipelines correspondientes a los entornos superiores.

- Promoción a Preproducción (PRE): Una vez validados los nuevos desarrollos en el entorno de DEV, los cambios se despliegan en PRE para validaciones adicionales mediante el uso de PRs. Este proceso está completamente automatizado, lo que asegura una integración fluida y sin intervenciones manuales. Sin embargo, se debe cambiar el ARM template ajustando los objetos de PRE (siempre que sea necesario)

- Despliegue en Producción (PRO): Previa autorización y gestión del cambio, este proceso está completamente automatizado, lo que asegura una integración fluida en el entorno productivo. Sin embargo, se debe cambiar el ARM template ajustando los objetos de PRO (siempre que sea necesario)

3.7.6 CI/CD en Azure Databricks

En Databricks, los distintos proyectos que en ella se ejecutan comparten un único workspace por entorno. Dentro de este workspace, la ejecución de los procesos se gestiona a través de clústeres configurados según un modelo de "talla de camiseta", donde cada clúster está dimensionado en función de la capacidad de cómputo requerida. Este enfoque permite optimizar el uso de recursos, asegurando que los procesos que demandan mayor capacidad computacional se ejecuten en clústeres más grandes, mientras que aquellos con menor necesidad operan en entornos más ligeros, garantizando así un equilibrio entre rendimiento y eficiencia operativa.

El proceso de CI/CD incluye:

- Validación en Desarrollo (DEV): El repositorio de trabajo contiene una plantilla con una estructura de archivos ya definida, donde se incorporan los notebooks con el código fuente de los desarrollos. Se crea una rama /feature para el desarrollo de nuevas funcionalidades.

- Promoción a Preproducción (PRE): Una vez validados los nuevos desarrollos en el entorno de DEV, los cambios se despliegan en PRE para validaciones adicionales mediante el uso de PRs. Este proceso está completamente automatizado, lo que asegura una integración fluida y sin intervenciones manuales.

- Despliegue en Producción (PRO): Previa autorización y gestión del cambio, este proceso está completamente automatizado, lo que asegura una integración fluida en el entorno productivo.

3.7.7 Mejora continua

Dado que Aigües de Barcelona se encuentra en un profundo proceso de mejora continua, con una evolución constante en sus procesos y herramientas de gestión del dato, la adaptabilidad del servicio es un factor clave. En este sentido, el adjudicatario deberá colaborar activamente en la adopción de nuevas formas de trabajo,

metodologías y mejoras en la automatización del ciclo de vida del desarrollo, promoviendo la optimización de procesos y asegurando una integración eficiente de las mejores prácticas en la plataforma de datos.

Asimismo, se espera del adjudicatario un enfoque proactivo, proponiendo mejoras que aporten valor a la operación. En caso de detectar procesos que puedan beneficiarse de una integración con CI/CD o de la adopción de mejores prácticas en despliegue y gestión del ciclo de vida, conjuntamente con el equipo de Arquitectura se evaluará su viabilidad y alineación con los estándares corporativos. Toda iniciativa que contribuya a la eficiencia, seguridad y sostenibilidad del ecosistema de datos será evaluada para su posible incorporación.

4. Condiciones operativas para los desarrollos (proyectos)

4.1 Metodología

4.1.1 Metodología proyectos Agile

Aigües de Barcelona está apostando decididamente por la incorporación de la metodología Agile en sus proyectos, aunque puede no ser adecuada para algún proyecto particular.

En la metodología actualmente implementada se consideran las siguientes fases de proyecto, tras el *Kick-off*:

- ***Discovery***. Donde se detallarán las historias de usuario a incluir en el *Backlog.*
- ***Delivery*** (*Sprints* y *Releases*). El calendario previsto de sprint y de liberación de *Releases* se determina en la fase de Discovery.
- **Pruebas** (de integración y de aceptación). Integradas en los Sprint, aunque las pruebas UAT pueden ser globales para cada *Release.*
- **Traspaso a producción de cada *Release*.**
- **Traspaso a servicio**.

La estructuración de estas fases no tiene porqué seguir un calendario secuencial, dependiendo de la planificación de las entregas, puede solaparse por ejemplo la construcción de una Release con la formación de la anterior.

Aigües de Barcelona no dispone aún de un marco metodológico propio, aunque está en proceso de construcción y deberá ser adoptado por las empresas adjudicatarias cuando éste esté a disposición.

Actualmente Aigües de Barcelona cuenta con JIRA como herramienta para el registro y seguimiento del *Backlog* del proyecto, así como de los Sprint que se definan. La documentación asociada se registrará en *Confluence,* Google Drive o alguna herramienta similar.

Fase *Discovery*

Una base fundamental del proyecto será la etapa de *Discovery* para la definición del product backlog, planificación detallada, dependencias, detalle de las integraciones, squads de trabajo, acuerdos de trabajo, etc. Se espera que esta primera fase del proyecto incluya:

- La toma de requerimientos detallada. Durante este análisis se trasladará el alcance definido en el *Pliego de Especificaciones del proyecto* a un conjunto de actividades a realizar para la implantación de la oferta técnica que haya resultado adjudicada [según lo previsto en la cláusula 16 del Pliego de Condiciones Particulares (PCP)]. Se espera que los Prestadores del Servicio definan en su oferta cómo plantean organizar las sesiones para esta fase donde se detallarán las historias de usuario y se construirá el *Product Backlog* del proyecto.

- Elaboración de un plan de pruebas detallado que incluirá los casos de prueba y los criterios de aceptación.

El *Product Backlog* contendrá todas las historias de usuario a ejecutar por el Prestador del servicio durante el desarrollo del proyecto que se le haya asignado.

En esta fase se identificará el Producto Mínimo Viable (PMV) que determinará el éxito del proyecto y quedará ligado a los hitos de facturación.

Esta fase de Discovery también puede planificarse de forma iterativa, en función de la previsión de entregables, según el proyecto.

Fase *Delivery*

Empezará normalmente con el fin del *Discovery*, teniendo ya definido el backlog del proyecto. Aunque puede partirse el proyecto en diversas fases cada una con su propio *Discovery/Delivery*. Al inicio de esta fase debería disponerse de una planificación detallada incluyendo.

- Desarrollo e implantación de los requerimientos contextualizados en un marco temporal estructurado en *Sprints.*

- Hitos importantes por fase, así como el detalle y la planificación de las distintas entregas, junto con los tiempos previstos para cada una.

- Los mecanismos de control de incidencias e informes de seguimiento.

- Desarrollo de pruebas técnicas y funcionales. Se deberá ofrecer y ejecutar un conjunto de pruebas y, llegado el caso, corrección y modificación para el correcto funcionamiento que garanticen la calidad de los desarrollos y el comportamiento funcional esperado, cubriendo los requerimientos esperados según su definición.

Fase Pruebas

Deberá de entregarse el plan de pruebas detallado y correctamente documentadas la evidencias, junto con el correspondiente al criterio de aceptación de las mismas. La documentación de las pruebas realizadas por el Prestador del servicio se entregará previo a la fase de UAT.

El Prestador del servicio que haya desarrollado el proyecto deberá dar soporte durante las fases de pruebas de aceptación (UAT) y atender y gestionar las incidencias reportadas durante esta fase de pruebas.

La herramienta de seguimiento del proyecto de las incidencias generadas en la etapa de pruebas de usuario será el JIRA, que Aigües de Barcelona pondrá a disposición de los Prestadores del Servicio. El Prestador del servicio tendrá que actualizar dentro de la herramienta el estado de las incidencias. La actualización de las incidencias en JIRA una vez modificadas no puede ser superior a UN (1) día.

Traspaso a producción de cada *Release*

Una vez dadas por finalizadas de forma satisfactoria las pruebas de una *Release*, se realizará su promoción y traspaso al entorno productivo, culminando en el pase a producción con el *downtime* mínimo posible.

Debe contemplarse para cada Release que se despliegue en producción el soporte post-implantación con una duración de 1 ó 2 meses en función del volumen de funcionalidades desplegadas. Este soporte post-implantación debe considerar tres aspectos fundamentales:

- Ampliación del soporte al usuario final para la resolución de dudas.
- Priorización de la corrección de las incidencias encontradas.
- Revisión del uso correcto por parte de los usuarios para detectar incidencias o falta de formación.

Traspaso al Servicio

Para poder formalizar la Ficha de Cierre del del proyecto, el Prestador del servicio que haya ejecutado el proyecto tiene que haber dotado, al equipo que preste el servicio de mantenimiento de la aplicación, de la información y la formación necesaria para dar este soporte. Se deberá de celebrar una reunión o sesión de traspaso, donde el responsable del proyecto del prestador del servicio y analistas revisen junto con el equipo de servicio de mantenimiento los cambios y nuevas funcionalidades implementadas.

La documentación mínima requerida para dar por buena la etapa de traspaso al servicio constará:

- Diagrama de los procesos de negocio afectados.
- Explicación de los cambios y nuevas funcionalidades implementadas.
- Documentación de la definición de las posibles integraciones desarrolladas o modificadas.
- Lista de los elementos afectados, tanto a nivel de procesos, objetos y programas como de los elementos de la arquitectura.
- Procedimiento de actuación por parte del servicio ante un error de los nuevos procesos desarrollados.

Consideraciones generales

Se espera que durante el desarrollo de los proyectos se realice un despliegue continuo en producción de diversas *Release*, para maximizar la aportación de valor. De esta manera estas etapas definidas/entregas se ejecutarán de forma sucesiva, o en paralelo, para cada una de ellas.

La aplicación de la metodología deberá encontrar el equilibrio entre la necesidad de seguir los procedimientos establecidos y la conveniencia de actuar con flexibilidad en función de la situación, todo ello con el objetivo de simplificar y unificar procesos, aportar la máxima eficiencia y contribuir al éxito del proyecto.

- En la fase de ***Ejecución*** de los Sprints se desarrollarán los procesos y objetos, así como también se deberán de establecer los accesos, roles y conectividades. dando por finalizada cada historia de usuario cuando se haya dado cumplimiento a su definición de "Done".

