



**Aigües de
Barcelona**

**PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE DEBE REGIR EL CONTRATO DE
SUMINISTRO DE EQUIPOS EN ARRENDAMIENTO POR LA MODALIDAD DE PAGO
POR USO QUE INCORPORA EL SERVICIO DE MANTENIMIENTO Y GESTION DEL
PARQUE DE IMPRESORAS PARA AIGÜES DE BARCELONA**

Nº Exp.: AB/ABAST/2019/69

En Barcelona, junio de 2019



1. OBJETO DEL CONTRATO.....	3
2. INTRODUCCIÓN	3
3. HORARIO DE COBERTURA DEL SERVICIO.....	4
4. CONDICIONES MEDIOAMBIENTALES	4
5. CONDICIONES GENERALES DEL SERVICIO.....	5
5.1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y PREVENCIÓN	5
5.2. ESPECIFICACIONES DE SEGURIDAD.....	5
5.3. CONTROL Y SEGUIMIENTO DEL CUMPLIMIENTO DE LAS MEDIDAS EN MATERIA DE PROTECCIÓN DE DATOS Y MEDIDAS DE SEGURIDAD.....	6
6. GOBERNANZA DEL SERVICIO DE IMPRESIÓN	6
6.1. SERVICEMANAGER.....	6
6.2. GESTIÓN ADMINISTRATIVA.....	7
6.3. ADMINISTRACIÓN DE LA PLATAFORMA	8
6.4. SERVICIO DE ATENCIÓN AL USUARIO.....	8
6.5. INVENTARIO, CONFIGURACIONES Y ETIQUETAS.....	9
6.6. RETIRADA DE LOS DISPOSITIVOS Y MATERIAL	10
6.7. APROVISIONAMIENTO DE CONSUMIBLES.....	10
6.8. SERVICIO PREVENTIVO.....	11
6.9. GARANTÍA.....	11
6.10. REPARACIONES.....	12
6.11. REPORTING DEL RESULTADO DEL SERVICIO.....	12
6.12. CARACTERÍSTICAS PUESTO DE TRABAJO	12
6.13. CONDICIONES PARTICULARES IMPRESORAS.....	12
7. CONDICIONES GENERALES TECNICAS DEL SERVICIO	13
7.1. SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN.....	14
7.2. SEGURIDAD CORPORATIVA.....	15
7.2. CARACTERÍSTICAS TÉCNICAS REQUERIDAS PARA LA GESTIÓN DEL SERVICIO DE IMPRESIÓN	15
7.3. CARACTERÍSTICAS TÉCNICAS DE LOS DISPOSITIVOS	16
8. GESTIÓN DE LA CALIDAD DEL SERVICIO.....	17
8.1. OPERATIVA DEL SERVICIO.....	17
8.2. ANS.....	18
8.3. DEFINICIÓN INDICADORES DE NIVELES DE SERVICIO.....	18
8.4. INDICADORES DE NIVEL DE SERVICIO	19
8.5. PENALIZACIONES POR INCUMPLIMIENTO DEL NIVEL DE SERVICIO	20
8.6. EQUIPOS CON AVISOS REPETITIVOS.....	20
9. DETALLE DIMENSIONAMIENTO.....	20
9.1. DIMENSIONAMIENTO DE EQUIPOS SEGÚN SU TIPOLOGÍA	20
9.2. VOLUMETRÍA DE IMPRESIÓN	22
10. PROYECTO IMPLANTACIÓN	22
10.1. METODOLOGÍA	22
10.2. MARCO ORGANIZATIVO DEL PROYECTO. ROLES.....	22
10.3. PLANIFICACIÓN Y PLAN DE IMPLEMENTACIÓN.....	22
10.4. GESTIÓN DEL CAMBIO.....	23
10.5. FORMACIÓN	23
10.6. DOCUMENTACIÓN Y TRASPASO DE CONOCIMIENTO TI.....	23
11. DEVOLUCIÓN DEL SERVICIO	24
11.1. FASE PREPARACIÓN SALIDA	24
11.2. FASE DE TRANSICIÓN DE SALIDA	24
12. ANEXOS	25



1. OBJETO DEL CONTRATO

El presente Pliego de Prescripciones Técnicas tiene por objeto la definición y caracterización de las condiciones técnicas que han de regir el procedimiento de licitación del Servicio de Impresión (en adelante "el Servicio") para **Aigües de Barcelona, Empresa Metropolitana de Gestió del Cicle Integral de l'Aigua, S.A.** (en adelante, "Aigües de Barcelona ó AB"), cuyos destinatarios son sus usuarios (en adelante, "Usuario/s").

En este sentido, en el Pliego de Prescripciones Técnicas, se especifican las características y condiciones de obligado cumplimiento para el proveedor que resulte adjudicatario sobre el suministro de hardware, consumibles, componentes de software y los servicios asociados del Servicio de Impresión, para las sedes de Aigües de Barcelona.

El objetivo de este Pliego es la contratación del Suministro de equipos en arrendamiento por la modalidad de pago por uso que incorpora el servicio de mantenimiento y gestión del parque de impresoras para Aigües de Barcelona con las siguientes prestaciones:

- ▶ Una cuota fija mensual de arrendamiento de equipo por cada tipo de impresora que incluye el servicio de impresión y mantenimiento.
- ▶ Un importe variable mensual de copia monocromo y otro de copia en color que variará en función del nº de copias realizadas en el mes de facturación, siendo de aplicación los mismos precios para todos los tipos de impresora.

Estos importes deben incluir la gestión de la cuenta, la gestión administrativa, el mantenimiento, cualquier consumible (recambio, kit, limpieza, ...) el software de control y monitorización, y cualquier otro elemento requerido en este pliego.

2. INTRODUCCIÓN

En Aigües de Barcelona, vamos hacia una cultura de PaperLess, donde la reducción del consumo del papel, el uso de papel reciclado y el respeto por el medioambiente, son un objetivo claro de la compañía.

El usuario de Aigües de Barcelona, es un usuario de ámbito:

- ▶ Administrativo, donde el consumo de impresión y escaneo principalmente son: documentos, contratos, documentos oficiales, listados e impresiones varias.
- ▶ Técnico y/o departamento de Operaciones, donde el consumo de impresión y escaneo principalmente son: partes de trabajo, planos y diagramas, listados e impresiones varias.
- ▶ Atención al Usuario, donde el consumo de impresión y escaneo principalmente son: contratos, facturas, recibos, documentos oficiales e impresiones varias.

Los objetivos que se deben alcanzar con el lanzamiento de este procedimiento de licitación son:

- ▶ Mejorar la calidad del servicio.
- ▶ Avanzar hacia un modelo medioambiental más sostenible en consumo energético y en emisión de gases de efecto invernadero.
- ▶ Contratación de un único servicio que incluya todas las condiciones que forman parte del ámbito del servicio.
- ▶ Implantación de un modelo de pago por uso (cuota fija de arrendamiento más pago por copia).
- ▶ Disponer de una figura de ServiceManager, para gestión de la explotación del contrato.
- ▶ Incorporación de nuevas tecnologías.
- ▶ Optimizar la infraestructura de copia, escaneo y FAX.



- ▶ Control y monitorización del parque mediante un software de Gestión de autenticación, autorización y contabilización (en adelante, "Software AAA") .
- ▶ Disponer de un modelo que garantice la adaptación a los cambios de la compañía.
- ▶ Reducir el gasto fundamental mediante un uso racional de los sistemas de impresión.
- ▶ Disponer de una Gestión del Servicio minimizando los elementos de infraestructura, a través de una homogenización del parque gestionado por una única marca y unificando el número de modelos.
- ▶ Reducir el tráfico de la Red Corporativa.
- ▶ Facilitar la digitalización.
- ▶ Garantizar la seguridad y control de la impresión.

En definitiva, se procederá a un modelo de Servicio innovador tecnológicamente, con gestión proactiva, tendente a optimizar y reducir los costes económicos, consumo energético y ambientales. Así mismo, y para una mayor optimización, el equipamiento incluirá un software de gestión cuyas principales funcionalidades serán las de mantener el control de la privacidad de la impresión, usabilidad y consumo tanto de las impresoras como sus consumibles, que permita la facturación por equipo/usuario, así como un sistema de monitorización que sea capaz de gestionar eventos y alertas.

Con este procedimiento de licitación se pretende renovar el parque actual de impresoras, por dispositivos, componentes y consumibles de impresión, nuevos y originales del fabricante en su totalidad.

