PLIEGO DE CONDICIONES TÉCNICAS QUE HAN DE REGIR EL CONTRATO PARA EL "SERVICIO CORRESPONDIENTE A LA GESTIÓN DE LAS INFRAESTRUCTURES INFORMÁTICAS DEL ENTORNO DE OPERACIONES"

Índice

1. Objeto

El presente Pliego de Prescripciones Técnicas (en adelante, PPT) establece las prescripciones técnicas que rigen el procedimiento de contratación para el " **Servicio de gestión de las infraestructuras informáticas del entorno de operaciones** " promovido por **Aigües de Barcelona, Empresa Metropolitana de Gestió del Cicle Integral de l'Aigua, S.A.** (en adelante, AB), así como la ejecución del mismo.

2. Alcance

2.1. Inventario

Se desea disponer de un servicio de gestión proactivo, reactivo, evolutivo, administrativo y de desarrollo para todo el equipamiento informático que ejerce de servidor en las sedes de operaciones de la empresa.

El inventario de hardware que se incluirán dentro del servicio es el siguiente:

Servidores

Físico/Virtual/Cloud	SO	Entorno	Horario	Criticidad	Nº Servidores
Físico	ESX	Producción	24x7	Crítico	**6**
Físico	Linux	Producción	24x7	Crítico	**2**
Físico	Linux	NO Producción	laboral	no Crítico	**1 (*)**
Físico	Windows	Producción	24x7	Crítico	**30**
Físico	Windows	NO Producción	laboral	no Crítico	**1 (*)**
Virtual	Linux	Producción	24x7	Crítico	**2**
Virtual	Linux	NO Producción	laboral	no Crítico	**2**
Virtual	vCenter	Producción	24x7	Crítico	**2**
Virtual	Windows	Producción	24x7	Crítico	**48**
Virtual	Windows	NO Producción	laboral	no Crítico	**16**
Cloud	Linux	Producción	24x7	Crítico	**1 (*)**
Cloud	Linux	NO Producción	laboral	no Crítico	**1 (*)**
Cloud	Windows	Producción	24x7	Crítico	**1 (*)**
Cloud	Windows	NO Producción	laboral	no Crítico	**1 (*)**

Cabinas de discos

Físico/Virtual/Cloud	SO	Entorno	Horario	Criticidad	Nº Cabinas
Físico	cabinas Disco	Producción	24x7	Crítico	**6**

Instancias

Tipo	Instancia	Entorno	Horario	Criticidad	NºInstancias
BBDD	Microsoft SQL	NO Producción	Laboral	No Crítico	**2**
BBDD	Microsoft SQL	Producción	24x7	Crítico	**2**
BBDD	MySQL	NO Producción	Laboral	No Crítico	**1 (*)**
BBDD	MySQL	Producción	24x7	Crítico	**1 (*)**
BBDD	PostgreSQL	NO Producción	Laboral	No Crítico	**1 (*)**
BBDD	PostgreSQL	Producción	24x7	Crítico	**1 (*)**
BBDD	Oracle	NO Producción	Laboral	No Crítico	**1 (*)**
BBDD	Oracle	Producción	24x7	Crítico	**1 (*)**
Servidor de aplicaciones	Apache	NO Producción	Laboral	No Crítico	**1 (*)**
Servidor de aplicaciones	Apache	Producción	24x7	Crítico	**1 (*)**
Servidor de aplicaciones	IIS	NO Producción	Laboral	No Crítico	**1 (*)**
Servidor de aplicaciones	IIS	Producción	24x7	Crítico	**1 (*)**
Servidor de aplicaciones	Tomcat	NO Producción	Laboral	No Crítico	**1 (*)**
Servidor de aplicaciones	Tomcat	Producción	24x7	Crítico	**1 (*)**
Servidor de aplicaciones	JBoss	NO Producción	Laboral	No Crítico	**1 (*)**
Servidor de aplicaciones	JBoss	Producción	24x7	Crítico	**1 (*)**

- **SE ADVIERTE**:
- Este inventario está actualizado a fecha mayo de 2020. En el momento de la licitación puede haber experimentado algunos cambios, pero es válido para valorar el volumen general.
- (*) Estas unidades no formaran parte del contrato en el inicio de su vigencia y su incorporación no está garantizada.

Durante la vigencia de este servicio están planificadas las siguientes actuaciones, que se estima modificarán el inventario actual en los siguientes términos:

- Adquisición y puesta en marcha de hosts de virtualización basados en Microsoft Hyper-V (5 sedes, 1 servidor por sede)
- Adquisición y puesta en marcha de cabinas NAS de gama baja para ejercer de almacén de copias de seguridad (5 sedes, 1 cabina por sede)
- Adquisición y puesta en marcha de un sistema de backup para 5 sedes, con infraestructura aún por definir (5-7 sedes).

