PLIEGO DE PRESCRIPCIONES TÉCNICAS
QUE DEBE REGIR EL CONTRATO PARA LA EJECUCIÓN DE ACTUACIONES RELATIVAS AL
MANTENIMIENTO DEL ENTORNO MICRO FOCUS Y LOS COMPONENTES SATÉLITE DE LA PLATAFORMA QUE SOPORTA LA APLICACIÓN COMERCIAL (SICAB) DE AIGÜES DE BARCELONA

Nº EXP.: AB/ABAST/2020/76

1. OBJETO 4
2. ALCANCE 4
2.1. Diseño del sistema 4
2.2. Volumetría 7
2.3. Objetivos del servicio 7
2.3.1. Micro Focus Enterprise Server 7
2.3.2. Micro Focus Enterprise Server + Developer en puestos de desarrollo 7
2.3.3. Control-M 8
2.3.4. VPSX 8
2.3.5. IBM QMF Analytics for Multiplatforms 9
2.3.6. OpenLDAP para Microfocus 9
2.3.7. Git y Jenkins 10
2.3.8. Soporte problemas 10
2.4. Gestión del servicio 10
2.5. Organización del servicio 11
2.5.1. Servicio de Operación. 12
2.5.1.1. Control de operación 12
2.5.1.2. Planificación de trabajos 13
2.5.1.3. Realización de pruebas en entorno de contingencia 13
2.5.2. Servicio de Administración 13
2.5.2.1. Gestión de planificación alto nivel 13
2.5.2.2. Soporte a cambios de aplicación 14
2.5.2.3. Gestión de incidencias 14
2.5.2.4. Gestión de informes automáticos del servicio 14
2.5.2.5. Administración del control de accesos al Sistema 14
2.5.2.6. Soporte Técnico Componentes 15
2.5.2.7. Git y Jenkins 15
2.6. Servicios no contemplados 16
3. CONDICIONES TECNICAS 16
3.1.1. Distribución geográfica 16
3.1.2. Protocolos y normativas 16
3.1.3. Sistema de monitorización y reacción a alertas 17
3.1.4. Gestión de accesos administrativos a los sistemas 17
3.1.5. Herramientas para la gestión del servicio 17
4. CONDICIONES OPERATIVAS 17
4.1.1. Horario de prestación del servicio 17

4.1.2. Canales de comunicación 18
4.1.3. Sistema de ticketing para la comunicación de incidencias y peticiones de servicio 18
4.1.4. Desarrollo de nuevas funcionalidades 18
4.1.5. Documentación 19
4.1.6. Facturación del servicio - Gestión Proactiva, Reactiva, Evolutiva, Administrativa 19
4.1.7. Facturación del servicio - Desarrollo de nuevas funcionalidades 19
4.1.8. Transición del servicio 20
4.1.9. Devolución del servicio 20
4.1.10. Terminación del servicio 21
5. OTROS REQUERIMIENTOS 21
5.1.1. Organización del servicio 21
5.1.2. Acuerdos de Nivel de Servicio (ANS) 22
5.1.3. Penalizaciones derivadas del incumplimiento con los ANS 23
5.1.4. Informes de servicio 29
5.1.4.1. Informe ejecutivo 29
5.1.4.2. Informe de seguimiento 30
5.1.4.3. Informe de SLA 30
5.1.5. Gestión y Coordinación de la ejecución 30
5.1.6. Procedimientos para la realización del Servicio 32
5.1.7. Idioma 32
5.1.8. Recursos Materiales requeridos 32
5.1.9. Acceso 32
6. Seguridad corporativa 32
Anexo 1 - Normas de seguridad IT d'Aigües de Barcelona 33
ANEXO Nº 1 - NORMAS DE SEGURIDAD IT DE AIGÜES DE BARCELONA 34

1. OBJETO

El presente Pliego de Prescripciones Técnicas (en adelante, PPT) establece las prescripciones técnicas que rigen el procedimiento de contratación del *"Mantenimiento del entorno Micro Focus y los componentes satélite de la plataforma que soporta la aplicación comercial (SICAB) de Aigües de Barcelona"*, promovido por **Aigües de Barcelona, Empresa Metropolitana de Gestió del Cicle Integral de l'Aigua, S.A.** (en adelante, "Aigües de Barcelona" o "AB"), así como la ejecución del mismo.

Los objetivos generales del proyecto son contratar la operación, administración y soporte de los productos que son objeto de trabajo en este proyecto.

2. ALCANCE

Se desea disponer de un servicio de gestión proactivo, reactivo, evolutivo, de operación y de administración en el ámbito del entorno Micro Focus que soporta la aplicación comercial de AB (SICAB), esto es:

- el entorno Micro Focus Enterprise Server en productivo, integración, desarrollo y contingencia,
- Micro Focus Enterprise Developer + Eclipse en entorno de desarrollo y puestos de usuario de desarrollo
- entorno Control-M, entorno VPSX, entorno LDAP en todos los servidores Micro Focus
- entorno IBM QMF Analytics for Multiplatforms
- Se deberá tener conocimiento sobre las personalizaciones que Microfocus requiere en la BD y deberá dar soporte sobre ello en parcheado y subidas de versión de la base de datos.

Se incluirá también el mantenimiento y mejora de los procedimientos y tareas de compilación bajo Microfocus y despliegue integrados en la plataforma Git de AB y Jenkins.

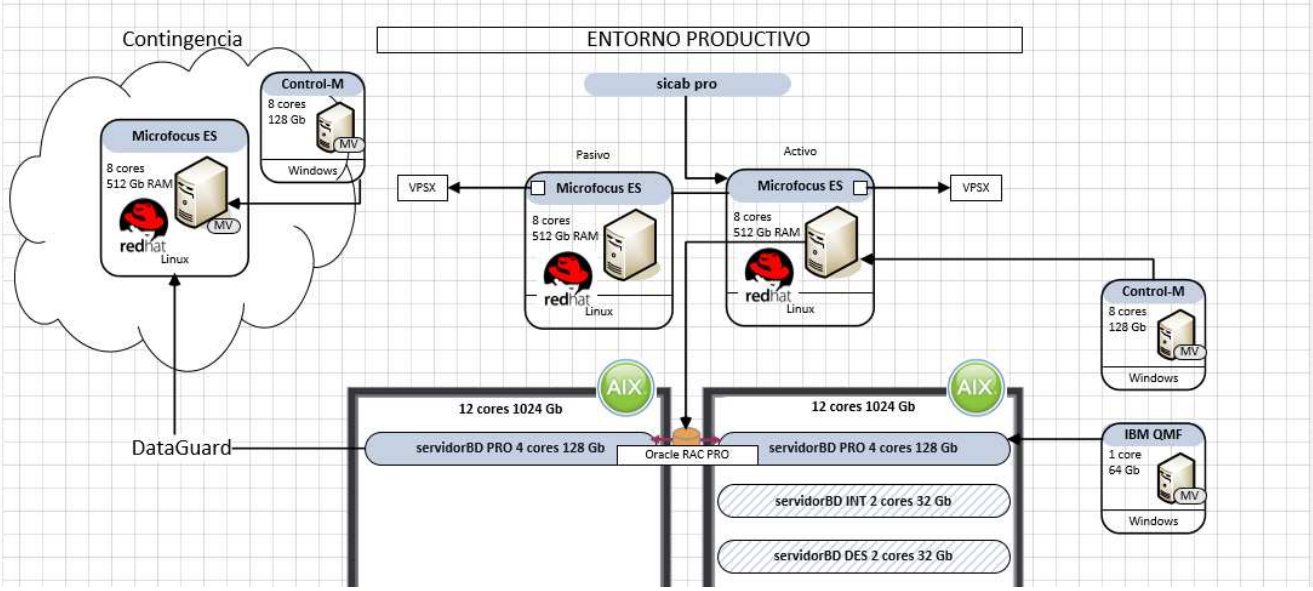
Los servicios prestados por el adjudicatario deberán asegurar el acceso, la disponibilidad y el óptimo grado de funcionamiento de la plataforma Micro Focus desde el punto de vista técnico, con los siguientes objetivos principales:

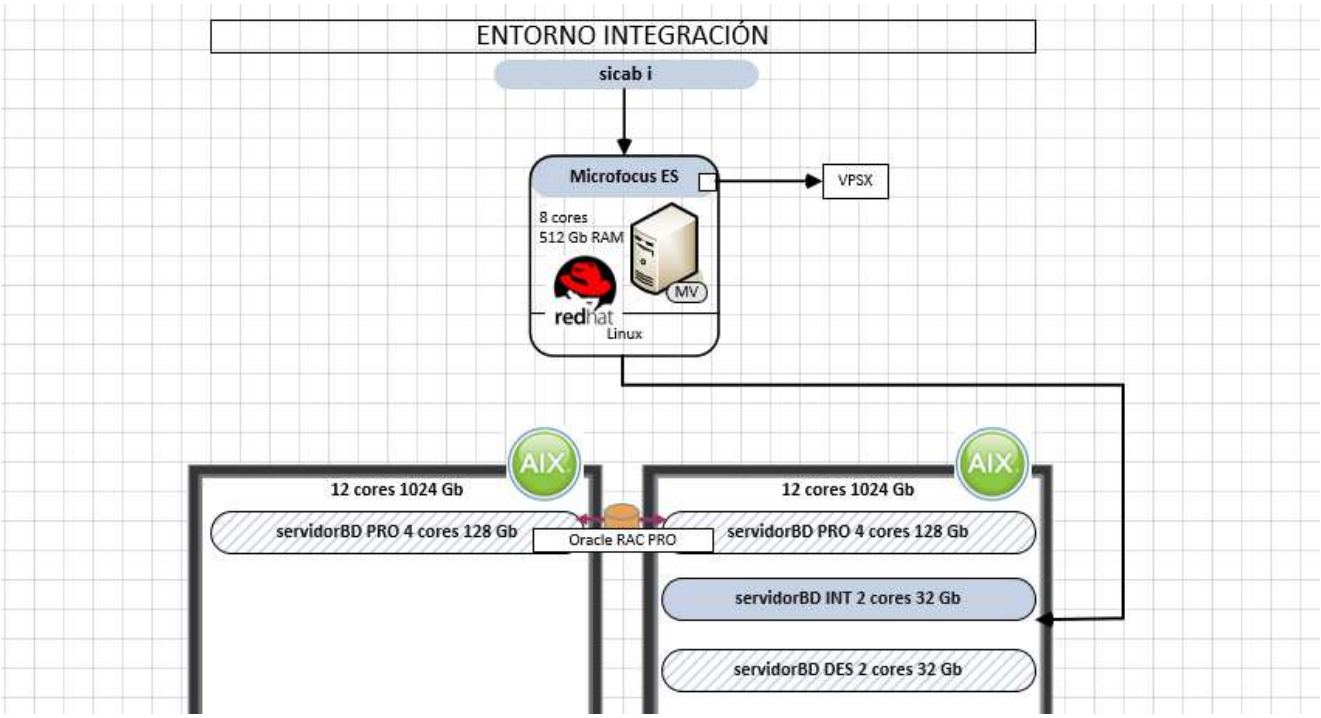
- Establecer una operativa de los servicios con garantías de eficiencia, transfiriendo la responsabilidad de las actividades de mantenimiento del servicio a la empresa adjudicataria.
- Establecer métodos y procedimientos que aporten a AB la información necesaria para controlar los servicios objeto del contrato.
- Maximizar el aporte de valor a las unidades que soportan sus procesos en dichas aplicaciones.

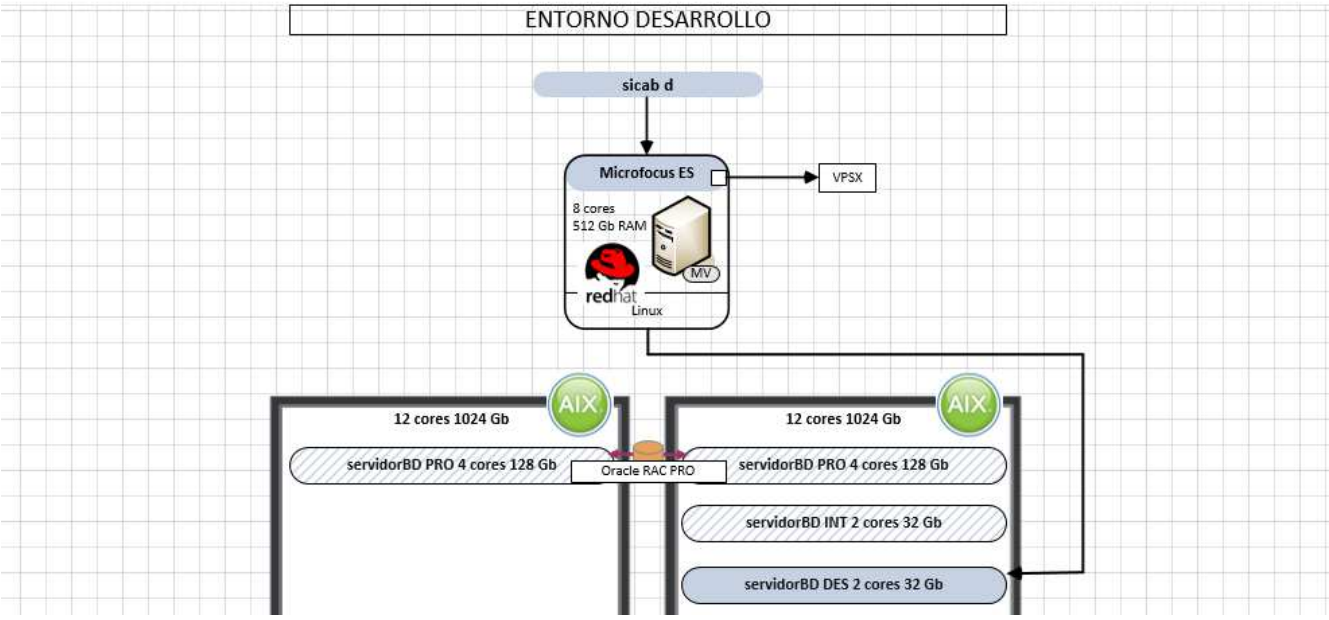
Dada la complejidad del entorno, el adjudicatario deberá disponer de recursos profesionales expertos en varias tecnologías de distinta naturaleza, que se detallarán en los siguientes apartados.

2.1. Diseño del sistema

El esquema hardware del entorno Micro Focus SICAB es el siguiente:


Contingencia
ENTORNO PRODUCTIVO
sicab pro
Control-M
8 cores
128 Gb
MV
Windows
Microfocus ES
8 cores
512 Gb RAM
MV
redhat
Linux
Pasivo
Activo
VPSX
Microfocus ES
8 cores
512 Gb RAM
redhat
Linux
Microfocus ES
8 cores
512 Gb RAM
redhat
Linux
VPSX
Control-M
8 cores
128 Gb
MV
Windows
AIX
12 cores 1024 Gb
AIX
12 cores 1024 Gb
DataGuard
servidorBD PRO 4 cores 128 Gb
Oracle RAC PRO
servidorBD PRO 4 cores 128 Gb
IBM QMF
1 core
64 Gb
MV
Windows
servidorBD INT 2 cores 32 Gb
servidorBD DES 2 cores 32 Gb


ENTORNO INTEGRACIÓN
sicab i
Microfocus ES
8 cores
512 Gb RAM
MV
redhat
Linux
VPSX
AIX
12 cores 1024 Gb
AIX
12 cores 1024 Gb
servidorBD PRO 4 cores 128 Gb
Oracle RAC PRO
servidorBD PRO 4 cores 128 Gb
servidorBD INT 2 cores 32 Gb
servidorBD DES 2 cores 32 Gb



- **Entorno de Producción**: El entorno de producción consta de:
    - 2 servidores físicos Intel/Linux, para los servidores de aplicación **Micro Focus Enterprise Server**, donde también estarán alojados los servicios **VPSX** y **OpenLDAP** dedicado, con 1 procesador de 8 cores Intel y 512 GB de RAM para cada servidor,
    - 2 servidores virtuales Power8/AIX de base de datos **Oracle 19 (12.2.0.3)**, con 4 cores y 128GB de RAM cada uno.
    - 1 servidor virtual para **Control-M** y 1 servidor virtual para el **QMF**.
- **Entorno de integración**: El entorno de integración consta de:
    - 1 servidor virtual Intel/Linux para el servidor de aplicación **Micro Focus Enterprise Server**, donde también estarán alojados los servicios **VPSX** y **OpenLDAP** dedicado, con 2 cores y 256 GB de RAM,
    - 1 servidor virtual Power8/AIX de base de datos **Oracle 19**, con 2 cores y 32GB de RAM.
- **Entorno de desarrollo**: 1 entorno para desarrollo que consta de:
    - 1 servidor de aplicación Intel/Linux **Micro Focus Enterprise Server**, donde estarán alojados los servicios **VPSX** y **OpenLDAP** dedicado, en entorno virtual ESX con 2 cores y 256 GB de RAM y
    - 1 servidor virtual Power8/AIX de base de datos con 2 cores y 32GB de RAM. En estos servidores.
- **Entorno de contingencia**: Un entorno de contingencia en el CPD alternativo de producción, con 1 servidor virtual de aplicación en ESX con 1 procesador/8 cores y 512 GB de RAM y 1 servidor virtual Power8/AIX de base de datos Oracle con 4 cores y 128GB de RAM.

- **Entorno de base de datos clonada**: El entorno de clonado de producción consta de 1 servidor virtual Power8/AIX de base de datos **Oracle**, copia de base de datos, para consultas externas, con 2 cores y 32GB de RAM.

2.2. Volumetría

Se especifica una volumetría aproximada en el entorno de producción:

- Peticiones Simples: 50 mensuales
- Incidencias: 30 mensuales

En próximos apartados se distinguen entre las distintas peticiones e incidencias y se indican SLA's a cumplir.

2.3. Objetivos del servicio

El objetivo del servicio que se pretende contratar bajo condiciones de este pliego se corresponde con los servicios descritos a continuación.

2.3.1. Micro Focus Enterprise Server

- Administración del entorno **Micro Focus Enterprise Server** en los servidores de **producción**. Gestión proactiva 12x5 y reactiva en régimen 24x7 mediante el servicio de Operaciones y el de Administración, gestión evolutiva y administrativa en régimen 12x5 mediante el servicio de Administración.
- Administración del entorno **Micro Focus Enterprise Server** en los servidores de **integración, desarrollo y contingencia**. Gestión proactiva, reactiva, evolutiva y administrativa en régimen 12x5 mediante el servicio de Administración.

Servicio	Entorno	Tipo de servicio	Nivel servicio
Micro Focus Enterprise Server	PRO	Operación	12x5 + Guardia 24x7
		Administración	12x5 + Guardia 24x7
	INT	Administración	12x5
	DES	Administración	12x5
	CONT	Administración	12x5

2.3.2. Micro Focus Enterprise Server + Developer en puestos de desarrollo

- Administración del entorno **Micro Focus Enterprise Developer** en los puestos de desarrollo. Gestión proactiva, reactiva, evolutiva y administrativa en régimen 12x5 mediante el servicio de Administración.
  Se excluye la gestión del SO del puesto de usuario, el servicio incluye el despliegue de software sobre el puesto de usuario.