3. HORARIO DE COBERTURA DEL SERVICIO

El horario en que el proveedor deberá realizar la prestación del Servicio y servicios asociados será de 08:00 a 18:00 de lunes a viernes, excepto festivos nacionales. Este horario se aplicará para el cálculo de los niveles de servicio indicados en el **apartado 8** de este pliego que recibirá cualquier elemento del servicio, como por ejemplo el tiempo de suministro de consumibles, tiempo de resolución de incidencias, así como el tiempo de retirada de los equipos de las sedes.

A nivel geográfico, el alcance del servicio abarca todas las sedes de la empresa Aigües de Barcelona. En el **Anexo núm. II**, se incluye el listado de todas las sedes actuales como referencia. El proveedor asumirá que estas localizaciones pueden sufrir modificaciones y/o ampliaciones durante la vigencia del contrato, y lo deberá tener en cuenta a fin de prestar el servicio, suministrar las impresoras y los consumibles.

4. CONDICIONES MEDIOAMBIENTALES

Todos los equipos han de cumplir con la Directiva 90/270/CEE del Consejo, de 29 de mayo de 1990, referente a las disposiciones mínimas de seguridad y salud relativas al trabajo con equipos que incluyen pantallas de visualización que regula la compatibilidad electromagnética, emisiones de radiación y aspectos medioambientales y ergonómicos.

Los materiales no contendrán plomo, cadmio, mercurio, cromo hexavalente, PBB ni PBDE según lo especificado en la Directiva 2011/65/UE del Parlamento Europeo y del Consejo, de 8 de junio de 2011, sobre restricciones a la utilización de determinadas sustancias peligrosas en aparatos eléctricos y electrónicos y sus enmiendas.

Además, deben ser conformes con las normativas técnicas en vigor sobre esta materia (ISO-9241, asumida como Norma EN 2941 y UNE-EN 29241 ó equivalentes), y cumplir las siguientes certificaciones:

- ▶ Certificación Energy Star o equivalente.
- ▶ Calificación medioambiental EPEAT Gold o equivalente.



Adicionalmente, a fin de ayudar a reducir el impacto medioambiental y asegurar que son productos sostenibles, se requiere que las impresoras cumplan con la siguiente certificación: Certificación de Sostenibilidad TCO-Certified o equivalente.

En cuanto a la reducción del impacto medioambiental sobre el uso de la impresora, todas deberán cumplir lo siguiente:

- ▶ Podrán imprimir a doble cara (función dúplex) y 2 o más páginas por página.
- ▶ Podrán conectarse en red para ser usados por varios usuarios.
- ▶ Gestionarán diferentes formatos de papel, automáticamente, sin necesidad de intervención del usuario.
- ▶ Funcionarán perfectamente con papel 100% reciclado de calidad según EN 12281:2002 o equivalente.
- ▶ En máquinas a color, los cartuchos/tóner de colores se deben de poder cambiar por separado.

En caso de no cumplimiento de estas condiciones medioambientales, Aigües de Barcelona podrá desestimar la oferta.

Queda expresamente excluido de esta contratación la gestión de recogida de toner.

5. CONDICIONES GENERALES DEL SERVICIO

En este apartado se describen los componentes que debe incluir el Servicio, servicios asociados y los requerimientos técnicos, que deben ser contemplados en la licitación.

5.1. Políticas de Seguridad de la información y prevención

El prestador del servicio se deberá acoger obligatoriamente a las políticas de la compañía en materia de gestión de accesos, políticas de seguridad, GDPR y prevención.

- ▶ Accesos a la Red Corporativa: El cliente suministrará una conexión segura VPN con doble factor de autenticación, la cual será personal e intransferible. El acceso estará limitado a los equipos que forman parte del servicio.
- ▶ Usuarios de Dominio: Se crearán los usuarios nominales necesarios para la prestación del servicio en el Directorio Activo.
- ▶ Aigües de Barcelona, se reserva el derecho de trazar los accesos remotos del proveedor.
- ▶ El proveedor debe suministrar el nombre, apellidos, DNI y fotografía del personal que pueda estar con asiduidad en las instalaciones de AB, para darlos de alta en el aplicación de prevención laboral Coordinaqua.

5.2. Especificaciones de Seguridad

El Adjudicatario no podrá conservar ningún tipo de información de datos sensible más allá de lo estrictamente necesario para la prestación del servicio.

El Adjudicatario deberá describir:

- ▶ El sistema de borrado de los mismos y en general los sistemas de gestión de la información del servicio.
- ▶ Los elementos de seguridad física de que dispone.

Así mismo, el Adjudicatario deberá garantizar:

- ▶ La destrucción de cualquier material que genere el servicio (deteriorados) que no se entregue al distribuidor para su reparto.
- ▶ La seguridad en el acceso a sus instalaciones, así como a los datos utilizados en la prestación del servicio (Identificaciones de usuarios, contraseñas, etc.).



- ▶ El cumplimiento de las regulaciones generales de protección de datos (GDPR), así como aquellas específicas que indique AB.
- ▶ Garantizar los niveles de confidencialidad que indique AB.

5.3. Control y seguimiento del cumplimiento de las medidas en materia de protección de datos y medidas de seguridad.

A la firma del contrato, AB acordará el método de comunicación con la empresa adjudicataria. Esta comunicación, punto a punto, VPN, etc., deberá estar bien definida y seguir las normas de seguridad (conexiones de servicio, soporte, etc.).

Debe garantizarse que los documentos "impresos" NI credenciales de usuario no salen del ámbito de AB para garantizar la confidencialidad. Adicionalmente:

- ▶ Política de gestión de activos de información
- ▶ Destrucción segura y confidencial de la documentación

Los accesos remotos del proveedor a la solución (on Site) deberían, en la medida de lo posible, ser trazados y que dejen logs a los que podamos acceder.

- ▶ Sistema de identificación y autenticación de usuarios
- ▶ Sistema de gestión de privilegios de acceso
- ▶ Límite de intentos reiterados de acceso no autorizado
- ▶ Sistema de control de acceso al sistema de información
- ▶ Registro de accesos al sistema de información (vgr. log de accesos)

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.

AB 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 mencionadas, 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 AB un Informe actualizado y detallado del cumplimiento de cada una de las medidas de seguridad anteriormente indicadas.
- ▶ Por otro lado, AB se reserva el derecho, en cualquier momento, de realizar cuantas auditorías que considere pertinentes a efectos de verificar el grado de cumplimiento indicado en el Informe referenciado en el apartado anterior.

6. GOBERNANZA DEL SERVICIO DE IMPRESIÓN

Se debe incluir en la licitación un servicio de Gobernanza como punto de referencia de interlocución entre AB y el proveedor, para la gestión del servicio, interlocución técnica y seguimiento de niveles de servicio (ANS).

6.1. ServiceManager

El prestador del servicio debe incorporar dentro del servicio la figura de ServiceManager, el cual gestionará la gobernanza del servicio. Dicha figura debe ser conocedor del contrato, sus cláusulas y anexos. Esta figura asumirá las siguientes funciones dentro de su ámbito de responsabilidad:



- ▶ Velará por la correcta prestación del servicio.
- ▶ Actuará como Gestor funcional de la cuenta asegurando el cumplimiento de las obligaciones contractuales.
- ▶ Resolverá de forma satisfactoria cualquier asunto sobre la facturación o contabilización del servicio que pudiera surgir con AB.
- ▶ Velará por la correcta información de los datos de las impresoras en la base de datos de Configuration Management DataBase (en adelante, "CMDB") de AB (en estos momentos Remedy, pudiendo ser otra en el futuro), y su coherencia con los datos de inventario del proveedor.
- ▶ Gestionará cuantos recursos del proveedor sean necesarios para el correcto funcionamiento del servicio.
- ▶ Será el punto de contacto entre AB y el proveedor, para temas de escalado de incidentes, temas administrativos, tecnológicos e implantación de nuevas funcionalidades, aportando el máximo valor de negocio al cliente en base a su experiencia y que permitan la toma de decisiones para la mejora continua del servicio. Establecerá planes de consultoría o asesoría que permitan avanzar en esa dirección.
- ▶ Velará por el cumplimiento de los niveles de servicio pactados.
- ▶ Gestionará el cálculo de los ANS que se gestionan con la herramienta proporcionada por AB (en estos momentos Remedy, pudiendo ser otra en el futuro).
- ▶ Presentará periódicamente los informes e indicadores (ANS) sobre el estado del servicio, que permitan realizar una revisión y aplicar las penalizaciones si procede descritas en el **apartado 8**.
- ▶ Redactará las actas sobre las reuniones y acuerdos alcanzados.
- ▶ Se reunirá de forma periódica con AB en reuniones operacionales, estratégicas y tácticas del servicio.
- ▶ Proporcionará los informes de servicio necesarios en caso de incidencia de degradación y/o denegación del servicio.