Por lo tanto, las volumetrías son estimativas, atendiendo a la situación actual del servicio y sujetas a la evolución del inventario de equipos. Las cantidades de elementos a que se refiere el presente apartado del PPT, únicamente son orientativas de los volúmenes que puede llegar el servicio teniendo en cuenta la previsión inicial, sin que esté garantizada su incorporación durante la vigencia del servicio contratado.

Conforme a lo anterior, el adjudicatario no tendrá derecho a indemnización alguna si no se llegan a alcanzar los volúmenes estimados.

2.2. Objetivos del servicio

Los objetivos son:

- *Gestión proactiva del equipamiento inventariado*

- Monitorización de los sistemas para garantizar su disponibilidad y rendimiento óptimo.
- Operación de los sistemas. Creación y utilización de protocolos de operación eficientes y adecuados.
- Seguimiento de los procesos automatizados (backups, procesos periódicos). Documentación y generación de alertas de control.
- Diseño y desarrollo de pruebas que permitan garantizar el correcto funcionamiento de los sistemas de contingencia
- Intervenciones in situ en los diferentes CPDs para tareas que lo requieran.

- *Gestión reactiva del equipamiento inventariado*
  - Actuación en régimen 24x7 ante incidencias. Resolución de estas dentro de los acuerdos de nivel de servicio (en adelante 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 el servicio de gestión de eventos.
  - Escalado de los incidentes hardware a los proveedores de mantenimiento y garantía contratados por AB.
  - Intervenciones in situ en los diferentes CPDs para tareas que lo requieran.

- *Gestión evolutiva del equipamiento inventariado*
  - Aplicación periódica y bajo demanda de parches de seguridad en los sistemas operativos y aplicaciones de uso general (navegadores de Internet, servidores Web, bases de datos ...).
  - Adecuación de los sistemas a los requerimientos y estándares de la empresa.
  - Resolución de peticiones de modificación y mejora, dentro de los ANS establecidos.
  - Intervenciones in situ en los diferentes CPDs para tareas que lo requieran.

- *Gestión administrativa del equipamiento inventariado*
  - Mantenimiento de un documento diariamente actualizado donde aparezca el inventario del equipamiento gestionado, con toda la información que se considere relevante para cada elemento: identificador único, marca, modelo, nº serie, fecha compra, fecha alta en el servicio, sistema operativo ...
  - Altas y bajas de los equipos dentro del servicio, con impacto mensual sobre la facturación. Todas las altas y bajas producidas antes del día 15 del mes en curso serán incluidos en la facturación de este mes, quedando el resto para incluirse en la facturación a partir del mes siguiente.
  - Etiquetado de todos los equipos físicos con identificador único claramente visible.
  - Intervenciones in situ en los diferentes CPDs para tareas que lo requieran.

- *Desarrollo de nuevas funcionalidades*
  - Dentro del servicio se incluirán tarifas y horas de técnico que AB utilizará para pedir al Prestador del Servicio tareas evolutivas y de mantenimiento periódico a desarrollar sobre el equipamiento gestionado.

  Intervenciones in situ en los diferentes CPDs para tareas que lo requieran.

2.3. Exclusiones del servicio

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

- *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 estas 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 porque el servicio del cual es responsable cumpla las políticas de seguridad corporativas operando y adecuando 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 técnicas

3.1. Distribución geográfica

Todos los centros de operaciones de Aguas de Barcelona se encuentran ubicados en el área metropolitana de Barcelona, a excepción del centro de contingencia situado en C / Ulises de Madrid.

Aguas de Barcelona proporcionará medios para acceder remotamente a todo el equipamiento siempre que éste disponga de esta funcionalidad.

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

Cuando el acceso remoto no sea posible o el personal autorizado de AB lo solicite el Prestador del Servicio deberá disponer de personal que se desplazará físicamente a las sedes para realizar los trabajos necesarios. Estos desplazamientos deberán coordinarse con el personal de Sistemas de AB y realizarse conforme a las normas de Seguridad y Prevención de Riesgos Laborales de la compañía.

Aunque la gestión del servicio sea principalmente remota y el Prestador del Servicio deberá especificar el lugar o lugares desde los que prestará el servicio. En caso de producirse cambios durante la vigencia del contrato, estos deberán comunicarse a AB por su aprobación.