- La fase de **UAT**, puede excluirse según se decida en la fase de *Discovery* si no se considera preciso una validación específica por parte de los *Key Users* de las nuevas funcionalidades tras la revisión del plan de pruebas ejecutado por parte del prestador del servicio.

4.1.2 Metodología proyectos Waterfall

En el caso de ejecutar los proyectos bajo un modelo de desarrollo *waterfall*, se hará sobre la infraestructura y entornos de Aigües de Barcelona, con una metodología basada en el ciclo de mejora continua de los procesos:

- Inicio (I)
- Planificación (P)
- Ejecución (E)
- Seguimiento y Control (S & C)
- Cierre (C)

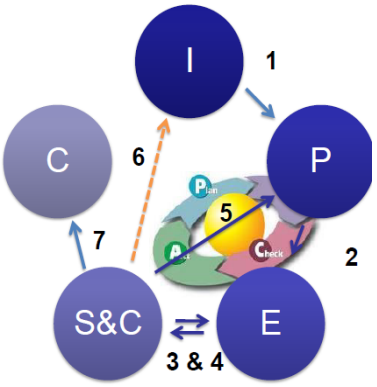


Figura 2. Ciclo de Mejora Continua

Este grupo de procesos se repetirá en cada una de las fases de la ejecución del proyecto:

1. Definición y Análisis
2. Diseño
3. Construcción
4. Pruebas
5. Paso a producción

Figura 3. Fases ejecución proyecto

- En la fase de ***Inicio***, se tendrá que establecer el equipo de trabajo, lanzar el kickoff, confirmando los objetivos y la planificación de las actividades.
- Durante el ***Diseño*** tendrán que definirse las instrucciones de los procesos y de los objetos/elementos, las integraciones y posibles automatizaciones.
- En la fase de ***Construcción***, se desarrollarán los procesos y objetos/elementos, así como también se deberán establecer los accesos, roles y conectividades.
- La ejecución del plan de pruebas, análisis de los escenarios, la validación funcional y técnica, y finalmente las pruebas de aceptación, serán las tareas a realizar en la fase de **Pruebas.**
- Finalmente, con la validación del entorno, verificación de los resultados y rendimiento, se dará por finalizado el ***Paso a Producción*** y el inicio del período de garantía.

La aplicación de la metodología deberá encontrar el equilibrio entre la necesidad de seguir los procedimientos establecidos y la conveniencia de actuar con flexibilidad en función de la situación, todo ello con el objetivo de simplificar y unificar procesos, aportar la máxima eficiencia y contribuir al éxito del proyecto.

En cualquier caso, aunque la metodología sea *Waterfall* siempre deberán contemplarse diversas fases en el proyecto para su entrega parcial.

Fase Diseño

Una base fundamental del proyecto será la etapa de Diseño para la definición del análisis funcional y técnico, planificación detallada, dependencias, detalle de las integraciones, acuerdos de trabajo, etc. Se espera que esta primera fase del proyecto incluya:

- La toma de requerimientos detallada. Durante este análisis se trasladará el alcance definido en el *Pliego de Especificaciones del proyecto* a un conjunto de actividades a realizar para la implantación de la oferta técnica que haya resultado adjudicada [según lo previsto en la cláusula 16 del Pliego de Condiciones Particulares (PCP)].
- El diseño funcional y técnico de la solución.
- La planificación de las entregas por fases ya sea en Desarrollo o en Producción.
- Elaboración de un plan de pruebas detallado que incluirá los casos de prueba, los criterios de aceptación, mecanismos de control de incidencias e informes de seguimiento.

Fase Construcción

Empezará normalmente con el fin del Diseño, teniendo ya creado el documento de diseño funcional y técnico. Aunque puede partirse el proyecto en diversas fases cada una con su propio Diseño/construcción. Al inicio de esta fase debería disponerse de una planificación detallada incluyendo:

- Desarrollo e implantación de los requerimientos contextualizados en un marco temporal.
- Hitos importantes por fase, así como el detalle y la planificación de las distintas entregas, junto con los tiempos previstos para cada una.
- Revisión y actualización del plan de pruebas detallado, si aplicara.
- Desarrollo de pruebas técnicas y funcionales. Se deberá ofrecer y ejecutar un conjunto de pruebas y, llegado el caso, corrección y modificación para el correcto funcionamiento que garanticen la calidad de los desarrollos y el comportamiento funcional esperado, cubriendo los requerimientos esperados según su definición.

Fase Pruebas

El Prestador del servicio que haya desarrollado el proyecto deberá dar soporte durante las fases de pruebas de aceptación (UAT). La documentación de las pruebas realizadas por el Prestador del servicio se entregará previo a la fase de UAT.

Estas pruebas de aceptación podrán agruparse en función del calendario previsto de despliegues en producción de las distintas fases.

La herramienta de seguimiento del proyecto de las incidencias generadas en la etapa de pruebas de usuario será el JIRA, que Aigües de Barcelona pondrá a disposición de los Prestadores del Servicio. El Prestador del servicio tendrá que actualizar dentro de la herramienta el estado de las incidencias. La actualización de las incidencias en JIRA una vez modificadas no puede ser superior a UN (1) día.

Traspaso a producción de cada Fase

Una vez dadas por finalizadas las pruebas de una Release satisfactoriamente, se realizará la promoción al entorno productivo, culminando en el pase a producción con el *downtime* mínimo posible.

Antes del pase a producción, igual que en el caso del uso de una metodología Agile, se tendrá que celebrar la reunión de ***traspaso al servicio***, de la misma manera que se ha planteado en dicho caso y con los mismos entregables. Esté traspaso al servicio del desarrollo realizado, será imprescindible para formalizar la *ficha de cierre* del proyecto.

Debe contemplarse para cada Fase que se despliegue en producción el soporte post-implantación con una duración correspondiente al periodo de garantía. Este soporte post-implantación debe considerar tres aspectos fundamentales:

- Ampliación del soporte al usuario final para la resolución de dudas.
- Priorización de la corrección de las incidencias encontradas.

- Revisión del uso correcto por parte de los usuarios para detectar incidencias o falta de formación.

4.2 Garantía

El período de garantía que se establezca deberá aplicarse de forma individual a cada una de las Releases o fases que se desplieguen en producción, incluida la última de finalización del proyecto.

El periodo mínimo de garantía que tendrán que tener los desarrollos y servicios entregados (proyectos) será de TRES (3) meses, a contar desde el traspaso a producción y activación de cada Release y, en el caso de la última, tras la firma de la *Ficha de cierre de Proyecto*.

No obstante lo anterior, tal como se indica en la cláusula 9 del Pliego de Condiciones Particulares (PCP), los Prestadores del servicio podrán ofertar un aumento del período de garantía respecto a los TRES (3) meses indicados, que aplicará a la totalidad de los proyectos que se les encargue.

En cualquier caso, este período de garantía, tras cada entrega de una Release en producción y tras la firma de la citada *Ficha de cierre de proyecto*, es el que se considerará para el recuento de las incidencias en el cálculo de los ANS.

4.3 Entregables

Durante el periodo de definición hasta la entrega y puesta en producción del proyecto, se requiere que el Prestador del Servicio entregue, como mínimo, la siguiente documentación a Aigües de Barcelona:

En la reunión de *Kick-off:*

- **Planificación y roadmap del proyecto**.
- **Documento de *Kick-off*,** se presentará a las personas y equipos interesados y contendrá las premisas y puntos clave para entender el proyecto.

Durante el *Discovery*/Diseño:

- **Backlog de proyecto**. Este entregable será el resultado de la fase *Discovery* para los proyectos **Agile** y deberá contener, en función del volumen del proyecto:
    - El listado de todos los requerimientos a desarrollar durante el *Delivery*, agrupados de manera lógica para el desarrollo de dichos requerimientos.
    - El detalle necesario de cada uno de los requerimientos para poder desarrollar de manera independiente la solución, tales como: qué se espera por parte de los usuarios, permisos y visibilidades a otorgar, definición consensuada de cuándo consideraremos un requerimiento aceptado y listo para ser desplegado, criterios de validación y aceptación, solución técnica, etc.

- La priorización del propio *Backlog* del proyecto, de manera que se tenga visibilidad de las prioridades de negocio y desarrollar en función de ello.
- Plan de capacidad (*Capacity Plan*) de los sistemas a utilizar (bases de datos, máquinas virtuales, OS, almacenamiento, etc.…), en función del volumen del proyecto.
- Documento técnico de arquitectura.
- Documento de diseño del sistema.

- **Análisis funcional y Diseño técnico**

El documento de análisis funcional y diseño técnico será el entregable resultado de las fases de análisis y diseño de la solución a entregar, para los proyectos Waterfall, para su aceptación por Aigües de Barcelona. En este documento deberá detallarse el diseño, funcionamiento e integración de los diferentes componentes a desarrollar o modificar para dar cumplimiento a la totalidad de los requerimientos.

A modo ilustrativo, y en función de la naturaleza del proyecto, se incluyen los siguientes ejemplos de contenido esperado:

- En el caso de un **modelo de datos o capa semántica**, deberá quedar definida la estructura de entidades, atributos, relaciones, reglas de negocio aplicadas y criterios de granularidad, así como el glosario de métricas e indicadores y su forma de cálculo.
- En el caso de un **pipeline o flujo de ingesta y transformación de datos**, deberá definirse el origen y naturaleza de las fuentes, las transformaciones aplicadas, la frecuencia y modo de ejecución, las dependencias con otros procesos, el tratamiento de errores y las condiciones de reintento o recuperación.
- En el caso de un **cuadro de mando o producto de visualización**, deberá quedar recogido el diseño propuesto, incluyendo las visualizaciones, métricas, dimensiones de análisis, filtros, niveles de agregación y el comportamiento interactivo esperado, así como el público objetivo y el caso de uso que da soporte.
- En el caso de un **modelo analítico o de inteligencia artificial**, deberá describirse el enfoque metodológico, las variables de entrada y salida, los criterios de evaluación del modelo, las condiciones de reentrenamiento y las limitaciones conocidas.

A nivel técnico, deberá detallarse la lista de elementos a desarrollar, las interfaces y mecanismos de integración con otras capas o sistemas, el modelo de datos físico, la definición de parámetros o variables de ejecución, los elementos de infraestructura y plataforma implicados, así como los requisitos de rendimiento, volumetría y escalabilidad.