6.2. Gestión Administrativa

El servicio se encargará de gestionar todos los procesos administrativos y de Accounting del servicio, a partir de los datos obtenidos por el software de gestión del Servicio. Sus principales responsabilidades serán:

- ▶ Generar los ficheros de facturación interna de AB, en forma y formato específico, teniendo en cuenta como parámetros del fichero, los datos de imputación departamental (proporcionados por Aigües de Barcelona), de manera que facilite el reparto de costes internos. Dicho fichero será configurado partiendo de la información obtenida por las siguientes fuentes de datos:
 - ▶ La información proporcionada por el Software AAA.
 - ▶ El Directorio Activo de AB.
 - ▶ El fichero Excel resultante que se suministrará al departamento financiero, deberá contener la información de los siguientes campos:
 - ▶ Usuario de Windows
 - ▶ Datos del usuario
 - ▶ Departamento
 - ▶ Gasto (número de páginas impresas por el usuario/mes)
 - ▶ Centro de coste (elemento PEP)
 - ▶ Gestionará administrativamente la incorporación, sustitución y retirada de los dispositivos.
 - ▶ Gestionará el suministro de consumibles.



- ▶ Velará por la entrega de los consumibles en tiempo y ubicación.
- ▶ Gestionará los accesos del personal del proveedor para la prestación del servicio en las instalaciones de AB, con anticipación suficiente para facilitar las gestiones internas según normativa de seguridad vigente de AB. Deberá mantener permanentemente informados a los responsables de AB, la lista de personas que prestan el servicio in-situ, y comunicar los cambios, sustituciones y nuevas incorporaciones

6.3. Administración de la plataforma

El servicio dispondrá de los recursos técnicos necesarios para la administración de software y hardware de la plataforma. Y en general:

- ▶ Se ocupará de la administración del Software de Control y Hardware.
- ▶ Dispondrá de Conexión Remota y Usuario Administrador sobre la aplicación.
- ▶ Resolverá las incidencias de 2o Nivel y 3er Nivel, o las asignará al grupo de resolución correspondiente.
- ▶ Gestionará el ticketing con la herramienta de Gestión de Servicios TI (en adelante "ITSM") de AB (en adelante REMEDY, pudiendo ser otra en el futuro), mediante un grupo de resolución específico.
- ▶ Escalará las incidencias y gestionará las prioridades a través de la herramienta ITSM proporcionada por AB.
- ▶ Actualizarán los datos resultantes de los cambios que precisen actualización, modificación o baja, de los dispositivos en la base de datos de inventario del prestador del servicio y velará para que estos sean coherentes con los de la base de datos de inventario de AB.
- ▶ Se ocupará de actualizar la plataforma del software, updates o nuevas versiones del producto.
- ▶ Se ocupará de la instalación de paquetes o módulos de nuevas funcionalidades.
- ▶ Se ocupará de la actualización del firmware de las impresoras.
- ▶ Se ocupará de revisar y gestionar las alertas, y abrirá las incidencias necesarias que de estas se deriven.

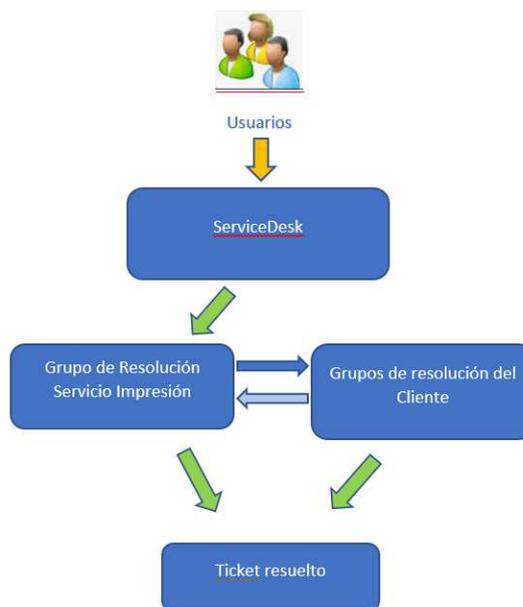
Y en definitiva de todas las tareas de administración de la plataforma requeridas por el Servicio y no definidas en este punto.

6.4. Servicio de Atención al Usuario

En general el servicio de atención al usuario (CAU) de Aigües de Barcelona, es el punto de contacto del usuario para la resolución de Nivel 1 de incidencias o consultas. Este servicio o el propio usuario, podrá abrir incidencias al grupo de resolución creado específicamente dentro de la herramienta de ITSM de AB, para que el servicio de gestión de incidencias, peticiones o problemas del prestador del servicio disponga de la capacidad de gestión y resolución de estas.

El volumen de incidencias aproximado se estima en 600 ticket anuales. No obstante, el presente pliego no garantiza estos volúmenes, ya que se utilizan estrategias incorporadas en esta prestación y descritas en el presente pliego de prescripciones técnicas, para intentar reducir tanto como sea posible el volumen de incidencias.

Los tickets sobre el Servicio de Impresión, serán asignados en primera instancia al grupo de resolución creado expresamente para tal efecto. Estos deberán ser resueltos atendiendo a los ANS descritos en el **apartado 8**, o bien pueden ser asignados a otros grupos de resolución internos de AB, si se considera que pertenecen a otro ámbito o no han sido correctamente asignados.



Modelo de relación a alto nivel

- ▶ Se utilizará la herramienta de ticketing de AB Remedy, pudiendo ser otra en el futuro.
- ▶ El prestador del servicio resolverá los tickets asignados a su grupo de resolución, entendiéndose que un ticket puede ser el conjunto de incidencias, peticiones, consultas, reclamaciones, problemas, cambios y operaciones que se gestionan desde el Servicio.
- ▶ Los tickets serán documentados y catalogados según la categorización de la herramienta ITSM REMEDY de AB.
- ▶ Los tickets tendrán una prioridad determinada y serán atendidos en función del ANS descrito en el **apartado 8**.
- ▶ El proceso incluye las actividades de:
 - ▶ Identificar
 - ▶ Registrar
 - ▶ Priorizar y clasificar
 - ▶ Investigar y diagnosticar
 - ▶ Informar de la evolución
 - ▶ Escalar
 - ▶ Resolución
 - ▶ Comunicación al usuario
 - ▶ Cerrar ticket

6.5. Inventario, configuraciones y etiquetas

- ▶ Inventario: El prestador del servicio generará y actualizará en una base de datos integrada, los elementos de configuración con la información sobre su estado, ciclo de vida, relación entre los elementos y toda la información que sea necesaria para gestión eficiente y de calidad de los servicios contratados. Dicho inventario debe ser accesible por AB, pudiendo generar reporting y extracción en formato excel de los datos del servicio. El proveedor



tendrá acceso en modo visualización o consulta a la CMDB de AB, para asegurar la coherencia entre ambos repositorios de información (en estos momentos Remedy, pudiendo ser otra en el futuro).

Los datos mínimos obligatorios que se deben constar en el inventario del proveedor son:

- ▶ Número de inventario proporcionado por Aigües de Barcelona.
 - ▶ Número de Serie de la Impresora.
 - ▶ Nombre NetBios de la impresora.
 - ▶ Dirección IP de la impresora.
 - ▶ Número de FAX (si el dispositivo dispone de esta funcionalidad activada).
 - ▶ Marca y modelo de la impresora.
 - ▶ Ubicación de la impresora.
- ▶ **Etiquetas:** Los equipos serán etiquetados por el prestador del servicio, y llegarán a las oficinas de AB ya etiquetados. Además de las etiquetas del propio fabricante, el prestador del servicio deberá etiquetar las impresoras con las etiquetas que identifican que un dispositivo está registrado para su uso en las instalaciones de AB. Todas las etiquetas de las impresoras deberán estar enganchadas al dispositivo en un lugar de fácil visibilidad para su rápida identificación.
- ▶ Las etiquetas que identifican que el dispositivo está registrado y es para uso de Aigües de Barcelona, deben cumplir con los siguientes requisitos:
- ▶ Han de ser seguras (no removibles).
 - ▶ Llevarán un código numérico correlativo a indicar por AB (Número de Inventario).
 - ▶ Llevarán Logotipo de AIGÜES de Barcelona (AB proporcionará el logotipo corporativo).
 - ▶ Incorporarán un código de barras (EAN128 o equivalente) generado desde el código numérico correlativo. Este código tendrá el prefijo **P**, seguido de 6 dígitos numéricos (ejemplo P000001).
 - ▶ Incorporarán el texto "*Para incidencias contactar con cau@agbar.es (93 342 25 23)*" pudiendo ser otro texto en el futuro.
 - ▶ La dirección email genérica para la impresión vía correo.
 - ▶ Tendrán un tamaño proporcional al tamaño del dispositivo y suficiente para que se lea correctamente tanto el número como el código de barras.
 - ▶ Se pegarán sobre una posición que permita leerse desde arriba o desde el frente.