3.2. Descripción de los sistemas a gestionar

Los sistemas a gestionar el futuro Prestador del Servicio se pueden catalogar en estos grupos:

- *Hardware de Transporte*: dan servicio al sistema de transporte de agua. Tienen estas características:
    - Servidores virtuales sobre VMware 6.5 alojados en el CPD del polígono industrial Pedrosa (Hospitalet de Llobregat).
    - Los host ESX forman un clúster con alta disponibilidad.
    - Sincronizados mediante VMware SRM con el CPD de la calle Ulises, en Madrid
    - Alojan la mayoría de ellos software SCADA
    - Con ellos se controla toda la red de transporte de agua para el área metropolitana, por lo tanto, su criticidad es máxima
    - Actualmente son mayoritariamente Windows 2008, pero está prevista su actualización durante 2020 a Windows 2016 y últimas versiones del software SCADA.
- *Hardware de las plantas depuradoras (ETAP)*: dan servicio a todos los sistemas de control de las plantas de depuración. Tienen estas características:
    - Servidores virtuales sobre VMware 6.5 (entorno productivo) y VMware 5.5 (entorno no productivo). Hay servidores SCADA y servidores con otros roles.
    - Los host ESX forman un clúster con alta disponibilidad.
    - Una de las plantas dispone de un sistema de backup basado en Veeam Backup con una cabina DataDomain local sincronizada con una DataDomain alojada en el CPD del polígono Pedrosa (Hospitalet de Llobregat)
    - Sistema operativo mayoritariamente Windows 2016, aunque hay algún equipo Linux y algún otro Windows de versiones anteriores.
- *Hardware de las plantas de saneamiento (EDAR):* dan servicio a todos los sistemas de control de las plantas de saneamiento. Tienen estas características:
    - Servidores SCADA: físicos, redundantes en cada sede para dar alta disponibilidad. Sistema operativo Windows 2016.
    - Otros servidores: físicos de diferentes tipologías y sistemas operativos. Durante 2020 se ejecutará un proyecto para convertirlos en máquinas virtuales sobre Microsoft Hyper -V.
    - Los sistemas operativos de las máquinas trasladadas a Hyper -V será como mínimo Windows 2012. También habrá máquinas Linux.
- *Hardware del sistema de Drenaje*: dan servicio al sistema de pozos de drenaje controlado por Aguas de Barcelona. Tienen estas características.
    - Aunque hay algún servidor físico son mayoritariamente virtuales, sobre plataforma VMware 5.5
    - Están alojados físicamente en TIC que Telefónica tiene en Terrassa, en régimen de housing
    - Sistema operativo Windows 2003 en la mayoría de los casos
    - Tienen Directorio Activo propio, independiente del resto
- *Hardware del Directorio Activo:* existe un directorio activo propio para este entorno en el que el Prestador del Servicio dispondrá de privilegios administrativos sobre las OU (Unidades Organizativas) necesarias.
    - Actualmente hay máquinas del entorno de operaciones que no pertenecen a ningún dominio o que pertenecen a un dominio diferente. Durante 2020 todas las máquinas gestionadas en este servicio deberán pasar a este dominio.
    - Durante 2020 haremos que todas las sedes dispongan de un controlador de dominio propio de este dominio.
- *Hardware del Área de desarrollo funcional*: el departamento encargado de la evolución funcional del software SCADA dispone de un conjunto de servidores propios con estas características:

- Servidores virtuales sobre VMware 6.5 alojados en los mismos host ESX del entorno de transporte (por lo tanto, el CPD del polígono industrial Pedrosa, Hospitalet de Llobregat).
- Sistema operativo Windows 2008, aunque está prevista su evolución a Windows 2016 durante el año 2020.
- Disponen la mayoría de ellos de software SCADA instalado.

- *Hardware del CPD calle Ulises (Madrid)*: aquí se dispone de un servidor ESX que ejerce de destino del sistema SRM y donde se replican con periodicidades diversas los servidores del entorno de transporte. Se programa y ejecuta una prueba de contingencia anual para garantizar que los sistemas funcionan correctamente cuando son trasladados al entorno secundario

3.3. Protocolos y normativas

Todos los trabajos desarrollados por los técnicos del servicio deberán ir alineados con las normas y protocolos existentes en materias de Seguridad, Prevención de Riesgos Laborales, Sistemas y cualquier otro departamento que tenga responsabilidad sobre el material gestionado.

3.4. Gestión de vulnerabilidades en sistemas operativos y software

Esta gestión consiste en el proceso de mitigación de vulnerabilidades y eliminación de agujeros de entrada para todo tipo de malware. Esta gestión consiste en un servicio prestado por el Prestador del Servicio e incluso al servicio de gestión evolutiva.

El Prestador del Servicio facilitará a AB la información que AB considere necesaria (versiones de SO y software, logs, etc.) para obtener evidencias por las auditorías de seguridad periódicas y para la resolución de incidencias e intervenciones puntuales.

Todos los equipos quedarán incluidos en un protocolo de aplicación de parches de seguridad y modificaciones diversas (actualizaciones de software, eliminación de protocolos inseguros, etc.) que garantice que periódicamente cumplen con los requisitos del departamento de Seguridad.

Todas las aplicaciones de parches y modificaciones derivadas de esta gestión deberán ser autorizadas por el personal correspondiente de AB y coordinadas con el resto de los elementos de la organización que estén afectados.

Se tendrán en cuenta aspectos específicos del software que se ejecuta en los equipos, para evitar aplicar parches o mejoras que generen indisponibilidad en el servicio.