En cualquier caso, en estos documentos deberá quedar especificado en qué condiciones deberá funcionar y qué limitaciones tendrá el producto a entregar, incluyendo aspectos relativos a la calidad del dato, la trazabilidad y el linaje de la información.

Dependiendo del alcance del desarrollo, el análisis funcional y técnico podrá presentarse como un único documento, siempre y cuando esté bien estructurado, o podrá separarse en dos documentos independientes.

- **Plan de pruebas**, se entregará una primera versión del plan de pruebas que incluirá los casos de prueba y los criterios de aceptación.

Dadas las necesidades del proyecto concreto, es posible que durante la fase de construcción o de pruebas, sea necesaria la revisión y actualización de estos documentos por parte del Prestador del Servicio y a requerimiento de Aigües de Barcelona.

Durante el Delivery/Construcción:

- **Plan de pruebas**, que se irá completando a lo largo del proyecto. Primero con la definición consensuada para aceptar los requerimientos. También como parte del desarrollo de las tareas en el *Delivery*, ya que el equipo del Prestador del Servicio probará las distintas casuísticas, antes de pasar requerimientos a completados y dejará evidencias de la eficacia del producto.

- **Prueba automática**, para cada historia de usuario, permitiendo las pruebas de regresión entre distintas Releases cuando sea posible. En cualquier caso, será necesario la documentación de las pruebas unitarias ejecutadas durante la fase de construcción, a entregar antes del inicio de la ejecución del Plan de pruebas

- **Informes de seguimiento**. En función de la estrategia de modelo de gobierno y la herramienta de seguimiento a adoptar, se podrá pedir al Prestador del Servicio un informe que recoja el estado del proyecto, el avance de desarrollo, bloqueantes, riesgos y mitigación de estos. Se espera que el Prestador del servicio incluya en sus informes de seguimiento KPIs y métodos de seguimiento, tales como: *burndown*, velocidad, bloqueantes, etc.

Para el despliegue a producción de cada Release/Fase:

- Artefactos de despliegue. Contendrán los elementos a desplegar según la naturaleza del proyecto: scripts SQL (Liquibase), modelos dbt, DAGs de Airflow, notebooks de Databricks, pipelines de Azure Data Factory (ARM templates), configuraciones de infraestructura (Terraform), u otros componentes propios del stack tecnológico utilizado.

- Historias de Usuario / Requerimientos a desplegar a producción. Se especificarán los elementos del backlog o los requerimientos que se desplegarán en los distintos entornos hasta culminar con su despliegue a producción. En caso de proyectos Waterfall se especificarán los requerimientos y sus componentes para cada despliegue.

- Documentación de integraciones. En el caso de desplegar integraciones con otros sistemas o capas de la plataforma, se requerirá la entrega de un mínimo de documentación que defina las integraciones realizadas.

- Documentación técnica. Incluyendo en función del tipo de proyecto: documento técnico de arquitectura (actualizado), documentación de flujos y pipelines críticos, manual de despliegue y operación, informes de entrega sobre las pruebas realizadas, y documentación del código fuente en la medida necesaria para garantizar su comprensión y mantenibilidad.

En las sesiones formativas:

- **Documento de traspaso al servicio**, tal y como se indica en el punto 4.1.1.

- En el caso que se especifique en los requerimientos previos o en los establecidos durante el *Discovery*, deberán contemplarse sesiones formativas de las nuevas funcionalidades para los no participantes en el proyecto.

- En este caso se entregará la información/documentación a seguir durante las diferentes sesiones formativas, así como todos los soportes requeridos para su impartición, seguimiento y consulta posterior (manuales, material audiovisual, etc.).

Cierre de proyecto:

- **Ficha de Cierre de Proyecto**. Con este documento se podrá valorar los objetivos cumplidos y si el resultado ha sido exactamente lo que se esperaba. Deberá también recoger aquellas lecciones aprendidas durante las diferentes etapas de la ejecución del servicio/proyecto. Se formalizará la entrega del documento en una reunión y, tras la firma del acta correspondiente, se dará por finalizado y aceptado el proyecto quedando activo el periodo final de garantía establecido en el apartado 4.2 del presente pliego.

- **Informe de incidencias abiertas**. Recogiendo aquellas incidencias no cerradas y que serán traspasadas al mantenimiento de común acuerdo entre Aigües de Barcelona y el proveedor.

- **Informe final de proyecto**, conforme éste cumple con los requisitos de seguridad exigidos en la cláusula del Anexo Nº 2 del PPT.

A lo largo de la duración del proyecto:

- **Informes de Seguimiento**. Serán informes recurrentes que tendrá que presentar el Jefe/Gestor de proyecto en las reuniones de seguimiento del proyecto. Dichos informes deberán recoger información sobre el estado del proyecto, el avance, problemas encontrados, riesgos y mitigación de los mismos.

  Para todos aquellos proyectos de más de TRES (3) meses de duración se requerirá un informe mensual, a contar desde la fecha de inicio del proyecto (reunión de Kick Off) y a entregar en los siguientes CINCO (5) días hábiles transcurrido el periodo mensual (30 días naturales). En el caso de proyectos de menor duración, como norma general se requerirá que la entrega del informe de seguimiento se realice quincenalmente y en los siguientes CINCO (5) días hábiles transcurrido el periodo (15 días naturales).

Durante el periodo de garantía:

- **Informe de Incidencia Significativa.** Una vez puesta una entrega parcial o total y hasta la finalización de la garantía, de generarse una incidencia grave (tipificadas como *Crítica* o *Alta*) sobre algunos de los procesos o una indisponibilidad parcial o total del sistema, el Prestador del servicio deberá generar un informe de Incidencia Significativa, detallando el motivo por el cual se ha producido y el plan de acción para su resolución. Este informe tendrá que ser entregado en un tiempo máximo de TRES (3) días laborables desde la comunicación de la incidencia por parte de Aigües de Barcelona.

4.4 Ubicación

Los servicios se prestarán desde las propias oficinas del Prestador del Servicio, no obstante, se darán situaciones que requieran de la presencia en las propias oficinas de Aigües de Barcelona por motivo de asistencia a reuniones, seguimiento del servicio y de los proyectos de desarrollo específicos, puestas en común, etc.

Así mismo, en función de las características específicas del proyecto y/o tareas a ejecutar, Aigües de Barcelona podrá exigir al Prestador del servicio que el personal que asigne al proyecto desarrolle los trabajos, o parte de los mismos sin limitación, de forma presencial en centros de trabajo de Aigües de Barcelona, dentro del ámbito territorial del Área Metropolitana de Barcelona y sin que esto pueda suponer un incremento en el coste de los servicios.

5. Perfiles Técnicos y capacitación del equipo de Trabajo

El adjudicatario deberá disponer, en todo momento durante la vigencia del contrato, del equipo humano necesario para garantizar la correcta ejecución de los servicios objeto del presente pliego, con independencia de la denominación concreta de los perfiles profesionales empleados.

Dado el carácter tecnológicamente agnóstico de los presentes requerimientos, y habida cuenta de la diversidad de arquitecturas, plataformas y ecosistemas tecnológicos existentes en el ámbito del dato —incluyendo, sin carácter limitativo, soluciones de ingeniería de datos, analítica avanzada, inteligencia artificial, visualización, gobierno del dato y plataformas cloud o híbridas—, no se establece una relación cerrada de perfiles técnicos, sino que se exige al licitador que, en su propuesta técnica, justifique y acredite la composición del equipo de trabajo propuesto en función de los siguientes criterios:

- La arquitectura y stack tecnológico de la plataforma sobre la que se desarrollará cada proyecto o servicio.
- Las características funcionales y técnicas específicas de cada encargo, atendiendo a su complejidad, alcance y requisitos de calidad.
- La necesidad de garantizar una cobertura integral de todas las fases del ciclo de vida del dato: desde la ingesta y transformación, hasta la explotación, visualización y gobierno.

En consecuencia, será responsabilidad del adjudicatario dimensionar, seleccionar y acreditar los perfiles profesionales más adecuados para cada proyecto, debiendo quedar suficientemente justificada dicha selección en los documentos técnicos que acompañen a cada encargo o en el plan de trabajo correspondiente.

A efectos de valoración de la solvencia técnica, el licitador deberá acreditar experiencia previa en proyectos de naturaleza análoga, así como la disponibilidad de profesionales con competencias contrastadas en las disciplinas propias del área del dato, sin que ello implique la exigencia de certificaciones o titulaciones específicas vinculadas a tecnologías concretas, salvo que así se establezca expresamente para un proyecto determinado.

No obstante lo anterior, y a efectos exclusivamente de **tarificación y comparación de ofertas económicas** en el marco del presente acuerdo marco, se establece a continuación un catálogo de perfiles de

referencia. Dicho catálogo no tiene carácter exhaustivo ni limita la composición de los equipos de trabajo en cada proyecto, sino que sirve como base para la valoración económica de los servicios prestados y para la facturación de las horas dedicadas por cada tipo de profesional. El licitador deberá ofertar un precio hora para cada uno de los perfiles definidos, pudiendo proponer perfiles adicionales debidamente justificados si la naturaleza de un proyecto concreto así lo requiriera.

PERFIL 1 — Ingeniero de Datos / Data Engineer

Descripción del perfil

Profesional especializado en el diseño, desarrollo y mantenimiento de pipelines de datos, responsable de garantizar la disponibilidad, calidad y rendimiento de los flujos de información desde las fuentes hasta las capas de consumo.

Competencias técnicas requeridas

- Experiencia en plataformas de **streaming y mensajería** (Confluent, Apache Kafka)
- Dominio de herramientas de **transformación de datos** (dbt)
- Experiencia en **orquestación de workflows** (Apache Airflow)
- Python
- Stack Azure (Cloud Azure, Azure Data Factory, Databricks)
- Conocimiento de bases de datos relacionales y no relacionales
- Experiencia en desarrollo de **pipelines ELT/ETL**
- Conocimientos de SQL avanzado

Experiencia mínima requerida

- Mínimo **TRES (3) años** de experiencia en ingeniería de datos
- Experiencia demostrable en al menos **DOS (2) proyectos** de implementación de pipelines en entornos productivos

Titulación

- Grado en Ingeniería Informática, Telecomunicaciones o similar
- Se valorarán certificaciones en Confluent, Airflow o tecnologías afines

---

PERFIL 2 — Arquitecto de Datos / Data Architect

Descripción del perfil

Profesional responsable del diseño y evolución de la arquitectura de la plataforma de datos, garantizando la escalabilidad, rendimiento y alineación con los requisitos del negocio. Lidera las decisiones tecnológicas en materia de almacenamiento, modelado y acceso al dato.

