

**PLIEGO DE PRESCRIPCIONES TÉCNICAS
QUE DEBE REGIR EL ACUERDO MARCO RELATIVO AL "SERVICIO DE
DESARROLLO DE SISTEMAS DE INFORMACIÓN (SI) DEL ÁREA COMERCIAL
DE AIGÜES DE BARCELONA"**

Nº EXP.: AB/ABAST/2019/45



Contenido

1.	OBJETO	3
2.	ALCANCE	3
3.	SITUACION ACTUAL DE LAS APLICACIONES	4
3.1.	LOTE Nº 1: SICAB, SISTEMÁTICOS y AVERIAS	4
3.1.1.	Sistema de Información Comercial de Aigües de Barcelona (SICAB).	4
3.1.2.	Gestión de ordenes de trabajo planificadas (SISTEMÁTICOS).....	5
3.1.3.	Gestión de ordenes de trabajo urgentes (AVERÍAS)	6
3.2.	LOTE Nº 2: SIEBEL-CRM	6
3.2.1.	Atención a Clientes (SIEBEL-CRM).....	6
3.3.	LOTE Nº 3: HOJA DE RUTA	7
3.3.1.	Inventario de las tareas de las ordenes de trabajos realizadas (HOJA DE RUTA).....	7
4.	CONDICIONES TECNICAS DE LAS APLICACIONES	8
4.1.	Lote Nº 1: SICAB, SISTEMÁTICOS y AVERIAS.....	8
4.2.	Lote Nº2: SIEBEL-CRM	9
4.3.	Lote Nº3: HOJA DE RUTA	10
5.	CONDICIONES OPERATIVAS PARA LOS DESARROLLOS (PROYECTOS)	10
5.1.	Metodología.....	10
5.2.	Entorno bimodal.....	12
5.3.	Entregables	12
5.4.	Ubicación	14
6.	OTROS REQUERIMIENTOS DEL SERVICIO	15
6.1.	Recepción, control, resolución y canalización de incidencias	15
6.2.	Acuerdos de Nivel de Servicio (ANS)	16
6.3.	Penalizaciones derivadas del incumplimiento con los ANS.....	19
6.4.	Garantía	21
6.5.	Gestión y Coordinación	21
6.6.	Recursos Materiales requeridos	23
6.7.	Especificaciones de RGPD y SEGURIDAD	24
7.	SOLICITUD DE OFERTAS.....	24
	ANEXO Nº 1 - CALIFICACIÓN DE LAS INCIDENCIAS	25
	ANEXO Nº 2 - NORMAS DE SEGURIDAD IT DE AIGÜES DE BARCELONA	28

1. OBJETO

El presente Pliego establece las prescripciones técnicas que rigen el procedimiento de contratación para la obtención del "Acuerdo Marco relativo al servicio de desarrollo de sistemas de información (SI) del Área comercial", 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

Las aplicaciones que forman parte del ámbito del presente procedimiento han sido agrupadas en función de sus características funcionales y/o peculiaridades técnicas, en 3 lotes:

- **Lote Nº 1 – SICAB, SISTEMATICOS y AVERIAS:** Aplicaciones Comerciales del Ciclo de Gestión Comercial y gestión de órdenes de trabajo planificadas y urgentes.
- **Lote Nº 2 – SIEBEL-CRM:** Aplicación para la Atención a Clientes.
- **Lote Nº 3 – HOJA DE RUTA:** Inventario de tareas de las órdenes de trabajo.

Cada una de las aplicaciones que constituyen los diferentes lotes son descritas en detalle en el capítulo 3.

Para cubrir las diferentes tareas a realizar, se han establecido tres tipos de perfiles profesionales:

- Jefe de Proyecto / Gestor de proyecto.
- Analista de sistemas información.
- Programador / Analista programador.

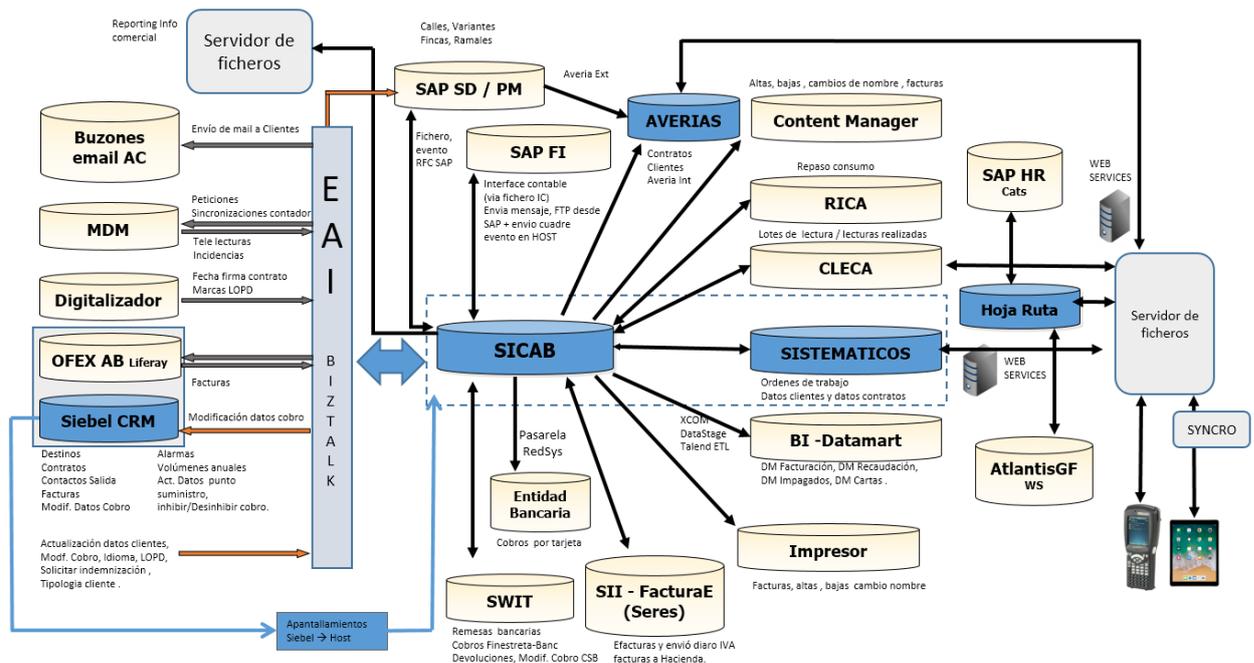
El volumen de horas a demandar dependerá del volumen de proyectos aprobados para su ejecución. Como número orientativo y sin ningún tipo de compromiso por parte de Aigües de Barcelona, teniendo en cuenta los históricos acumulados en los 3 últimos ejercicios (2016-2018), puede considerarse una línea base de 18.500 horas al año para el conjunto de los lotes a licitar. Una aproximación de la distribución en horas anuales de esta línea base para los diferentes lotes y perfiles profesionales sería la siguiente:

Lotes Acuerdo Marco	Estimación de horas para un año			
	Totales	Jefe de Proyecto	Analista de sistemas	Programador
LOTE Nº 1- SICAB, SISTEMATICOS y AVERIAS:	12.210	1.320	3.300	7.590
LOTE Nº 2- SIEBEL-CRM:	5.550	600	1.500	3.450
LOTE Nº 3- HOJA DE RUTA:	740	80	200	460

3. SITUACION ACTUAL DE LAS APLICACIONES

En este capítulo se describen funcionalmente las aplicaciones del Área Comercial que forman parte del alcance de este pliego y de cada uno de los lotes que lo constituyen.

En el siguiente diagrama se pueden observar el conjunto de aplicaciones, sus integraciones y resaltadas en color azul aquellas que forman parte del alcance del presente pliego.



3.1. LOTE Nº 1: SICAB, SISTEMÁTICOS y AVERIAS

3.1.1. Sistema de Información Comercial de Aigües de Barcelona (SICAB).

Es la aplicación que soporta la gestión el ciclo comercial y consta de los siguientes módulos funcionales:

- **Contratación:** Alta, mantenimiento y rescisión de los contratos del agua en los diferentes puntos de suministro. Este módulo tiene una importante integración con SIEBEL-CRM (aplicación que también se recoge dentro del ámbito de este pliego como lote Nº 2).
- **Atención al cliente:** Gestión de los requerimientos de clientes desde Oficinas o desde el "call center". Se realizan las modificaciones de cobros, cambios de titularidad, anulación de facturas, etc. La gestión del requerimiento se inicia en SIEBEL-CRM y acaba finalizando, una buena parte de ellos, en SICAB mediante apantallamiento de la aplicación comercial.
- **Lecturas:** Generación de los lotes de lecturas por recorrido, obtención y consolidación de las lecturas desde los diferentes sistemas (CLECA para los TPL's, MDM para Telelectura, Transacción en el caso de recibirla por cliente, etc.).
- **Facturación:** Procesos diarios de generación y emisión de facturas, junto con las funcionalidades para el control de la facturación (lotes, frecuencia, tarifas, etc).
- **Recaudación e Impagados:** Seguimiento contable de la vida de las facturas, desde que se generan, hasta que son cobradas, devueltas, impagadas, canceladas, etc. Gestión



especial para aquellos clientes que están considerados como riesgo de exclusión social, en el caso de impagos de facturas.

- **Gestión de Contadores:** Mantenimiento de los contadores ubicados en los puntos de suministro tanto para la instalación, retirada, renovación, como la actualización de sus características técnicas.
- **RICA:** Cálculo, estimación y procesado de lectura sobre datos anómalos de consumos obtenidos.
- **Contabilidad:** Generación de los cuadernos de carga diarios para la integración con SAP.

Las principales integraciones de la aplicación comercial se establecen con los siguientes sistemas:

- Módulo de SAP de gestión financiera, gestión de mantenimiento, ventas y distribución.
- Gestor documental e impresor.
- Gestión de lotes de lectura y repaso de lecturas anómalas.
- Módulo FacturaE, Swift para la integración bancaria y Redsys para el pago con tarjeta.
- Ordenes de trabajo urgentes y planificadas.
- Datamart y BI para el reporting.
- Siebel-CRM y la Oficina Virtual para la Atención a clientes.

3.1.2. Gestión de ordenes de trabajo planificadas (SISTEMÁTICOS)

Con la aplicación de SISTEMÁTICOS se gestionan las Órdenes de Trabajo planificadas o preventivas, además de la explotación de los elementos del punto de suministro (baterías, contadores, puntos de lectura remota, etc.). Aunque desde el punto de vista funcional y operativo pertenece al área técnica dentro de las aplicaciones de negocio de Aigües de Barcelona, no es una aplicación independiente, sino que está integrada como un módulo dentro de la aplicación de SICAB, compartiendo las mismas características técnicas y de arquitectura que la aplicación comercial.

Anualmente la aplicación de SISTEMÁTICOS gestiona unas 400.000 órdenes de trabajo. El sistema se integra con una plataforma de movilidad, siendo una aplicación que da servicio 24x7. Sus principales funcionalidades son:

- **Recepción de las Ordenes de Trabajo:** Con diferentes orígenes, en la aplicación se reciben las operaciones a realizar en campo, desde la instalación de un contador por la contratación de un nuevo cliente, pasando por el mantenimiento (sustitución del contador) y la retirada del mismo.
- **Tratamiento de las Ordenes de Trabajo:** Permite agrupar las operaciones en lotes de trabajo, que serán la información que se transfieren a los terminales en campo de los operarios. Además, cuenta con funcionalidades de back office para realizar una correcta gestión y seguimiento de las ordenes ejecutadas.
- **Respuesta y finalización de la Orden de Trabajo:** Una vez realizada la operación se recoge la respuesta comunicada por el operario, se gestiona el cierre en la aplicación y se comunica al sistema origen. En el caso de que la operación no se haya podido realizar con éxito, la orden de trabajo entraría en un nuevo ciclo de tratamiento.

Las principales integraciones de Sistemáticos se establecen con los siguientes sistemas:

- El sistema comercial (SICAB).
- Movilidad.
- Datamart para el reporting.
- Siebel-CRM para la gestión de clientes.

