PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL

SERVICIO DE MANTENIMIENTO CORRECTIVO Y EVOLUTIVO PLATAFORMA BI

N. º EXP.: AB/ABAST/2020/09

PROCEDIMIENTO ABIERTO

Índex

1. OBJETO

El presente Pliego de Prescripciones Técnicas (en adelante, PPT) establece las prescripciones técnicas que rigen el procedimiento de contratación para el Contrato de servicios de Business Intelligence de Aguas de Barcelona (AB), 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. INTRODUCCIÓN

El objeto de la presente solicitud de oferta es la selección de un adjudicatario para la provisión de los servicios profesionales de soporte, mantenimiento y desarrollo de los distintos entornos analíticos que forman parte del área Business Intelligence de AIGÜES DE BARCELONA, tal y como se detalla en el catálogo de Servicios (párrafo 4).

La unidad de inteligencia de negocio, por su transversalidad, proporciona información para la toma de decisiones a varios departamentos, sobre todo al área técnica y al área comercial, utilizando una arquitectura mixta constituida por un entorno Big data en la nube Azure y un entorno de BI más tradicional "on premise".

Dada la complejidad del entorno, el adjudicatario deberá disponer de recursos profesionales expertos en varias tecnologías de distinta naturaleza, que se detallaran en el siguiente apartado (párrafo 3).

3. ESPECIFICACIONES DEL ENTORNO Y DESCRIPCIÓN TÉCNICA

3.1 Entorno Big Data

3.1.1 Premisas

La arquitectura que a continuación se presenta se propone como objetivo soportar desde el punto de vista tecnológico las diferentes fases del proyecto, actualmente en curso, para la implementación de un sistema analítico sobre los datos de telelectura: desde la recogida de los datos de los ficheros que contienen las lecturas y su ingestión, pasando por preparación de los datos y la aplicación de la lógica necesaria para el cálculo de los ratios necesarios, hasta la explotación a través de las herramientas de BI.

3.1.2 Arquitectura Big Data Azure

3.1.2.1 Descripción general

La arquitectura para el proyecto MDM – Meter data Management (Telelectura) se basa en la implantación de un sistema Big Data sobre Microsoft Azure.

Dentro del marco Azure Cloud se han elegido los componentes básicos para posibilitar la capacidad de ingesta, procesamiento y análisis de los datos de tele lectura, que si bien tienen un formato estructurado, exceden la capacidad de procesamiento de los sistemas convencionales de bases de datos.

3.1.2.2 Fases del procesamiento y componentes básicos

A continuación, se explica desde una visión de muy alto nivel cuales son las fases principales del procesamiento de los datos de telelectura y cuales los componentes que han sido seleccionados para dar respuesta a los requerimientos del proyecto.

ORIGEN DE DATOS: El proveedor encargado de proporcionar las lecturas dejará los ficheros, a medida que se vayan generando, en un Blob Storage dentro del área de Staging del Cloud Azure propiedad de Aguas de Barcelona.

INGESTA: Azure data Factory V2: este componente de integración de datos permite la ingestión de datos batch, independientemente de su formato (estructurado o no) y de su localización (locales o en la nube). Permite la conexión a una amplia variedad de orígenes de datos. Debido a sus características es la solución elegida para la actividad de intercambio de datos entre los almacenes de datos locales y la nube.

ALMACENAMIENTO: La solución elegida para el almacenamiento de los ficheros de telelectura es Azure Blob Storage. Su capacidad de almacenamiento de datos estructurados pero sobre todo no estructurados representa una ventaja en términos de flexibilidad porqué permite no solo cumplir los requerimientos de este proyecto sino también estar preparados para la ingestión de macrodatos con formato distinto en el futuro.

Además, se contará con Azure Cosmos DB como repositorio de almacenamiento optimizado para ser consultados mediante consultas atómicas.

PROCESAMIENTO: una vez que los macrodatos estén almacenados en el Blob storage será tarea de Databricks preparar y si es necesario entrenar los datos para que puedan ser llevados al EDW. AB usa SQL y Phython para la programación de este componente.

SQL DWH: como solución de almacenamiento de datos agregados en la nube se usará Azure Synapse Analytics (anteriormente SQL Data Warehouse)

ANALISIS E INFORMES: Los usuarios de AB dispondrán de un entorno de consulta de los datos contenidos en el repositorio. Para el acceso en consulta a los datos (en sólo lectura) por parte de los usuarios internos a AB, se usará un visor de datos web. Ésta web servirá para facilitar a los usuarios el acceso a consultas operacionales de máximo detalle.

NOTA: el mantenimiento y los servicios evolutivos sobre aplicaciones móviles, aplicaciones web y extracciones no forman parte de los requerimientos del presente pliego y se licitarán en un pliego separado. Es evidente que al formar parte del entorno Big data será necesaria la máxima colaboración del adjudicatario para proporcionar a AB el soporte requerido para la investigación y resolución de eventuales incidentes.

Para las consultas agregadas de análisis, se usará la herramienta de reporting corporativa de Aguas de Barcelona, Microstrategy 2019, que se encontrará ya instalada y licenciada en el entorno Azure. Microstrategy atacará directamente a las tablas relacionales de Azure Synapse Analytics.

ORQUESTACIÓN: Se usará Azure data Factory V2 visto que su integración con otros servicios incluidos en Azure hace aconsejable su uso como herramienta de orquestación

3.2 Entornos

En el cloud Azure convivirán tres entornos:

- Desarrollo: es el entorno para llevar a cabo las tareas de desarrollo, prueba y depuración
- Preproducción: entorno para las pruebas de releáse y aceptación de los usuarios validadores
- Producción: entorno accesible por el usuario final donde se ejecutarán todos los procedimientos desarrollados

3.3 Entorno On premise

3.3.1 Descripción funcional Datamarts

El actual Área de BI se compone de Datamarts de ámbito técnico y comercial.

3.3.1.1 Área Técnica AB

3.3.1.1.1 DM Xarxes (XADM)

Datamart que tiene por objetivo el control y análisis de la infraestructura de redes incluyendo su evolución y seguimiento. Se recopilan y preparan datos cuantitativos y cualitativos de determinados elementos físicos de red, datos de red instalada y retirada, y datos de Activos Fijos.

3.3.1.1.2 DM Instal·lacions Interiors (DMII)

Datamart que recoge la información necesaria para el control que el departamento de Suministros realiza sobre las instalaciones, suministros, contadores, cambios de equipos, verificaciones, estado del parque, etc.