Competencias técnicas requeridas

- Experiencia avanzada en **Snowflake** (arquitectura, optimización, administración)
- Conocimiento de **metodologías de modelado de datos** (Kimball, Data Vault, EDM)
- Diseño de arquitecturas **Data Warehouse / Data Lakehouse**
- Experiencia en modelado conceptual, lógico y físico de datos
- Conocimiento de patrones de integración y acceso al dato
- Capacidad para definir **estándares y buenas prácticas** de arquitectura

Experiencia mínima requerida

- Mínimo **5 años** de experiencia en arquitectura de datos
- Experiencia demostrable en al menos **DOS (2) proyectos** de arquitectura de plataformas de datos en entornos empresariales

Titulación

- Grado en Ingeniería Informática, Telecomunicaciones o similar
- Se valorarán certificaciones en **Snowflake SnowPro Core/Architect** o equivalentes

---

PERFIL 3 — Ingeniero DevSecOps / Platform Engineer

Descripción del perfil

Profesional especializado en la automatización de infraestructuras, despliegue de plataformas de datos y aplicación de políticas de seguridad en entornos cloud. Garantiza la fiabilidad, seguridad y eficiencia operativa de los sistemas de datos.

Competencias técnicas requeridas

- Dominio de **infraestructura como código** (Terraform, Terragrunt)
- Experiencia en **CI/CD** y automatización de despliegues (GitLab CI, GitHub Actions, Jenkins)
- Conocimiento de plataformas **cloud** (AWS, Azure o GCP)
- Experiencia en **seguridad aplicada a plataformas de datos**:
- Conocimientos de contenedores y orquestación (Docker, Kubernetes)

Experiencia mínima requerida

- Mínimo **TRES (3) años** de experiencia en DevOps/DevSecOps
- Experiencia demostrable en entornos cloud con componentes de datos

Titulación

- Grado en Ingeniería Informática, Telecomunicaciones o similar
- Se valorarán certificaciones cloud (AWS, Azure, GCP) y de seguridad (CISSP, CISM o equivalentes)

PERFIL 4 — Analista de Gobierno del Dato / Data Governance Analyst

Descripción del perfil

Profesional responsable de definir, implantar y mantener los marcos de gobierno del dato de la organización, asegurando la calidad, trazabilidad, seguridad y cumplimiento normativo de los activos de información.

Competencias técnicas requeridas

- Conocimiento de **marcos de gobierno del dato** (DAMA-DMBOK, DCAM)
- Experiencia en definición e implantación de **políticas y estándares de datos**
- Manejo de herramientas de **catálogo de datos** y linaje (Collibra, Purview o similares)
- Conocimiento de **métricas y procesos de calidad del dato**
- Experiencia en definición de **roles y responsabilidades** sobre el dato (Data Owners, Data Stewards)
- Conocimiento de normativa aplicable: **GDPR**, regulación sectorial

Experiencia mínima requerida

- Mínimo **TRES (3) años** de experiencia en gobierno del dato o gestión de datos empresariales
- Experiencia en proyectos de implantación de marcos de gobierno en organizaciones de tamaño medio-grande

Titulación

- Grado en Ingeniería Informática, ADE, Estadística o similar
- Se valorarán certificaciones **CDMP (DAMA)** o equivalentes

---

PERFIL 5 — Jefe de Proyecto / Project Manager

Descripción del perfil

Profesional responsable de la planificación, seguimiento y control de los proyectos en el área del dato, garantizando el cumplimiento de plazos, presupuesto y calidad de las entregas. Actúa como interlocutor principal entre el equipo técnico y el cliente.

Competencias técnicas requeridas

- Experiencia en **gestión de proyectos** tecnológicos en el área del dato
- Dominio de **metodologías de gestión** de proyectos (PMI/PMBOK, PRINCE2, metodologías ágiles)
- Capacidad de elaboración y seguimiento de **planes de proyecto**, cronogramas y presupuestos
- Gestión de **riesgos e incidencias**
- Habilidades de **comunicación y reporting** a nivel directivo
- Conocimiento funcional suficiente del área del dato para interlocución técnica

Experiencia mínima requerida

- Mínimo **CINCO (5) años** de experiencia en gestión de proyectos tecnológicos
- Experiencia demostrable en al menos **TRES (3) proyectos** en el ámbito de datos o analítica

Titulación

- Grado en Ingeniería Informática, ADE o similar
- Se valorarán certificaciones **PMP, PRINCE2** o **Scrum Master**

PERFIL 6 — Desarrollador de Reporting / Visualización

Descripción del perfil

Profesional especializado en el desarrollo de soluciones de reporting y visualización de datos, con foco principal en Microsoft Power BI. Su función es transformar datos en informes, dashboards e indicadores que den respuesta a las necesidades analíticas del negocio, participando en todas las fases del ciclo de vida del reporting. Puntualmente podrá requerirse experiencia en MicroStrategy.

Competencias técnicas requeridas

- Desarrollo de informes y dashboards en Power BI Desktop y Power BI Service
- Modelado de datos, lenguaje DAX y transformación con Power Query
- Conexión a fuentes de datos corporativas (bases de datos relacionales, data warehouses, data lakes)
- SQL para extracción y transformación de datos
- Se valorará experiencia en desarrollo de MicroStrategy

Experiencia mínima requerida

- Mínimo CUATRO (4) años de experiencia en herramientas de reporting Business Intelligence
- Mínimo TRES (3) años como desarrollador de Power BI en entornos productivos

- Se valorará experiencia equivalente en MicroStrategy

Titulación

- Titulación universitaria en Ingeniería Informática, Telecomunicaciones o disciplinas afines
- En su defecto, Formación Profesional de Grado Superior en informática con DOS (2) años adicionales de experiencia
- Se valorará positivamente la disposición de certificaciones oficiales relacionadas con Power BI

6. Otros Requerimientos

6.1 Recepción, control, resolución y canalización de incidencias

Los adjudicatarios del Acuerdo Marco deberán utilizar las herramientas de Aigües de Barcelona para el reporting y seguimiento de las incidencias detectadas:

- En fase de pruebas de aceptación y puesta en marcha, deberán hacer uso de la herramienta JIRA.

- Mientras que, en fase de post implantación (parcial o total) deberán hacer uso de la herramienta de ticketing utilizada por Aigües de Barcelona (actualmente *BMC Remedy*).

El Prestador del Servicio deberá utilizar las herramientas de ticketing para el control de las incidencias detectadas, en las cuales el Prestador del Servicio se compromete a reportar cualquier acción realizada sobre las mismas y el tiempo dedicado a cada acción.

La frecuencia y contenidos de estos reportes serán consensuados por ambas partes en la fase correspondiente. Estos procedimientos pueden ser cambiados en cualquier momento por Aigües de Barcelona, previa comunicación y aceptación por parte de los Prestadores del Servicio objeto del Acuerdo Marco, quienes se comprometen a adoptarla en el plazo máximo que se establezca.

Cada ticket vendrá informado con una prioridad asignada por Aigües de Barcelona según lo previsto en el **Anexo Nº1**, que será revisada por el Prestador del Servicio en el momento de la recepción del ticket, para su aceptación o solicitud de cambio.

Dentro de las actividades de soporte, se incluyen específicamente la ejecución de procedimientos de operación bien definidos y documentados.

En caso necesario, se escalará y demandará soporte presencial.

Así mismo, en el caso que Aigües de Barcelona lo considere necesario, solicitará un informe de estado de resolución de las incidencias generadas en el período de garantía. Esto último, sin menoscabo del ya citado Informe específico para cada una de las incidencias significativas.

De cara a valorar el servicio que se ofrece se considerará resuelta la incidencia cuando en el entorno de integración, se haya realizado el despliegue del correctivo y comprobado que funciona. No obstante, la incidencia no se cerrará hasta que se haya desplegado en el entorno de producción y validado que funciona correctamente.

En el siguiente cuadro se establecen los Tiempos máximos de Solución esperados para las diferentes prioridades de las incidencias detectadas.

Prioridad Incidencia	Tiempos maximos de Solución (TS) en jornadas laborables
Crítica	1 jornadas (donde 1 jornada = 8 horas)
Alta	2 jornadas
Media	10 jornadas
Baja	35 jornadas

En cualquier caso, independientemente de lo indicado en el cuadro anterior, la totalidad de las incidencias deberán ser resueltas dentro del período de garantía.

6.2 Acuerdo Nivel de Servicio

El presente apartado tiene por objeto fijar los niveles de servicio (ANS), estándares de ejecución y los criterios y procesos de medición o valoración de los resultados exigidos a los Prestadores del Servicio para la provisión de los mismos.

- **ANS-01 (Puntualidad en la entrega de los Informes de Seguimiento de los proyectos de más de 3 meses):** Desviación en el número de días, respecto al plazo de entrega del informe mensual establecido en el apartado 4.3 del presente pliego, para los proyectos de más de TRES (3) meses de duración.

Indicador:	Puntualidad en la entrega de los Informes de Seguimiento de los proyectos de más de 3 meses de duración (**ANS-01**).
Cumplimiento:	Si **ANS-01 ≤ 0** ☐ Sin efecto. Si **ANS-01 > 0** ☐ Incumplimiento.
Periodicidad de cálculo:	Finalizado cada período mensual (30 días naturales).
Fórmula aplicada:	**ANS-01 = (Nde – 5)** *(expresado en días)* *Donde,* **Nde:** *Una vez finalizado un período mensual (30 días naturales), número de días hábiles transcurridos hasta la entrega del Informe de seguimiento correspondiente.*
Cálculo de la Penalización acumulada P1:	Por cada incumplimiento se añade un **2,00%** al índice de penalización acumulado.