3.5. Conocimiento Técnico y certificaciones

El personal técnico aportado por el Prestador del Servicio deberá disponer conocimiento, experiencia probada y certificaciones en, como mínimo, las siguientes plataformas tecnológicas:

- *Sistemas Operativos*
  - Windows Server (cualquier versión desde Windows 2003)
  - Windows Server - Terminal Server
  - Linux Server (Red Hat, CentOS, SUSE)
- *Administración de Bases de Datos*
  - Oracle
  - SQL Server
  - PostgreSQL
  - MySQL
- *Servidores Web*

- Microsoft IIS
- Apache, Liferay

- *Sistemas de Seguridad y Autenticación de Usuarios*
  - Microsoft Active Directory, Open LDAP
  - Gestión de seguridad SSL, Gestión de certificados
  - Antivirus: TrendMicro, McAfee
- *Sistemas de Virtualización*
  - Microsoft Hyper -V
  - VMware
- *Sistemas de Monitorización*
  - Nagios
  - Grafana
- *Sistemas de Backup*
  - Veeam Backup
  - TSM
  - otros

El Prestador del Servicio deberá aportar evidencias de la capacidad tecnológica de su personal para, como mínimo, las plataformas mencionadas

3.6. Personal técnico

El servicio será realizado por personal propio (o subcontratado) del Prestador del Servicio. Este personal tendrá la cualificación necesaria para efectuar esta prestación, según se ha definido en el apartado anterior 3.5.

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

AB verificará durante toda la prestación del servicio que el personal asignado cumple con los requisitos de experiencia y nivel técnico exigidos en el presente pliego y que este es adecuado para llevar a cabo el servicio

3.7. Sistema de monitorización

El sistema de monitorización actual de AB está Basado en Nagios 4 y Grafana.

El prestador del Servicio implementará un sistema de monitorización basado en la misma tecnología que el de AB y será utilizado por sus Operadores y Técnicos para la gestión proactiva y reactiva de los sistemas.

El sistema de monitorización implementado deberá integrarse con el de AB de forma que los técnicos de AB dispongan de visión, directa e integrada en el sistema corporativo, del estado de funcionamiento de los sistemas gestionados.

La integración deberá permitir al sistema de monitorización corporativo de AB recibir información sobre todo el equipamiento gestionado, tanto a nivel de disponibilidad como de rendimiento, con un histórico de rendimiento mínimo de un año.

Dentro de un respeto estricto a las reglas de seguridad y uso, AB proporcionará al sistema de monitorización del Prestador del Servicio los accesos y protocolos que sean necesarios.

El sistema de monitorización debe funcionar bien antes de 3 meses a partir del inicio del servicio, y monitorizar perfectamente los equipamientos más críticos antes de 1 mes.

El sistema de monitorización será alojado en la infraestructura VMware que AB tiene en su CPD principal. Deberá quedar perfectamente documentado y será propiedad de AB, por tanto, permanecerá plenamente funcional en caso de finalización del contrato.

3.8. Gestión de Copias de Seguridad (Backups)

El prestador de Servicio realizará la gestión de las copias de seguridad de todos los elementos del inventario mediante las herramientas actualmente existentes o las que se implanten en el futuro.

Actualmente, las copias se están realizando mediante las siguientes herramientas:

- Veeam backup. Esta herramienta gestiona parte del parque virtual. Debería ser gestionada íntegramente por el prestador de Servicio
- IBM TSM. Esta herramienta de gestión de backups es gestionada actualmente por otro proveedor y el prestador del Servicio sólo configura los clientes en los servidores. Posteriormente parte de los servidores que actualmente hacen backup con TSM serán migrados a la nueva herramienta que se desplegará a lo largo de 2020
- Symantec BESR. Esta herramienta se gestiona por el mismo proveedor que TSM y al igual que los backups realizados con TSM será migrada parcialmente a la nueva herramienta de backup.

Durante los próximos meses y antes de la entrada en funcionamiento de este servicio está prevista la adquisición y puesta en marcha de un sistema de backup para 5 sedes, con infraestructura aún por definir. Este nuevo sistema de backup también pasará a ser gestionado por el prestador de Servicio.

3.9. Gestión CMDB

La Base de datos de Elementos de Inventario (técnicamente llamada Configuration Management Database), desde ahora DMDB de AB, centraliza no solo la información relacionada con este Servicio sino también la información del resto de elementos del Sistema de Información de AB. Tener su contenido completo y actualizado es un objetivo prioritario. El Prestador del Servicio utilizará las herramientas indicadas por AB para mantener en perfecto estado la información de inventario de los equipamientos incluidos en el Servicio.

El Prestador del Servicio deberá asegurar que con la información almacenada se puedan comprobar los ítems de facturación, según el modelo de facturación que se haya concretado, manteniendo un histórico de modificaciones y variaciones desde el inicio del contrato, consultable en cualquier momento.

En este sentido el Prestador del Servicio podrá utilizar adicionalmente de forma interna las herramientas que considere, si bien cualquier coste derivado del desarrollo de las interfases que sean necesarios será responsabilidad de este.