6.6. Retirada de los dispositivos y material

La retirada de cualquier dispositivo o accesorio (excepto consumibles) y todos los costes que se deriven de la retirada completa, parcial, o accesorios del dispositivo, serán a cargo del prestador del servicio, y se establecerá en el plazo marcado dentro del **apartado 8**, referente a Acuerdos de Niveles de Servicio.

El prestador del servicio, se ocupará de proveerse de los recursos logísticos necesarios para proceder a la retirada de los dispositivos.

El prestador del servicio deberá gestionar los accesos a las ubicaciones con suficiente antelación, debiéndose adaptar a las características de las oficinas.

6.7. Aprovisionamiento de consumibles

El prestador del servicio debe asegurar el envío de consumibles a las oficinas en función del porcentaje de tóner restante que se muestre el sistema de monitorización. Debido a que los consumos de Tóner de las impresoras y multifuncionales dependen de su usabilidad y estos pueden ser dispares, el prestador del servicio evaluará de manera proactiva el porcentaje idóneo para el envío del consumible para cada impresora o multifuncional.

Con la finalidad de garantizar la continuidad en el Servicio y tiempos de respuesta en todas las sedes de Aigües de Barcelona, el prestador del servicio debe garantizar un aprovisionamiento de stock imprescindible para cada tipo de impresora de cada una de las sedes. Dicho Stock debe ser suministrado con la identificación del número de serie del



equipo para el cual es el suministro y la persona responsable de la oficina (la lista de responsables será suministrada por AB).

Ver **apartado 8**, para tiempos de respuesta de reposición de Stock.

Los consumibles, entendiéndose como: tóner, contenedor residual de tóner, etc., deben de disponer de unas instrucciones claras y concisas que permitan al usuario realizar el cambio del consumible en el equipo.

Si el usuario no es capaz de realizar el cambio, solicitará al proveedor mediante ticket tipo petición, que se encargue de realizarlo, en los tiempos acordados dentro del ANS descrito en el **apartado 8**.

En cualquier caso, el usuario no será el responsable de cualquier avería o deterioro que se pudiera producir por el cambio del consumible en el dispositivo de impresión, y si procede, su coste asociado.

La Dirección de entrega de los consumibles será la que figure en el **anexo II**.

6.8. Servicio Preventivo

El prestador del servicio deberá incluir el servicio que permita el mantenimiento preventivo del equipamiento, físico o lógico, y de sus componentes y partes fungibles (depósitos de tóner residual, tóner, etc...) que forman parte del Servicio.

Se requiere un servicio preventivo que, apoyado por la consola de monitorización y eventos, consista en la asistencia de un técnico "in situ" como mínimo una vez cada 6 meses, por cada uno de los centros de Aigües de Barcelona, para realizar el mantenimiento de los equipos y asegurar su correcto funcionamiento.

El técnico en cada visita atenderá a las cuestiones o peticiones de los usuarios previamente registradas en la herramienta ITSM de AB o las registrará el propio técnico una vez atendidas. Se encargará de la puesta a punto de los equipos, para ofrecer la excelencia en el servicio.

Dentro de las visitas mencionadas en el párrafo anterior se encargará, como mínimo, de realizar las tareas a continuación descritas:

- ▶ Reposición de los consumibles antes de que se agoten.
- ▶ Limpieza general del equipo: limpieza de chasis, tapas, cristales del escáner, lubricación de las piezas mecánicas, tractores y rodillos, revisión de motores eléctricos, unidad fotoconductora, unidad fusor y fuente de alimentación.
- ▶ Realización de test de diagnóstico mediante software que identifiquen posibles errores ocultos.
- ▶ Comprobación y puesta a punto del equipo.
- ▶ Una vez realizada la revisión, se facilitará automáticamente un informe general donde a alto nivel, se indiquen las fechas de revisión, impresoras y detalles sobre la revisión, además de uno por cada dispositivo con más detalle, que permita tomar las decisiones pertinentes.

Además, el servicio debe incluir un servicio preventivo en el software de gestión y control de impresión, el cual será a cargo del prestador del servicio, que incluirá:

- ▶ Revisión de actualizaciones de Software y Firmware.
- ▶ Informará sobre las novedades que aporta cada cambio de versión respecto a la anterior.
- ▶ Revisará si se precisan nuevos paquetes o módulos para nuevas funcionalidades.
- ▶ Revisión de alertas.

6.9. Garantía

El Proveedor vendrá obligado a ofrecer una garantía de los equipos durante la vigencia del contrato.



6.10. Reparaciones

El prestador del servicio realizará las reparaciones i/o configuraciones en remoto siempre que sea posible. En caso de que no pueda acceder al dispositivo en remoto o que la reparación requiera de desplazamiento, deberá presentarse in-situ en las oficinas de AB, descritas en el **Anexo II**.

Los tiempos de resolución de estas incidencias se ajustarán a los plazos indicados en ANS del servicio, ver **apartado 8**.

Todos los costes asociados serán a cargo del prestador del servicio.

6.11. Reporting del resultado del servicio

El prestador del servicio generará cuantos informes y cuadros de mando con indicadores sean necesarios para la evaluación del servicio. Para ello, se presentarán informes con periodicidad mensual y el acumulado anual.

El reporting de servicio mensual como mínimo deberá incluir:

- ▶ Parque de máquinas instaladas por periodo.
- ▶ Actividad: Incidencias, peticiones, consultas, cambios, problemas y operaciones y métricas gestionadas por el servicio.
- ▶ Consumo de los dispositivos (pág. impresas por mes por dispositivo/ubicación y tipo de impresión (color o B/N), consumo de tóner, etc..).
- ▶ Diferenciación entre incidencias reportadas por la herramienta de monitorización y las incidencias abiertas por el usuario.
- ▶ Diferenciación entre los cambios de consumibles efectuados antes y después del consumo total.
- ▶ Detalle de averías.
- ▶ El reporting de ANS del servicio con carácter mensual:
- ▶ Generación de informes de seguimiento de cumplimiento de nivel de servicios según las métricas descritas en el **apartado 8**
- ▶ Solicitudes más recurrentes y propuestas para reducir las.
- ▶ Dificultades del servicio.

6.12. Características Puesto de Trabajo

Debe considerarse que la estrategia de la compañía en cuanto al puesto de trabajo está orientada hacia la Transformación del Workplace (puestos de trabajo flexibles), aumentando la movilidad del usuario, con la consecuente repercusión sobre la distribución de carga sobre la impresión.

- ▶ El sistema de impresión debe ser compatible con plataformas basadas en la virtualización mediante Citrix o VMWare.
- ▶ Todo el equipamiento y software ofertado se debe integrar sin problemas dentro de la plataforma de 'puesto cliente' de Aigües de Barcelona, no generando ninguna incidencia.

6.13. Condiciones Particulares Impresoras

Todas las impresoras deberán disponer de drivers firmados digitalmente y certificados sobre:

- ▶ Windows 10 Client X64 Current Branch for Business
- ▶ Windows 7
- ▶ Windows XP



El prestador del servicio deberá acreditarlo presentando en su oferta al menos uno de estos dos documentos:

- ▶ Documento de drivers: para todos los drivers que estén firmados digitalmente se detallarán los campos: descripción, nombre, fecha de lanzamiento, versión y versión(es) de Windows para las que está firmado. Si tuviera algún driver no firmado digitalmente no se indicará.
- ▶ Enlace o captura de la web de Microsoft <https://sysdev.microsoft.com/en-us/hardware/lpl/> o página equivalente donde se lea la descripción del equipo.

7. CONDICIONES GENERALES TECNICAS DEL SERVICIO

El prestador del servicio tendrá que diseñar e implantar la infraestructura ideal en base a las necesidades de AB, además de proveerse de los recursos técnicos y tecnológicos necesarios para la correcta prestación del servicio.