Su objetivo es recoger toda la información del estado y de los cambios del parque de contadores y los suministros, durante el periodo. Información cuantitativa y cualitativa. Una vez consolidada, se elaboran informes de estado, seguimiento y control, y los indicadores de compañía y del Acuerdo Marco.

3.3.1.1.3 DM Tècnic Subministraments

Datamart que permite cubrir las necesidades de Suministros para realizar un seguimiento del proceso de lecturas de contadores. Actualmente hay tres empresas externas que se encargan de leer y exportar los datos leídos hacia el SIC. El Datamart permite facilitar el control de las lecturas previstas, así como las ausencias y las incidencias por no lectura.

3.3.1.1.4 DM Territorial

Este Datamart, también llamado de Operaciones Territoriales, tiene por objetivo analizar las operaciones realizadas sobre el territorio: operaciones sistemáticas, trabajos urgentes, órdenes de ramal nueva creación, averías exteriores, mantenimiento preventivo, etc.

A parte de las funcionalidades propias del Datamart, desde este Datamart se traspasa cada mes a SAP (CO) el número de operaciones realizadas por cada Gerencia (solo las externas al SAP/PM).

3.3.1.1.5 DM Consumos Facturados

Datamart cuyo objetivo es el estudio del agua consumida por ramal, según diferentes criterios geográficos (gerencia, municipio, distritos), hidráulicos (sector hidráulico, piso de presión) o propios del suministro (uso del agua). En paralelo, el Datamart de Sectorización estudia el agua entregada a la red. La comparación permite estudiar el rendimiento de la red y la detección de fugas o fraudes.

El Datamart envía mensualmente datos de consumos al Sistema Información Centro Control Operativo (SICCO).

3.3.1.1.6 DM SICCO

El Sistema de Información del Centro Control Operativo (SICCO) es una solución que permite tener una visión global de toda la información consolidada del Área Técnica.

Se constituye de varios universos construidos en Business Objects y de dos cuadros de Mando construidos en Xcelsius.

Desde el Datamart SICCO actualmente se dispone de interfaces con sistemas externos como el ACA, AMB o SMC.

3.3.1.2 Área Comercial AB

3.3.1.2.1 DM Volum Facturat Client

Este Datamart tiene por objetivo proporcionar un entorno analítico que permita al usuario clasificar los clientes a partir de una segmentación y poder al mismo tiempo analizar la facturación (consumo y volumen) para diferentes dimensiones de estudio, llegando hasta el código de factura. Incluye facturas originales, facturas anuladas, facturas sustitutivas (corrección de errores) y, también, facturas canceladas.

Dispone del detalle de todas y cada una de las facturas del mes.

También permite realizar simulaciones de Tarifa.

3.3.1.2.2 DM Recaptació

Este Datamart puede considerarse dos Datamart: "Recaudación" e "Impagados, Cartas y Morosos". El primero tiene como objetivo analizar la cartera de facturas pendientes al final de cada mes. El segundo permite analizar todas las acciones realizadas durante el mes para la gestión de facturas impagadas.

Por lo tanto, gestiona la situación de las pólizas de morosos, de las pólizas de impagados, de las facturas vivas cada final de mes y de las que han entrado en situación de fin de gestión durante el último mes.

3.3.1.2.3 DM Estadístiques

Datamart que tiene por objetivo analizar la información de los contratos de suministro en vigor el último día del mes natural. Se considera la 'fecha de alta' del subministro y la posible 'fecha de rescisión' del mismo. En la base de datos operacional es posible que el día 1, 2, 3,.. dar de alta un subministro con fecha de alta del mes anterior, y lo mismo para las fechas de rescisión. Incluye información de los contadores instalados.

3.3.1.2.4 DM ALGOL

Datamart que tiene por objetivo analizar los siguientes ámbitos de atención al Cliente: Contactos, Contratación, Clientes y Requerimientos (Consultas, Solicitudes y Reclamaciones comerciales y técnicas).

El Datamart proporciona información de Clientes (sensibles y/o singulares) a SICCO, con una frecuencia diaria.

3.3.1.2.5 DM OFEX - Tancaments

El Datamart de OFEX está orientado a la consulta de la información relacionada con los cierres o interrupciones del suministro de agua y la comunicación de estos a los usuarios. Esta información se obtiene principalmente de Siebel y SAP.

El objetivo de la información de gestión contenida en el Datamart de OFEX es:

- Hacer el seguimiento de los cierres y la afectación a los clientes
- Hacer el seguimiento del funcionamiento del gestor de mensajes en los procesos de comunicación al cliente
- Monitorizar el proceso asociado a las actividades de cierre

3.3.1.3 Entorno analítico de la Dirección de sistemas de Información

3.3.1.3.1 Cuadro de Mando Ticketing

Entorno analítico para el seguimiento y control de incidencias y solicitudes de aplicación extraídas del "REMEDY". El análisis se realiza utilizando dimensiones temporales, organizativas y determinados niveles definidos en la aplicación de ticketing Remedy.

Este cuadro de mando se ha desarrollado en Power BI.

3.3.1.4 Interface envío a Sistemas Externos

3.3.1.4.1 Agencia Catalana del Agua (ACA)

Desde el DM SICCO se envían diariamente mediante procesos planificados de Talend:

- Información horaria de SJD Superficial y SJD Subterráneo
- Información de variables de producción con carácter diaria
- Información de Sondeos y Pozos con carácter semanal

3.3.1.4.2 Área Metropolitana Barcelona (AMB)

Con origen en DM SICCO, Volumen Facturado y Estadísticas y mediante procesos planificados de Talend se envía la siguiente información:

- Variables de SICCO (aportaciones, sondeos...)
- Nº suministros
- Nº aforos
- Volumen Facturado

3.3.2 Herramientas y aplicativos del servicio

A continuación se enumeran las principales herramientas, aplicaciones y tecnologías que el prestador del servicio deberá conocer para llevar a cabo sus funciones:

- **Reporting**
- Plataforma MicroStrategy 2019 (11.1): es la herramienta de reporting corporativa de AB
- Plataforma Business Objects: solución completa de SAP Business Objects versión XI R2 *(InfoView, Xcelsius)*. Es una versión obsoleta, por lo tanto, no habrán desarrollos nuevos sobre esta herramienta, sólo mantenimiento.
- Power BI: De momento el uso de PWBI es reducido y actualmente sólo existe un Datamart de la Dirección de sistemas para la gestión de la herramienta de ticketing.
- **Herramientas procesos ETL**
  - PL/SQL
  - Talend: es la solución ETL corporativa
  - DataStage: es una versión muy antigua, hay numerosos Jobs desarrollados, sin embargo, no se prevén nuevos desarrollos. Todos los Jobs de Datastage se migrarán en el futuro a Talend.
  - COBOL