Los elementos inventariables en el ámbito del servicio, así como los atributos y relaciones entre los mismos y con los demás servicios serán determinados por AB durante la fase de transición.

Una vez el servicio esté en explotación la carencia de estos elementos y atributos o bien su carencia de actualización en la CMDB invalidará el activo para que forme parte de la facturación mensual.

Las herramientas de CMDB a considerar son las vigentes en AB durante la fase de transición del servicio, sin perjuicio de que durante la fase de evolución del servicio AB determine que estas deben ser sustituidas o ampliadas. El servicio de inventariado en la CMDB es parte intrínseca de este contrato en el ámbito de sus servicios asociados y no debe representar un coste adicional.

3.10. 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 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.

3.11. Herramientas para la gestión del servicio

Aguas de Barcelona 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

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

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

3.12. 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.

3.13. Informes de Servicio

Con una periodicidad mínima mensual el Prestador del Servicio proporcionará un informe de seguimiento del servicio, donde aparezca como mínimo la siguiente información:

- *Evolución del equipamiento* administrado. Lista de altas y bajas.
- *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 estas.
- *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.

4. Condiciones operativas para el desarrollo del Servicio

4.1. Horario de prestación del servicio

El servicio prestado por el Prestador del Servicio tendrá una cobertura horaria **24x7** para todos los días del año.

Dentro del Servicio, los equipamientos gestionados se dividirán en los siguientes horarios:

24x7 → 24 horas, 7 días por semana. Fines de semana y festivos incluidos, sean nacionales o autonómicos.

12x5 → 12 horas (De 7:00 a 19:00), De lunes a viernes. Festivos excluidos, tanto los nacionales como los autonómicos.

4.2. 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 Aguas de Barcelona, actualmente BMC Remedy. Aguas de Barcelona 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 acuerdos 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.

4.3. 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	95%	0,25 horas	1 hora
	alta	24x7	95%	0,5 horas	6 horas
	media	24x7	95%	4 horas	20 horas
	baja	24x7	95%	8 horas	55 horas
no Productivo	alta	12x5	95%	0,5 horas	6 horas
	media	12x5	95%	4 horas	20 horas
	baja	12x5	95%	8 horas	55 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	objetivo
productivo	24x7	99,99%
no Productivo	12x5	99,90%

El objetivo aquí es el porcentaje de disponibilidad mínima de los sistemas gestionados, medido mensualmente y calculado dentro del horario indicado.

Compromisos por la gestión de peticiones de servicio

entorno	tipo Petición	prioridad	horario	T. Resolución	objetivo
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.*

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. La facturación se realizará 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 incidencias.
- No son aplicables a las tareas evolutivas periódicas que se definan como incluidas dentro del servicio, como la aplicación de parches de SO y actualización de aplicaciones base.
- Hay un conjunto de tareas simples que obligatoriamente deben considerarse simples: provisión de un servidor virtual "virgen" (sin aplicaciones que no aparezcan en la plantilla base), gestión de altas, bajas y modificaciones de permisos y usuarios ... Esta lista se definirá en detalle a la fase de kick -off.

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**	**objetivo**
Petición No Simple	3 días laborables	99,99%
Proyecto (> 1 Semana)	2 semanas	98,99%

4.4. Cumplimiento de los Acuerdos de Nivel de Servicio

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 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 por requerimiento del creador del ticket o de los responsables de AB.

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 ANSs, se establecen un conjunto de sanciones de penalización en la siguiente tabla:

				ANS y penalizaciones requeridos		
código	**Descripción**	**métrica**	**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 actas aceptadas por parte de las áreas responsables del servicio por parte de AB sin enmiendas o iteraciones en su elaboración	mensual	95% actas aceptadas en primera instancia	75% actas aceptadas en primera instancia	2,00%

ANS Gestión Operativa						
GO_001	Gestión del Inventario	Porcentaje máximo de errores detectados en la CMDB e inventarios	mensual	1,00%	3,00%	5,00%
GO_002	Disponibilidad del servicio de los Sistemas Críticos	Se medirá la disponibilidad agregada de los Sistemas Productivos Críticos contabilizando el tiempo de interrupción de esta (sin incluir las ventanas de mantenimiento pactadas de forma previa con AB)	mensual	99,99%	99,00%	10,00%
GO_003	Disponibilidad del servicio de los Sistemas No Críticos	Se medirá la disponibilidad agregada de los Sistemas Productivos No Críticos contabilizando el tiempo de interrupción de esta (sin incluir las ventanas de mantenimiento pactadas de forma previa con AB)	mensual	99,90%	99,00%	3,00%
GO_004	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_005	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%	10,00%
GO_006	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%	5,00%