La solución debe incluir los aspectos funcionales y tecnológicos que se describen en todo este apartado, siendo un punto crítico para la prestación del servicio la optimización del tráfico de Red. La solución debe cumplir con las siguientes condiciones:

- ▶ Infraestructura basada en ServerLess y estrategias Cloud, sin que represente pérdida de funcionalidades.
- ▶ Implantar una solución de Software AAA, capaz de gestionar las autenticaciones, autorizaciones y contabilizar las impresiones y copias, monitorizar alertas del servicio y control de los dispositivos.
- ▶ La gestión global del servicio de impresión debe ser a través de una única solución Software AAA, que integre todas las funcionalidades requeridas, no pudiendo ser dos o más productos de software distintos o módulos.
- ▶ Obtener los volúmenes de impresión con la imputación a usuarios concretos para la correcta facturación.
- ▶ Obtener informes sobre el servicio de impresión.
- ▶ Impresión a una Cola de Windows "Virtual" que permita al usuario escoger la impresora en la que imprimir el documento.
- ▶ Impresión directa a una Impresora para minimizar el tráfico de impresión entre sedes.
- ▶ Instalación desatendida de los drivers de las impresoras.
- ▶ Realizar balanceo de carga entre equipos de impresión.
- ▶ Se requiere alta disponibilidad en el servicio de impresión, proporcionando continuidad en el servicio.
- ▶ En caso de caída del Servicio de Impresión, o cualquier otro mal funcionamiento de cualquier tipo, las colas de impresión directa a una impresora deben poder funcionar sin afectación a los usuarios. En este caso, la retención del log debe permitir el Accounting sin dependencia del servidor.
- ▶ En ningún caso, un mal funcionamiento en el sistema de control y gestión de la impresión podrá afectar a las impresiones de los equipos.
- ▶ Todos los dispositivos, componentes y consumibles deben ser nuevos. Los modelos ofertados en la licitación deben ser los más actuales de su serie, debiéndose acreditar mediante el Certificado de Lanzamiento al Mercado del producto o similar.
- ▶ Todos los componentes y consumibles deben ser de la propia marca, no pudiéndose usar otros compatibles u otras marcas genéricas.
- ▶ Tipología de Red de las oficinas:



SEDE	Línea de DATOS		Línea Respaldo	Oficina Atención Cliente
ETAP Besós	MacroLan	100 / 30	MacroLan	
Badalona	MacroLan	30 / 30	MacroLan	X
Gavà	MacroLan	30 / 30	MacroLan	X
Hospitalet	MacroLan	30 / 30	MacroLan	X
Consell de cent	MacroLan	30 / 30	MacroLan	X
Pallars	MacroLan	100 / 30	MacroLan	
Collblanc	MacroLan	1G / 400	MacroLan	
Cornellá	MacroLan	1G / 200	MacroLan	
Sant Joan Despi	MacroLan	100 / 90	ADSL	
EDAR Montcada	MacroLan	10 / 2	MacroLan	
EDAR Besos	MacroLan	100 / 30	ADSL	
EDAR El Prat	MacroLan	10 / 9	ADSL	
EDAR St. Feliu	MacroLan	10 / 9	MacroLan	
EDAR Vallvidrera	ADSL	3 / 1	3G	
EDAR Gavà	MacroLan	10 / 2	ADSL	
EDAR Bagues	ADSL	3 / 1	3G	

7.1. Seguridad y Confidencialidad de la información

Toda la información contenida en los discos duros de los dispositivos de impresión son propiedad de Aigües de Barcelona, Empresa Metropolitana de Gestió del Cicle Integral de l'Aigua, S.A. El prestador del servicio deberá cumplir con las certificaciones de confidencialidad y la política de protección de datos GDPR.



El Servicio debe garantizar la confidencialidad de la información, y de la impresión de los documentos de cada usuario.

Los discos duros de los dispositivos deben estar encriptados, y una vez retirados deberán ser formateados y los datos destruidos, certificando a AB que estos no pueden ser recuperados. El responsable de la recepción a tal efecto será el responsable del contrato de AB.

7.2. Seguridad Corporativa

Tanto el Prestador del Servicio como sus trabajadores deberán respetar las normas y regulaciones internas 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 N° 3**).
- Dar cumplimiento a todas las normas, políticas y marcos reguladores vigentes durante el periodo del contrato.
- Permitir y facilitar la realización de auditorías de cumplimiento de las normativas establecidas para Seguridad Corporativa, internas o externas, sobre los sistemas de información vinculados a la prestación del servicio, y garantizar la posibilidad de trazabilidad de las acciones realizadas por el auditor para facilitar el seguimiento de las mismas y sus posibles impactos no deseados.
- Custodiar los equipos, así como la información que contengan relativa a Aigües de Barcelona.

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.

7.2. Características Técnicas requeridas para la Gestión del Servicio de Impresión

En este apartado se describen las características técnicas mínimas requeridas para gestionar el servicio:

La arquitectura, el hardware, componentes y elementos que configuran el sistema de impresión, además, deben:

Accountig:

- ▶ Ser capaces de recoger la actividad de impresión, copias o escaneo directamente de cada dispositivo de impresión, de modo que la información mostrada siempre se corresponderá con la información real de los dispositivos.
- ▶ Generar informes para la obtención de datos por uso por equipo, usuario, departamento, edificio, etc., de manera que se puedan asignar costes internamente.
- ▶ Fijar cuotas de impresión por usuario, agrupación contable de AB o departamento, y por tipo de impresión B/N y Color.
- ▶ Contabilizar todas las impresiones y relacionarlas con un usuario del Directorio Activo (en adelante "AD"), independientemente de si se han realizado a través de un servidor de impresoras o directamente a las impresoras.
- ▶ Permitir ejercer el control sobre el cobro de copias e impresiones a usuarios o departamentos, y generar el fichero de imputación de costes.

Seguridad, Privacidad, confidencialidad y gestión de accesos:

- ▶ Debe permitir la aplicación de políticas de seguridad y de restricción del uso de los equipos a nivel general (cuota de impresión), a nivel de opciones (Doble cara, color, etc...).
- ▶ Permitir establecer políticas de impresión por grupos del AD e Integración con el Directorio Activo y LDAP de Aigües de Barcelona.
- ▶ Disponibilidad de protocolos de seguridad SSL y comunicación encriptada.
- ▶ Encriptación de los datos de los discos duros de las impresoras mediante algoritmo de encriptación "AES256"



- ▶ Encriptación de los logs de las impresoras.
- ▶ Permitir programar una tarea para eliminar los trabajos de los usuarios.
- ▶ Permitir la configuración de borrado periódico de datos de los discos duros, mediante un Proceso Programado.
- ▶ Mantener la información en las sustituciones de los discos duros.
- ▶ Permitir programar un time-out de sesión de usuario por inactividad.
- ▶ Permitir el uso de Usuarios temporales "Invitados" sin necesidad de dar de alta en el AD.
- ▶ Permitir la impresión delegada.
- ▶ Permitir el uso sin usar una cola de Impresión Windows (acceso por Web, email, etc.)
- ▶ Garantizar la confidencialidad de los documentos e impresiones.
- ▶ Autenticación de los usuarios mediante lectura tarjetas RFID, NFC, además de PIN + Password utilizando el Directorio Activo de Aigües de Barcelona. Se valorará el acceso por huella digital.
- ▶ Disponer de funcionalidades con el objetivo de reducir la impresión inapropiada, errónea o innecesaria.
- ▶ Permitir el control remoto de los dispositivos de impresión.
- ▶ Gestionar las colas virtuales de impresión de manera que la impresión no se libere hasta que el usuario la reclame desde cualquier dispositivo de impresión (Follow-Me).
- ▶ Permitir colas de impresión directas de los PC's a las impresoras y colas virtuales, en las que la impresión quedará en espera de ser reclamada por el usuario, pudiendo elegir este desde que cola quiere que se libere el trabajo.
- ▶ Dispondrá de una consola de gestión de eventos, para la monitorización proactiva de los dispositivos en cuanto a averías y consumibles.
- ▶ Personalización del panel de multifunción por usuario o grupos de usuarios.
- ▶ Gestión de la impresión descentralizada para oficinas de atención al cliente, para evitar exceso de tráfico por la red corporativa. La impresora hace de servidor dentro de la oficina y reporta el log para el Accounting o auditoria.
- ▶ Escaneo a Mail.
- ▶ Escaneo a unidad de Red, OneDrive, FTP, SharedPoint y PenDrive.
- ▶ Conversión de documentos escaneados mediante OCR integrado a Word, Excel, PowerPoint, pdf, etc.
- ▶ Posibilidad de integración con otras aplicaciones por WebServices para automatizar el flujo de digitalización.
- ▶ Impresión directa desde PenDrive.
- ▶ Impresión de Movilidad a través de entorno web, para dispositivos que no se encuentren en la red corporativa o dispositivos no registrados en el Directorio Activo (PCs, Tablets, SmartPhones, etc.), los cuales sean capaces de lanzar y liberar las impresiones.
- ▶ Todas las impresoras tendrán la capacidad de imprimir papel de etiquetas y papel reciclado.
- ▶ Si no se presenta ningún software de gestión, el licitador podrá ser descartado.