- **ANS-02 (Puntualidad en la entrega de los Informes de Incidencia Significativa):** Desviación en el número de días, respecto al plazo de entrega del informe establecido en el apartado 4.3 del presente pliego del presente pliego.

Indicador:	Puntualidad en la entrega de los Informes de Incidencia Significativa (**ANS-02**).
Cumplimiento:	Si **ANS-02 ≤ 3** □ Sin efecto. Si **ANS-02 > 3** □ Incumplimiento.
Periodicidad de cálculo:	Cuando se produzca la incidencia grave (tipificadas como *Crítica* o *Alta*).
Fórmula aplicada:	**ANS-02 = (Fei – Fci)** *(expresado en días hábiles)* *Donde,* **Fei:** *Fecha de envío a Aigües de Barcelona del Informe de Incidencia Significativa.* **Fci:** *Fecha de la comunicación de la incidencia.*
Cálculo de la Penalización acumulada P2:	Por cada incumplimiento se añade un **2,00%** al índice de penalización acumulado.

- **ANS-03 (Retraso en la fecha de finalización del proyecto):** Desviación en el número de días, respecto al plazo máximo de finalización del proyecto acordado.

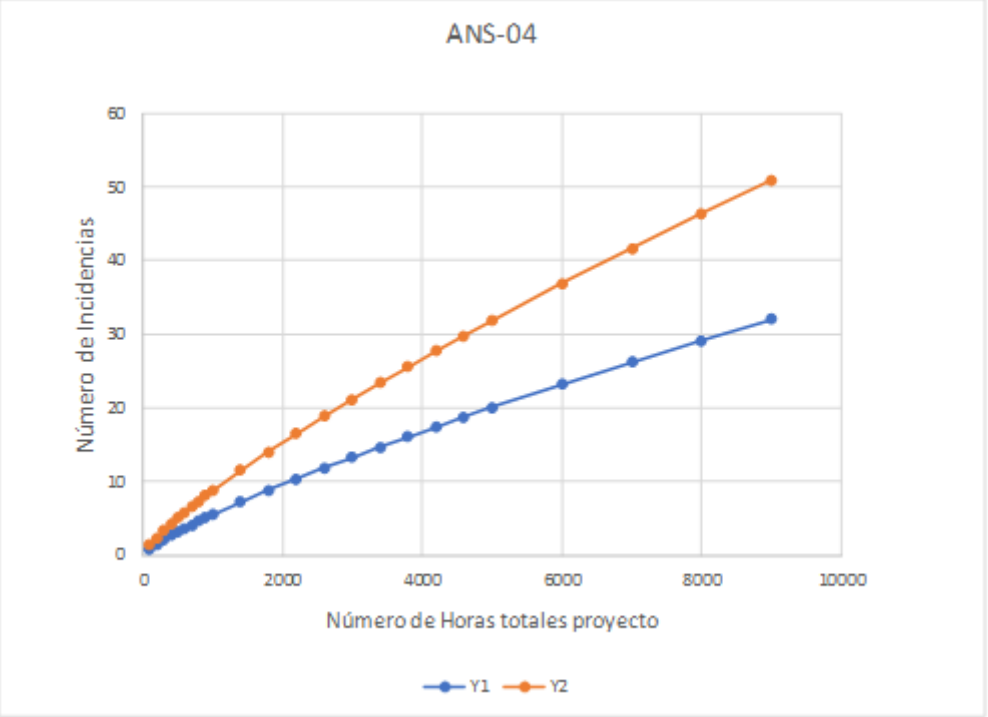
Indicador:	Retraso en la fecha de finalización del proyecto (**ANS-03**).
Cumplimiento:	Si **ANS-03 ≥ 0** □ Sin efecto. Si **ANS-03 < 0** □ Incumplimiento (*excepto cuando sea por causas no imputables al Prestador del Servicio*).
Periodicidad de cálculo:	A la finalización del proyecto (entregados en producción todos los requerimientos del alcance del proyecto - entrega de la Ficha de cierre de Proyecto).
Fórmula aplicada:	**ANS-03 = (Ndpe - Ndre)** *(expresado en días naturales)* *Donde,* **Ndpe:** *Número de días previstos para la ejecución del proyecto.* **Ndre:** *Número de días reales empleados para la ejecución del proyecto.*

Indicador:	Retraso en la fecha de finalización del proyecto (**ANS-03**).		
Cálculo de la Penalización P3:	Si 0%<(**ANS-03/Ndpe**)≤8% se añade un **2%** al índice de penalización acumulado.	Si 8%<(**ANS-03/Ndpe**)≤1,5% se añade un **4%** al índice de penalización acumulado.	Si (**ANS-03/Ndpe**)>15% se añade un **8%** al índice de penalización acumulado.

- **ANS-04 (Calidad del desarrollo entregado I):** Número de incidencias totales generadas con posterioridad a las puestas en marcha (post implantación) parciales o de la totalidad del proyecto. A medir durante el período de garantía establecido.

Indicador:	Calidad del desarrollo entregado (**ANS-04**).
Cumplimiento:	Si **ANS-04 ≤ Y1** → Sin efecto. Si **ANS-04 > Y1** → Incumplimiento. Donde, $Y1 = 0.022 * (Nho)^{0.8}$ **Nho**: *Número de horas ofertadas para el proyecto concreto por el Proveedor del Servicio que resulte adjudicatario del mismo.*
Periodicidad de cálculo:	A la finalización del período de garantía.
Fórmula aplicada:	**ANS-04 =** *Número de incidencias generadas durante el período de garantía*
Cálculo de la Penalización P4:	Siendo, $Y2 = 0.03 * (Nho)^{0.8}$, se consideran los siguientes niveles de penalización: ▪ Si **Y1**< **ANS-04** ≤**Y2**, se añade un **3,00%** al índice de penalización acumulado. ▪ Si **ANS-04** >**Y2**, se añade un **6,00%** al índice de penalización acumulado.

Indicador:	Calidad del desarrollo entregado (**ANS-04**).



- **ANS-05 (Calidad del desarrollo entregado II):** Número de incidencias de tipología Crítica o Alta generadas con posterioridad a las puestas en marcha (post implantación) parciales o de la totalidad del proyecto. A medir durante el período de garantía establecido aplicado en cada Release/Despliegue.

Indicador:	Calidad del desarrollo entregado II (**ANS-05**).
Cumplimiento:	Para **Nho** ≤ 2.000 horas: ▪ Si **ANS-05 ≤ 1** ☐ Sin efecto. ▪ Si **ANS-05 ≥ 2** ☐ Incumplimiento. Para **Nho** > 2.000 horas: ▪ Si **ANS-05 ≤ 3** y **T≤TS en todos los casos**☐ Sin efecto. ▪ Si (**ANS-05 ≤ 3** y **T>TS en alguno de los casos**) o (**ANS-05 ≥ 4**) ☐ Incumplimiento. Donde, **Nho**: *Número de horas ofertadas para el proyecto concreto por el Prestador del Servicio que resulte adjudicatario del mismo.* **T**: *Tiempo de solución real de la incidencia (Crítica o Alta).* **TS**: *Tiempo máximo de solución de la incidencia Crítica o Alta, según los criterios establecidos en el puntos 6.1 .*

Indicador:	Calidad del desarrollo entregado II (**ANS-05**).
Periodicidad de cálculo:	A la finalización del período de garantía.
Fórmula aplicada:	**ANS-05 =** *Número de incidencias Críticas y Altas generadas durante el período de garantía*
Cálculo de la Penalización P5:	Si se genera un incumplimiento del **ANS-05**, se consideran los siguientes niveles de penalización: ▪ Si el tiempo de solución de la incidencia (T), no supera los máximos (TS) establecidos en la cláusula 6.1 del presente PPT, desde la notificación de la misma por parte de Aigües de Barcelona: Se añade un **3%** al índice de penalización acumulado. ▪ Si el tiempo de solución de la incidencia (T), supera los máximos (TS) establecidos en la citada cláusula 6.1 del presente PPT, desde la notificación de la misma por parte de Aigües de Barcelona: Se añade un **6%** al índice de penalización acumulado.

6.3 Penalizaciones derivadas del incumplimiento de los ANS

Los Prestadores del Servicio se comprometen a cumplir con los ANS establecidos en el presente Pliego. Por tanto, el no cumplimiento de estos derivará en las penalizaciones expuestas en este apartado.

El incumplimiento de los ANS podrá reducir el importe a facturar como máximo un 10,00% del total adjudicado para la ejecución del proyecto.

El porcentaje de penalización a aplicar se obtiene a partir de la suma de los porcentajes parciales acumulados como consecuencia de los incumplimientos registrados con los ANS, según los siguientes criterios:

Penalización	Criterio
P1	Por cada incumplimiento del **ANS-01**, se añade un **2,00%** al índice de penalización acumulado. Por tanto: $P1 = (\sum_{i=1}^{n} 2)\%$, donde n es el número de incumplimientos del **ANS-01**.
P2	Por cada incumplimiento del **ANS-02**, se añade un **2,00%** al índice de penalización acumulado. Por tanto: $P1 = (\sum_{i=1}^{n} 2)\%$, donde n es el número de incumplimientos del **ANS-02**.
P3	Por incumplimiento del **ANS-03**, se añaden los siguientes porcentajes de penalización, según cada caso: ▪ **P3.1**: Si [0,00% <(**ANS-03/Ndpe**)≤ 8,00%], se añade un **2%** al índice de penalización acumulado. ▪ **P3.1**: Si [8,00% <(**ANS-03/Ndpe**)≤ 1,50%], se añade un **4,00%** al índice de penalización acumulado.