Servicio	Entorno	Tipo de servicio	Nivel servicio
Micro Focus Enterprise Developer + Eclipse	Puestos de desarrollo	Administración	12x5

2.3.3. Control-M

- Administración del entorno **Control-M y gestión de Operación/planificación BATCH y ONLINE en entorno productivo**. Gestión proactiva 12x5 y reactiva en régimen 24x7 mediante el servicio de Operaciones y el de Administración, gestión evolutiva y administrativa en régimen 12x5 mediante el servicio de Administración.

- Administración del entorno **Control-M para tareas del entorno integración**. Gestión proactiva y reactiva en régimen 12x5 mediante el servicio de Operaciones y el de Administración, gestión evolutiva y administrativa en régimen 12x5 mediante el servicio de Administración

- Administración del entorno **Control-M para tareas del resto de entornos incluido contingencia**. Gestión proactiva, reactiva, evolutiva y administrativa en régimen 12x5 mediante el servicio de Administración.

Servicio	Entorno	Tipo de servicio	Nivel servicio
Control-M	PRO	Operación	12x5 + Guardia 24x7
		Administración	12x5 + guardia 24x7
	INT	Operación	12x5
		Administración	12x5
	DES	Administración	12x5
	CONT	Administración	12x5

2.3.4. VPSX

- Administración del entorno **VPSX** en **producción**. Gestión proactiva 12x5 y reactiva en régimen 24x7 mediante el servicio de Operaciones y el de Administración, gestión evolutiva y administrativa en régimen 12x5 mediante el servicio de Administración.

- Administración del entorno **VPSX** en **resto entornos**. Gestión proactiva, reactiva, evolutiva y administrativa en régimen 12x5 mediante el servicio de Administración.

Servicio	Entorno	Tipo de servicio	Nivel servicio
VPSX	PRO	Operación	12x5 + Guardia 24x7
		Administración	12x5 + guardia 24x7
	INT	Administración	12x5
	DES	Administración	12x5
	CONT	Administración	12x5

2.3.5. IBM QMF Analytics for Multiplatforms

- Administración del entorno **IBM QMF Analytics for Multiplatforms**. Gestión proactiva, reactiva, evolutiva y administrativa en régimen 12x5 mediante el servicio de Administración.

Servicio	Entorno	Tipo de servicio	Nivel servicio
IBM QMF	PRO	Administración	12x5

2.3.6. OpenLDAP para Microfocus

- Administración de **OpenLDAP para Microfocus en el entorno de producción**. Gestión proactiva 12x5 y reactiva en régimen 24x7 mediante el servicio de Operaciones y el de Administración, gestión evolutiva y administrativa en régimen 12x5 mediante el servicio de Administración.
- Administración de **OpenLDAP para Microfocus en el resto de entornos**. Gestión proactiva, reactiva, evolutiva y administrativa en régimen 12x5 mediante el servicio de Administración.

Servicio	Entorno	Tipo de servicio	Nivel servicio
OpenLDAP para Microfocus	PRO	Operación	12x5 + Guardia 24x7
		Administración	12x5 + guardia 24x7
	INT	Administración	12x5
	DES	Administración	12x5
	CONT	Administración	12x5

2.3.7. Git y Jenkins

- Administración y mantenimiento de las tareas y procedimientos establecidos de compilación y despliegue de la aplicación SICAB usando **Git y Jenkins**. Gestión reactiva, administrativa en régimen 12x5 mediante el servicio de Administración.

Servicio	Entorno	Tipo de servicio	Nivel servicio
Gestion procedimientos Git y Jenkins	PRO	Administración	12x5

2.3.8. Soporte problemas

- Apertura de casos por **problemas en los productos** en régimen 24x7 mediante Operación o Administración del servicio apoyándose en los contratos de soporte y mantenimiento que AB tiene con los fabricantes de los productos.

2.4. Gestión del servicio

Entrando al detalle de las distintas gestiones que se realizarán sobre la plataforma Micro Focus, productos y componentes descritos en el apartado 2.3, podemos diferenciar:

- **Gestión proactiva,** en la que se incluye
  - Operación y explotación del entorno productivo y resto de entornos en 12x5 a través de procesos periódicos/automatizados o manuales.
  - Ejecución de procedimiento de pruebas y activación de contingencia para su comprobación periódica a través de documentación entregada por AB.
  - Establecimiento de protocolos y caminos de comunicación entre AB y los servicios de gestión de eventos
  - Escalado de incidencias de las aplicaciones a los proveedores de mantenimiento y garantía contratados por AB

- **Gestión reactiva**, en la que se incluye
  - Actuación en régimen 24x7 ante incidencias en los entornos productivos y en régimen de 12x5 en el resto de entornos y resolución de las mismas dentro del marco de los acuerdos de nivel de servicio (ANS) establecidos.
  - Gestión de eventos, detección de alertas y actuación en base a los procedimientos establecidos
  - Establecimiento de protocolos y caminos de comunicación entre AB y los servicios de gestión de eventos
  - Escalado de incidencias de las aplicaciones a los proveedores de mantenimiento y garantía contratados por AB

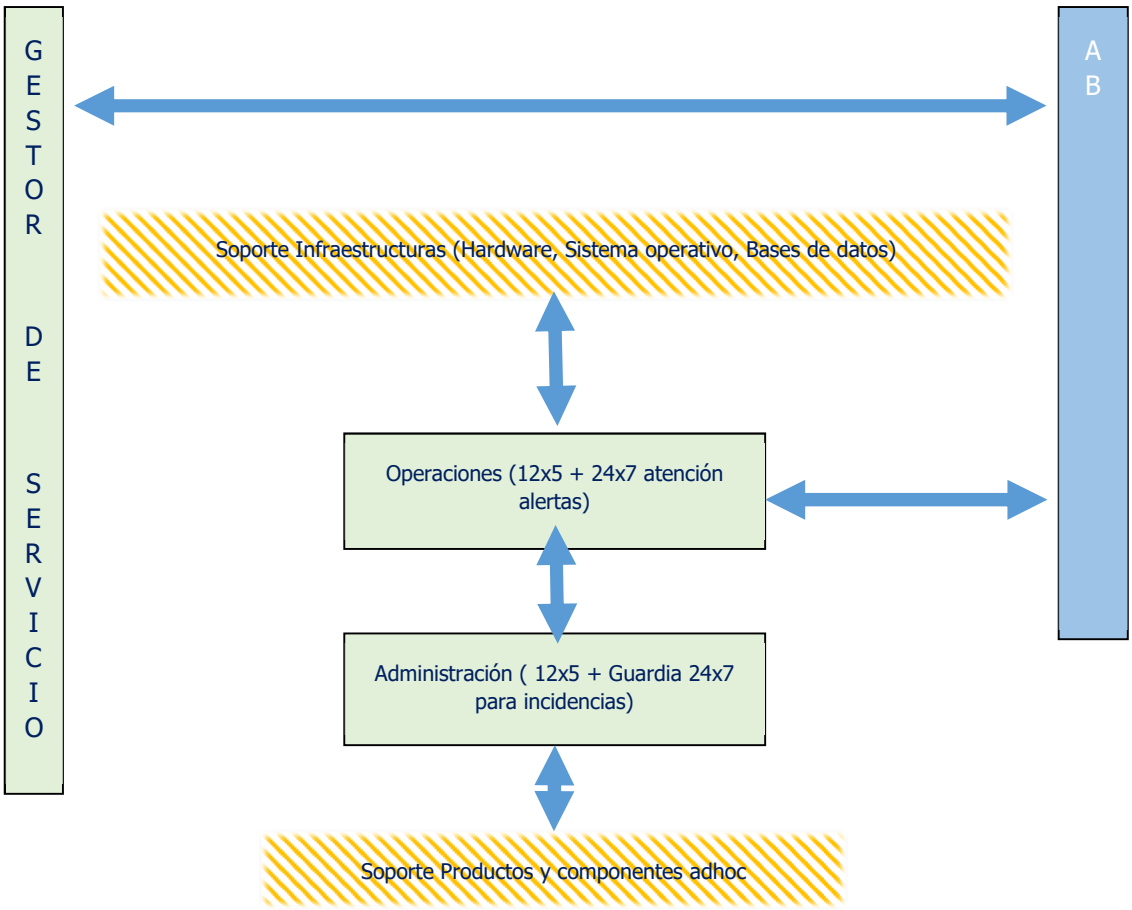
- **Gestión evolutiva**, en la que se incluye
  - aplicación de parches sobre los componentes especificados en el apartado 2.3,
  - propuestas de mejora dentro de los ANS establecidos
  - mantenimiento de documentación relativa al servicio.

- **Desarrollo de nuevas funcionalidades y mejoras** se incluirán dentro del servicio tarifas y horas de técnico, que AB utilizará para pedir al gestor del servicio tareas

evolutivas y de mantenimiento periódico a desarrollar. Así mismo el servicio se verá limitado por la estimación del número máximo de horas anuales especificada en el punto 4.1.7.

2.5. Organización del servicio

Para poder llevar a cabo la gestión optima del servicio, de manera ideal se deberían estructurar en varios niveles, para focalizar en cada uno de ellos las tareas adecuadas. Un esquema orientativo podría ser el siguiente:



Se proporcionarán como mínimo dos niveles de servicio.