7.3. Características Técnicas de los dispositivos

Los servidores físicos o virtuales (si fueran necesarios) que soporten los productos y herramientas de software de la solución ofertada pueden ser suministrados por el prestador del servicio si así lo requiere AB, y se deben ajustar a las características técnicas y homologadas por de AB. Los servidores, estarán ubicados en el Centro de Procesos de Datos de Aigües de Barcelona.



El proveedor se hará cargo del mantenimiento del software en los servidores para la prestación del servicio.

El departamento de TI de AB será el responsable del Windows, Parches, y sistema de Backup sobre estos servidores. Deberá ser una infraestructura basada en ServerLess y estrategias Cloud, sin que represente pérdida de funcionalidades.

Las características técnicas de los sistemas de impresión de detallan en el **Anexo I**.

8. GESTIÓN DE LA CALIDAD DEL SERVICIO

El objetivo de disponer de unos acuerdos de nivel de servicio es proporcionar un ciclo de medición y análisis de la calidad del servicio prestado. El ANS aplica a todos los servicios de Gestión, Software y dispositivos multifuncionales e impresoras.

8.1. Operativa del Servicio

Las operativas de servicio están sujetas a ANS.

Peticiones: Toda petición debe ser reportada informando del número de serie de la máquina afectada a través de la herramienta de ITSM REMEDY de Aigües de Barcelona. El técnico del proveedor determina el grado de la petición y abre aviso de intervención. Supuestos de peticiones:

- ▶ Alta y baja de impresoras
- ▶ Instalación y retirada de impresoras
- ▶ Cambios de ubicación de impresoras
- ▶ Operativas de administración en la plataforma
- ▶ Gestión de Accesos

Incidencias: Una incidencia podrá deberse a cualquier funcionalidad que componga el servicio, por ejemplo: copia, fax, escaneo, escaneo con OCR, impresión, impresión desde dispositivos móviles, solución de software, solución scan to OneDrive, accesos. A continuación, se detallan las diferentes incidencias dentro del Servicio:

- ▶ Mal funcionamiento detectado y comunicado al proveedor del Servicio a través de la herramienta ITSM, teléfono o correo.
- ▶ Evento registrado como tal por el sistema de monitorización.
- ▶ Situación identificada en una visita preventiva.
- ▶ Incidencia tipo problema, es decir una incidencia repetitiva.
- ▶ Indisponibilidad del servicio.
- ▶ Fallos en la plataforma.
- ▶ Reposición de tóner y botes de residuos.

En el caso de que una incidencia no esté resuelta en los plazos y condiciones establecidos , el equipo deberá ser sustituido por un equipo similar o de igual características, según lo especificado en el **apartado 8.6** del presente pliego

Reclamaciones: Según la naturaleza de la reclamación, Aigües de Barcelona tendrá a su disposición un ServiceManager que será el responsable de resolver dicha reclamación con la máxima celeridad.



8.2. ANS

Los Acuerdos de Niveles de Servicio (en adelante, "ANS") son medidos mensualmente y son reflejados en los diferentes informes de seguimiento del Servicio. El seguimiento del servicio será mensual.

El siguiente cumplimiento de niveles de servicio se basa en el horario laboral de: 8h a 18h.

8.3. Definición indicadores de niveles de servicio

ANS	Descripción
Tiempo de respuesta	El tiempo se calcula desde que el ticket es registrado en la herramienta de ITSM y asignado al grupo de resolución del Servicio de Impresión, hasta el inicio de las actividades* ¹ encaminadas a la solución del ticket por parte del proveedor de servicio.
Tiempo de Atención	El tiempo se calcula desde que el ticket es asignado al grupo de resolución del servicio de impresión de AB, hasta realizar una valoración sobre la solución de la incidencia. Este tiempo incluye, si es necesario, la presencia in-situ en las oficinas de AB para solucionar la incidencia.
Solución Incidencias	El tiempo se calcula desde que ticket es registrado en la herramienta de ITSM y asignado al grupo de resolución del Servicio de Impresión, hasta que el dispositivo queda totalmente operativo.
Solución de peticiones	El tiempo se calcula desde que ticket es registrado en la herramienta de ITSM y asignado al grupo de resolución del Servicio de Impresión, hasta que la petición está resuelta en su totalidad.
Instalación de dispositivos	El tiempo se calcula desde que se realiza solicitud formal de instalación hasta que el dispositivo queda totalmente operativo.
Entrega de Consumibles	El tiempo se calcula desde que aparece alerta de falta de consumible en sistema de monitorización hasta que el consumible es entregado en la sede correspondiente.
Tiempo reposición stock consumibles	Tiempo que transcurre desde que el ticket es registrado en la herramienta ITSM y asignado al grupo de resolución del Servicio de Impresión, hasta que se realiza la entrega de este en la ubicación requerida
Retirada de equipos	El tiempo se calcula desde que ticket es registrado en la herramienta de ITSM y asignado al grupo de resolución del Servicio de Impresión, hasta que el equipo es retirado.
Indisponibilidad global del servicio	Tiempo que el servicio está indisponible o con un servicio degradado* ²
Reapertura de tickets	Numero de tickets que se reabren por no conformidad con su resolución.
Reporte de la Actividad	Mide las entregas de informes acordados mensuales y de los diferentes Comités de Seguimiento del Servicio.

*1. Se considera inicio de actividad en el momento en que el ticket es registrado y asignado al grupo de resolución del servicio de impresión de AB.

*2. Sin tener en cuenta las paradas planificadas.



8.4. Indicadores de nivel de servicio

ANS	PERIODICIDAD PARA CALCULO ANS	TIEMPO	CUMPLIMIENTO
Tiempo de respuesta	Mensual	4h	≥97%
Tiempo de Atención	Mensual	8h	≥97%
Solución Incidencias	Mensual	16h	≥97%
Solución de peticiones	Mensual	24h	≥97%
Instalación de dispositivos	Anual	15 días	≥97%
Entrega de consumibles	Mensual	2 días	≥97%
Tiempo reposición stock consumibles	Mensual	24h	≥97%
Retirada de equipos	Semestral	5 días	≥97%
Indisponibilidad global del servicio	Anual	-	≥99%
Reapertura de tickets	Mensual	-	≥97%
Reporte de la Actividad	Anual	-	≥97%

*El cómputo para el cálculo de horas se realizará sobre las horas laborables establecidas en el servicio.



8.5. Penalizaciones por incumplimiento del nivel de servicio

Se aplicarán penalizaciones si en 3 meses consecutivos se produce un incumplimiento de ANS en cualquiera de los indicadores mencionados anteriormente, siempre y cuando el número de incidencias durante este periodo supere las 10. El valor porcentual a considerar para el cálculo de las penalizaciones será el del Nivel de Servicio más bajo acontecido durante el periodo (3 meses). La penalización será efectiva sobre la facturación del mes siguiente a la revisión del Nivel de Servicio (ANS).

Se podrá aplicar penalizaciones sobre la facturación de coste por página, según el siguiente cuadro:

Nivel de servicio	Penalización % sobre la facturación de coste por página del periodo			
	N/A	10%	20%	30%
Tanto por ciento:	N/A			
100-99	X			
98-85		X		
84-80			X	
< 80				X

8.6. Equipos con avisos repetitivos

En el caso que un equipo tenga 2 o más avisos de avería (no imputables a mal uso por parte del usuario), en el plazo de un mes, durante dos meses consecutivos, será reemplazado por uno del mismo modelo o características superiores. Igualmente, en el caso que un dispositivo tenga más de 6 incidencias con el mismo síntoma en el plazo de un año, será reemplazado por uno del mismo modelo o características superiores.

Los tiempos para reemplazar un dispositivo por repetición de avisos serán los estipulados para el indicador de instalación de dispositivos.

9. DETALLE DIMENSIONAMIENTO

La valoración económica de la licitación se realizará por la cantidad total de todos los componentes del Servicio de Impresión, incluyendo los costes derivados de la implantación del proyecto y despliegue.