- **Base de datos:**

Oracle 11G. En la actualidad, en paralelo a los Datamarts descritos, existe un esquema de BBDD que constituye el núcleo del futuro DWH de BI, y donde en este momento se está desarrollando un **nuevo Datamart para el análisis del proceso de cobro e impagados, que también se incluye en el alcance del servicio.**

- **Otras Aplicaciones**

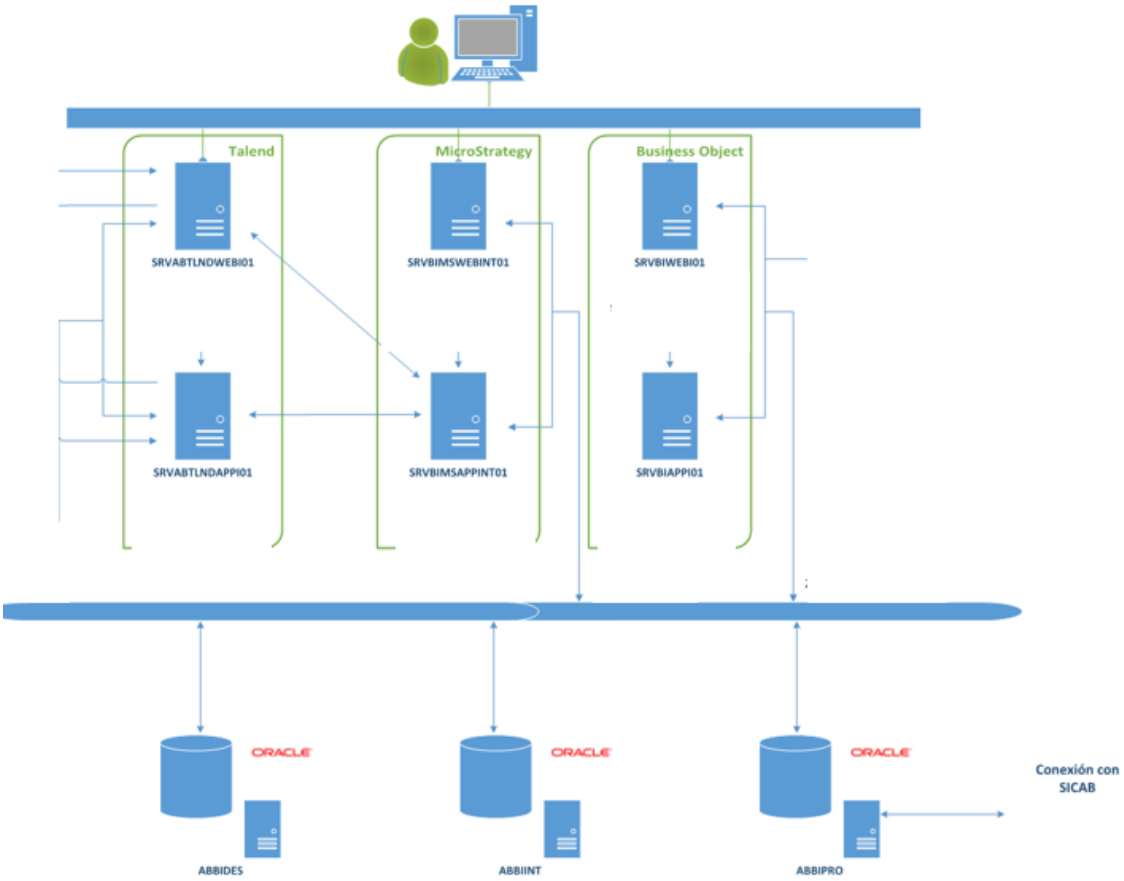
Hay dos aplicaciones Java de Entrada Manual de datos, complementarias a los distintos Entornos Analíticos.

- **Polar**: aplicación de entrada manual de datos, aplicación J2EE utilizando como Framework Struts. Utiliza la versión de java 1.4 y compatible con 1.7
- **Piccolo** tiene como objetivo principal ser una aplicación que realice extracciones de información de georeferencia e hidráulica de los sistemas SIGAB-SAP y cruzarla con información de los Datamarts Técnicos con el objetivo de realizar simulaciones y enviar los resultados hacia la aplicación PICCOLO. Utiliza tecnología Java con gráficas Highchart.

3.3.2.1 Entornos de trabajo

A continuación se aporta una visión de alto nivel del entorno de trabajo de integración, siendo desarrollo y producción entornos similares. . La administración de los servidores no forma parte de los servicios requeridos en este pliego

Entorno Integración


Talend
MicroStrategy
Business Object
SRVABTLNDWEBI01
SRVBIMSWEBINT01
SRVBIWEBI01
SRVABTLNDAPPI01
SRVBIMSAPPINT01
SRVBIAPPI01
ORACLE
ORACLE
ORACLE
Conexión con SICAB
ABBIDES
ABBIINT
ABBIPRO

Relación de servidores

Herramienta	*Entorno*	*Entorno AB*
BBDD	Producción	ABBIPRO
	Integración	ABBIINT
	Desarrollo	ABBIDES
BO	Producción	SRVBIWEBP01
	Producción	BI-WEB
	Integración	SRVBIAPPI01
	Integración	SRVBIWEBI01
	Desarrollo	SRVBIAPPD01
MSTR	Producción	srvbimswebpro01
	Producción	SRVBIMSAPPPRO01
	Integración	SRVBIMSAPPINT01
	Integración	SRVBIMSWEBINT01
	Desarrollo	srvbimsappdes01
MSTR cloud	Producción	------
	Integración	------
	Desarrollo	------
Metadatos Micro	Producción (on premise)	MICROSTR_94
	Integración (on premise)	MICROSTR_94
	Desarrollo (on premise)	MICROSTR_D_94
	Producción (cloud)	--------
	Integración (cloud)	--------
	Desarrollo (cloud)	--------
Talend	Producción	SRVABTLNDAPPP01
	Producción	SRVABTLNDWEBP01
	Integración	SRVABTLNDAPPI01
	Integración	srvabtlndwebi01
	Desarrollo	SRVABTLNDAPPD01
	Desarrollo	SRVABTLNDWEBD01
DataStage	Producción	srvdsdes01

3.3.3 Acceso

El acceso del proveedor a los sistemas de información de Aguas de Barcelona se realizará mediante conexión VPN a una infraestructura de escritorios virtuales (VDI) proporcionada por AB.