3.1.3. Gestión de ordenes de trabajo urgentes (AVERÍAS)

La aplicación de AVERÍAS permite la gestión de las Órdenes de Trabajo urgentes sobre los componentes de la red de distribución (averías exteriores) o de un punto de suministro (averías interiores). Esta aplicación pertenece al área técnica y aun siendo una aplicación independiente, comparte las mismas características técnicas y de arquitectura que la aplicación comercial de SICAB, por lo que se integra dentro del mismo lote, igual que SISTEMÁTICOS.

Anualmente desde la aplicación de AVERIAS se gestionan unas 80.0000 órdenes de trabajo. El sistema se integra, igual que las ordenes de trabajo planificadas, con una plataforma de movilidad, siendo una aplicación que da servicio 24x7. Sus principales funcionalidades son:

- **Localizar Averías:** Permite realizar el seguimiento y mantenimiento de las averías desde la entrada en el sistema, envío a terminarles del operario, respuesta, hasta el cierre técnico de la orden de trabajo. Tiene la posibilidad de incorporar nuevas acciones a nivel de operario, supervisor, contratista (ejecución de obras previa a la resolución de la avería), cliente y laboratorio.
- **Operativa de Back Office:** Conformar el conjunto de funcionalidades que permiten completar la gestión de las averías como el mantenimiento de operarios, validación de trabajos, supervisión de las ordenes, etc.

Las principales integraciones de averías se establecen con los siguientes sistemas:

- El sistema comercial (SICAB).
- Movilidad.
- Datamart para el reporting.
- Siebel-CRM para la gestión de clientes y la creación de todas las averías y posterior gestión de las interiores.
- Módulo de SAP de gestión de mantenimiento.

3.2. LOTE N° 2: SIEBEL-CRM

3.2.1. Atención a Clientes (SIEBEL-CRM)

Es un Producto de mercado personalizado para la comercialización y soporte a la gestión de la relación con los clientes de Aigües de Barcelona. Estas relaciones se establecen desde diferentes canales de atención como el presencial, telefónico, vía mail, SMS, gestión de cita, cartas, faxes o la Oficina en Red.

La relación se inicia a partir de un contacto de entrada y las funcionalidades que permite la aplicación está focalizada en la gestión de diferentes tipos de requerimientos:

- **Consultas:** Cualquier tipo de consulta sobre la gestión del contrato, del ciclo de facturación, del ámbito técnico y comercial.
- **Solicitudes:** Desde la cita, gestión documental, modificación de datos del cliente, del contrato, de la factura, y especialmente sobre el punto de suministro (alta, rescisión, cambio de titular, condiciones contractuales, etc.).
- **Reclamación Técnicas:** Relacionas con la calidad del agua, falta de agua, falta de presión, de la instalación, escapes, etc.
- **Reclamaciones Comerciales:** Sobre la calidad del servicio, carta de compromiso, condiciones contractuales, consumo facturado, quejas, RGPD, etc.

Las principales integraciones de Siebel se establecen con los siguientes sistemas:

- El sistema comercial (SICAB).
- La Oficina virtual, tanto App como Web.
- Datamart para el reporting.
- Gestor documental.
- Ordenes de trabajo urgentes y planificadas.
- Módulos comunes para los canales de comunicación con el cliente (sms, mail, etc.).
- Módulo SAP de gestión de mantenimiento, ventas y distribución.

3.3. LOTE Nº 3: HOJA DE RUTA

3.3.1. Inventario de las tareas de las ordenes de trabajos realizadas (HOJA DE RUTA)

Hoja de Ruta es una aplicación desarrollada a medida para disponer del inventario de trabajos realizados y agruparlos según los criterios de gestión. Adicionalmente permite la imputación directa de las dedicaciones en SAP y poder obtener informes y estadísticas del rendimiento de trabajo de los operarios de forma diaria.



La aplicación se divide en dos componentes:

- **Aplicación PC:** Desde donde se permite consultar, modificar, validar las hojas de ruta de cada uno de los operarios, además de enviar a SAP las correspondientes imputaciones horarias.
- **Aplicación de Movilidad:** Donde se generan las hojas de ruta de los operarios. Este componente de la aplicación queda fuera del alcance de este pliego.

Las principales integraciones de Hoja de Ruta se establecen con los siguientes sistemas:

- El módulo de SAP de recursos humanos.
- La aplicación para la gestión de flotas de vehículos.
- Movilidad.

4. CONDICIONES TECNICAS DE LAS APLICACIONES

Los ofertantes deberán de ser conocedores de la tecnología especificada en cada una de las aplicaciones que constituyen los lotes a los que concurren.

4.1. Lote Nº 1: SICAB, SISTEMÁTICOS y AVERIAS

Las tres aplicaciones de este Lote comparten componentes y tienen una definición técnica muy parecida, por lo que tienen una estrecha relación.

La aplicación **SICAB** cuenta con un front-end en JAVA (JRE 1.6 y 1.8) con la siguiente configuración:

- Componentes AWT, personalizados, para los módulos funcionales de Recaudación y Atención a Clientes.
- Swing-XML para el resto de los módulos de la aplicación.
- En el caso de Facturación y Lecturas, el grueso del transaccional se ejecuta en pantallas desde el CICS.
- La comunicación con HOST (donde se aloja la mayoría de procesos de negocio y la BB.DD.) se efectúa vía CTG (CICS Transaction Gateway).
- Los servidores Windows son servidores IIS donde se alojan los fuentes de la aplicación (SICAB no es una aplicación WEB).
- Los usuarios se descargan la aplicación accediendo a servidores IIS, a partir de un fichero jnlp (Java Network Protocol Language) y la ejecutan en local desde su PC's.
- En el caso del módulo de RICA está desarrollada en Visual Basic v6. bajo Oracle.

La aplicación de **SISTEMÁTICOS** también cuenta con un front-end en JAVA (JRE 1.6 y 1.8), con la siguiente configuración:

- Componentes AWT, igual que los módulos de Recaudación y Atención a Clientes de SICAB.
- La comunicación con HOST (donde se aloja la mayoría de procesos de negocio y la BB.DD.) se efectúa vía CTG (CICS Transaction Gateway).
- Los servidores Windows son servidores IIS donde se alojan los fuentes de la aplicación (SISTEMÁTICOS no es una aplicación WEB).
- La notificación del envío de las ordenes de trabajo a los terminales se realizan a través del Syncro.