9.1. Dimensionamiento de equipos según su tipología

Tipo I	11
CORNELLA	3
EDAR GAVA	1
EDAR MONTCADA	2
EDAR PRAT	1
SANT JOAN DESPI	3
EDAR LA LLAGOSTA	1
Tipo II	13
BADALONA	1
COLLBLANC	2
CONSEJO DE CIENTO	2
CORNELLA	4
EDAR BESOS	1
GAVA	1



HOSPITALET	1
SANT JOAN DESPI	1
Tipo III	37
BADALONA	6
COLLBLANC	3
CONSEJO DE CIENTO	11
EDAR PRAT	3
GAVA	5
HOSPITALET	7
PALLARS	1
ETAP BESOS	1
Tipo IV	13
COLLBLANC	3
EDAR BESOS	1
EDAR GAVA	1
EDAR PRAT	1
EDAR SAN FELIU	2
GAVA	1
SANT JOAN DESPI	4
Tipo V	15
BADALONA	2
COLLBLANC	3
CORNELLA	3
EDAR BESOS	1
EDAR MONTCADA	1
EDAR SAN FELIU	1
SANT JOAN DESPI	3
SEDE SINDICAL	1
Tipo V + Clasificador	13
BADALONA	2
COLLBLANC	1
CONSEJO DE CIENTO	1
CORNELLA	1
EDAR BESOS	1
EDAR GAVA	1
EDAR PRAT	1
GAVA	2
HOSPITALET	1
PALLARS	2
Tipo VI + Clasificador	8
COLLBLANC	7
PALLARS	1
Total general	110



9.2. Volumetría de impresión

	Estimación Anual (Copias)
BN	2.563.977
Color	1.315.804

Estos volúmenes son aproximados y se han calculado con el dimensionamiento actual del parque de impresoras de AB. No obstante, el presente pliego no garantiza ningún volumen mínimo de impresión, ya que se utilizan estrategias incorporadas en esta prestación y descritas en el presente pliego de prescripciones técnicas para intentar reducir tanto como sea posible el volumen de impresiones realizadas.

10. PROYECTO IMPLANTACIÓN

El proyecto de implantación debe garantizar una puesta en marcha en el tiempo y forma acordada, así como una rápida adaptación de los usuarios a los nuevos equipos y dispositivos. Deberá especificarse un proyecto de implantación donde se detalle cada una de sus fases, que incluya una gestión del cambio y plan de comunicación, documentación y formación in-situ a usuarios y técnicos.



10.1. Metodología

Se deberá detallar los siguientes puntos:

- ▶ De desarrollo, especificar ciclo de vida del proyecto con sus fases.
- ▶ De implantación (pilotos incluidos en caso de ser necesario).
- ▶ De estrategia de pruebas (plan de pruebas, tipos de prueba, entornos necesarios, etc....).
- ▶ Gestión de riesgos.
- ▶ Definición de los criterios de aceptación de los hitos del proyecto.

10.2. Marco organizativo del proyecto. Roles

Descripción de la organización del proyecto, de los recursos asignados y de las funciones de cada uno de ellos:

- ▶ Jefe de Proyecto: que pueda acreditar 3 o más años de experiencia en proyectos de igual o mayor alcance.
- ▶ Consultor Senior: que pueda acreditar 3 o más años de experiencia en proyectos de igual o mayor alcance.
- ▶ Técnico Senior: que pueda acreditar 3 o más años de experiencia en proyectos de igual o mayor alcance.
- ▶ Consultor de gestión de cambio: que pueda acreditar 3 o más años de experiencia en proyectos de igual o mayor alcance.

10.3. Planificación y plan de implementación

Adaptar una planificación y despliegue progresivo, teniendo en cuenta las necesidades de AB y priorizando la continuidad del negocio, no pudiendo en ningún caso generar una indisponibilidad en el Servicio y operativa del negocio. El periodo de despliegue de la solución y suministro se realizará dentro de los 3 meses siguientes a partir de la fecha de la firma del contrato.

- ▶ Periodicidad y contenido de las entregas (Entrega 1, Entrega 2... Entrega X)



- ▶ Periodicidad y Despliegue en las ubicaciones (Ubicación 1, Pruebas Ubicación 1, Despliegue Ubicación 2, Pruebas Ubicación 2...)
- ▶ Periodicidad sobre Gestión del Cambio
- ▶ Los hitos y su valor para el cálculo del Grado de Avance Técnico (GAT)

10.4. Gestión del Cambio

Establecer un programa de acogida y plan de comunicación de la nueva solución, donde se incluyan materiales para la comunicación al usuario tales como por ejemplo trípticos, audiovisuales, manuales, etc.

Se deberán planificar y gestionar las oleadas de migración.

10.5. Formación

Establecer un plan de formación que contemple al menos los siguientes aspectos:

- ▶ Las formaciones se realizarán in-situ en la sede donde se haya instalado la/s impresora/as. Se establecerán dos convocatorias de formación en fechas distintas para cada sede.
- ▶ Formación a usuarios: se deberá establecer un plan de formación del personal en el manejo de los dispositivos, opciones de impresión, así como en la resolución de las pequeñas incidencias diarias que pudiesen surgir y la sustitución de consumibles.
- ▶ Formación para personal de TI: se deberá realizar una formación específica para el departamento de TI en el que se detallen los elementos de la infraestructura, características, su ubicación y configuración, manejo de los dispositivos, administración del software de gestión, y el procedimiento para la gestión de incidencias.

10.6. Documentación y Traspaso de conocimiento TI

Se realizarán las sesiones de traspaso de conocimiento al departamento de TI de AB, y se entregará la documentación necesaria, con al menos la siguiente información:

- ▶ Entrega de manuales y guías, presentaciones o audiovisuales de funcionamiento de los diferentes equipos involucrados en cada uno de los centros en formato electrónico para ser incorporados en el repositorio de documentación de Aigües de Barcelona.
- ▶ Documentación de los dispositivos: Manuales, certificado de garantía, certificado de cumplimiento de normativa medioambiental y guía de usuario.
- ▶ Equipos instalados, características y localización.
- ▶ Gestión del software de Facturación.
- ▶ Gestión del software de Administración, tanto de la parte servidora, como de las consolas de las impresoras.
- ▶ Manuales y guías de usuario.
- ▶ Características de servicio técnico, métodos de contacto.



11. DEVOLUCIÓN DEL SERVICIO

Con la finalidad de ordenar la devolución del servicio sin afectación al propio servicio prestado al cliente, esta devolución se realizará en dos fases diferenciadas:

- ▶ Fase de preparación de salida.
- ▶ Fase de transición de salida.

11.1. Fase Preparación Salida

En esta fase continúa el servicio prestado por este contrato, sin embargo se requiere preparar la sustitución de servicio/contrato, aportando en estas fases los recursos necesarios para que los niveles de servicio no se vean afectados, y sin que ello represente un coste adicional para AB.

El prestador del servicio se obliga a que en la semanas previas a la finalización del servicio prestará la máxima colaboración para la trasferencia del servicio al nuevo contratista: transferencia de documentación, formación, demostración de procedimientos, proceso de facturación, etc.

El prestador del servicio se compromete a facilitar toda la documentación generada por el servicio: CMDB, planos y ubicaciones.

El prestador del servicio deberá facilitar un informe ejecutivo sobre el servicio prestado donde conste un resumen anual sobre las volúmetrías descritas en el **apartado 6.11**.

Toda la información se debe facilitar en formatos .pdf y .csv

La fase de preparación de salida forma parte de los términos de la ejecución del contrato vigente.

11.2. Fase de Transición de Salida

Se prevé que al final del contrato se producirá una renovación de los equipos suministrados, la infraestructura de hardware y sus licencias, por nuevos equipos aprovisionados por un nuevo contrato resultado de una licitación similar a la actual.

En esta fase el nuevo contratista instalará sus equipos y software según el proyecto de implantación descrito en la nueva licitación, ajustándose en plazo con la retirada de los equipos proporcionados en este contrato. Se empezará la sustitución por los equipos más críticos. Tanto el prestador del servicio de este contrato, como el nuevo adjudicatario resultante de la nueva licitación, deberán colaborar para garantizar una transición sin impacto en el servicio y por consiguiente a los usuarios.

La responsabilidad de la retirada de los equipos recaerá en el adjudicatario del presente contrato, y se ajustará a lo descrito en el **apartado 6.6**.

Durante esta fase los volúmenes de impresión asociados a este contrato se reducirán progresivamente hasta que sean 0.

La duración de esta fase se prevé dentro de los 3 primeros meses desde la firma del nuevo contrato pudiéndose extender hasta 6 meses.

El prestador del servicio del presente contrato estará obligado a continuar prestando el servicio hasta la finalización del periodo de transición con las mismas condiciones económicas de este contrato.