1. **Operación** (12x5 + Guardia 24x7):

   - **Gestión proactiva y reactiva del entorno:** Corresponderá al servicio de operaciones, que se encargará de vigilar y operar el servicio (disparados por eventos, procedimientos o peticiones adhoc) y llegado el caso abrirá petición al nivel de administración en el caso de incidencia de producto u operación que requiera su implicación. Será el punto de entrada a los correos de AB para peticiones de administración y mejoras. También se podrá comunicar con el equipo de soporte infraestructuras y de soporte a componentes adhoc de Microfocus, si detectase algún problema a nivel de BBDD, SO, componentes, etc.

2. **Administración** (12x5 + Guardia 24x7):

    - **Gestión proactiva, reactiva, administrativa, evolutiva del entorno y nuevas funcionalidades:** Corresponderá al servicio de administración, atenderá incidencias sobre productos y/o de operación, atender a peticiones de mejoras sobre los procedimientos preestablecidos. Apertura, seguimiento, aplicación y cierre de incidencias a fabricantes de los productos y al fabricante de los componentes Microfocus generados adhoc para el entorno.

A modo de resumen, se detallan a continuación las acciones que llevaría a cabo cada nivel de servicio, sin que estas sean exhaustivas:

2.5.1. Servicio de Operación.

Explotación mediante la ejecución de procesos y tareas necesarias para la operación diaria de los equipos, las utilidades que las albergan y las aplicaciones "on-line" y "batch" del entorno Microfocus y Control-M, que serán recibidas por eventos de monitorización, planificación, etc.

Este objetivo se cumple en coordinación con el servicio de administración que proporcionan el soporte al servicio de operaciones. La operación es ejecutor de procedimientos preestablecidos pudiendo siempre sugerir cambios y mejoras en los mismos.

El primer nivel de soporte a los usuarios será proporcionado por el servicio de CAU de AB.

Algunos de los trabajos que realizará el equipo de operaciones serían:

- Control de operación,
- Planificación de trabajos entregados por otros departamentos,
- Realización de pruebas en entorno de contingencia

2.5.1.1. Control de operación

Como operación se entiende la supervisión del correcto funcionamiento de los entornos operativos sobre los que se debe garantizar la continuidad del servicio.

Actividades principales:

- Operación de los entornos y componentes especificados en el apartado 2.3, realizando el seguimiento de la disponibilidad de los mismos
- Atención a alertas de monitorización que indiquen una situación anómala con respecto a las tareas programadas (excluyendo las tareas programadas de técnica de sistemas), a las regiones Microfocus, al estado de las aplicaciones, y en general a todos los aspectos que tienen relación con los servicios expuestos en el apartado 2.3.
- Realizar las paradas y reinicializaciones de las aplicaciones y componentes especificados en el apartado 2.3 que sean necesarias.
- Gestión de diagnóstico y escalado de incidencias a nivel de administración.
- Documentación y cierre de las incidencias.
- Actuación frente a alertas recibidas relativas a la ejecución de los procesos batch planificados, resolución y escalado de incidencias correspondientes a dicho batch.
- Informes de las incidencias en el batch de producción planificado
- Participación en la gestión de cambios de software necesarios para el servicio mediante procedimientos documentados.

2.5.1.2. Planificación de trabajos

Consiste en la gestión y administración de la base de datos de Control-M para la planificación de los trabajos batch para la correcta puesta en funcionamiento de los diversos trabajos a realizar siguiendo un plan y un calendario acordado atendiendo a las necesidades de AB. Estos trabajos serán entregados por desarrollo o de sistemas.

También se contempla el mantenimiento de los calendarios, así como atender a instrucciones especiales propuestas por AB.

- Crear y mantener las reglas de dependencia entre procesos en la herramienta Control-M de Planificación.
- Generación plan diario y plan a largo plazo.

2.5.1.3. Realización de pruebas en entorno de contingencia

Control del entorno de contingencia mediante monitorización y escalado de incidencias al nivel necesario si se detectan problemas en la sincronización.

Sincronización de aplicación con refrescos periódicos cuando sea necesario.

Se deberá realizar pruebas de contingencia dentro de un plan de DRP en periodos preestablecidos que se definirán conjuntamente con AB mediante documentación preestablecida.

Se establece la periodicidad de las pruebas en 1 al año.

2.5.2. Servicio de Administración

Este servicio proporciona una gestión integral de los componentes especificados en el apartado 2.3 incluidos en la Plataforma Microfocus, incluyendo la configuración, los sistemas transaccionales y utilidades que conforman estos entornos en su ciclo de vida completo.

Así mismo, proporcionará la asistencia necesaria al equipo de operaciones, a los equipos responsables de las aplicaciones en el mantenimiento de las mismas:

Las tareas relativas al servicio de administración son:

- Gestión de planificación alto nivel
- Gestión de incidencias
- Soporte a cambios de aplicación
- Soporte a cambios de versión en base de datos, en lo relativo a las personalizaciones necesarias para el correcto funcionamiento de la plataforma Microfocus y los aplicativos asociados
- Gestión de informes automáticos del servicio
- Administración de control de accesos al sistema
- Soporte técnico a componentes

2.5.2.1. Gestión de planificación alto nivel

Consiste en la gestión de administración de la parte de Control-M que no realizará Operaciones.

- Administración de la herramienta de planificación Control-M con jobs house-keeping y de aplicativo mediante Jobs entregados por AB.
- Monitorización de los ciclos de planificación y resolución de conflictos en la programación de trabajos.
- Gestión de cambios en el batch de aplicativo planificado.

- Gestión de cambios en los horarios de Teleprocesos.
- Planificación de batch opcional de aplicativo.
- Mantenimiento de calendarios.
- Planificación de instrucciones especiales.

2.5.2.2. Soporte a cambios de aplicación

Función que incluye el soporte adicional si fuera necesario y bajo petición previa, a los traspasos a producción de altas o cambios de aplicación propuestos por desarrollo:

- Soporte a nuevas interfases con otros sistemas
- Alta de transacciones
- Revisión de JCL

2.5.2.3. Gestión de incidencias

Resolución de incidencias a cualquier nivel dentro de la responsabilidad del servicio, seguimiento, documentación y cierre de las incidencias para garantizar una correcta gestión de las mismas.

- Resolución de incidencias a primer nivel
- Resolución de incidencias a segundo nivel provocadas por sistemas
- Documentación de incidencias de acuerdo con los procedimientos en vigor

La resolución de incidencias, se regirán por los acuerdos de nivel de servicio establecidos en el presente pliego.

2.5.2.4. Gestión de informes automáticos del servicio

Realización, gestión y reporting de informes automatizados referentes al estado del servicio, en todos los entornos, como puede ser, rendimientos, consumos, tiempos de procesos batch, etc. Siempre desde herramientas propias de AB que elaboran dicha información.

Los informes pueden ser:

- Ticketing (volumen de incidencias, peticiones, cambios mensuales, tiempos de resolución, ANS, reportes de escalados etc.)
- Rendimiento, tiempo de respuesta de transacciones
- Informes de auditoría de seguridad de los productos

2.5.2.5. Administración del control de accesos al Sistema

La función consiste en gestionar las políticas y procedimientos de seguridad de un modo eficiente, garantizando en todo momento el adecuado acceso de los distintos usuarios a los distintos sistemas, aplicaciones, etc. que conforman el entorno Micro Focus a través de los LDAP's instalados en cada uno de los entornos.

- Alta/Baja/Modificación de entradas de LDAP (usuarios y permisos) mediante peticiones de servicio
- Definición y mantenimiento de usuarios de AB, del adjudicatario y de terceros que ocasionalmente deban acceder al sistema Microfocus.
- Informe de usuarios que no acceden al sistema en los últimos tres meses para su valoración (eliminación)
- Revisar informes de auditoria de Microfocus para la toma de medidas/acciones

- Administrar los accesos a las aplicaciones. AB tendrá la única autoridad para aprobar las peticiones y requerimientos de acceso y notificará al adjudicatario de las entidades y personal con derechos de acceso y la composición de los mismos.
- Realizar todas las tareas requeridas por las auditorías externas e internas de AB o el cumplimiento de los requerimientos y requisitos legales.
- Definición y mantenimiento de usuarios de AB, del adjudicatario y de terceros que ocasionalmente deban acceder al sistema Micro Focus.
- Capturar y almacenar los datos pertinentes a los registros de actividades que permitan su auditoria posterior por parte de AB o Terceras Partes autorizadas.
- Revisar las actividades que hayan involucrado un proceso de excepciones, un número de intentos elevado o un número de recursos extraordinarios (pe., Transferencia de datos), especialmente en aquel os sistemas críticos.
- Establecer los mecanismos de información a AB en caso de incidencias y violaciones de la seguridad e iniciar las acciones correctivas para minimizar y prevenir futuras incidencias.

2.5.2.6. Soporte Técnico Componentes

El servicio de Soporte a los componentes especificados en el apartado 2.3 consiste en el mantenimiento, configuración, y optimización siempre que sea posible, para una mejora del rendimiento de los mismos.

Así mismo incluye la resolución de problemas de segundo nivel, como tareas que han de efectuarse a dichos productos para su correcta gestión.

- Mantenimiento preventivo y correctivo cuando se requiera del software base necesario para dar el servicio e incluido en la descripción técnica de este pliego.
- Instalación, parametrización y puesta en producción de nuevas versiones del software base contratado tanto en el entorno de Desarrollo como de Producción incluido en la descripción técnica de este pliego.
- Gestión del rendimiento de los componentes especificados en el apartado 2.3
- Resolución de problemas de segundo nivel en el software base contratado incluyendo la recepción e instalación de las correcciones a que hubiera lugar
- Soporte técnico para el análisis de problemas y consultas en la explotación de procesos de AB,
- Asignación de recursos CICS (terminales, programas, transacciones, etc...) del sistema y de las aplicaciones del cliente
- Mantenimiento interfaces de comunicación entre CICS y otros entornos incluidos en el contrato

2.5.2.7. Git y Jenkins

Dentro de la gestión proactiva y reactiva de administración, se deberán mantener los mecanismos necesarios para la compilación de código integrado en la plataforma Git de AB del aplicativo SICAB y el despliegue entre los entornos mediante Jenkins del servicio Micro Focus, es decir, programas o cualquier código relativo a SICAB.