GO_007	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_008	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%	2,00%
GO_009	Reapertura de Incidencias	Porcentaje de incidencias reabiertas responsabilidad del adjudicatario	mensual	1,00%	5,00%	5,00%
GO_010	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%	5,00%
GO_011	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_012	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%	2,00%
GO_013	Reapertura de Peticiones	Porcentaje de peticiones reabiertas responsabilidad del adjudicatario	mensual	1,00%	5,00%	3,00%
GO_014	Corrección de vulnerabilidades de servidores.	Porcentaje vulnerabilidades corregidas en un tiempo igual o inferior a 3 meses desde su detección	mensual	90,00%	80,00%	6,00%
GO_015	Actualizaciones de parches de sistema operativo	Porcentaje de servidores parcheados con los parches que periódicamente vaya publicando el proveedor de cada uno de los sistemas operativos.	mensual	90,00%	80,00%	6,00%

GO_016	Restauración de backups	Porcentajes de backups restaurados con éxito	trimestral	100,00%	99,50%	8,00%
GO_017	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%	3,00%
GO_018	Cumplimiento en fechas de entrega en proyectos	Desviación temporal respecto a las fechas de entrega establecidas en los proyectos	trimestral	3 días	9 días	3,00%
						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 <= 10% → Penalización = **0%**
  - SPVL > 10% **O** SPVO> 20% → Penalización = Máximo (SPVL**, 5%)**

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"

4.5. Desarrollo de nuevas funcionalidades

Tal como se ha definido en el apartado 2, el servicio incluirá un sistema tarifario y de facturación para el desarrollo de nuevas funcionalidades y procesos periódicos de mantenimiento.

Al inicio del servicio se establecerán tarifas para cada tipo de técnico que pueda intervenir en estos desarrollos (jefe de proyecto, técnico nivel 2 Windows, técnico nivel 2 monitorización...). Estas tarifas permanecerán invariables durante todo el contrato.

El consumo de horas se realizará mediante estas vías:

- *Peticiones comunicadas mediante ticket y consideradas "no simples":* peticiones que quedan fuera del servicio porque la valoración de esfuerzo realizado 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 sacar adelante contra las horas de este servicio. Cada presupuesto incluirá al menos una descripción de los trabajos a realizar, compromisos de hitos intermedios 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.

4.6. Documentación

El Prestador del Servicio se compromete a mantener documentación actualizada sobre las infraestructuras 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.

- El Prestador del Servicio deberá mantener en todo momento información detallada y suficiente para la reinstalación completa de cada servidor, incluyendo:
  - Sistema Operativo y versión
  - Configuraciones del sistema y del software base
  - Configuración de almacenamiento, redes, etc.
  - Pasos instalación software base y middleware necesario

4.7. Especificaciones de RGPD y SEGURIDAD

Los desarrollos realizados y entregados deberán cumplir con el Reglamento (UE) 2016/679, General de Protección de Datos ("RGPD"). La empresa adjudicataria deberá identificar todos aquellos puntos que puedan vulnerar el RGPD, resolverlos y presentar las evidencias conforme cumplen con el mismo.

En cualquier caso, a los efectos de dar cumplimiento a la normativa en materia de protección de datos y dada la condición de "Encargado de tratamiento de datos personales" por cuenta de AB que ostentaría el prestador del servicio durante la ejecución del Contrato, previamente a la adjudicación del Contrato, AB requerirá únicamente al licitador que haya presentado la proposición económicamente más ventajosa al efecto de que remita debidamente cumplimentado, de acuerdo con la normativa mencionada, que acompaña al presente Pliego.

Asimismo, durante la ejecución del Contrato se deberán observar por parte del adjudicatario las medidas de seguridad que constan en la Anexo nº 5 del Pliego de Condiciones Particulares.

4.8. Idioma del servicio

El servicio deberá ser prestado en catalán y castellano. Las respuestas que se realicen, tanto por escrito como por voz, deberán hacerse en el idioma utilizado en la creación de la incidencia o petición.

4.9. Facturación del servicio-Gestión Proactiva, Reactiva, Evolutiva, administrativa

Se *solicita un precio mensual por (servidor Físico/Virtual/Cloud) gestionado*. Por lo tanto, el número de servidores a tener en consideración son los correspondientes al volumen anual estimado que se detalla en el apartado 2.1. del presente pliego.

El mismo criterio se aplicará para el resto de los elementos incluidos en el servicio: cabinas de disco, software en general. Para todos se deberá especificar un precio mensual.