- Los usuarios se descargan la aplicación accediendo a servidores IIS, a partir de un fichero jnlp (Java Network Protocol Language) y la ejecutan en local desde su PC's.

La aplicación de **AVERIAS** cuenta igualmente con un front-end en JAVA (JRE 1.6 y 1.8) con la siguiente configuración:

- Componentes SWIX-XML, como algunos de los módulos de la aplicación SICAB.
- La comunicación con un HOST – DB2 para la gestión de Averías Interiores.
- La comunicación con SAP, vía RFC's (Remote Function Call), para la gestión de Averías exteriores. La aplicación de Averías necesita del cliente SAP para su funcionamiento.
- Los servidores Windows son servidores IIS donde se alojan los fuentes de la aplicación (AVERIAS no es una aplicación WEB).
- El servidor (Windows Server 2008) de intercambio de ficheros entre la aplicación central, de PC, y los terminales móviles.
- Los usuarios se descargan la aplicación accediendo a servidores IIS, a partir de un fichero JNLP (Java Network Protocol Language) y la ejecutan en local desde su PC's.

En las tres aplicaciones, los procesos de negocio están desarrollados mayoritariamente en Cobol (Enterprise COBOL 05.01) sobre un Mainframe de IBM con sistema operativo Z/OS v.2.1, base de datos DB2 v. 11.1 y CICS como entorno transaccional, CICS/TS v5.2 con CTG v9.1.

Bajo el mismo entorno Mainframe se comparte tanto la base de datos como la ejecución de los procesos de negocio.

Actualmente existe un entorno de desarrollo, que es utilizado como entorno de integración y pruebas, y un entorno productivo. Ambos están situados en instalaciones de un proveedor de servicio en Munich (Alemania) bajo LPAR diferentes.

En el caso de SICAB existen también procesos planificados fuera del entorno Mainframe, como son la generación de la factura electrónica y gestión de estados, recepción de documentos digitalizados, integración de ramales con SAP, WEB Service de integración con MDM, recepción de respuesta de Ayuntamientos, etc., que están desarrollados con Java/Cics y ejecutados como tareas programadas en el servidor windows o con JEE gestionadas mediante JBOSS.

En el caso de AVERIAS y SISTEMÁTICOS, la integración con la movilidad cuenta con unos servicios Java ejecutados en un servidor Windows Server 2008, uno para las averías exteriores, otro para las interiores y un tercero para las operaciones de sistemáticos.

4.2. Lote Nº2: SIEBEL-CRM

La aplicación CRM que se utilizada es Oracle Siebel 8.0.0.12 con los siguientes elementos de arquitectura para el entorno productivo:

- 2 Servidores IIS sobre W2008.
- 3 Servidores de aplicación Siebel sobre W2008.
- Base de datos Oracle 11.2 sobre AIX 7.1.

Las herramientas Siebel de desarrollo utilizadas son:

- Siebel Tools.
- Siebel eScript.

5. Paso a producción.



- En la **Definición y Análisis**, 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, las integraciones y posibles automatizaciones.
- En la fase de **Construcción**, se desarrollarán los procesos y objetos, así como también se deberán de 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.

A continuación, se enumeran otros aspectos importantes a tener en cuenta a nivel metodológico:

- Disponibilidad de los entornos (desarrollo, integración y producción). No todas las aplicaciones cuentan con esta disponibilidad de entornos.
- Gestión de la configuración en la convivencia con otros proyectos y el propio mantenimiento de la aplicación.
- Cambios en el Modelo de Datos. Pactar específicamente las modificaciones en las bases de datos (nuevas entidades y modificaciones).
- Los despliegues a producción podrán requerir implementar cambios ya realizados en el mantenimiento o por otros proyectos recientemente implantados.
- Los accesos a los SI de Aigües de Barcelona serán bien por conexión VPN lan-to-lan o usuarios VPN nominales.
- Todos los colaboradores que tengan que trabajar en un proyecto tendrán usuarios personalizados, por lo que al inicio del proyecto tendrán que facilitar el DNI y nombre competo.
- En el caso de trabajar en aplicaciones bajo Mainframe, el proveedor tendrá que disponer de un emulador 3270 para el acceso a los fuentes. En el caso de las aplicaciones Java se requerirá Eclipse y SubVersión como repositorio de los fuentes.



- Todas las modificaciones de fuentes de programa deberán ser marcadas. En el caso de herramientas de desarrollo que no lo faciliten, como el caso de los programas COBOL, tendrá que realizarse manualmente.
- Antes de la puesta en marcha en producción y tras las pruebas de regresión realizadas, cualquier error provocado por los cambios efectuados deberá de corregirse con carácter de urgencia dentro del ámbito de las tareas del proyecto.
- Las llamadas entre SIEBEL y SICAB-SISTEMÁTICOS-AVERIAS se harán mediante Web Service directos, sin utilizar herramientas de integración (actualmente se utiliza Biztalk como EAI y está en fase de eliminación), salvo que se puede reutilizar integraciones ya existentes.
- En la planificación de los proyectos se tendrá que coordinar y acordar con negocio la disponibilidad de los usuarios para las pruebas de aceptación.

5.2. Entorno bimodal

Un punto a tener muy en cuenta será la apuesta por metodologías Agiles en el desarrollo de los proyectos. Será un proceso de transformación que Aigües de Barcelona tendrá que implementar en la organización y que obligará al proveedor a trabajar en un entorno bimodal, es decir, actuar y establecer sinergias entre dos escenarios tecnológicos complementarios y con características diferenciadas, una vez que las aplicaciones afectadas hayan evolucionado a los entornos que permitan dichas metodologías de trabajo Agile.

De esta forma, el proveedor tendrá que ser capaz de gestionar y combinar unas metodologías de trabajo dinámicas e innovadoras de tipo Agile con los modelos más tradicionales de gestión interna ya instalados en la organización, de tipo Waterfall o Cascada. Como parte del servicio, el licitador deberá adoptar la metodología a definir por Aigües de Barcelona, tanto para modelos Waterfall como modelos Agile.