Todos los trabajadores que tengan que trabajar en el proyecto tendrán usuarios personalizados en los sistemas necesarios. A tal efecto se deberá proporcionar al inicio del proyecto nombre, apellidos y DNI/NIE de los mismos.

Es necesario prever un periodo de unos 15 días como máximo para la configuración de los accesos necesarios.

4. CATALOGO DE SERVICIOS

4.1 Administración y mantenimiento de las herramientas del Servicio

El proveedor deberá de administrar, configurar y mantener las herramientas de carga (Talend y DataStage) y explotación del dato (Microstrategy, BO) como los servicios Azure descritos en el entorno Big data, así como herramientas o interfaces relacionadas con la operativa habitual de entrada o envío de datos.

Esto implica también hacer los "upgrades" de versión menor de las mismas.

4.2 Actualización periódica de los datos

En general, el proveedor deberá velar por el funcionamiento de todas aquellas herramientas, tecnologías y servicios implicados en el proceso de extracción, transformación, almacenamiento y explotación de los datos con fines decisionales, aunque no se nombren de forma explícita en este documento.

El objetivo final es la disponibilidad en tiempo y forma de la información decisional, llevando a cabo los procesos de carga periódicos establecidos para ello. La mejora continua de los procesos de carga de los datos actualizados es la prioridad operativa principal de cualquier sistema de información de negocio y el proveedor deberá prestar especial atención a este punto, con un objetivo de mejora continua.

4.3 Mantenimiento correctivo

Se entiende por mantenimiento correctivo aquella actuación encaminada al diagnóstico y la resolución de errores, funcionamientos indebidos o comportamientos no deseados de los sistemas productivos, incluidos problemas de rendimiento de las aplicaciones.

La corrección de los defectos funcionales y técnicos de las aplicaciones por el servicio de mantenimiento correctivo incluye:

- Análisis del error/problema.
- Análisis funcional y técnico de la solución.
- Desarrollo de las modificaciones a los sistemas (programación y/o configuración), incluyendo pruebas unitarias documentadas.
- Mantenimiento de la documentación técnica y funcional del sistema.

4.4 Mantenimiento preventivo

El mantenimiento preventivo está enfocado a la prevención de errores en las aplicaciones, y/o en la optimización del rendimiento, de cara a aumentar la fiabilidad y la reducción de problemas en el futuro. Se basa en la información de gestión que se aporta periódicamente, de la que se extraen las conclusiones que permiten sugerir acciones encaminadas a la mejora continua.

El mantenimiento preventivo se integra, por tanto, dentro del ciclo de mejora continua, siendo un generador más de oportunidades de mejora.

4.5 Mantenimiento adaptativo

Modificaciones que afectan a los entornos en el que el sistema opera, por ejemplo cambios de configuración de la base de datos o cambios de algún parámetro del hardware o cambio de las interfaces con sistemas terceros.

4.6 Soporte a consultas operativas

Se entiende por consulta operativa, aquella consulta sobre el funcionamiento del Sistema o sobre algún resultado de alguno de los procesos ejecutados sobre el sistema que requiera justificación o aquellas que, habiendo entrado en primera instancia en el flujo de soporte como correctivos, queda posteriormente verificado que no responden a malos funcionamientos del sistema y, por tanto, no requieren de ninguna acción de desarrollo ni correctivo.

Aquellas consultas operativas que sustituyan tareas propias de usuario como cuadre de resultados, verificaciones de procesos, etc. podrán incluirse en el servicio bajo aprobación del responsable del servicio de AB.

4.7 Soporte a peticiones operativas

Se entiende por petición operativa, aquella solicitud de ejecución de una acción sobre una aplicación que no sea la resolución de una incidencia, el desarrollo de un evolutivo (Petición Funcional) y que no suponga tener que programar nueva funcionalidad en el código fuente de la aplicación. La gran mayoría de veces se trata de preparar scripts SQL para generar/modificar listados de datos o informes ad hoc para un análisis de datos.

4.8 Soporte presencial a procesos de negocio críticos

Se entiende por soporte presencial o "in situ" al soporte a consultas, incidencias o problemas propios de las aplicaciones o procesos de negocio descritos en la presente solicitud de Oferta.

En general no será necesario que el equipo funcional y técnico, o cualquier otro componente del equipo del adjudicatario se desplacen a las oficinas de AB, para realizar este tipo de soporte. No obstante, en el caso de que de forma extraordinaria sea necesaria ésta asistencia el adjudicatario deberá facilitarla.

4.9 Desarrollo Evolutivo menor

El desarrollo evolutivo cubre todas las incorporaciones, modificaciones y eliminaciones de nuevas funcionalidades en los sistemas y módulos funcionales ya sea por cambios debido a nuevas normativas legales o fiscales, o bien por nuevos requerimientos de negocio. Según el criterio de AB un desarrollo evolutivo no debería superar las 160 horas.

4.10 Desarrollo Evolutivo mayor

En el caso que puntualmente haya que realizar algún tipo de desarrollo evolutivo mayor (superior a 160 horas) por motivos legales, requerimientos de negocio o reducción del riesgo vinculado a la obsolescencia de herramientas usadas en el área BI (Datastage, BO) se considerará incluido en las obligaciones del adjudicatario del servicio, que deberá disponer de los perfiles adecuados para llevarlo a cabo.

5. MODELO DE GESTIÓN DEL SERVICIO

El servicio se estructurará en tres fases, a saber:

- Fase de Transición, en la que el adjudicatario adquirirá los conocimientos para el inicio de la actividad propia del servicio, descrita en los apartados anteriores.
- Fase de Operación, en la que el adjudicatario efectuará el servicio propiamente dicho, según las actividades descritas en los apartados anteriores.
- Fase de Devolución del Servicio. Tras la finalización del periodo acordado de prestación del servicio, se ejecutarán por parte del adjudicatario, las acciones que se definan en el comité de seguimiento del servicio, para la internalización y recaptura del conocimiento del sistema, a la Dirección de Aplicaciones IT de AB y/o al nuevo adjudicatario del servicio.

5.1 Fase de Transición del Servicio

La fase de transición es el periodo de tiempo que empieza en el momento en que el nuevo adjudicatario inicia las tareas para hacerse cargo del servicio y que por definición acaba cuando dicho servicio está estabilizado y el adjudicatario es autosuficiente para proveer los niveles de servicio solicitados. Este periodo no podrá en ningún caso exceder los dos meses de duración.