2.6. Servicios no contemplados

Para clarificar el ámbito de actuación del nuevo Prestador del Servicio se indica que no forma parte del alcance de esta licitación, bien porque se gestione con un contrato marco diferente o bien porque la gestión sea responsabilidad de AB:

- Gestión y mantenimiento de las bases de datos
- Gestión y mantenimiento del sistema operativo
- Gestion y mantenimiento de sistemas de virtualización
- Gestión del sistema operativo del puesto de usuario
- La selección y adquisición tecnológica (infraestructura, proveedores de servicios, aplicaciones, licencias, herramientas). El nuevo Prestador del Servicio podrá realizar recomendaciones tecnológicas pero la decisión sobre la conveniencia y uso de las mismas será responsabilidad única de AB sin perjuicio de que para la gestión del servicio el Prestador del Servicio organice como considere y utilice los medios que considere más apropiados.
- La gestión y operación de los CPD y salas técnicas actualmente gestionadas por otro proveedor de servicios.
- La gestión y operación de las comunicaciones.
- Las directrices de seguridad asociadas a los servicios siguen una política corporativa. El Prestador del Servicio velará por que el servicio es responsable cumpla las políticas de seguridad corporativas operándose y adecuándolo la configuración sobre estas premisas.
- La gestión y operación de los sistemas de almacenamiento dedicado y proporcionado por otro proveedor de servicio.

En todo caso el Prestador del Servicio se coordinará con los proveedores de estos y otros servicios cuando sea necesario para la correcta prestación del servicio y para garantizar que la operación se realiza dentro del marco normativo determinado por AB.

3. CONDICIONES TECNICAS

3.1.1. Distribución geográfica

El servicio se prestará en remoto desde la ubicación física que el gestor del servicio considere más conveniente y siempre que las instalaciones contengan las medidas de seguridad del puesto de trabajo adecuadas y los medios necesarios para llevar a cabo las tareas propias del servicio. El gestor del servicio es el responsable en última instancia de velar por el cumplimiento de las condiciones de prestación.

Aunque la gestión del servicio sea principalmente remota, se podrá solicitar la presencia en las oficinas de AB. El gestor de servicio deberá especificar el lugar desde los que prestará el servicio. En caso de producirse cambios durante la vigencia del contrato, estos deberán ser comunicados a AB para su aprobación.

A modo informativo, todos los servidores están ubicados en el área metropolitana de Barcelona a excepción del servidor de contingencia que se encuentra en Madrid.

3.1.2. Protocolos y normativas

Todos los trabajos desarrollados por los técnicos del servicio deberán estar alineadas con las normas y protocolos existentes en materia de seguridad, prevención de riesgos laborales, sistemas y cualquier otro departamento que tenga responsabilidad sobre los sistemas.

3.1.3. Sistema de monitorización y reacción a alertas

El sistema de monitorización actual de AB está basado en Nagios y Grafana.

El prestador del servicio usará la tecnología actual o un sistema de monitorización propio, siempre que las alertas se reciban también en el actual de AB, con las alertas integradas necesarias y será el utilizado por sus operadores y técnicos para la gestión proactiva y reactiva de los sistemas, con lo que los técnicos de AB tendrán una visión directa e integrada en el sistema corporativo.

3.1.4. Gestión de accesos administrativos a los sistemas

Las credenciales que darán acceso administrativo a los sistemas gestionados por el Prestador del Servicio se almacenarán exclusivamente en el almacén de credenciales de AB, implementado con la herramienta Cyberark.

El Prestador del Servicio se compromete a no mantener almacenes alternativos ni siquiera con carácter temporal.

Dispondrán de credenciales administrativas tanto los técnicos escogidos por el Prestador del Servicio como los técnicos propios de AB. Cada técnico dispondrá de los privilegios administrativos que sean necesarios para desarrollar las tareas que le correspondan por su perfil.

AB se reserva el derecho de auditar la actividad administrativa realizada en los sistemas de AB gestionados por el Prestador del Servicio incluyendo incluso la grabación completa de sesiones.

3.1.5. Herramientas para la gestión del servicio

AB proporcionará al Prestador del Servicio un acceso VPN utilizable desde Internet y/o línea privada de comunicaciones que lo conectará con todo el equipamiento gestionado, con los privilegios y accesos necesarios para desarrollar perfectamente las tareas.

Quedará a cargo del Prestador del Servicio cualquier licenciamiento y/o derecho de uso de herramientas de gestión, administración y acceso remoto que no estén incluidas en los productos y equipamientos administrados.

También permanecerá a cargo del Prestador del Servicio cualquier coste de adquisición y mantenimiento de hardware y software necesario para el equipamiento y programas necesarios por los técnicos y operadores, tanto remotamente como presencial, que no esten especificados en el apartado 2.3.

No obstante lo anterior, AB proporcionará al Prestador del Servicio:

- Usuarios locales o de dominio con los permisos necesarios
- Herramientas de reporting y seguimiento de las incidencias detectadas: en la actualidad BMC Remedy.

4. CONDICIONES OPERATIVAS

4.1.1. Horario de prestación del servicio

El servicio prestado por el Prestador del Servicio tendrá una cobertura horaria 24x7 para todos los días del año, con la excepción de las ventanas de mantenimiento que se acordarán entre AB y el adjudicatario.

Dentro del servicio los entornos gestionados se dividirán en los siguientes horarios:

- 24x7 → 24 horas, 7 días por semana. Fines de semana y festivos incluidos, sean nacionales o autonómicos. El servicio de operación se considera 24x7, excepto la gestión de cambios que se considerará 12x5.
- 12x5 → 12 horas (de 8:00 a 20:00), de lunes a viernes. Festivos excluidos, tanto los nacionales como los autonómicos. El servicio de administración se considerará 12x5, a excepción del servicio de guardia que se considerará 24x7.

4.1.2. Canales de comunicación

Las incidencias y peticiones generadas por el personal de AB podrán llegar al Prestador del Servicio por diferentes canales, como mínimo los siguientes:

- Herramienta de ticketing proporcionada por AB
- Teléfono. El Prestador del Servicio proporcionará uno o varios números de teléfono mediante los que contactar.
- Buzón de correo electrónico. Se pondrá a disposición de AB un buzón único para la comunicación relacionada con los tickets del servicio.

Al menos uno de los canales de comunicación deberá estar disponible y supervisado en horario 24x7, preferiblemente el canal telefónico. El objetivo de este canal o canales fuera del horario laboral habitual del Prestador del Servicio será permitir la gestión y solución de tickets que por su criticidad requieran este nivel de atención.

4.1.3. Sistema de ticketing para la comunicación de incidencias y peticiones de servicio

La herramienta mediante la que se realizará la comunicación de incidencias y peticiones de servicio será la utilizada en AB, actualmente BMC Remedy. AB proporcionará el acceso, licenciamiento y usuarios necesarios.

Dentro del sistema de ticketing quedará registrada toda la actividad realizada por los técnicos en respuesta a peticiones e incidencias comunicadas por el personal de AB.

Se utilizarán las funcionalidades de seguimiento de compromisos de nivel de servicio de la herramienta de ticketing para calcular el nivel de cumplimiento de los acuerdos de nivel de servicio establecidos entre AB y el Prestador del Servicio.

4.1.4. Desarrollo de nuevas funcionalidades

El servicio incluirá un sistema tarifario y de facturación para el desarrollo de nuevas funcionalidades de la plataforma y procesos periódicos de mantenimiento que no se facturará por adelantado, sino que requerirá de un presupuesto aprobado y sus trabajos realizados.

En el punto 4.1.7 se describe en detalle el funcionamiento del sistema de facturación para este servicio.

El consumo de horas se realizará mediante estos caminos:

- *Peticiones comunicadas mediante ticket y consideradas "no simples":* peticiones que quedan fuera del servicio porque la valoración de esfuerzo realizada por los técnicos del Prestador del Servicio supera las 2 horas de trabajo. Se requerirá siempre la aceptación de los responsables de AB para asignar el consumo contra las horas de este servicio.
- *Peticiones de proyecto*: peticiones generadas con un documento de requerimientos con el que el Prestador del Servicio ha generado un presupuesto y que los responsables de AB han decidido aceptar a cargo de las horas de este servicio. Cada presupuesto incluirá

al menos una descripción de los trabajos a realizar, compromisos de metas intermedias y fecha de finalización a partir de la fecha de aceptación del presupuesto y un detalle de horas a consumir por cada perfil técnico implicado.

4.1.5. Documentación

El Prestador del Servicio se compromete a mantener documentación actualizada sobre las aplicaciones que estén bajo su responsabilidad.

Esta documentación deberá quedar almacenada y formateada siguiendo las normas y procedimientos indicados por los responsables de AB.

Además de la documentación técnica, funcional y de mantenimiento del servicio, como parte de este el Prestador del Servicio también mantendrá actualizadas las herramientas de monitorización, registrando los equipos monitorizados y los elementos controlados por cada equipo.

4.1.6. Facturación del servicio - Gestión Proactiva, Reactiva, Evolutiva, Administrativa

El servicio que cubre las gestiones Proactiva, Reactiva, Evolutiva, de operación y Administrativa se facturará por mensualidad vencida.