Las tarifas deben estar estructuradas en base a la tipología siguiente:

Tarifario servidores OT-AB por Tipología

Fis/ Vir / Clo	SO	Entorno	Horario	Criticidad	Tarifa mensual
físico	ESX / Hyper -V	producción	24x7	crítico	€
físico	Linux	producción	24x7	crítico	€
físico	Linux	NO Producción	laboral	no Crítico	€
físico	Windows	producción	24x7	crítico	€
físico	Windows	NO Producción	laboral	no Crítico	€
virtual	Linux	producción	24x7	crítico	€
virtual	Linux	NO Producción	laboral	no Crítico	€
virtual	vCenter	producción	24x7	crítico	€
virtual	Windows	producción	24x7	crítico	€
virtual	Windows	NO Producción	laboral	no Crítico	€
Cloud	Linux	producción	24x7	crítico	€
Cloud	Linux	NO Producción	laboral	no Crítico	€
Cloud	Windows	producción	24x7	crítico	€
Cloud	Windows	NO Producción	laboral	no Crítico	€

Tarifario Cabinas Disco

Entorno	Horario	Criticidad	Tarifa mensual
producción	24x7	crítico	€

Tarifario instancias BBDD y Servidores de Aplicaciones

Tipo	Instancia	Entorno	Horario	Criticidad	Tarifa mensual
BBDD	Microsoft SQL	NO Producción	laboral	no Crítico	€
BBDD	Microsoft SQL	producción	24x7	crítico	€
BBDD	MySQL	NO Producción	laboral	no Crítico	€
BBDD	MySQL	producción	24x7	crítico	€
BBDD	PostgreSQL	NO Producción	laboral	no Crítico	€
BBDD	PostgreSQL	producción	24x7	crítico	€
BBDD	Oracle	NO Producción	laboral	no Crítico	€
BBDD	Oracle	producción	24x7	crítico	€
servidor de aplicaciones	Apache	NO Producción	laboral	no Crítico	€
servidor de aplicaciones	Apache	producción	24x7	crítico	€
servidor de aplicaciones	IIS	NO Producción	laboral	no Crítico	€
servidor de aplicaciones	IIS	producción	24x7	crítico	€
servidor de aplicaciones	Tomcat	NO Producción	laboral	no Crítico	€
servidor de aplicaciones	Tomcat	producción	24x7	crítico	€
servidor de aplicaciones	JBoss	NO Producción	laboral	no Crítico	€
servidor de aplicaciones	JBoss	producción	24x7	crítico	€

El servicio que cubre las gestiones Proactiva, Reactiva, Evolutiva y Administrativa se facturará por mensualidad vencida, aplicando los precios unitarios ofertados por el adjudicatario para cada uno de los servidores incluidos en el inventario en el momento de cerrar la facturación de cada mes.

A efectos de facilitar el cierre de las facturaciones mensuales se considerarán nuevos elementos facturables aquellos que hayan sido introducidos en el servicio antes del día 15 del mes a facturar. Aquellos que hayan sido introducidos el día 16 en adelante comenzarán a aparecer en la facturación el mes siguiente.

También a efectos de facilitar el cierre de las facturaciones mensuales se considerarán elementos eliminados aquellos que hayan sido retirados del servicio antes del día 15 del mes a facturar. Aquellos que hayan sido retirados del día 16 en adelante serán retirados del servicio en la facturación del mes siguiente.

El Prestador del Servicio permitirá la entrada o salida de elementos en el servicio en cualquier momento, siempre a demanda del personal autorizado de AB sin que ello suponga coste adicional para AB.

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.

4.10. Facturación del servicio - Desarrollo de nuevas funcionalidades

El importe estimado para estos servicios se consumirá de la bolsa de horas anual estimada de 480 horas mediante la realización de trabajos derivados de los proyectos y tareas consideradas no simples previamente autorizadas por los responsables de AB.

En caso de otros tipos de proyectos se recogerán bajo una bolsa de horas independiente y se aplicarán los mismos precios.

Se facturará aplicando la dedicación efectivamente prestada por cada uno de los técnicos asignados a cada proyecto en base a los precios/hora ofertados por el adjudicatario.

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	**Valores requeridos**
Jefe Proyecto	**Laboral 24x7**
Técnico sistemas (cualquier tecnología)	
Técnico sistemas Cloud (PaaS, IaaS)	
Técnico IN-SITU	
Técnico Micro A	
Traslados	

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.

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 en las reuniones de inicio del servicio.

5. Transición del servicio

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

Se definirán al menos 3 fases:

- **Prestación actual:** en esta fase opera el servicio el actual Prestador del Servicio.
- **Transición:** período que va entre la entrada en vigor del contrato y asunción del control del servicio por parte del nuevo Prestador del Servicio. Durante la transición el nuevo Prestador del Servicio deberá cubrir las siguientes actividades:
    - *Due Diligence*: a 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*: se 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 los servicios con los que interactúe. Durante la fase de transferencia el anterior Prestador del Servicio continuará realizando la prestación con los ANS comprometidos en el contrato.
    - *Implantación*: se 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 transición tendrá una duración máxima de 3 meses.

6. 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 requirieran el actual Prestador del Servicio deberá prestar el servicio de la misma manera que en la fase de prestación estable durante un plazo máximo de 6 meses desde la citada comunicación sin coste adicional.

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.

7. Terminación del servicio

3 (tres) 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.

8. 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.