Además, siguiendo el énfasis en la implantación incremental de metodologías de tipo Agile, en respuesta a la creciente necesidad de cambio y transformación de Aigües de Barcelona para dar una respuesta más rápida a la implementación y operación de aplicaciones, el proveedor deberá adoptar en concreto el modelo Agile-DevOps en los ámbitos donde Aigües de Barcelona lo crea necesario.

Este aspecto se tendrá en consideración, ya que el objetivo final es evolucionar hacia este entorno de trabajo e implementar de forma plena en la organización la metodología DevOps para favorecer la innovación y las exigencias del entorno.

En todo caso, el cambio de perfiles asignados al servicio para balancear la carga entre las distintas metodologías de desarrollo (de cascada a Agile), no supondrán coste adicional alguno para Aigües de Barcelona.

5.3. Entregables

Durante el periodo que dure el desarrollo del servicio hasta la entrega y puesta en producción del proyecto, así como durante el período de garantía, se deberá generar y entregar, como mínimo, la siguiente documentación, siempre y cuando la metodología aplicada sea en cascada (ver especificación 5.1):

Antes del inicio de la fase de Definición y Análisis:

- **Documento de inicio de proyecto o Kickoff**, que tendrá que presentarse a los interesados (tal como negocio, gestión de la demanda, equipo interno de Aigües de Barcelona y el resto de equipos de trabajo) en la reunión de formalización de inicio del proyecto.

A la finalización de la fase de Diseño:

- **Análisis funcional y Análisis Técnico.** El documento de análisis funcional será el entregable resultado de las fases de análisis y diseño de la solución a entregar, 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. Por ejemplo, en el caso de un panel de una transacción, deberá de quedar dibujado una propuesta del diseño donde queden recogidos los campos, tamaño, etiquetas, botones, etc., además del comportamiento de cada uno de ellos y el flujo o transacción de paneles que pueden darse. En el caso de un proceso batch, deberá de definirse los inputs y outputs del proceso, en qué condiciones y cómo va a funcionar, planificación del proceso, dependencias con otros procesos, etc.

A nivel técnico, deberá detallarse la lista de elementos a desarrollar, las interfaces, modelo de datos, la definición de parámetros o variables de ejecución, los elementos de la infraestructura, etc.

En cualquier caso, en estos documentos deberá quedar especificado en que condiciones deberá funcionar y que limitaciones tendrá el producto a entregar.

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

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 la fase de Construcción:

- Documentación de las **pruebas unitarias** ejecutadas durante la fase de construcción, a entregar antes del inicio de la ejecución del Plan de pruebas.

A la finalización de la fase de Diseño y en la fase de Pruebas:

- **Plan de Pruebas.** Este documento se entregará en dos fases. En una primera entrega, sin ejecutar, junto con el documento de análisis funcional. La segunda entrega se hará tras su ejecución y validación, una vez finalizada la fase de construcción y previa a la ejecución del Plan de pruebas de aceptación por parte del usuario. Será un documento vivo que, en su caso, tendrá que ir actualizándose durante toda la fase del desarrollo.

Al inicio de la fase correspondiente al Paso a Producción:

- **Plan de Implantación.** Tendrá que ser revisado y aprobado por Aigües de Barcelona, una vez realizadas las pruebas de aceptación por parte del usuario.
- **Traspaso al Servicio de Mantenimiento.** Donde deberá recogerse el alcance técnico y funcional para poder realizar un correcto mantenimiento de los procesos modificados, los de nueva creación y de la infraestructura. Se deberá entregar a Aigües de Barcelona, como

mínimo, una semana antes (cinco días hábiles) del inicio de la implantación de los desarrollos (paso a producción).

A la finalización del Paso a Producción:

- **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 de desarrollo, quedando activo el periodo de garantía establecido.

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 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 puesto en marcha el proyecto 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 licitador 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.

5.4. Ubicación

Los servicios se prestarán desde las propias oficinas del adjudicatario, 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 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.

6. OTROS REQUERIMIENTOS DEL SERVICIO

6.1. Recepción, control, resolución y canalización de incidencias

Los adjudicatarios 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 de los desarrollos entregados, deberán hacer uso de la herramienta JIRA.
- Mientras que, en fase de post implantación (parcial o total) deberán hacer uso de la herramienta BMC Remedy.

El Prestador del Servicio deberá utilizar dichas herramientas de ticketing para el reporte y 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 será consensuados por ambas partes en la fase correspondiente. Estos procedimientos pueden ser cambiadas en cualquier momento por Aigües de Barcelona, previa comunicación y aceptación por parte del Prestador del Servicio, quién se compromete a adoptarla en el plazo máximo que se establezca.

En lo que se refiere a la fase de post implantación (período de garantía), cada ticket vendrá informado con una prioridad asignada por Aigües de Barcelona según lo previsto en el **Anexo Nº 1**, que será revisada por el Prestador del Servicio en el momento de la recepción del ticket, para su aceptación o solicitud de cambio. En lo que se refiere a los tiempos máximos de solución (TS), éstos se establecen para cada tipología de incidencia según el cuadro siguiente:

Prioridad de la incidencia	Tiempo máximo de solución (TS) <i>(horas desde la comunicación de la incidencia)</i>
Crítica	12 h
Alta	24 h
Media	110 h
Baja	240 h

El servicio de mantenimiento para las aplicaciones que integran los diferentes lotes, tiene una disponibilidad horaria de 8:00 h hasta las 20:00 h, siendo 12 horas las que se cubren en una jornada de trabajo y por tanto ésta es la amplitud horaria establecida para contabilizar los tiempos máximos de solución de las diferentes incidencias comunicadas en fase de garantía.

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

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 de 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.

6.2. Acuerdos de Nivel de Servicio (ANS)

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 capítulo 5.3 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) <i>(expresado en días)</i> <i>Donde,</i> Nde: <i>Una vez finalizado un período mensual (30 días naturales), número de días hábiles transcurridos hasta la entrega del Informe de seguimiento correspondiente.</i>
Cálculo de la Penalización acumulada P1:	Por cada incumplimiento se añade un 2% 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 capítulo 5.3 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 <i>Crítica</i> o <i>Alta</i>).
Fórmula aplicada:	ANS-02 = (Fei – Fci) <i>(expresado en días hábiles)</i> <i>Donde,</i> Fei: <i>Fecha de envío a Aigües de Barcelona del Informe de Incidencia Significativa.</i> Fci: <i>Fecha de la comunicación de la incidencia.</i>
Cálculo de la Penalización acumulada P2:	Por cada incumplimiento se añade un 2% al índice de penalización acumulado.