Para la entrada de elementos nuevos AB notificará previamente al Prestador del Servicio sus características. Todas estas notificaciones se harán mediante la herramienta de ticketing.

4.1.7. Facturación del servicio - Desarrollo de nuevas funcionalidades

El importe estimado para estos servicios se consumirá de la bolsa de horas anual estimada en 120 horas mediante la realización de trabajos derivados de los proyectos y tareas consideradas no simples previamente autorizadas por los responsables de AB.

Se facturará aplicando a la dedicación efectivamente prestada por cada uno de los técnicos asignados a cada proyecto los precios / hora establecidos en el presente apartado.

El servicio de desarrollo de nuevas funcionalidades y mejoras se facturará mensualmente teniendo en cuenta el tarifario de referencia según la tabla de perfiles y valores requeridos:

Perfil	**Especialista**	**Experto**
Project Manager	100 €/h	120 €/h
Solution Arquitect		
Técnicos expertos en ONLINE		
Técnicos expertos en BATCH		
Técnicos expertos en BBDD y ficheros		
Técnicos expertos en QMF		
Técnicos expertos en Micro Focus Enterprise Server		
Técnicos expertos en Control-M		
Técnicos expertos en printing usando LRS		

Dentro de la relación de informes mensuales se incluirá uno que visualice con total claridad la situación de la bolsa de horas a fin de mes y su evolución, incluyendo el importe de la bolsa a finales del mes anterior, el incremento debido a la facturación del mes y los consumos derivados de proyectos y tareas no simples.

Para que un consumo de la bolsa de horas pueda ser considerado deberá haber sido autorizado por los responsables de AB, siguiendo el protocolo que se decida a las reuniones de inicio del servicio. La estimación del tamaño de la bolsa de horas es anual, siendo imposible trasladar importes no consumidos durante el año anterior al año actual. Cada año el contador de consumo de bolsa se iniciará desde 0.

4.1.8. Transición del servicio

El Prestador del Servicio deberá incluir en sus propuestas una descripción detallada de la metodología a utilizar en la transición del servicio, así como la adaptación a la casuística propia de AB.

Se definirán al menos 2 fases:

- **Traspaso de conocimiento**: período que va entre la entrada en vigor del contrato y la asunción del control del servicio por parte del nuevo Prestador del Servicio. Durante esta fase el nuevo Prestador del Servicio deberá cubrir las siguientes actividades:
    - *Due Diligence*: consecuencia de la adjudicación contractual y durante un plazo que no superará los 2 meses el adjudicatario realizará el proceso de verificación del inventario, comprobación y completitud de la información facilitada durante la fase de licitación.
    - *Transferencia*: inicia a consecuencia de la adjudicación contractual. El nuevo Prestador del Servicio recibirá apoyo del Prestador del Servicio actual, que facilitará y colaborará en el traspaso de conocimiento, así como en la habilitación de la nueva operación. Igualmente, durante esta fase el nuevo Prestador del Servicio implantará el modelo de gobierno del servicio y concretará el modelo de relación con el resto de servicios con los que interactúa. Durante la fase de transferencia del anterior Prestador del Servicio continuará realizando la prestación con los ANS comprometidos en el contrato.
    - *Implantación*: inicia a consecuencia de la adjudicación contractual. En esta fase el nuevo Prestador del Servicio iniciará la activación de todas las herramientas, procesos, formaciones y mecanismos indicados en su plan de implantación para la posterior explotación del servicio.

- **Nueva prestación**: se inicia una vez finalizada la fase de transición. El nuevo Prestador del Servicio prestará el mismo considerando el alcance del pliego.

La fase de traspaso de conocimiento tendrá una duración máxima de 3 meses.

4.1.9. Devolución del servicio

La fase de devolución del servicio tiene como finalidad la transferencia de los servicios externalizados a un tercero designado por AB. En esta fase el adjudicatario deberá cumplir con los niveles de servicio comprometidos para que no se produzca ningún impacto negativo en el servicio recibido por AB. Paralelamente se requerirá la colaboración de los Gestores del Servicio antiguo y nuevo con la transferencia del servicio.

Previamente a la finalización de la relación contractual entre AB y la actual Prestador del Servicio por cualquier causa, AB comunicará la misma con suficiente antelación. Después se pondrá en

marcha el plan para la devolución del servicio. El Prestador del Servicio actual estará obligado a devolver el control de los servicios objeto del contrato, debiendo realizar en paralelo los trabajos de devolución con los de presentación del servicio, sin coste adicional para AB.

Para esta devolución el actual Prestador del Servicio estará obligado a prestar la colaboración necesaria en todos los ámbitos por un periodo estimado de 3 meses. Si las circunstancias lo requieren el actual Prestador del Servicio deberá prestarlo de la misma manera que en la fase de prestación estable durante un plazo máximo de 6 meses.

La devolución del servicio debe incluir al menos los siguientes puntos:

- Traspaso a AB de la propiedad de los activos del Prestador del Servicio susceptibles de ser transferidos.
- Traspaso a AB de la información alojada en la infraestructura del Prestador del Servicio que esté relacionada con los sistemas de AB.
- Traspaso de los datos de los sistemas que no sean propiedad de AB a los sistemas destino que se determine en el momento de la devolución del servicio.
- Traspaso de contratos de terceros y titularidad de licencias según el caso atendiendo a la solicitud y conformidad de AB.
- Traspaso del conocimiento de gestión de los recursos.
- Traspaso de la documentación del servicio.
- Permiso para que AB pueda suscribir un contrato de uso sobre los sistemas del Prestador del Servicio cuando fueran necesarios para asegurar la continuidad del servicio.

El Prestador del Servicio incluirá en sus propuestas la metodología y planificación específica para la devolución del servicio teniendo en cuenta las tareas anteriormente mencionadas y el alcance de los servicios a devolver, así como las obligaciones que suscriben y el apoyo concreto (formación, documentación, procedimientos) que darán al nuevo Prestador del Servicio.

4.1.10. Terminación del servicio

TRES (3) meses antes de la finalización del servicio se activará el Plan de Devolución del servicio a AB o al nuevo Prestador del Servicio designado por AB.

5. OTROS REQUERIMIENTOS

5.1.1. Organización del servicio

Los objetivos que se cubrirán con la Gestión del Servicio serán:

- Asegurar que el Servicio se realiza acorde a los niveles requeridos por contrato
- Garantizar que todas las incidencias reportadas por el HelpDesk de AB al Service Desk del adjudicatario se resuelven satisfactoriamente en el menor tiempo posible
- Generar informes de Nivel de Servicio y lanzar las acciones de mejora necesarias
- informar inmediatamente a AB sobre cualquier incidencia relevante que suceda
- Identificar y sugerir mejoras de servicio
- Discutir y acordar soluciones a los problemas con el Responsable del Servicio de AB

La Gestión del Servicio se basará en una coordinación estrecha entre el interlocutor con poder de decisión de AB y el Gestor del servicio.

El nivel de comunicación entre ellos ha de ser frecuente y, como mínimo, con una periodicidad mensual, revisarán os aspectos más relevantes del Servicio, entre los cuales se pueden destacar:

- Nivel del Servicio.
- Problemas detectados.
- Situación de proyectos en curso.
- Petición de modificaciones.

De estas reuniones se emitirá un comunicado/acta a la persona de contacto designada por AB.

5.1.2. Acuerdos de Nivel de Servicio (ANS)

Los Acuerdos de Nivel de Servicio (ANS) suponen el compromiso del Prestador del Servicio para dar respuestas efectivas ante las peticiones e incidencias que se vayan produciendo.

Estos acuerdos serán revisables anualmente con el objetivo de adecuarlos a la realidad del servicio.

Compromisos por la gestión de incidencias

Entorno	Severidad	Horario	Objetivo	T. Respuesta	T. Resolución
Productivo	Crítica	24x7	90%	15 min	2 horas
	Alta	24x7	90%	1 hora	8 horas
	Media	24x7	90%	4 horas	16 horas
	Baja	24x7	90%	8 horas	24 horas
No Productivo	Alta	12x5	90%	30 min	6 horas
	Media	12x5	90%	4 horas	24 horas
	Baja	12x5	90%	8 horas	48 horas

El objetivo aquí es el porcentaje mínimo de consecución del ANS, calculado mensualmente con todas las incidencias abiertas dentro del mes y contabilizando el número de resueltas dentro del ANS vs. el número de incidencias con ANS excedido.

Compromisos por la disponibilidad de los entornos

Entorno	Horario	Objectivo
Productivo	24x7	99,99%
No Productivo	12x5	99,90%

El objetivo aquí es el porcentaje de disponibilidad mínima de los componentes de software gestionados, medido mensualmente y calculado dentro del horario indicado, que a su vez dependen de la plataforma sobre la que corren de cómputo, almacenamiento y comunicaciones, que están excluidas de la responsabilidad de este servicio.