Penalización	Criterio
	▪ **P3.1**: Si [(**ANS-03/Ndpe**)> 15,00%], se añade un **8,00%** al índice de penalización acumulado. **Ndpe:** *Número de días previstos para la ejecución del proyecto.*
P4	Por incumplimiento del **ANS-04**, se añaden los siguientes porcentajes de penalización, según cada caso: ▪ **P4.1**: Si [**Y1**< **ANS-04** ≤**Y2]**, se añade un **3,00%** al índice de penalización acumulado. ▪ **P4.2**: Si [**ANS-04** >**Y2**], se añade un **6,00%** al índice de penalización acumulado.
P5	Por incumplimiento del **ANS-05**, se añaden los siguientes porcentajes de penalización, según cada caso: ▪ Si el tiempo de solución de la incidencia (T), no supera los máximos (TS) establecidos en la cláusula 6.1 del presente PPT, desde la notificación de la misma por parte de Aigües de Barcelona: Se añade un **3%** al índice de penalización acumulado. ▪ Si el tiempo de solución de la incidencia (T), supera los máximos (TS) establecidos en la citada cláusula 6.1 del presente PPT, desde la notificación de la misma por parte de Aigües de Barcelona: Se añade un **6,00%** al índice de penalización acumulado.

Donde el índice de penalización total (**PT**), será el valor que resulte de aplicar la siguiente fórmula: ***PT= P1 + P2 + P3 + P4 + P5***

Mientras **PT** sea inferior al 15%, no se aplicarán penalizaciones económicas derivadas del incumplimiento con los ANS. Cuando PT alcance o supere el valor del 15%, se aplicará una única penalización correspondiente al 10% del total adjudicado para la ejecución del proyecto.

Dicha penalización económica se aplicará coincidiendo con los hitos de facturación establecidos en el Acuerdo Marco y/o hasta la finalización del período de garantía, y una vez que PT alcance o supere el valor del 15,00%.

En el caso de que un Prestador del Servicio, en tres proyectos que se le hayan asignado, alcance un **PT** igual o superior al 15,00%, Aigües de Barcelona estará facultada para:

(i) resolver el Acuerdo Marco con dicho Prestador del Servicio, o bien

(ii) continuar con la imposición de penalizaciones en los términos previstos anteriormente.

6.4 Gestión y Coordinación

Se indican a continuación los requerimientos mínimos de seguimiento, control y organización que deberán cumplir los Prestadores del Servicio durante la vigencia del Acuerdo Marco.

Roles y responsabilidades

Los Prestadores del Servicio deberán nombrar los siguientes roles, aportando recursos cuya experiencia y nivel de decisión se adapte al nivel de sus responsabilidades.

A nivel de Acuerdo Marco:

- ***Responsable del Servicio*** *[UNO (1) para todo el Acuerdo Marco]*

  El adjudicatario deberá designar UN (1) Responsable del Servicio para la totalidad del Acuerdo Marco. Esta figura será el principal interlocutor con Aigües de Barcelona en todo lo relativo a la gestión global del contrato, con independencia de los proyectos concretos en curso.

  Entre sus funciones destacan las siguientes:

  - Asegurar el cumplimiento general de los Acuerdos de Nivel de Servicio (ANS).
  - Asegurar la correcta asignación de recursos para el cumplimiento de los objetivos de los diferentes proyectos.
  - Garantizar la rápida resolución y priorización de las incidencias graves.
  - Asegurar el cumplimiento de la planificación general y de los compromisos contractuales.
  - Garantizar la correcta gestión y respuesta a las solicitudes de oferta.
  - Generar un informe de seguimiento global del servicio con periodicidad semestral.
  - Gestionar las discrepancias sobre la validez de los ANS medidos y las penalizaciones que puedan derivarse.
  - Actuar como interlocutor principal para la gestión de las modificaciones al alcance del servicio.
  - Controlar que la facturación se realiza conforme a los acuerdos y resolver cualquier problema relacionado con el precio o los pagos.

  El Responsable del Servicio deberá tener un interlocutor designado por parte de Aigües de Barcelona. Con el objetivo de monitorizar y controlar la ejecución de los servicios, se establecerán reuniones periódicas, al menos semestralmente, o con la frecuencia que razonablemente se considere necesaria, o dentro de los TRES (3) días laborables siguientes a la petición de cualquiera de las partes.

A nivel de Proyecto: Equipo de Trabajo

Para la realización de cada proyecto solicitado bajo el Acuerdo Marco, el Prestador del Servicio deberá proponer un equipo competente y experimentado, compuesto por los perfiles adecuados según lo definido en el apartado 5 del presente pliego.

El equipo deberá estar dimensionado con el número de técnicos necesarios en cada momento para garantizar la correcta ejecución del proyecto, cubriendo las disciplinas requeridas en función de la naturaleza, complejidad y stack tecnológico del encargo. La composición del equipo deberá quedar justificada en la propuesta técnica correspondiente a cada proyecto.

La sustitución de cualquier miembro del equipo no podrá llevarse a cabo sin el consentimiento previo de Aigües de Barcelona. En caso de sustitución, deberá asignarse un profesional con cualificación equivalente. Si para garantizar la transferencia del conocimiento adquirido fuera necesaria la concurrencia entre el recurso saliente y el entrante, durante dicho período únicamente se contabilizarán como horas productivas las de uno de los dos recursos.

En cualquier caso, los equipos de trabajo deberán disponer de las siguientes habilidades comunes:

- Destreza comunicativa e interpersonal.
- Nivel nativo de castellano, tanto hablado como escrito, para una fluida comunicación con los técnicos de Aigües de Barcelona y con los usuarios.
- Capacidad de detección y resolución de problemas.
- Alta capacidad de organización y gestión de la información.
- Actitud proactiva y orientación a la mejora continua del servicio.
- Orientación al trabajo en equipo.

Cada proyecto deberá contar obligatoriamente con UN (1) Jefe de Proyecto, cuyo perfil, competencias y experiencia mínima requerida se detallan en el apartado 5 del presente pliego. Esta figura será el principal interlocutor con Aigües de Barcelona en lo relativo al proyecto asignado, y asumirá, cuando así lo requiera la metodología aplicada, las funciones propias del rol de Scrum Master en entornos Agile.

Aigües de Barcelona designará un Responsable de Proyecto como interlocutor del Jefe de Proyecto del Prestador del Servicio para cada proyecto en curso.

Los Prestadores del Servicio deberán garantizar que sus equipos disponen de la autonomía y capacidad de gestión necesarias para acometer, sin limitación, las siguientes tareas:

- Lanzamiento y liderazgo de reuniones.
- Gestión de riesgos y planes de mitigación o contingencia.
- Gestión de conflictos entre áreas intervinientes.
- Interlocución con el usuario final.
- Coordinación con otros proyectos en curso para pruebas integradas y puestas en producción coordinadas.
- Gestión del alcance y control de plazos.

Aigües de Barcelona entiende que el coste de estas actividades de gestión debe estar incluido por el Prestador del Servicio como parte de su oferta económica.

6.5 Acceso

El acceso del Prestador del Servicio a los sistemas de información de Aigües de Barcelona se realizará mediante conexión VPN de usuarios nominales. Se valorará posteriormente la posibilidad de usar una VPN Lan-to-Lan.

Todo el personal externo que tenga que trabajar en el servicio tendrá usuario personalizado en los sistemas necesarios. A tal efecto se deberá proporcionar al inicio del servicio el nombre, apellidos y DNI/NIE de los mismos.

6.6 Seguridad Corporativa

Tanto el Prestador del Servicio como sus trabajadores deberán de respetar las normas y regulaciones internas que dicte el área de Seguridad Corporativa, en materia de Seguridad de la información y uso de las TIC, como mínimo:

- Aceptar las normas establecidas en el área de Seguridad Corporativa tanto en el momento de su incorporación como después de cada cambio importante de las políticas, normas o regulaciones (ver Anexo Núm. 2)

- Dar cumplimiento a todas las normas, políticas y marcos reguladores vigentes durante el periodo del contrato.

- Permitir y facilitar la realización de auditorías de cumplimiento de las normativas establecidas para Seguridad Corporativa, internas o externas, sobre los sistemas de información vinculados a la prestación del Servicio, y garantizar la posibilidad de trazabilidad de las acciones realizadas por el auditor para facilitar el seguimiento de las mismas así como sus posibles impactos no deseados.

A la finalización del contrato, el adjudicatario quedará obligado a la entrega o destrucción en caso de ser solicitada, de cualquier información obtenida o generada como consecuencia de la prestación del servicio.

6.7 Idiomas

El servicio deberá prestarse a nivel comunicativo en castellano y/o catalán tanto hablado como escrito para una fluida comunicación con técnicos de Aigües de Barcelona y con los usuarios.

7. Solicitud de ofertas y asignación de pedidos

El proceso de solicitud de ofertas y de asignación de pedidos (proyectos de SI) se establece en la cláusula 16 del PCP.

ANEXO NÚM. 1 – CLASIFICACIÓN DE LAS INCIDENCIAS

1. Introducción

En el siguiente anexo se describen los criterios a aplicar para categorizar y priorizar las incidencias gestionadas por la actual herramienta de ITSM en Aguas de Barcelona.

A estos efectos, se considerará como Incidencia: Error o cualquier anomalía funcional o técnica que desencadena un resultado indeseado, no esperado o incompleto detectado en el sistema disponible para el cliente.

2. Criterios

2.1 Impacto

Determina la importancia del incidente dependiendo de cómo éste afecta a los procesos de negocio y/o del número de usuarios afectados. Es decir, el grado de afección que la incidencia tiene en el servicio.

Criterios para establecer el impacto		
Impacto	**Descripción**	**Ponderación**
0-Crítico (Extenso/Generalizado)	• Parada total de un Proceso Crítico de Negocio. • Parada total de un servicio/aplicación crítico; • Degradación de un servicio/aplicación crítico con afectación masiva; • Incidencia reportada por un usuario SVIP.	9
1-Alto (Significativo/Amplio)	• Degradación de un servicio/aplicación crítico sin afectación masiva; • Parada total o degradación de un servicio/aplicación NO crítico con afectación masiva; • Incidencia reportada por un usuario VIP; • Petición de servicio de un usuario SVIP;	5
2-Medio (Moderado/Limitado)	• Parada total o degradación de un servicio/aplicación NO crítico sin afectación masiva; • Petición de servicio de un usuario VIP.	3
3-Bajo (Menor / Localizado)	• El resto de incidencias y peticiones de servicio.	0

El impacto puede tener un valor predeterminado por el tipo de servicio afectado o ser calculado directamente por el técnico. El impacto predeterminado puede modificarse de forma automática si el usuario en nombre del que se realiza el registro pertenece a un nivel SVIP o VIP.