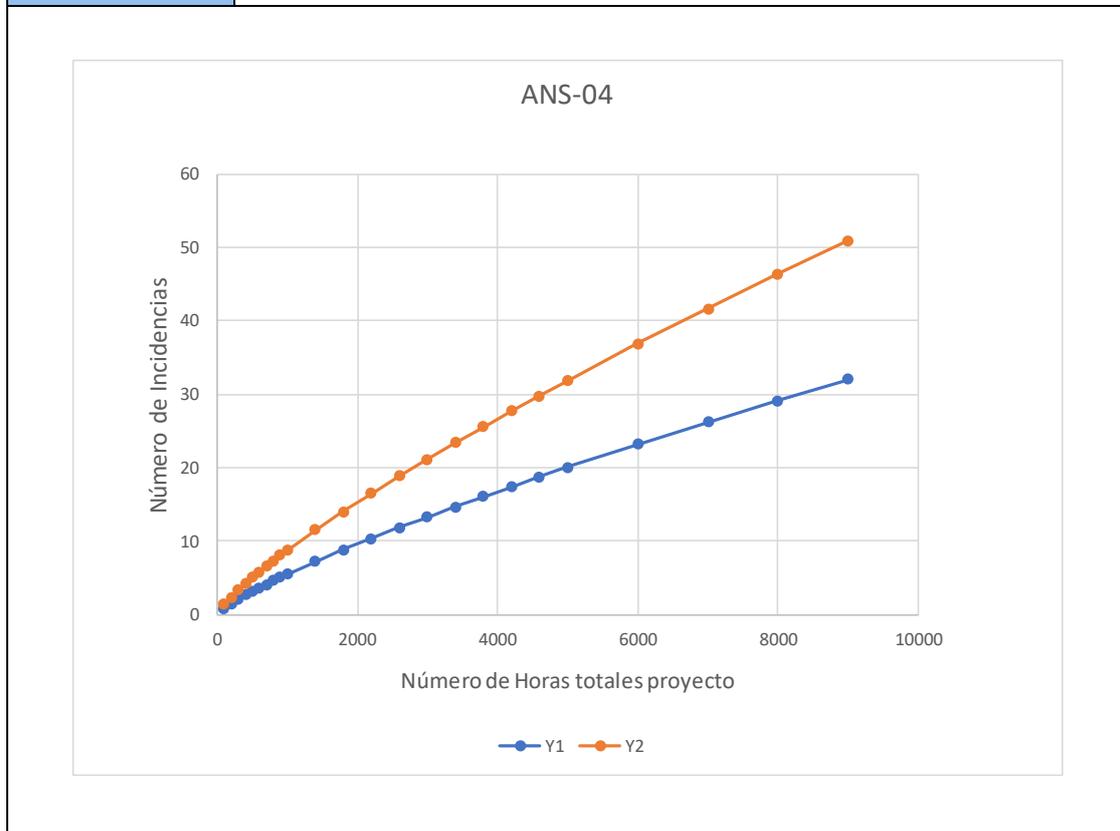
- **ANS-03 (Retraso en la fecha de finalización del proyecto):** Desviación en el número de días, respecto al plazo máximo de finalización del proyecto acordado.

Indicador:	Retraso en la fecha de finalización del proyecto (ANS-03).		
Cumplimiento:	Si ANS-03 ≥ 0 \rightarrow Sin efecto. Si ANS-03 < 0 \rightarrow Incumplimiento (<i>excepto cuando sea por causas no imputables al Prestador del Servicio</i>).		
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:	<p style="text-align: center;">ANS-03 = (Ndpe - Ndre) (<i>expresado en días naturales</i>)</p> <p><i>Donde,</i></p> <p>Ndpe: <i>Número de días previstos para la ejecución del proyecto.</i></p> <p>Ndre: <i>Número de días reales empleados para la ejecución del proyecto.</i></p>		
Cálculo de la Penalización P3:	Si $0% < (\text{ANS-03}/\text{Ndpe}) \leq 8\%$ se añade un 2% al índice de penalización acumulado.	Si $8% < (\text{ANS-03}/\text{Ndpe}) \leq 15\%$ se añade un 4% al índice de penalización acumulado.	Si $(\text{ANS-03}/\text{Ndpe}) > 15\%$ 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.

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: <i>Número de horas ofertadas para el proyecto concreto por el Proveedor del Servicio que resulte adjudicatario del mismo.</i>
Periodicidad de cálculo:	A la finalización del período de garantía.
Fórmula aplicada:	ANS-04 = <i>Número de incidencias generadas durante el período de garantía</i>
Cálculo de la Penalización P4:	Siendo, $Y2 = 0.03 * (Nho)^{0.8}$, se consideran los siguientes niveles de penalización: <ul style="list-style-type: none"> ▪ Si Y1 < ANS-04 ≤ Y2, se añade un 3% al índice de penalización acumulado. ▪ Si ANS-04 > Y2, se añade un 6% al índice de penalización acumulado.



- **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.