12. ANEXOS

Anexo I: Tipología de impresoras

A Continuación, se detalla la tipología de las impresoras y las características mínimas técnicas imprescindibles que deben cumplir:

	Tipo I	Tipo II	Tipo III	Tipo IV	Tipo V	Tipo VI
Tipo de Dispositivo	Impresora BN A4	Impresora Color A4	Multifuncional BN A4	Multifuncional Color A4	Multifuncional Color A3	Multifuncional Color A3
Tecnología	Láser	Láser	Láser	Láser	Láser	Láser
Velocidad Impresión a una cara	40 ppm	20 ppm	50 ppm en B/N	30 ppm en B/N	30 ppm en B/N	45 ppm en B/N
Velocidad Escaneo a doble cara			40 ppm cen Color	40 ppm cen Color	100 ppm cen Color	160 ppm cen Color
Alimentador de Originales			Escaneo a doble cara en una sola pasada	Escaneo a doble cara en una sola pasada	Escaneo a doble cara en una sola pasada	Escaneo a doble cara en una sola pasada
Fomato Escaner			PDF, PDF Buscable, TIFF, JPG			
Envío Escaner			SMB2, SMTP, FTP	SMB2, SMTP, FTP, OneDrive, Sharepoint	SMB2, SMTP, FTP, OneDrive, Sharepoint	SMB2, SMTP, FTP, OneDrive, Sharepoint
Funcion Escaneo Rápido			A carpeta de Red / Email			
Impresión Privada			Follow-Me	Follow-Me	Follow-Me	Follow-Me
Escaneo Privado				Scan-Me	Scan-Me	Scan-Me
Autenticación RFID			RFID tipo MIFARE	RFID tipo MIFARE	RFID tipo MIFARE	RFID tipo MIFARE
Autenticación AD			Usuario + Pass	Usuario + Pass	Usuario + Pass	Usuario + Pass
Pantalla Digital			SI	SI	SI	SI
Tiempo de Calentamiento	< 20 Seg	< 20 Seg	< 25 Seg	< 20 Seg	< 20 Seg	< 20 Seg
Tiempro de primera impresión	< 10 Seg	< 10 Seg	< 8 Seg	< 8 Seg	< 8 Seg	< 8 Seg
Calidad de Impresión	600x600 ppp	600x600 ppp	1200x1200 ppp	600x600 ppp	600x600 ppp	600x600 ppp
Bandeja de Entrada Papel	> 250 hojas	> 250 hojas	>= 500 hojas	>= 500 hojas	>= 500 hojas	>= 500 hojas
Bandeja Bypass	> 50 hojas					
Gramaje			Hasta 220 g/m2	Hasta 220 g/m2	Hasta 300 g/m2	Hasta 300 g/m2
Bandeja Entrada Papel Adicionales	Opcional	Opcional	Opcional	3 adicionales >=500 hojas	3 adicionales >=500 hojas	3 adicionales >=500 hojas
Finalizador Clasificador					Opcional	Opcional
Duplex	Automático	Automático	Automático	Automático	Automático	Automático
Memoria RAM	>= 512Mb	>= 512Mb	>= 1024Mb	>= 1024Mb	>= 3GB	>= 3GB
HDD					>= 160Gb Encriptado	>= 160Gb Encriptado
Red	10/100/1000	10/100/1000	10/100/1000	10/100/1000	10/100/1000	10/100/1000
FAX					SI	SI
Impresión Códigos de Barras	EAN8, EAN13, EAN128					
Volumen Medio Sostenido Mensual	> 13000 Paginas	> 9000 Paginas	> 13000 Paginas	> 18000 Paginas	> 18000 Paginas	> 24000 Paginas
Duración del Toner			> 15000 Paginas	> 15000 Paginas	> 15000 Paginas	> 15000 Paginas
Duración del Tambor			> 50000 Paginas	> 50000 Paginas	> 50000 Paginas	> 50000 Paginas
Medidas (En Cm)	Máximo: 37 x 42 x 34 Ancho x Profundo x Alto	Máximo: 40 x 45 x 32 Ancho x Profundo x Alto	Máximo: 47 x 48 x 58 Ancho x Profundo x Alto	Máximo: 56 x 51 x 80 Ancho x Profundo x Alto	Máximo: 68 x 80 x 80 Ancho x Profundo x Alto	Máximo: 68 x 80 x 80 Ancho x Profundo x Alto



▶ **Tipo I - Servicio de Impresión de puesto de trabajo individual BN**

Servicio de Impresión de puesto de trabajo individual. Se corresponde a puestos de trabajo en los que por su ubicación física o por las características de las tareas que se realizan es necesario un equipo de impresión junto al ordenador personal.

▶ **Tipo II - Servicio de Impresión de puesto de trabajo individual Color**

Servicio de Impresión de puesto de trabajo individual y equipos de Autoservicio (ver imágenes). Se corresponde a puestos de trabajo en los que por su ubicación física o por las características de las tareas que se realizan es necesario un equipo de impresión asociado. Los licitadores podrán ofertar cinco (5) dispositivos Tipo II con salida de impresión invertida, tal como se especifica en la cláusula 11 del del Pliego de Condiciones Particulares (PCP).



▶ **Tipo III - Servicio de Impresión puesto trabajo Comercial**

Servicio de Impresión de puesto de trabajo Comercial. Se corresponde a puestos de trabajo en los que por su ubicación física o por las características de las tareas que se realizan es necesario un equipo de Multifunción junto al ordenador personal.

▶ **Tipo IV - Servicio de Impresión media capacidad A4**

Servicio de Impresión de Departamental media capacidad A4 ubicado en puestos comunes.

▶ **Tipo V - Servicio de Impresión grandes formatos y media capacidad**

Servicio de Impresión de Departamental media capacidad A3 ubicado en puestos comunes. Estos modelos de impresora deberán incorporar clasificador para el número de dispositivos indicados en el **apartado 9.1**.

▶ **Tipo VI - Servicio de Impresión grandes formatos y alta capacidad**

Servicio de Impresión de Departamental alta capacidad A3 ubicado en puestos comunes. Estos modelos de impresoras deberán incorporar clasificador. **Ver apartado 9.1**



Anexo II: Sedes Corporativas

En este apartado se describen las Sedes corporativas de Aigües de Barcelona:

SEDE	DIRECCIÓN	C.P.	POBLACIÓN	Oficina Atención Cliente
BADALONA	Creu, 67-69	08912	Badalona	X
ETAP BESÓS	Carretera de Ribes, s/n	08030	Barcelona	
CORNELLÀ	Crtra. De Sant Joan Despí, 1	08940	Cornellà	
SANT JOAN DESPÍ	Crtra. Santa Creu a Calafuell (C-245), s/n	08970	Sant Joan Despí	
COLLBLANC	General Batet, 1-7	08028	Barcelona	
CONSELL DE CENT	Consell de Cent 396	08009	Barcelona	X
GAVÀ	Olocau, 6	08850	Gavà	X
HOSPITALET	Baró de Maldà, 26-28	08901	Hospitalet de Llobregat	X
PALLARS	Pallars, 477	08019	Barcelona	
SEDE SINDICAL	Calle Clot 187 ent-2	08027	Barcelona	
EDAR BESÓS	Final Rambla Prim interior s/n	08019	Barcelona	
EDAR EL PRAT	Avinguda Estany de Port s/n	08820	El Prat de Llobregat	
EDAR GAVA	Crtra. C-31, Km. 186,9	08840	Viladecans	
EDAR LA LLAGOSTA	Camí de Barcelona a Puigcerdà, s/n (Polígono Industrial Mas Rampinyo)	08110	Montcada i Reixac	
EDAR MONTCADA	Ctra. de la Roca Km 6,5	08110	Montcada i Reixac	
EDAR SANT FELIU	Riera de la Salut s/n (Costat B-23)	08980	Sant Feliu de Llobregat	
EDAR VALLVIDRERA	Ctra. de Vallvidrera a Sant Cugat Km 6,5	08198	Vallvidrera	



**"NORMAS DE SEGURIDAD IT DE
AIGÜES DE BARCELONA"**

ÍNDICE

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



1. Objeto e introducción del documento

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

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

El intercambio de información o software calificados como de uso interno, restringido o confidencial que realice 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 autenticación y se garantice su identificación unívoca.

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

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

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

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

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



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

3.2. Administración segura

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

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

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

4. Identificación y autenticación de usuarios

Todos los sistemas de información no públicos de las unidades y sociedades operativas de 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 autenticación de cada sistema se podrá implantar mediante:

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

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

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

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

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

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

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

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

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



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

5. Identificación de usuario

El acceso a cualquiera de los sistemas de información de 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.