Se consideran propias de esta fase las siguientes actividades:

- Revisión de la documentación de las aplicaciones que forman parte del entorno objeto de esta propuesta.
- Identificación de los roles, usuarios y técnicos implicados.
- Revisión de las interfases de BI con otros sistemas corporativos.
- Validación del rendimiento y de la ejecución de los procesos de ejecución periódica
- Revisión del backlog de incidencias y evolutivos a fecha de la fase de transición.
- Revisión de la arquitectura de BI.
- Definición del Comité de Seguimiento.
- Elaboración del Informe de Situación de Recepción del Servicio por parte del adjudicatario.
- Celebración de la reunión de inicio con el resumen del conocimiento adquirido por parte del adjudicatario.

5.2 Fase de Prestación del Servicio

La fase de Prestación del Servicio es el periodo de tiempo que empieza inmediatamente después de la reunión de inicio de prestación del servicio (última actividad de la fase de transición) y que marca el momento en que el nuevo adjudicatario inicia las tareas para proveer los niveles de servicio solicitados. En esta fase, y a partir del conocimiento recopilado en la fase de transición, el adjudicatario desarrolla las actividades definidas como contenido del servicio.

En base al mantenimiento Correctivo, las tareas fundamentales a desarrollar serán:

- La recepción y diagnóstico de las incidencias existentes e identificadas, anteriores al inicio de la prestación del servicio, así como de todas las que vayan entrando al sistema de gestión utilizado en AB a partir del inicio de la actividad del adjudicatario.
- La resolución y seguimiento de las incidencias existentes e identificadas y de las nuevas en base a los términos del párrafo anterior.
- La realización de las pruebas de validación y de los correspondientes despliegues al entorno de pre-Producción de las versiones correctivas.
- La realización de las pruebas de validación y de los correspondientes despliegues al entorno de Producción de las versiones correctivas.
- Mantenimiento actualizado de la documentación afectada por la ejecución de los correctivos en la medida que corresponda.
- Seguimiento y planificación de prioridades con el responsable del servicio de AB.
- Generación de los informes definidos para el seguimiento del servicio.

En base al mantenimiento Adaptativo, las tareas propias son:

- Diagnóstico e identificación de las novedades legales y tecnológicas que puedan tener impacto sobre el Sistema, anteriores al inicio de la prestación del servicio, así como de todas las que vayan sucediendo a partir del inicio de la actividad del adjudicatario.
- La recepción, análisis y valoración de las peticiones existentes e identificadas, anteriores al inicio de la prestación del servicio, así como el análisis y valoración de todas las que vayan entrando al sistema de gestión utilizado en AB a partir del inicio de la actividad del adjudicatario, relacionadas con actualizaciones funcionales de mantenimientos y evolutivos de terceras aplicaciones corporativas conectadas con BI.
- Seguimiento y planificación de prioridades con el responsable del servicio de AB.
- La resolución y seguimiento de las propuestas y peticiones existentes e identificadas y de las nuevas en base a los términos de los puntos anteriores.
- La realización de las pruebas de validación y de los correspondientes despliegues al entorno de pre-Producción de las versiones correspondientes.
- La realización de las pruebas de validación y de los correspondientes despliegues al entorno de Producción de las versiones correspondientes.
- Mantenimiento actualizado de la documentación afectada por la ejecución de los desarrollos en la medida que corresponda.
- Generación de los informes definidos para el seguimiento del servicio.

En base al mantenimiento Preventivo y Perfectivo, las tareas propias son:

- Diagnóstico e identificación de las novedades legales y tecnológicas que puedan tener impacto sobre el Sistema, anteriores al inicio de la prestación del servicio, así como de todas las que vayan sucediendo a partir del inicio de la actividad del adjudicatario.
- Seguimiento y planificación de prioridades con el responsable del servicio de AB.
- La resolución y seguimiento de las propuestas y peticiones existentes e identificadas y de las nuevas en base a los términos del primer punto.
- La realización de las pruebas de validación y de los correspondientes despliegues al entorno de pre-Producción de las versiones correspondientes.
- La realización de las pruebas de validación y de los correspondientes despliegues al entorno de Producción de las versiones correspondientes.
- Mantenimiento actualizado de la documentación afectada por la ejecución de los desarrollos en la medida que corresponda.
- Generación de los informes definidos para el seguimiento del servicio.

En base al mantenimiento Evolutivo, las tareas propias son:

- La recepción, análisis y valoración de las peticiones existentes e identificadas, anteriores al inicio de la prestación del servicio, así como el análisis y valoración de todas las que vayan entrando al sistema de gestión utilizado en AB a partir del inicio de la actividad del adjudicatario.
- La resolución y seguimiento de las peticiones existentes e identificadas y de las nuevas en base a los términos del párrafo anterior.
- La realización de las pruebas de validación y de los correspondientes despliegues al entorno de pre-Producción de las versiones evolutivas.
- La realización de las pruebas de validación y de los correspondientes despliegues al entorno de Producción de las versiones evolutivas.
- Mantenimiento actualizado de la documentación afectada por la ejecución de los evolutivos en la medida que corresponda.
- Seguimiento y planificación de prioridades con el responsable del servicio de AB.
- Generación de los informes definidos para el seguimiento del servicio.

En base al Servicio de Soporte, las tareas que le dan contenido son:

- Control y seguimiento del servicio en general a partir de los tickets emitidos y recibidos, asignados al grupo de resolución correspondiente al sistema BI, en la plataforma de "ticketing" utilizada por AB.
- Mantenimiento y custodia de los entornos de trabajo asignados, asegurando la operativa de los entornos; Desarrollo, Pre-producción y Producción. En colaboración con terceros equipos designados por AB, implicados en estas tareas.
- Administración y configuración funcional del sistema en los ámbitos no delegados al usuario final.
- Soporte al usuario final en las consultas sobre funcionamiento de la plataforma.
- Soporte al mantenimiento de los módulos que componen la plataforma BI
- Seguimiento y planificación de prioridades con el responsable del servicio de AB.
- Generación de los informes definidos para el seguimiento del servicio.

5.3 Fase de Devolución del Servicio

La Fase de Devolución del Servicio comprende el mes anterior a la finalización del contrato, bien sea por finalización normal del contrato, como por resolución anticipada por cualquier motivo, siempre que sea procedente.

En la fase de Devolución se planifica y ejecuta el traspaso del servicio a la Dirección de Aplicaciones IT de AB y/o al nuevo adjudicatario.

En la fase de Devolución se deberá realizar el traspaso de toda la documentación y del conocimiento desde el adjudicatario al personal designado por AB

Los objetivos de esta fase son dos:

- La continuidad del servicio, generando el mínimo impacto en el usuario y en la operativa del sistema que debe mantenerse en los mismos términos de calidad de Servicio que lo rigen desde el inicio de la prestación.
- El traspaso del conocimiento generado por el adjudicatario durante la fase operativa a AB.