2.2 Urgencia

Depende del tiempo máximo de demora que acepte el cliente para la resolución del incidente y/o el nivel de servicio acordado en los ANS. En definitiva, es el grado hasta el que es posible demorar la solución.

Criterios para establecer la urgencia		
Urgencia	**Descripción**	**Ponderación**
1-Crítica	• El Proceso Crítico de Negocio no se puede ejecutar. • El usuario o departamento no puede realizar ninguna de las funciones principales que tiene asignadas. El usuario o departamento se encuentra parado hasta la resolución de la incidencia.	20
2-Alta	• El usuario o departamento no puede realizar alguna de las funciones principales que tiene asignadas. El usuario o departamento puede continuar con otras actividades hasta la resolución de la solicitud.	15
3-Media	• El usuario o departamento puede realizar las funciones principales que tiene asignadas pero presenta dificultades (lentitud, errores puntuales,...). El usuario o departamento puede continuar con otras actividades hasta la resolución de la solicitud.	10
4-Baja	• Se ven afectadas funciones secundarias del usuario o departamento que no impiden el desempeño de sus principales funciones.	0

2.3 Prioridad y tiempo de respuesta

El cálculo de la prioridad en la herramienta de gestión de incidencias se realiza de forma automática a partir de los valores de impacto y urgencia. La siguiente tabla muestra el cálculo en base a ambos parámetros.

Cuantificación de la prioridad = Impacto + Urgencia						
Criterio			Urgencia			
	Valor		Crítica	Alta	Media	Baja
		Ponderación	20	15	10	0
Impacto	Extenso / Generalizado	9	29 Crítica	24 Crítica	19 Alta	9 Baja
	Significativo / Amplio	5	25 Crítica	20 Alta	15 Media	5 Baja
	Moderado / Limitado	3	23 Alta	18 Alta	13 Media	3 Baja
	Menor / Localizado	0	20 Alta	15 Media	10 Media	0 Baja

El tiempo de respuesta para cada una de las tipologías de incidencias deberá ser el siguiente:

Prioridad	Valor	Actuación
1. Crítica	[24-29]	El tiempo de respuesta a la incidencia debe ser inmediato. Se pospondrá cualquier actividad que se esté realizando en ese momento excepto aquellas que tengan el mismo nivel de prioridad.
2. Alta	[18-23]	El tiempo de respuesta a la incidencia debe ser muy rápido. Se pospondrá cualquier actividad que se esté realizando en ese momento excepto aquellas que tengan el mismo nivel de prioridad o superior.
3. Media	[10-15]	El técnico al que se le asigna la incidencia deberá comenzar su resolución en cuanto termine las actividades de mayor prioridad.
4. Baja	[0-9]	El técnico al que se le asigna la incidencia deberá comenzar su resolución en cuanto termine las actividades de mayor prioridad.

ANEXO NÚM. 2 - NORMAS DE SEGURIDAD IT DE AIGÜES DE BARCELONA

Los Sistemas de Información proporcionados no deben de ser vulnerables, y según aplique, las TIP 10 de Owasp Security Mobile i/o OWASP Top 10 Security Web (https://www.owasp.org). A más a más deberán de cumplir la normativa de gestión de usuarios y contraseñas establecida en el presente Anexo.

Esta normativa puede cumplirse utilizando el Active Directory de Aigües de Barcelona como repositorio de los usuarios mediante una conexión segura con el sistema ADFS de Aigües de Barcelona o mediante el uso de Identity server.

"NORMAS DE SEGURIDAD IT DE AIGÜES DE BARCELONA"

ÍNDICE

1. Objeto e introducción del documento

El objeto del presente documento es establecer la normativa de seguridad en la gestión de los Sistemas de Información de Aigües de Barcelona y en la identificación, autentificación de usuarios y gestión de las contraseñas de acceso a los mismos.

2. Intercambio de información y software SI-N-07-02/01

El intercambio de información o software calificado como de uso interno, restringido o confidencial que realice Aigües de Barcelona con otras organizaciones, debe estar formalizado en acuerdos, validados por la Dirección Jurídica, que deben establecer las condiciones en las que se realizarán dichos intercambios.

Cuando, por razones de urgencia y eficiencia del servicio, sea imposible la formalización previa de dicho acuerdo, el intercambio de información estará sujeta a las condiciones generales previstas en esta norma y será el remitente el responsable de su cumplimiento.

El intercambio debe realizarse respetando la clasificación y el etiquetado de la información que se maneje durante dicho intercambio.

Los intercambios de información clasificada como restringida, así como de datos de carácter personal de nivel alto, se deben realizar empleando mecanismos de cifrado que impidan la divulgación no autorizada.

En los acuerdos se deben establecer los mecanismos oportunos para facilitar la gestión de estos intercambios y plasmar las responsabilidades y obligaciones legales cuando se lleven a cabo, especialmente las relacionadas con los datos de carácter personal.

Estos acuerdos deben indicar las responsabilidades de control y notificación del envío, transmisión y recepción de la información que se intercambia. Se debe asignar un gestor para cada acuerdo con la responsabilidad de controlar y hacer un seguimiento de su desarrollo.

En el ámbito legal, los acuerdos deben establecer las responsabilidades y obligaciones legales relativas al intercambio, especialmente aquellas derivadas del intercambio de datos de carácter personal con otras entidades, cesionarias o cedentes, de acuerdo con la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) y con el Reglamento de Desarrollo de la LOPD. No se podrán realizar intercambios de aquella información clasificada como confidencial.

Es responsabilidad de la Dirección de Seguridad TI identificar los mecanismos especiales requeridos para proteger activos críticos, como los de cifrado indicados anteriormente o el empleo de soluciones de no-repudio, con la finalidad de asegurar la recepción de la información por parte del destinatario.

3. Configuración y administración segura

3.1. Configuración segura

Todos los sistemas deberán estar configurados para verificar la identidad de los usuarios que acceden a ellos, de modo que no se comprometan las credenciales de autentificación y se garantice su identificación unívoca.

Asimismo, en función del perfil de los usuarios y la información que el sistema procese, se deberá determinar la asignación de privilegios y los servicios habilitados en cada caso. La configuración y asignación de privilegios debe regirse por el principio de menor privilegio, limitando los permisos únicamente a los estrictamente necesarios para la operativa diaria de trabajo de los usuarios. En este sentido, únicamente los administradores y operadores de los sistemas de información deben tener acceso a las utilidades de gestión y administración del sistema que requieren para el ejercicio de sus funciones, y pueden existir distintos niveles de derechos de administración.

Se deberán limitar los servicios de red abiertos en los diferentes sistemas de información. La configuración de los servicios de red activos debe regirse por el siguiente principio: "Se prohíbe todo aquello que no se encuentra explícitamente permitido", o lo que es lo mismo, se deben desactivar todos los servicios de red que se activan por defecto durante la instalación y cuyo uso no se encuentra motivado por una necesidad de negocio u operativa clara.

Adicionalmente, para evitar, en la medida de lo posible, la exposición a ataques de denegación de servicio, los dispositivos y elementos de comunicaciones deberán estar adecuadamente configurados mediante el establecimiento de medidas de protección como podrían ser:

- Limitaciones en el tiempo máximo de vida de conexiones inactivas.
- Limitaciones en el número máximo de conexiones abiertas.
- Restricciones en los algoritmos de propagación de información de encaminamiento.

Asimismo, en aquellos elementos de comunicaciones que provean acceso a la red de comunicaciones de Aigües de Barcelona o que utilicen algoritmos de encaminamiento dinámicos, deberán emplearse mecanismos de autentificación mutua basados en claves precompartidas, certificados digitales u otros mecanismos que proporcionen mayor seguridad.

Por último, los sistemas de información deberán estar configurados para registrar todos aquellos eventos que sean necesarios para asegurar la trazabilidad de las acciones realizadas en el sistema, con especial atención a los ficheros clasificados como de nivel alto según la LOPD.

3.2. Administración segura

La administración remota de los sistemas de información debe ser realizada por medio de herramientas y/o protocolos de administración que provean medios para identificar unívocamente al usuario administrador y para que las credenciales de dicho usuario administrador viajen cifradas por la red de comunicaciones empleando técnicas criptográficas.

Asimismo, se limitará el tiempo máximo de conexión de los usuarios administradores para evitar que las sesiones permanezcan abiertas de manera indefinida, lo que facilitaría la captura de sesiones por parte de usuarios no autorizados.

Incluido en los procesos de administración de sistemas, se deberá llevar a cabo un proceso de revisión periódica de ficheros temporales en servidores centrales y sistemas de información de Aigües de Barcelona, que corrija posibles fallos ocurridos durante el proceso de borrado de ficheros temporales. El tratamiento de estos ficheros temporales se debe ajustar a lo dispuesto en las normativas legales vigentes en materia de protección de datos de carácter personal (LOPD).

4. Identificación y autentificación de usuarios

Todos los sistemas de información no públicos de las unidades y sociedades operativas de Aigües de Barcelona deberán disponer de mecanismos que verifiquen la identidad de los usuarios que los usan, de tal forma que se restrinja los recursos a los que debe acceder cada usuario.

Los usuarios dispondrán de un único identificador para todos los sistemas de información, permitiendo determinar las operaciones que pueda realizar en los distintos sistemas a través de su identificador, salvo las excepciones reflejadas en el apartado "Identificador de usuario".

El mecanismo de autentificación de cada sistema se podrá implantar mediante:

- Software de control de acceso inherente al propio sistema.
- Herramienta de software de control de acceso agregado al sistema.

La autentificación, normalmente, se realizará mediante el empleo de contraseñas siguiendo los criterios de robustez de contraseñas indicados en el apartado de "Gestión de contraseñas y credenciales".

Todos los mecanismos de autentificación deberán ser supervisados por la Dirección de Seguridad TI, que verificará la correcta parametrización de la normativa de seguridad relativa a la autentificación de usuarios.

La autenticación en el sistema deberá garantizar que el usuario sólo tenga acceso a los recursos que necesite para el desempeño de sus funciones, no disponiendo de permisos de acceso a las herramientas propias del sistema, salvo que las necesite para el desarrollo de sus funciones (por ejemplo, administradores de sistemas).