Compromisos por la gestión de peticiones de servicio

Entorno	Tipo Petición	Prioridad	Horario	T. Resolución	Objectivo
Productivo	Simple	Alta	12x5	16 horas	95%
		Media		32 horas	95%
		Baja		64 horas	95%

	No Simple	Alta	12x5	*Cumplimiento de la estimación presupuestada por el Gestor del Servicio*	95%
		Media			95%
		Baja			95%
No Productivo	Simple	Alta	12x5	32 horas	95%
		Media		64 horas	95%
		Baja		128 horas	95%
	No Simple	Alta	12x5	*Cumplimiento de la estimación presupuestada por el Gestor del Servicio*	95%
		Media			95%
		Baja			95%

Petición simple: *petición de servicio valorada con un esfuerzo de menos de 2 horas de dedicación técnica. Estas peticiones serán atendidas directamente y el coste queda incluido dentro del servicio. Deberá estar procedimentada.*

Petición no simple o Proyecto*: petición de servicio valorada con un esfuerzo superior a 2 horas de dedicación técnica. Estas peticiones requerirán de la confección de un presupuesto que deberá ser aceptado por el personal responsable de AB antes de su realización. El presupuesto deberá enviarse al personal responsable de AB antes de 3 días laborables desde la creación de la petición e incluirá una previsión de fechas de finalización de los trabajos que se utilizará para el cálculo del Tiempo de Resolución y por tanto del ANS. Junto con la aceptación AB indicará si el coste se asume con las horas aprovisionadas o si debe facturar con las tarifas acordadas dentro del concepto "Desarrollo de nuevas funcionalidades y mejoras" definido en el apartado "2. Alcance ".*

Aclaraciones importantes para la aplicación de los conceptos "petición simple" y "petición no simple":

- Son sólo aplicables a peticiones de servicio, nunca a incidentes.
- No son aplicables a las tareas evolutivas periódicas que se defina como incluidas dentro del servicio, como la aplicación de parches de aplicación y actualización de aplicaciones base major version y minor version.
- Hay un conjunto de tareas simples que obligatoriamente deben considerarse simples: gestión de altas, bajas y modificaciones de permisos y usuarios ... Esta lista se definirá en detalle en la fase transición del servicio.

Objetivo: *Porcentaje mínimo de consecución del ANS, calculado mensualmente con todas las incidencias abiertas dentro del mes y contabilizando el número de resueltas dentro del ANS vs. el número de incidencias con ANS excedido.*

Compromisos por la gestión de proyectos

Tipo de proyecto	Plazo entrega presupuesto	Objectivo
Petición No Simple	3 Dias laborables	99,99%
Proyecto (> 1 Semana)	2 semanas	98,99%

5.1.3. Penalizaciones derivadas del incumplimiento con los ANS

El Gestor del Servicio presentará mensualmente un informe en el que se pueda comprobar el nivel de cumplimiento de los ANS. La información base para este informe saldrá de la herramienta

de ticketing de AB. AB proporcionará al Gestor del Servicio el acceso a las herramientas de extracción para la correcta configuración del informe.

Se definirá un protocolo de alegaciones con el que se podrán revisar y corregir los ANS incompletos dentro la herramienta de ticketing, siempre que los responsables del servicio por parte de AB validen estas correcciones. Dentro de este protocolo también se podrán revisar tickets con ANS cumplido y que los responsables de AB consideran que la han incumplido, siendo necesaria la validación del Gestor del Servicio para hacer las correcciones.

La herramienta de ticketing dispone de estados que permiten detener el contador de tiempo de ANS consumido cuando se dan las siguientes circunstancias:

- El ticket está a la espera de actuación por parte de su creador (por tanto sin posibilidad de actuación por los técnicos del Gestor del Servicio).
- El ticket está a la espera de actuación por parte de un tercero.

En caso de contingencia de Fuerza Mayor, que impida el normal desarrollo del servicio, los ANS establecidos dejarán de ser objeto de medición.

Se define contingencia de Fuerza Mayor como:

- El concepto Fuerza Mayor se define según las leyes españolas; evento forzado externo a una de las partes y más allá de su control, que impide o retrasa el cumplimiento de las obligaciones derivadas del contrato.

En función del grado de cumplimiento de los ANS, se establecen un conjunto de sanciones de penalización en la tabla siguiente:

				ANS y penalizaciones requeridos		
Código	**Descripción**	**Metrica**	**Periodicidad**	**Valor objetivo**	**Valor límite**	**%_Ponderación**
ANS Gestión de contrato						
GC_001	Errores cometidos en la facturación de los servicios de asistencia técnica informática	Facturas devueltas desde el departamento de Administración / Finanzas por errores de facturación	Anual	1 factura errónea	3 facturas erróneas	3,00%
GC_002	Puntualidad en la entrega de los informes de facturación mensuales.	Informes de facturación entregados dentro de los márgenes temporales previstos por los ANS	Anual	1 informe después del día 10 del mes siguiente	3 informes después del día 10 del mes siguiente	3,00%
GC_003	Puntualidad en la entrega de los informes de actividad, incidencias, calidad, seguimiento ANS, etc.	Ratio de informes entregados dentro de los márgenes temporales previstos por los ANS	Mensual	90% informes entregados puntualmente	65% de informes entregados puntualmente	2,00%
GC_004	Puntualidad en la entrega de los informes de incidencias críticas	Ratio de informes de incidencias críticas entregados en un período de tiempo igual o inferior a 48 horas	Mensual	90% informes entregados puntualmente	70% informes entregados puntualmente	3,00%
GC_005	Calidad de los documentos generados como parte de la actividad en la prestación de servicio	Ratio de documentos aceptados por parte de las áreas responsables del servicio por parte de AB sin enmiendas o iteraciones en su elaboración	Mensual	95% documentos aceptados en primera instancia	75% documentos aceptados en primera instancia	2,00%

GC_006	Calidad de las actas generadas de las reuniones como parte de la actividad en la prestación de servicio	Ratio de actos aceptadas por parte de las áreas responsables del servicio por parte de AB sin enmiendas o iteraciones en su elaboración	Mensual	95% actos aceptados en primera instancia	75% actos aceptadas en primera instancia	3,00%
ANS Gestión Operativa						
GO_001	Disponibilidad del servicio de Sistemas Críticos	Se medirá la disponibilidad agregada de los Sistemas Productivos Críticos contabilizando el tiempo de interrupción de la misma (sin incluir las ventanas de mantenimiento pactadas de forma previa con AB)	Mensual	99,99%	99,00%	14,00%
GO_002	Disponibilidad del servicio Sistemas No Críticos	Se medirá la disponibilidad agregada de los Sistemas Productivos No Críticos contabilizando el tiempo de interrupción de la misma (sin incluir las ventanas de mantenimiento pactadas de forma previa con AB)	Mensual	99,90%	99,00%	3,00%
GO_003	Tiempo de respuesta de atención de tickets	Porcentaje de tickets atendidos en un tiempo igual o inferior al establecido en la tabla de "T. Resolución" de Incidencias y peticiones	Mensual	95,00%	75,00%	3,00%
GO_004	Resolución de incidencias Prioridad Crítica	Porcentaje de incidencias resueltas en un tiempo igual o inferior al establecido en la tabla de Tiempo máximo de solución para Incidencias de prioridad Crítica	Mensual	95,00%	75,00%	14,00%

GO_005	Resolución de incidencias Prioridad Alta	Porcentaje de incidencias resueltas en un tiempo igual o inferior al establecido en la tabla de Tiempo máximo de solución para Incidencias de prioridad No Crítica	Mensual	95,00%	75,00%	7,00%
GO_006	Resolución de incidencias Prioridad Media	Porcentaje de incidencias resueltas en un tiempo igual o inferior al establecido en la tabla de Tiempo máximo de solución para Incidencias de prioridad Media	Mensual	95,00%	75,00%	3,00%
GO_007	Resolución de incidencias Prioridad Baja	Porcentaje de incidencias resueltas en un tiempo igual o inferior al establecido en la tabla de Tiempo máximo de solución para Incidencias de prioridad Baja	Mensual	95,00%	75,00%	3,00%
GO_008	Reapertura de Incidencias	Porcentaje de incidencias reabiertas responsabilidad del adjudicatario	Mensual	1,00%	5,00%	7,00%
GO_009	Resolución de Peticiones Prioridad Alta	Porcentaje de Peticiones resueltas en un tiempo igual o inferior al establecido en la tabla de Tiempo máximo de solución para Peticiones de prioridad Alta	Mensual	95,00%	75,00%	7,00%
GO_010	Resolución de Peticiones Prioridad Media	Porcentaje de Peticiones resueltas en un tiempo igual o inferior al establecido en la tabla de Tiempo máximo de solución para Peticiones de prioridad Media	Mensual	95,00%	75,00%	3,00%
GO_011	Resolución de Peticiones Prioridad Baja	Porcentaje de Peticiones resueltas en un tiempo igual o inferior al establecido en la tabla de Tiempo máximo de solución para Peticiones de prioridad Baja	Mensual	95,00%	75,00%	3,00%

GO_012	Reapertura de Peticiones	Porcentaje de peticiones reabiertas responsabilidad del adjudicatario	Mensual	1,00%	5,00%	3,00%
GO_014	Presentación de presupuestos de proyectos	Porcentaje de versiones definitivas de los presupuestos de proyectos presentados en un periodo inferior o igual a 15 días desde la solicitud de AB	Trimestral	90,00%	80,00%	7,00%
GO_015	Cumplimiento en fechas de entrega en proyectos	Desviación temporal respecto a las fechas de entrega establecidas en los proyectos	Trimestral	3 días	9 días	7,00%
						100,00%

Reglas para el cálculo de las penalizaciones:

- **Valor Objetivo**: Porcentaje requerido al proveedor de Servicio para cada uno de los indicadores de ANS.
- **Valor Límite**: Porcentaje mínimo por debajo del cual se aplican las penalizaciones.
- **Peso.** Peso de la actividad respecto al global de servicios. La suma de todas las actividades es 100%. Este valor es el que se utilizará para el cálculo de las penalizaciones, para ello utilizaremos las siguientes fórmulas:
    - **SPVO=** Suma de pesos de actividades que incumplen "Valor Objetivo"
    - **SPVL=** Suma de pesos de actividades que incumplen "Valor Límite"

- **Penalizaciones.**
    - SPVL <= 10% **Y** SPVO <= 20% → Penalización = **0%**
    - SPVL > 10% **O** SPVO > 20%→ Penalización = Mínimo (**SPVL,10%)**

En relación con la tabla anterior, los licitadores pueden:

- Proponer nuevos valores para el "Valor Objetivo" y "Valor Límite"

Los valores propuestos deben igualar o mejorar los determinados como "Requeridos"

5.1.4. Informes de servicio

Con una periodicidad mínima mensual el Prestador del Servicio proporcionará un informe de seguimiento del servicio, donde aparezca al menos esta información:

- Seguimiento ANS. Nivel de cumplimiento del último mes cerrado y evolución histórica.
- Seguimiento de actividad. Tickets creados vs. tickets cerrados, por tipo (Incidencia, Petición de Servicio) y criticidad. Datos del último mes cerrado y evolución histórica.
- Seguimiento problemas. Lista de incidentes de largo recorrido y que por tanto han derivado en problemas. Acciones correctoras previstas, previsión de la activación de las mismas.
- Seguimiento facturación. Visión del último mes cerrado e histórica sobre la facturación, diferenciando entre importe de la gestión del equipamiento y el importe de horas para peticiones no simples.
- Seguimiento peticiones no simples. Planificación de las tareas previstas, evolución consumo de horas acumuladas de técnico.