Se identifican las siguientes tres etapas a cubrir en esta fase:

- Planificación del traspaso.
- Operativa del traspaso.
- Garantía de soporte.

La fase de devolución o traspaso se ejecutará mediante una planificación de tareas acordadas entre AB y el adjudicatario. Los requisitos de esta fase para su inicio son:

- Identificación de los perfiles involucrados en el traspaso.
- Planificación de las tareas de traspaso, Calendario, Formación, Documentación, Acompañamiento.

Los puntos que se valorarán para aceptar el traspaso serán:

- Transferencia del conocimiento mediante la documentación y formación.
- Traspaso de responsabilidades y comunicación.
- Mantenimiento de la calidad del servicio durante la fase.
- Salida progresiva de recursos hasta la fecha de finalización de la prestación del servicio.
- Medidas de soporte posteriores a la fecha de finalización del servicio.

5.4 Dirección de los Trabajos

Corresponde a AB la supervisión, control y aprobación de los trabajos, a través de la designación de un Supervisor del Servicio.

El Adjudicatario designará un Coordinador de Servicio que asumirá las labores de interlocución con el Supervisor del Servicio nombrado por AB.

El Adjudicatario pondrá en conocimiento de AB cualquier eventualidad o decisión que redunde en una mayor rentabilidad y/o rapidez y orden de los trabajos, (Mantenimiento Perfectivo) no reservándose ningún tipo de información.

5.5 Equipo de Trabajo

El Adjudicatario aportará para la realización de los trabajos un equipo de trabajo multidisciplinar, integrado por lo menos por:

- Un Coordinador del Servicio con dedicación parcial y no inferior a un día a la semana (8 horas), responsable de la gestión y la coordinación del servicio, con al menos 2 años de experiencia como jefe de proyecto o responsable de servicios. Se valorará la disponibilidad de asistir semanalmente a reuniones de seguimiento de forma presencial.
- Al menos 1 consultor con certificación en Talend y experiencia mínima de dos años en desarrollos con herramientas ETL.
- Al menos 1 consultor con certificación en Microstrategy y experiencia mínima de dos años en desarrollos con Microstrategy
- Al menos 1 ingeniero de datos especialista en Big data, para asegurar las funciones de diseño, implementación de la gestión, monitorización, seguridad y privacidad de datos, mediante la pila completa de los servicios Azure. Se requiere experiencia mínima de un año en desarrollos con spark en entornos cloud.

  Para todos los perfiles mencionados se requieren estudios de educación Universitaria de carácter científico o tecnológico como masters o grados de ingeniería (industrial, telecomunicaciones, informática o similar)

En caso de necesidad de sustitución de algún miembro del equipo, se deberá asignar otra persona que disponga de la cualificación requerida, y si para asegurar la permanencia del conocimiento adquirido y su transferencia fuera necesaria la concurrencia entre los recursos entrantes y salientes, durante ese período solamente se contabilizarán como horas productivas las de uno de los recursos para cualquier contabilidad de esfuerzos.

Los actores que intervendrán en el servicio se identifican en cuatro grupos. Por parte de AB, Usuarios, Gestores de Demanda, Interlocutores IT y por parte del adjudicatario, El adjudicatario.

En los grupos de AB se distinguen los siguientes perfiles:

- **Usuarios:** No hay distinción de perfiles dentro de este grupo. Sus funciones son:
  - Uso de los sistemas BI
  - Generación de tickets de peticiones y de incidencias.
  - Validación de las soluciones desarrolladas o aportadas por IT AB y el adjudicatario.

- **Gestores de la demanda:** No hay distinción de perfiles dentro de este grupo. Sus funciones en el servicio son:
  - Interlocución entre los usuarios y IT AB para la generación de peticiones evolutivas funcionales.
  - Validación de nuevos desarrollos y de soluciones correctivas.

- **Interlocutores AB:** Se distinguen dos perfiles, el de Técnico y el de Gestor.
  - Las funciones del perfil Técnico son:
    - Interlocución con el resto de los grupos y perfiles.
    - Seguimiento operativo del servicio en representación de AB.
    - Coordinar las subidas a producción en los distintos entornos del sistema.
    - Comunicar la operativa y las desviaciones del servicio al Comité de Seguimiento.

  - Las funciones del perfil Gestor son:
    - Interlocución contractual del servicio con el adjudicatario.
    - Participar en los comités de seguimiento del Servicio.

- Participar en las reuniones semanales con el coordinador del servicio del proveedor para la revisión de los temas.

- **Adjudicatario:** Se distinguen dos perfiles, el de Técnico y el de Gestor. Las funciones del perfil Técnico son:
  - Recepción, Valoración y resolución en su caso de las incidencias del servicio.
  - Recepción, Valoración y desarrollo en su caso de las peticiones evolutivas.
  - Resolución de las consultas y de las acciones operativas del servicio.
  - Mantenimiento de la documentación derivada del servicio en los términos y actividades descritas en este documento.
  - Interlocución con el interlocutor de AB para el seguimiento y planificación de actividades y prioridades dentro del servicio.
  - Despliegue de las subidas a producción en los distintos entornos de sistema, en los términos de colaboración con terceros equipos que se establezca en cada caso según la naturaleza de cada despliegue y entorno, siguiendo las indicaciones de AB.

- **Las funciones del perfil Gestor son:**
  - Interlocución contractual del servicio con AB.
  - Participación en el comité de seguimiento del Servicio.

5.6 Herramientas de Gestión y Control

La gestión y control de las incidencias y peticiones, en adelante tickets, se realizará mediante la herramienta de ticketing de AB.

AB proveerá de usuario y de roles suficientes para la gestión requerida como parte del servicio.

AB se reserva el derecho a modificar la versión y plataforma para la gestión y control del servicio sin previo aviso durante el periodo de vida del servicio adjudicado.

Los informes se presentarán en formato Power point utilizando una plantilla que AB proveerá al adjudicatario como parte de la documentación del servicio.

5.7 Seguimiento y Control

El seguimiento y control de los trabajos se efectuará sobre las siguientes bases:

Seguimiento estratégico: se constituirá un Comité de Dirección, en el que se integren representantes de AB y el Adjudicatario.