" NORMAS DE SEGURIDAD IT DE AGUAS DE BARCELONA"

ÍNDICE

1. Objeto e introducción del documento

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

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

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

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

El intercambio se realizará respetando la clasificación y el etiquetado de la información que se haga durante dicho intercambio.

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

En los acuerdos se establecerán 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.

En estos acuerdos se indicará 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, con las de cifrado indicados anteriormente o el uso de soluciones de no repudio, con el fin 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 manera 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 procesa, 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 requieran para el ejercicio de sus funciones, y puedan existir diferentes niveles de derechos de administración.

Se deberán limitar los servicios en red abiertos en los diferentes sistemas de información. La configuración de los servicios en red activos se regirá por el siguiente principio: "se prohíbe todo lo que no se encuentre explícitamente permitido", o lo que es lo mismo, hay que desactivar todos los servicios en red que se activan por defecto durante la instalación y en que su uso no se encuentre 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 AB o que utilicen algoritmos de encaminamiento dinámicos, deberán usarse mecanismos de autentificación mutua basados en claves pre-compartidas, certificados digitales y 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 archivos 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 este usuario administrador viajen cifradas por la red de comunicaciones utilizando 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 archivos temporales en servicios centrales y sistemas de información de AB, que corrige posibles errores que aparezcan durante el proceso de borrado de ficheros temporales. El tratamiento de estos ficheros temporales se ajustará a lo dispuesto en las normativas legales vigentes en materia de protección de datos de carácter personal (LOPD).

4. Identificación y autentificación de usuarios

Todos los sistemas de información no públicos de las unidades y sociedades operativas de AB deberán disponer de mecanismos que verifican la identidad de los usuarios que los utilizan, de tal manera que se restringen los recursos a los que deben 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 diferentes sistemas a través de su identificador, salvo las excepciones del apartado "Identificación de usuario".

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

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

La autentificación, normalmente, se realizará mediante el uso 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, excepto 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 se deberá comunicar inmediatamente al Jefe de Seguridad de la Información de la entidad a la que pertenezca.

Cuando la criticidad del servicio o recurso lo requiera, la Organización de Seguridad de la Información promoverá el uso de mecanismos de autentificación 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 del usuario debe ser re-autentificado, en caso de que sea posible técnicamente.

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 de la ID 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 de este. 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 estos 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 AB 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 como la persona física.

El acceso a cualquiera de los sistemas de información de AB 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 ejercida 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 AB con independencia de los cambios de destino o de categoría que puede tener o, incluso de baja; y de acuerdo con la legislación vigente en materia de protección de datos de carácter personal.

Las personas que no pertenecen a la plantilla de trabajadores de AB 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 AB deben otorgarse solamente por el periodo de tiempo estrictamente necesario y deberán ser revaluados periódicamente.

No estará permitida la creación o utilización de usuarios genéricos excepto en aquellos casos en los que sea estrictamente necesario por razones operativas, funcionales, etc., que, por su naturaleza, aconsejan u obligan al uso de estos 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 conocen, en todo momento, el grupo de usuario que lo utilizan. Cuando la necesidad de usar 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 uso del usuario genérico más allá de sus necesidades.

Asimismo, excepto en situaciones justificadas por el ejercicio de las funciones, cada persona física tendrá asociado un único identificador de usuario. Como excepción, un usuario podrá disponer de más de un identificador de usuario en caso de que los privilegios asignados a cada uno sean diferentes y técnicamente no sea posible recoger todos los privilegios en un solo

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, estas deberán cumplir una serie de requisitos a la hora de la generación de estas.

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 coincide 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 el cambio de esta 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 disponga 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 desactivar el identificador asociado hasta su inicialización o desbloqueo.

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

- Restringir, individualizar, registrar, controlar y, eventualmente, bloquear el acceso a la información ya las aplicaciones.
- Proteger la información y las aplicaciones de accesos realizados por personal no autorizado.
- Autentificar a todos los usuarios antes de que estos 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 de la siguiente manera:
    - Almacenando el resumen o "hash" generado con algoritmos estándares 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 tratan.

- 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. Exceptuando 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 autentificación más seguro.

7. Comunicación de los incidentes de seguridad

En el 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 AB deberá ser informada con la mayor brevedad posible a través de las líneas de comunicación que se establecerán previamente con este propósito.

La Dirección de Seguridad se encargará de iniciar un informe con las figuras, escogidas entre aquellas que previamente habían sido identificadas, la cual su 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 por AB.

Se deberán reportar aquellos incidentes significativos a los niveles jerárquicos superiores establecidos con el fin de obtener autorizaciones o de informar sobre la actuación de AB en frente de incidentes de seguridad.

El reporting de información sobre incidentes de seguridad quedará restringido únicamente a aquellas personas absolutamente necesarias. Cualquier divulgación de esta 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 el fin de detectar una posible divulgación no autorizada.

Tanto los empleados de las entidades de AB como los trabajadores de empresas externas conocerán las líneas de reporting 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.