5.1.4.1. Informe ejecutivo

Este informe contendrá los datos básicos, en formato gráfico, y acumulados mensuales; de las diferentes tareas o funciones que componen el Servicio:

- **Incidencias**. Información sobre las incidencias que se han abierto y cerrado durante aquel mes y los que quedan pendientes una vez finalizado el período
- **Cambios.** Detalle de todos los cambios que se han abierto y cerrado durante aquel mes y los que quedan pendientes una vez finalizado el período
- **Niveles de Servicio**. Información del valor de los indicadores de los niveles de Servicio acordados en el ANS
- **Observaciones**. Apartado del informe para detallar aquellos aspectos importantes de la gestión del Servicio que se hayan producido a lo largo del período reportado, detallados por cada uno de los distintos niveles de soporte establecidos. Esto consistirá en un informe global sobre el funcionamiento de las instalaciones (puntos críticos y otros problemas detectados).

- Acciones correctoras a realizar por AB y el adjudicatario.

5.1.4.2. Informe de seguimiento

Este informe contendrá los datos de volumetrías del mes tratado. Este informe se entregará con los datos numéricos y gráficos, por ejemplo:

- Resumen incidencias del Sistema: control mensual de incidencias, con detalle de la fecha/hora de inicio y fin, afectación y breve descripción,
- Peticiones de AB: Resumen de peticiones y cambios
- Ejecución de las copias

5.1.4.3. Informe de SLA

Así mismo, al grupo de informes se añadirá el informe de SLA, que contendrá el evolutivo anual de los indicadores de servicio definiditos:

- Tabla evolutiva de indicadores ANS.
- Relación de incumplimientos.

5.1.5. Gestión y Coordinación de la ejecución

El Prestador del servicio (o proveedor) designará como mínimo los siguientes roles, aportando recursos cuya experiencia y nivel de decisión se correspondan a los indicados a continuación:

- **Gestor del servicio**

  Es la persona que tendrá la visión completa del Contrato 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 específicos del proyecto.
  - Garantizar la rápida resolución y priorización de las incidencias graves.
  - Asegurar el cumplimiento de la Planificación general y de los compromisos de contrato.
  - 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 Gestor 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, mensualmente o con la frecuencia que razonablemente se considere necesaria o después de 3 días laborables tras una petición de cualquiera de las partes.

- **Perfiles técnicos necesarios**

  El adjudicatario deberá configurar un equipo de personas con perfiles adecuados a las tareas a desarrollar en el servicio descrito, que deberá estar compuesto por el número de técnicos necesarios en cada momento, con conocimiento, experiencia probada y certificaciones

adecuadas de forma que quede garantizado que como mínimo se cubran los siguientes perfiles:

- **Técnicos expertos en herramientas Micro Focus Enterprise Server,** con experiencia mínima de DOS (2) años en administración en los últimos TRES (3) años. Así mismo deberá disponer de las siguientes certificaciones vigentes:
    - Micro Focus Enterprise Server Basic Diagnostics training
    - Micro Focus Enterprise Server Advance Diagnostics

- **Técnicos expertos en Control-M,** con experiencia mínima de DOS (2) años en administración en los últimos TRES (3) años.

- **Técnicos expertos en QMF,** con experiencia mínima de DOS (2) años en administración en los últimos TRES (3) años.

- **Administradores expertos en planificación BATCH en Control-M**, con experiencia mínima en administración de DOS (2) años usando Control-M acreditable, en los últimos TRES (3) años.

- **Operadores expertos en planificación BATCH en Control-M**, con experiencia mínima en administración de DOS (2) años usando Control-M acreditable, en los últimos TRES (3) años.

- **Técnicos en printing usando LRS**, con experiencia mínima de DOS (2) años en el uso de la herramienta VPSX, en los últimos TRES (3) años. Así mismo deberá disponer de las siguientes certificaciones vigentes:
    - VPSX Systems Operator
    - VPSX Systems Administration

- **Técnicos expertos en seguridad** experiencia mínima acreditable de DOS (2) años en Open LDAP, en los últimos TRES (3) años.

En cualquier caso, las personas integrantes en 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.
- Nivel nativo de castellano tanto hablado y escrito para una fluida comunicación con técnicos de AB y con los usuarios.
- 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.

El servicio será realizado por personal propio (o subcontratado) del gestor del servicio. Este personal tendrá la calificación necesaria para efectuar esta prestación, según se ha definido en el punto anterior.

En el caso que el gestor del servicio opte por subcontratar el servicio o parte de este, será obligatorio comunicar estas subcontrataciones a AB para su aceptación.

En las ofertas se incluirá una descripción detallada de las características técnicas y experiencia del personal asignado al servicio. AB verificará durante el inicio del servicio que el personal asignado en el presentado en la oferta.

5.1.6. Procedimientos para la realización del Servicio

Los procedimientos para la realización del servicio descrito anteriormente serán realizados por el adjudicatario con la colaboración de AB, basándose en los que actualmente se utilizan para gestionar los servicios en el HOST que el proveedor actual proporciona a AB en estos momentos.

5.1.7. Idioma

El proyecto se deberá prestar a nivel comunicativo en castellano y/o catalán tanto hablado como escrito para una fluida comunicación con técnicos de AB y con los usuarios.

5.1.8. Recursos Materiales requeridos

El Adjudicatario será responsable de disponer del equipo de trabajo, así como de todo el equipamiento hardware, software, y demás especificaciones fijadas en el presente Pliego, que sean necesarios 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 Contrato.

No obstante lo anterior, AB proporcionará al Prestador del Servicio las siguientes herramientas:

- Usuarios locales o de dominio con los permisos necesarios.
- Herramientas de reporting y seguimiento de las incidencias detectadas: en la actualidad el JIRA y el BMC Remedy.

5.1.9. Acceso

El acceso del Prestador del Servicio a los sistemas de información de Aguas de Barcelona se realizará mediante conexión VPN Lan-to-lan o con usuarios VPN nominales.

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. Seguridad corporativa

Tanto el Prestador del Servicio como sus trabajadores deberán 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 (véase **Anexo Nº 1**).
- 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 estas y sus posibles impactos no deseados.

A la finalización del contrato, el Prestador del Servicio 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.

Anexo 1 - Normas de seguridad IT d'Aigües de Barcelona

De forma general los Sistemas de Información proporcionados no deben ser vulnerables, y según aplique, los TOP 10 de *OWASP Security Mobile* y/o *OWASP* Top 10 Security Web (https://www.owasp.org). Además, deberá cumplirse la normativa de gestión de usuarios y contraseñas establecida en el presente Anexo.

Esta normativa puede cumplirse utilizando el Active Directory de AB como repositorio de los usuarios mediante una conexión segura con el sistema ADFS de AB.

El objeto de los siguientes apartados es detallar la normativa de seguridad en la gestión de los Sistemas de Información de AB y en la identificación, autentificación de usuarios y gestión de las contraseñas de acceso a los mismos.

En todo caso, durante la ejecución del contrato deberán observarse por parte de los adjudicatarios las medidas de seguridad que constan en el Anexo Nº 10 del Pliego de Condiciones Particulares (PCP), según lo previsto en la Cláusula 12 del mismo.

Aguas 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 Nº 10 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 Aguas de Barcelona, un informe actualizado y detallado del desempeño de cada una de las medidas de seguridad anteriormente indicadas.

- Por otra parte, Aguas de Barcelona se reserva el derecho, en cualquier momento, de realizar todas las auditorías que considere pertinentes a los efectos de verificar el grado de cumplimiento indicado en el Informe mencionado en el apartado anterior.

<u>ANEXO Nº 1</u> - NORMAS DE SEGURIDAD IT DE AIGÜES DE BARCELONA

"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 autentificación 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, autentificación de usuarios y gestión de las contraseñas de acceso a los mismos.

2. Intercambio de información y software

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 o confidencial, 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 GDPR.

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. 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 emplear en la medida de lo posible mecanismos de autentificación mutua basados en claves pre compartidas, 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

Durante la ejecución del proyecto, la administración remota de los sistemas de información debe ser realizada por medio de herramientas provistas por AB para la identificación unívoca al usuario administrador y para que las credenciales de dicho usuario administrador viajen cifradas.

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.

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.

El mecanismo de autentificación será OpenLDAP.

La autentificación 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 autentificación 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 autentificación 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.

Con el fin de evitar el acceso no autorizado, el proceso de identificación y autentificación 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.

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.

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.

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 un número determinado de 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.

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.

El proveedor deberá reportar aquellos incidentes significativos que puedan resultar 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.