Seguimiento táctico reuniones de seguimiento y revisiones técnicas entre el Supervisor del contrato por AB y el Coordinador del Servicio por el Adjudicatario, al objeto de revisar el grado de cumplimiento de los objetivos, las reasignaciones y variaciones de efectivos de personal dedicado al proyecto, las especificaciones funcionales de cada uno de los objetivos y la validación de las programaciones de actividades realizadas

Seguimiento operativo: reuniones de seguimiento de detalle de temas operativos, bloqueos, incidencias

6. ASPECTOS PRINCIPALES DEL SERVICIO

6.1 Lugares de prestación del Servicio

La realización de los trabajos descritos en este documento podrá tener lugar en distintas localizaciones, según las necesidades de las distintas actividades del servicio:

- Las oficinas de la Dirección de Aplicaciones IT de AB.
- Las oficinas del adjudicatario del servicio.

6.2 Categorización de las Peticiones de Servicio

Las peticiones de servicio de tipo evolutivo no tendrán otra categorización que la de peticiones evolutivas a las cuales se las otorgará una prioridad de ejecución de común acuerdo entre los actores definidos en el servicio, descritos en los apartados anteriores de este documento.

Las peticiones de tipo correctivo, incidencias, se clasificarán de la siguiente manera:

Altas

Se definen como altas las incidencias que cumplan alguna de las siguientes condiciones:

a) Implica una parada total del sistema.
b) Implica una parada completa de una funcionalidad clave.
c) Implica adoptar una forma de trabajo alternativa en un grupo funcional de usuarios.
d) Implica una corrección con un tercer sistema implicado con el que BI tiene conexión.
e) Implica una parada de una interfaz.
f) Implica un impacto sobre más de la mitad de los usuarios.
g) Se trata de una incidencia generada por un usuario definido como VIP o sensible dentro de la organización.
h) Actuaciones derivadas de alertas de seguridad.

Son incidencias de resolución inmediata e implican el aviso inmediato al responsable técnico de AB.

Medias:

Se definen como Medias las incidencias que cumplan alguna de las siguientes condiciones:

a) Implica adoptar una forma de trabajo alternativa a un usuario.
b) Implica adoptar una conexión alternativa con un tercer sistema implicado con el que BI tiene conexión.

Bajas:

Cualquier otra incidencia que no cumpla ninguna de las condiciones descritas en las categorías anteriores.

6.3 Cobertura del Servicio

El servicio se prestará en un horario de lunes a viernes todos los días laborables del año, en un horario que cubra la ventana de trabajo de los usuarios BI, bajo estas dos premisas:

- De lunes a jueves: de 07:00 a 18:00 horas
- Viernes y todos los días intensivos de verano marcados en el calendario laboral de AB: de 07:00 a 15:00 horas
- Se considerarán días festivos los sábados, domingos, fiestas autonómicas y fiestas nacionales.

El servicio incluirá el soporte presencial cuando se requiera dentro de los plazos de servicio marcados por los acuerdos de servicio aplicados a cada incidencia.

6.4 Especificaciones de RGPD y seguridad

Los desarrollos (proyectos) realizados y entregados deberán cumplir con el Reglamento (UE) 2016/679, General de Protección de Datos ("RGPD") y, en especial, con lo establecido en las cláusulas 9 y 20 del Pliego de Condiciones Particulares (PCP), así como en la cláusula 15 del Contrato. La empresa adjudicataria tendrán que identificar todos aquellos puntos que puedan vulnerar el RGPD, resolverlos y presentar las evidencias conforme cumplen con el mismo.

Por otra parte, los sistemas a desarrollar han de estar exentos de vulnerabilidades, según aplique el Top 10 de OWASP Security Mobile y/o OWASP Top Security Web (https://www.owasp.org). Además deberá cumplirse la normativa de gestión de usuarios y contraseñas establecida en el **Anexo Nº 1**.

En este sentido, se han de presentar las evidencias de las pruebas realizadas y se realizará una auditoría de seguridad por parte de AB.

En cualquier caso, los desarrollos objeto de este pliego serán analizados a través de una auditoría técnica interna de seguridad y análisis de código. El objetivo de dicho análisis es realizar un diagnóstico de la seguridad con el fin de detectar fallos de seguridad, posibles vectores de ataque, errores de programación, prevenir incidentes de seguridad y mejorar el nivel de seguridad de los sistemas de información. Está auditoría ser realizará bajo los estándares que marca OWASP.

Las evidencias y vulnerabilidades que resulten de la realización de dicha auditoría, deberán ser subsanadas por el Adjudicatario, asumiendo el mismo los costes dentro del importe de la adjudicación del contrato que hace referencia al presente pliego de prescripciones técnicas.

Así mismo, durante la ejecución del Contrato se deberán observar por parte de los adjudicatarios las medidas de seguridad que constan en el Anexo Nº 9 del citado PCP.

6.5 Modelo de Acuerdo de Nivel de Servicio

6.5.1 Indicadores de Nivel de Servicio (ANS)

Los ANS y penalizaciones se calcularán según la siguiente tabla, siendo:

Vc = Tramo de cumplimiento

Va=Tramo de atención

Vi= Tramo de incumplimiento

Código	Indicador	Descripción	Vc	Va	Vi	Unidad	Peso	Bonus	Malus
INC 01	Tiempo de resolución incidente con categoría asignada "alta"	% de incidentes catalogados como altos por impedir el trabajo de un gran número de usuarios o afectar a procesos críticos de la empresa, atendidos y resueltos en el plazo: Tiempo de respuesta <1 hora; Tiempo de resolución menor de 6 horas	100	95	85	%	25	% por encima del 95	- % entre el 95 y 85 - 10% de 85 para abajo
INC 02	Tiempo de resolución incidente con categoría asignada "media"	% de incidentes catalogados como medios, atendidos y resueltos en el plazo: Tiempo de respuesta <5 hora; Tiempo de resolución menor de 8 días hábiles	100	95	85	%	15	% por encima del 95	- % entre el 95 y 85 - 10% de 85 para abajo
INC 03	Tiempo de resolución incidente con categoría asignada "baja"	% de incidentes catalogados como bajos, atendidos y resueltos en el plazo: Tiempo de respuesta <6 hora; Tiempo de resolución menor de 30 días hábiles	100	95	85	%	10	% por encima del 95	- % entre el 95 y 85 - 10% de 85 para abajo
INC 04	Reaperturas de incidencias	Porcentajes de incidentes o peticiones que fueron dados como resueltos y han vuelto a producirse	0	5	15	%	10	% hasta el 5%	- % entre el 5 y 15 - 10% de 15 para abajo
INC 05	Tickets abiertos con ANS incumplido	% de tickets abiertos con ANS incumplido	0	5	15	%	5	% hasta el 5%	- % entre el 5 y 15 - 10% de 15 para abajo
CAM01	Tiempo medio de valoración Evolutivos (Max. 10 días)	Tiempo empleado para valorar el desarrollo de un evolutivo, tomando como referencia un valor máximo de 10 días *hábiles (o si se da el caso, el valor <10 propuesto por el proveedor en respuesta a la petición de mejora de este ANS según especificado en los criterios de adjudicación)*	5	10	15	Unidad	5	<10 →2% <5→4%	>10→-2% >15→-5%