Indicador:	Calidad del desarrollo entregado II (ANS-05).
Cumplimiento:	<p>Para Nho ≤ 2.000 horas:</p> <ul style="list-style-type: none"> ▪ Si ANS-05 ≤ 1 → Sin efecto. ▪ Si ANS-05 ≥ 2 → Incumplimiento. <p>Para Nho > 2.000 horas:</p> <ul style="list-style-type: none"> ▪ 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. <p>Donde,</p> <p>Nho: Número de horas ofertadas para el proyecto concreto por el Proveedor del Servicio que resulte adjudicatario del mismo.</p> <p>T: Tiempo de solución real de la incidencia (Crítica o Alta).</p> <p>TS: Tiempo máximo de solución de la incidencia Crítica o Alta, según los criterios establecidos en la cláusula 6.1 del PPT.</p>
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:	<p>Si se genera un incumplimiento del ANS-05, se consideran los siguientes niveles de penalización:</p> <ul style="list-style-type: none"> ▪ 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 con 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% 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	<p>Por cada incumplimiento del ANS-01, se añade un 2% al índice de penalización acumulado.</p> <p>Por tanto: $P1 = (\sum_{i=1}^n 2) \%$, donde n es el número de incumplimientos del ANS-01.</p>
P2	<p>Por cada incumplimiento del ANS-02, se añade un 2% al índice de penalización acumulado.</p> <p>Por tanto: $P2 = (\sum_{i=1}^n 2) \%$, donde n es el número de incumplimientos del ANS-02.</p>
P3	<p>Por incumplimiento del ANS-03, se añaden los siguientes porcentajes de penalización, según cada caso:</p> <ul style="list-style-type: none"> ▪ P3.1: Si $[0\% < (\text{ANS-03}/\text{Ndpe}) \leq 8\%]$, se añade un 2% al índice de penalización acumulado. ▪ P3.1: Si $[8\% < (\text{ANS-03}/\text{Ndpe}) \leq 15\%]$, se añade un 4% al índice de penalización acumulado. ▪ P3.1: Si $[(\text{ANS-03}/\text{Ndpe}) > 15\%]$, se añade un 8% al índice de penalización acumulado.
P4	<p>Por incumplimiento del ANS-04, se añaden los siguientes porcentajes de penalización, según cada caso:</p> <ul style="list-style-type: none"> ▪ P4.1: Si $[Y1 < \text{ANS-04} \leq Y2]$, se añade un 3% al índice de penalización acumulado. ▪ P4.2: Si $[\text{ANS-04} > Y2]$, se añade un 6% al índice de penalización acumulado.
P5	<p>Por incumplimiento del ANS-05, se añaden los siguientes porcentajes de penalización, según cada caso:</p> <ul style="list-style-type: none"> ▪ 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.

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%.

En el caso de que un Prestador del Servicio, en tres proyectos que se le hayan encargado, alcance un **PT** igual o superior al 15%, 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. Garantía

El periodo mínimo que tendrán que tener como garantía los desarrollos y servicios entregados (proyectos) será de TRES (3) meses, a contar desde la puesta en producción y activación de los mismos (entrega de la Ficha de cierre de Proyecto).

No obstante lo anterior, tal como se indica en la cláusula 11 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.

6.5. Gestión y Coordinación

Se indican a continuación unos requerimientos mínimos de seguimiento y control que deberán cumplir los Prestadores del Servicio:

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: Responsable del Servicio y equipos asignados a cada proyecto (Jefe/Gestor de proyecto; Analista de sistemas; Programador/Analista programador).

A nivel de Acuerdo Marco:

▪ ***Responsable del Servicio*** (1 para todo el Acuerdo Marco)

Es la persona que tendrá la visión completa del Acuerdo Marco y será el principal interlocutor con Aigües de Barcelona. 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 y de los ANS específicos.
- Garantizar la rápida resolución y priorización de las incidencias graves.
- Asegurar el cumplimiento de la Planificación general y de los compromisos de contrato en los diferentes proyectos.
- Garantizar la correcta gestión y respuesta a las solicitudes de oferta.
- Generar un informe de seguimiento del servicio en global (uno cada seis meses).
- Decidir o gestionar la decisión por parte del Prestador del Servicio 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 que puedan surgir.



- Controlar que la facturación se está realizando conforme a los acuerdos y resolver cualquier problema relacionado con el precio o los pagos.

El Responsable del Servicio deberá tener un interlocutor por parte de Aigües de Barcelona con quien mantendrá la comunicación, interlocución y resolución de problemas.

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 después de 3 días laborables tras una petición de cualquiera de las partes.

A nivel de Proyecto:

En lo que se refiere a los equipos asignados por el Prestador del Servicio a cada uno de los desarrollos específicos (proyectos), éstos estarán constituidos por los siguientes perfiles profesionales, los cuales tendrán los roles y responsabilidades básicas que se indican a continuación:

- ***Jefe de proyecto/Gestor de proyecto***

Es la persona que tendrá la visión completa del desarrollo a ejecutar (proyecto) y será el principal interlocutor con Aigües de Barcelona en lo concerniente a dicho proyecto. Entre sus funciones destacan las siguientes:

- Llevar a cabo el seguimiento de los hitos y avance del proyecto.
- Asegurar la calidad y cumplimiento con los objetivos del proyecto, plazos establecidos, entregas y ANSs.
- Validar, finalizar y hacer llegar a Aigües de Barcelona los entregables según planificación.
- Identificar posibles riesgos e implementar acciones mitigadoras.
- Asegurar la correcta atención de las incidencias detectadas, según la prioridad asignada a cada una.
- Gestionar la rápida resolución y priorización de las incidencias graves (tipificadas como Críticas o Altas).
- Coordinar el equipo del proyecto asignado al proyecto por el Prestador del Servicio.
- Supervisar que el personal integrante del equipo de trabajo desarrolla correctamente las funciones que tiene encargadas.
- Coordinar con Aigües de Barcelona las actividades en las que existe relación entre ambos, para la correcta consecución del proyecto.
- Participar en las reuniones de inicio, seguimiento y cierre del proyecto, que requiera Aigües de Barcelona, así como elaborar las actas de reunión correspondientes.
- Informar al Responsable de Proyecto de Aigües de Barcelona de cualquier circunstancia que pudiera afectar al desarrollo correcto del proyecto (retrasos en la planificación, estado en el cierre de las incidencias, nivel de avance, etc.).
- Actuar como interlocutor principal para la gestión de las modificaciones al alcance del proyecto que puedan surgir.
- Elaborar la Ficha de Cierre de Proyecto.
- Apoyar al Responsable del Servicio en su función de informar a Aigües de Barcelona sobre la marcha del servicio.

Los Jefes/Gestores de cada proyecto deberán tener su correspondiente interlocutor por parte de Aigües de Barcelona con el cual mantendrán la comunicación, interlocución y resolución de problemas. En este sentido, por cada proyecto a desarrollar, Aigües de Barcelona fijará un Responsable de Proyecto que actuará como interlocutor principal con el Jefe/Gestor de proyecto designado por el Prestador del Servicio.