En los procesos de autenticación a través de redes se evitará la transmisión de la clave de acceso de modo legible. Cuando el usuario acceda al sistema se le deberá mostrar, si es posible, la fecha y hora de su último acceso. Este aviso puede alertar al usuario de la existencia de accesos no autorizados. En este caso deberá de comunicarlo inmediatamente al Jefe de Seguridad de la Información de la entidad a la que pertenezca.

Cuando la criticidad del servicio o recurso lo requiera, la Organización de Seguridad de la Información promoverá el uso de mecanismos de autenticación basados en infraestructura de clave pública (PKI) y almacenamiento de claves en dispositivos externos (SmartCards, E-Tokens, etc.) Cuando se necesite acceso a archivos o transacciones especialmente sensibles el usuario debe ser re-autenticado, en caso de que sea posible técnicamente.

Con el fin de evitar el acceso no autorizado, el proceso de identificación y autenticación de usuarios deberá estar dotado de controles para el bloqueo automático del identificador de usuario y su inhabilitación temporal para el acceso al sistema en los siguientes casos:

- Por número de intentos de acceso incorrectos.
- Por inactividad del usuario en el sistema.

En estas situaciones, y en cualquier otra originada por el bloqueo de un identificador de usuario, el propio usuario deberá solicitar formalmente, a través del correo electrónico corporativo, la rehabilitación de sus privilegios de usuario. En el caso de que el identificador de usuario bloqueado sea el de correo electrónico, el superior jerárquico del usuario implicado deberá solicitar, por los procedimientos establecidos, la rehabilitación de los privilegios del mismo. Tanto si el desbloqueo se realiza manual como automáticamente deberán implantarse controles que permitan identificar y detectar intentos de acceso no autorizados.

Con el objetivo de evitar ataques de denegación de servicio a los usuarios administradores, los identificadores de usuarios administradores no se bloquearán. Se deberán establecer los controles compensatorios adecuados para monitorizar intentos fallidos de inicio de sesión para dichos usuarios, así como el aumento de tiempo para reintentos o bloqueos temporales, siempre que sea técnicamente posible.

5. Identificación de usuario

El acceso a cualquiera de los sistemas de información de Aigües de Barcelona se realizará utilizando un identificador de usuario convenientemente autorizado ([UserID]). El identificador de usuario deberá estar asignado a una persona física y tendrá carácter personal e intransferible. Consecuentemente, y asociado a cada identificador asignado a una persona física, se conservarán los datos que, como mínimo, permitan relacionar unívocamente el identificador de usuario con la persona física.

La nomenclatura del identificador de usuario se construirá con independencia de la función desempeñada por el usuario, de su puesto de trabajo, del departamento al que pertenece y del sistema al que se conecta. El identificador de usuario permanecerá asociado a su propietario de Aigües de Barcelona con independencia de los cambios de destino o de categoría que pudiera tener o, incluso de baja; y de acuerdo con la legislación vigente en materia de protección de datos de carácter personal.

Las personas que no pertenecen a la plantilla de trabajadores de Aigües de Barcelona deben recibir identificadores que sigan los mismos procesos de aprobación que para los nuevos empleados. Los derechos de acceso de los usuarios que no pertenecen a Aigües de Barcelona deben de otorgarse sólo por el periodo de tiempo estrictamente necesario y deberán ser reevaluados periódicamente.

No estará permitida la creación o utilización de usuarios genéricos salvo en aquellos casos en los que sea estrictamente necesario por razones operativas, funcionales, etc., que, por su naturaleza, aconsejan u obligan al uso de los mismos y previa autorización específica del Jefe de Seguridad de la Información de la entidad correspondiente. En estos casos, se extremará el seguimiento de las actividades realizadas con el usuario genérico, asegurando que se conoce, en todo momento, el grupo de usuarios que lo emplean. Cuando la necesidad de emplear el usuario genérico por un usuario del grupo finalice, se deberá modificar la contraseña de acceso compartida para hacer efectiva la salida de dicho usuario del grupo e impedir el empleo del usuario genérico más allá de sus necesidades.

Asimismo, salvo en situaciones justificadas por el desempeño de las funciones, cada persona física tendrá asociado un único identificador de usuario. Como excepción, un usuario podrá disponer de más de un identificador de usuario, en caso de que los privilegios asignados a cada uno sean distintos y técnicamente no sea posible recoger todos los privilegios en un sólo identificador de usuario o no sea recomendable mantener todos los privilegios en un único identificador de usuario por cuestiones de seguridad.

6. *Gestión de contraseñas y credenciales de clientes*

Para evitar la posible averiguación de las contraseñas por parte de terceros, éstas deberán cumplir una serie de requisitos a la hora de la generación de las mismas.

Como pauta general, las contraseñas de usuarios no deberán tener una longitud inferior a 6 (seis) caracteres alfanuméricos, incluyendo al menos dos caracteres numéricos y dos alfabéticos.

Para evitar la selección de contraseñas fácilmente adivinables, cuando sea tecnológicamente posible, los sistemas de control de acceso dispondrán de una colección de reglas de sintaxis que impedirán, por ejemplo, que la contraseña coincida con el identificador de usuario, o corresponda a una secuencia de longitud válida de un mismo carácter repetido, coincida con blancos o constituya una palabra conocida. Esta verificación se ejecutará de manera automática durante el proceso de cambio de contraseñas en las aplicaciones o herramientas en las que se utilice.

Los sistemas deben permitir al usuario el cambio de su contraseña de forma autónoma cuando éste lo estime oportuno. Asimismo, cuando se acceda por primera vez a un sistema o cuando se haya solicitado, a través de los procedimientos establecidos a tal efecto, una rehabilitación o desbloqueo de la contraseña, el sistema de control de acceso obligará al usuario al cambio de la misma en su primer acceso. La contraseña inicial deberá ser generada de manera aleatoria.

Los usuarios podrán solicitar, siguiendo los procedimientos establecidos, el desbloqueo de su identificador o un cambio de contraseña cuando no la recuerden o tengan sospecha de que ha perdido el carácter de secreta y no dispongan de la opción para cambiarla o desconozcan cómo realizar el cambio.

Después de cinco intentos fallidos consecutivos en la introducción de la contraseña por parte del usuario, como máximo, el sistema deberá deshabilitar el identificador asociado hasta su inicialización o desbloqueo.

Los sistemas de información de Aigües de Barcelona deberán disponer de mecanismos de control de acceso que permitan:

- Restringir, individualizar, registrar, controlar y, eventualmente, bloquear el acceso a la información y a las aplicaciones.
- Proteger la información y las aplicaciones de accesos realizados por personal no autorizado.
- Autenticar a todos los usuarios antes de que éstos accedan a cualquiera de los recursos de uso interno, restringido o confidencial para los que estén autorizados.
- Impedir la existencia de identificadores de usuario sin contraseña asignada.
- Proteger las contraseñas de los usuarios del siguiente modo:
    - Almacenando el resumen o "hash" generado con algoritmos estándar de cifrado.
    - No mostrarse en pantalla en texto claro
    - Restringir a todos los usuarios, en la medida de lo posible, la posibilidad de establecimiento de sesiones concurrentes.
    - Finalizar sesiones por inactividad durante un tiempo determinado. Se establecerá 5 minutos como valor de referencia, aunque deberá ser configurable en función de la criticidad y sensibilidad de los datos que se manejen.
    - No permitir la visualización de información referente al sistema hasta que el proceso de inicio de sesión haya terminado satisfactoriamente.
    - No permitir el almacenamiento de contraseñas en programas, "scripts" o códigos desarrollados para conexión automática a los sistemas de información. Salvo excepciones previamente autorizadas por la Dirección de Seguridad TI. La Dirección de Seguridad TI deberá definir mecanismos de control de acceso alternativos que efectúen controles no cubiertos por los sistemas de control de acceso instalados en los entornos, así como evaluar las ventajas y debilidades de las nuevas versiones y/o productos alternativos o complementarios.

La Dirección de Seguridad TI deberá evaluar los mecanismos de autenticación disponibles alternativos a las contraseñas, por ejemplo, biométricos, tarjetas, tokens, etc. para aquellos sistemas donde se requiera un nivel de autenticación más seguro.

7. Comunicación de los incidentes de seguridad

En caso de detección de un incidente grave de seguridad (mediante sistemas de detección de intrusiones, análisis de logs, comunicación de un tercero, alarmas de seguridad, etc.), la Dirección de Seguridad Aigües de Barcelona deberá ser informada a la mayor brevedad posible a través de líneas de comunicación que se establecerán previamente con este propósito.

La Dirección de Seguridad se encargará de iniciar un informe hacia las figuras, escogidas entre aquellas que previamente habían sido identificadas, cuya participación sea necesaria en la resolución del incidente. Esta elección se hará en función de la criticidad del incidente, el grado de conocimiento necesario o los sistemas a los que afecte.

Las Áreas de Asuntos Legales (Dirección Jurídica) y Recursos Humanos deberán ser informadas en caso de que el incidente necesite tomar acciones disciplinarias o legales y en caso de que pueda tener repercusiones legales para Aigües de Barcelona.

Se deberán reportar aquellos incidentes significativos a los niveles jerárquicos superiores establecidos con la finalidad de obtener autorizaciones o de informar sobre la actuación de Aigües de Barcelona frente a incidentes de seguridad.

El reporte de información sobre incidentes de seguridad quedará restringido únicamente a aquellas personas absolutamente necesarias. Cualquier divulgación de dicha información deberá ser autorizada por la Dirección de Seguridad.

Es responsabilidad de la Dirección de Seguridad mantener un registro con los datos de aquellas personas que han sido informadas de cada incidente con la finalidad de detectar una posible divulgación no autorizada.

Tanto los empleados de las entidades de Aigües de Barcelona como los trabajadores de empresas externas conocerán las líneas de reporte de incidentes de seguridad y tienen el deber de utilizarlas en caso de detectar un incidente de seguridad. Si la persona que detecta el incidente no está segura de si se trata de un incidente o no, deberá reportarlo igualmente.