CAM02	cumplimiento fechas entrega evolutivos	Cumplimiento de la fecha planificada de entrega de los desarrollos evolutivos (retraso en días sobre el total de días hábiles planificados para la entrega del evolutivo)	100	90	85	%	10	% hasta el 5%	- % entre el 5 y 15 - 10% de 15 para abajo
GES01	Calidad de entrega de nuevas versiones de software	Subidas a producción realizadas con algún error de criticidad alta o media descubierto en producción achacable a falta de plan de pruebas. Falta de actualización del código fuente. Disminución de la calidad del código según las reglas de SONAR.	0	1	3	unidad	15	5% para ANS=0	-% para ANS de 1 a 3 - 10% para 3 o peor
GES02	Incumplimiento del modelo de relación	Incumplimiento del modelo de relación acordado: informes de seguimiento no presentados, ANS mal calculados (en dos periodos)	0	1	3	unidad	5	5% para ANS=0	-% para ANS de 1 a 3 - 10% para 3 o peor

6.5.2 Penalizaciones

Se definen las siguientes variables:

Is (€) = Importe Servicio Mensual
Pi (%) =Peso Indicador
VPi (€) = Valor Penalización Indicador (Bi="Bonus" Indicador; Mi="Malus" Indicador)
Vp (%) =Valor Ponderado Mensual = $(\sum(Pi * VPi))/100$
Ip (€) =Importe Penalización Mensual

El cálculo del importe de penalización mensual será, por lo tanto:
Ip = Is * Vp

Si Ip < 0, AB se reserva la posibilidad de aplicar la penalización mensual.
Si Ip => 0, no se aplicarán penalizaciones.
Si a lo largo de la duración del contrato, en un momento dado, la suma de los Valores Ponderados Mensuales supera el 30 % ($\sum(VP) > 30$ %), AB se reserva el derecho de resolver unilateralmente el contrato.

7 ESTIMACIÓN HORAS DE TRABAJO

En base a la experiencia se ha estimado un volumen de horas para llevar a cabo las tareas listadas en el catálogo de servicios. Los desarrollos evolutivos mayores requieren en alguna fase de la intervención de perfiles más experimentado para el análisis, diseño y modelado, por lo tanto, AB ha considerado en la elaboración del presupuesto de este pliego una tarifa más alta para que el proveedor pueda poner a disposición ese tipo de recursos.

SERVICIO BI – ESTIMACION ANUAL	
BI tradicional / On premise	**Horas**
Mantenimientos (puntos 4.1, 4.2, 4.3, 4.4, 4,5, 4.6,4.7,4.8)	2145
Desarrollos Evolutivos menores (4.9)	537

TOTAL HORAS	2682
Big Data / Cloud	**Horas**
Mantenimientos (puntos 4.1, 4.2, 4.3, 4.4, 4,5, 4.6,4.7,4.8)	1430
Desarrollos Evolutivos menores (4.9)	358
TOTAL HORAS	1788

El volumen de horas dedicado a desarrollos evolutivo menores es el mínimo entregable, el proveedor tendrá el objetivo de aumentar este evolutivo menor a costa de eficientar el correctivo.

SERVICIO BI – ESTIMACION ANUAL	
BI tradicional + Big data	**Horas**
Evolutivos mayores (4.10)	3576

Si las horas destinadas a evolutivos mayores no se consumen dentro del periodo de un año a partir de la firma del contrato, se podrá traspasar un 20 % de las horas, como máximo, al periodo anual siguiente.

SERVICIO BI – TABLA RESUMEN	
Total Horas	8046

Durante los primeros 3 meses del servicio, el proveedor entrante deberá presentar un informe resultado de la Due Diligence que el mismo realizará y que será usado como Acta de Aceptación del Servicio según los criterios establecidos en la licitación. Para elaborar este informe, el proveedor tendrá acceso tanto a la información histórica de las peticiones del servicio (últimos 2 años) así como la propia información del servicio que ya habrá prestado en estos primeros meses

Adicionalmente deberá presentarse una Acta de Aceptación del Servicio BigData no más tarde de los 3 meses posteriores a la entrega del proyecto BigData.

8 NORMAS DE SEGURIDAD IT DE AIGÜES DE BARCELONA

Los Sistemas de Información proporcionados no deben ser vulnerables, según aplique , a los TIP 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 Anexo 1 del presente documento de Pliego de Prescripciones Técnicas.

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

ANEXO Nº 1 -

"NORMAS DE SEGURIDAD IT DE

AIGÜES DE BARCELONA."

ÍNDICE

1. Objeto e introducción del documento

El objeto del presente documento es establecer la normativa de seguridad en la gestión de los Sistemas de Información de 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 dichos intercambios.

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

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

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

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

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

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

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

3. Configuración y administración segura

3.1. Configuración segura

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

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

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

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

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

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

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

3.2. Administración segura

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

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

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

4. Identificación y autentificación de usuarios

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

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

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

- Software de control de acceso inherente al propio sistema.

- Herramienta de software de control de acceso agregado al sistema.

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

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

La 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.

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

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

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

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

5. Identificación de usuario

El acceso a cualquiera de los sistemas de información de 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 desempeñada por el usuario, de su puesto de trabajo, del departamento al que pertenece y del sistema al que se conecta. El identificador de usuario permanecerá asociado a su propietario de AB con independencia de los cambios de

destino o de categoría que pudiera tener o, incluso de baja; y de acuerdo a la legislación vigente en materia de protección de datos de carácter personal.

Las personas que no pertenecen a la plantilla de trabajadores de 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 de otorgarse sólo por el periodo de tiempo estrictamente necesario y deberán ser reevaluados periódicamente.

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

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

6. Gestión de contraseñas y credenciales de clientes

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

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

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

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

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

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

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

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

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

7. Comunicación de los incidentes de seguridad

En caso de detección de un incidente grave de seguridad (mediante sistemas de detección de intrusiones, análisis de logs, comunicación de un tercero, alarmas de seguridad, etc.), la Dirección de Seguridad AB 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 AB.

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

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

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

Tanto los empleados de las entidades de AB 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.