▪ ***Analista de sistemas información:***

- Velar por la correcta implantación de los cambios efectuados en las aplicaciones.
- Traspasar el requerimiento funcional a los equipos técnicos de las diferentes aplicaciones afectadas, velando por la integridad y coherencia en todos los sistemas.
- Elaborar los documentos de diseño técnico y funcional de la aplicación.
- Planificar y ejecutar el Plan de pruebas.
- Supervisar y dar soporte a las pruebas de aceptación.
- Dar soporte en la generación de la Ficha de Cierre de Proyecto, así como en la elaboración del resto de documentación a presentar.
- Trasferir el conocimiento para el traspaso del proyecto al Servicio de Mantenimiento.

▪ ***Programador/Analista programador:***

- Implementar el código a partir del diseño técnico.
- Definir y ejecutar el plan de pruebas unitario de los cambios realizados.
- Dar soporte a la ejecución del Plan de pruebas.
- Dar soporte a las pruebas de aceptación.

En el caso de aplicar una metodología Agile al proyecto, el reparto de roles y responsabilidades se hará en base a los criterios y funciones establecidos en la propia metodología Agile.

En cualquier caso, los equipos de trabajo deberán contar con las competencias y habilidades necesarias para desarrollar con garantías las actividades definidas y que permitan ofrecer una correcta prestación del servicio demandado:

- Destreza comunicativa e interpersonal.
- Capacidad de detectar y resolver problemas.
- Alta capacidad de organización y control de la información.
- Personas activas y con iniciativa, para la mejora de los servicios.
- Orientación al trabajo en equipo.

6.6. Recursos Materiales requeridos

Los Prestadores de los Servicios serán responsables de disponer del equipo de trabajo, así como de todo el equipamiento hardware, software, y demás especificaciones fijadas en el presente Pliego, que sea necesario para la ejecución del servicio contratado, sin que en ningún caso puedan facturarse la compra, el suministro o bien la instalación de equipos y recambios que sean necesarios para realizar el servicio objeto de este Acuerdo Marco.

No obstante lo anterior, Aigües de Barcelona proporcionará a los Prestadores de los Servicios las siguientes herramientas:

- Herramienta Acceso a BB.DD del Mainframe;
- WebSphere y Visualage, para la generación de commareas entre Java y Mainframe (CICS);
- Entorno de desarrollo de Siebel;
- Herramientas de reporting y seguimiento de las incidencias detectadas: en la actualidad el JIRA y el BMC Remedy.

6.7. Especificaciones de RGPD y SEGURIDAD

Los desarrollos (proyectos) realizados y entregados deberán cumplir con el Reglamento (UE) 2016/679, General de Protección de Datos ("RGPD") y, en especial, con lo establecido en las cláusulas 14 y 22 del Pliego de Condiciones Particulares (PCP), así como en la cláusula 15 del Acuerdo Marco. Las empresas adjudicatarias tendrán que identificar todos aquellos puntos que puedan vulnerar el RGPD, resolverlos y presentar las evidencias conforme cumplen con el mismo.

Por otra parte, los sistemas a desarrollar han de estar exentos de vulnerabilidades, según aplique el Top 10 de OWASP Security Mobile y/o OWASP Top Security Web (<https://www.owasp.org>). En este sentido, se han de presentar las evidencias de las pruebas realizadas y se realizará una auditoría de seguridad por parte de Aigües de Barcelona. En el caso de presentar disconformidades, será la empresa adjudicataria la responsable de solucionarlas como parte del servicio prestado.

En todo caso, durante la ejecución del Acuerdo Marco se deberán observar por parte de los adjudicatarios las medidas de seguridad que constan en el Anexo N° 9 del citado PCP, según lo previsto en la cláusula 14 del mismo.

Aigües de Barcelona conviene llevar a cabo un seguimiento y control del cumplimiento de la normativa en materia de protección de datos y de las medidas de seguridad detalladas en el Anexo N° 5.2 del PCP, el cual consistirá en las siguientes actuaciones:

- Semestralmente, a contar desde el inicio de la vigencia del presente Contrato, el adjudicatario deberá remitir por escrito a Aigües de Barcelona un Informe actualizado y detallado del cumplimiento de cada una de las medidas de seguridad anteriormente indicadas.
- Por otro lado, Aigües de Barcelona se reserva el derecho, en cualquier momento, de realizar cuantas auditorías que considere pertinentes a efectos de verificar el grado de cumplimiento indicado en el Informe referenciado en el apartado anterior.

7. SOLICITUD DE OFERTAS

El proceso de solicitud y selección de oferta se establece en la cláusula 17.4 del PCP.

ANEXO Nº 1 - CALIFICACIÓN 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)	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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.

Por otra parte, se ha de tener en cuenta que las aplicaciones SICAB, SISTEMÁTICOS, AVERIAS y SIEBL-CRM están tipificadas como Procesos Críticos de Negocio.



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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	Valor		Urgencia			
		Ponderación	Crítica	Alta	Media	Baja
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.

En lo que se refiere a los tiempos máximos de solución (TS), éstos se establecen para cada tipología de incidencia según el cuadro siguiente:

Prioridad de la incidencia	Tiempo máximo de solución (TS) <i>(horas desde la comunicación de la incidencia)</i>
Crítica	12 h
Alta	24 h
Media	110 h
Baja	240 h

ANEXO Nº 2 - NORMAS DE SEGURIDAD IT DE AIGÜES DE BARCELONA

ÍNDICE

- 1. Objeto e introducción del documento***
- 2. Intercambio de información y software SI-N-07-02/01***
- 3. Configuración y administración segura***
 - 3.1 Configuración segura***
 - 3.2 Administración segura***
- 4. Identificación y autenticación de usuarios***
- 5. Identificación de usuario***
- 6. Gestión de contraseñas y credenciales de clientes***
- 7. Comunicación de los incidentes de seguridad***

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, autenticación 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 calificados 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 autenticación 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 autenticación 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 autenticación 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 autenticación 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 autenticación, 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 autenticación deberán ser supervisados por la Dirección de Seguridad TI, que verificará la correcta parametrización de la normativa de seguridad relativa a la autenticación 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 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 a 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 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 éste 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.