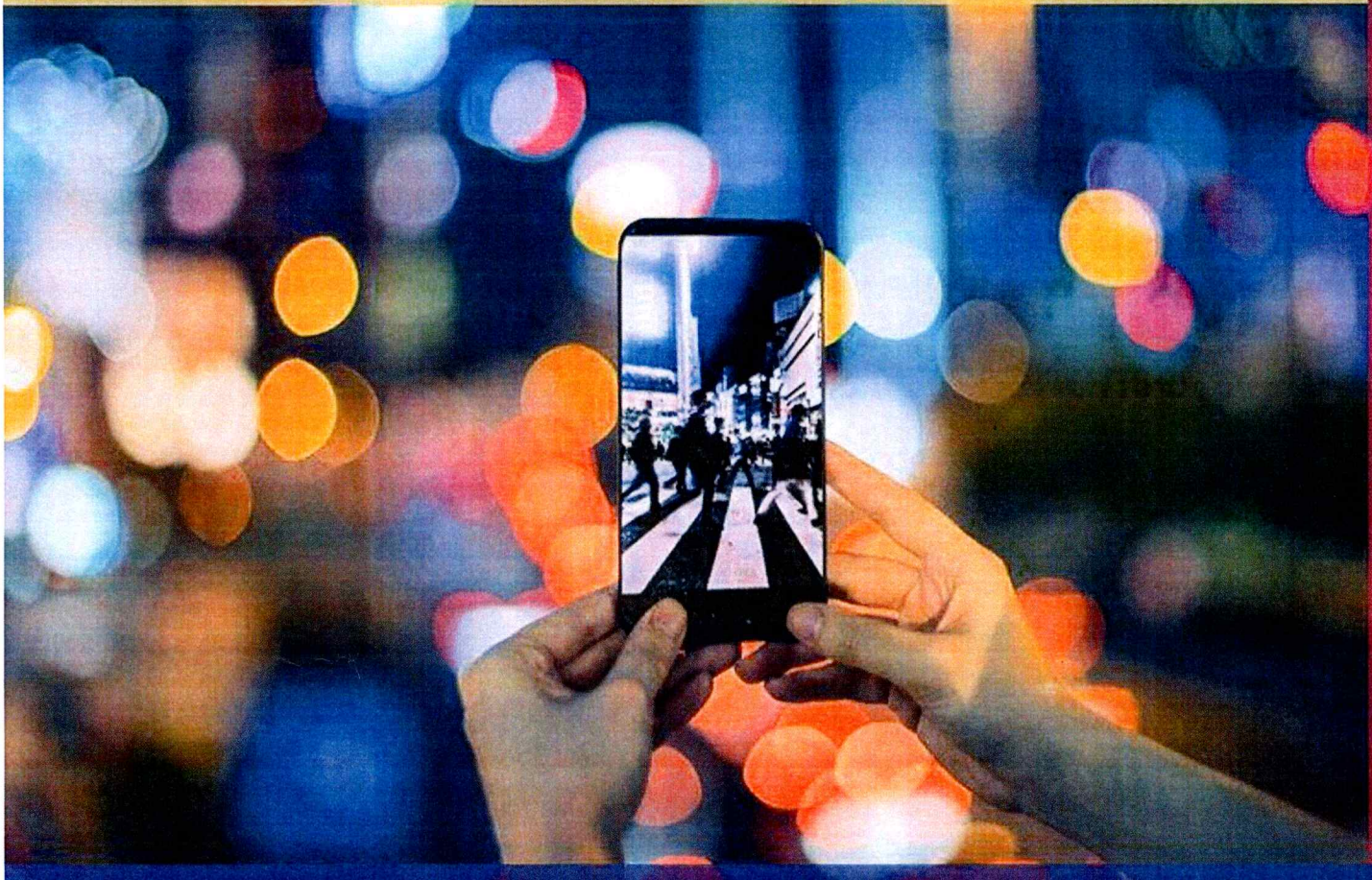
Consorcio Gestión del Ciclo Integral del Agua de Uso Urbano en el Poniente Almeriense

SICALWin

Tipo de documento: Privado



Índice

1. Objetivos y alcance

Este documento contiene la propuesta económica que *aytos Berger-Levrault* presenta a *Consorcio Gestión del Ciclo Integral del Agua de Uso Urbano en el Poniente Almeriense* para la prestación de los siguientes servicios:

- Servicio de soporte y mantenimiento, nivel estándar, de la aplicación SICALWin.

2. Servicio de Soporte y Mantenimiento

El **Servicio de Soporte y Mantenimiento**, que aytos Berger-Levrault ofrece desde la puesta en marcha de sus soluciones, facilita el uso correcto de los sistemas de información para **garantizar una implantación efectiva, obtener el máximo rendimiento de las aplicaciones, y la resolución de consultas o dudas de los usuarios**, a través de las siguientes prestaciones:

- Soporte y Atención Telefónica Especializada.
- Plataforma Web con Área de Clientes.
- Actualización del Software Contratado.

El modelo de gestión de las peticiones está alineado con la **metodología ITIL** y se basa en tres elementos clave:

- Registro y procesamiento de las peticiones.
- Priorización basada en el impacto que supone cada petición al usuario final.
- Niveles de servicio establecidos.

Se dispone de un **equipo de trabajo especializado y dedicado exclusivamente al Servicio de Atención a los Clientes**, cuya actividad se centra en atender las peticiones recibidas en base a los niveles de servicio definidos. A partir de estas premisas se establecen las pautas para ofrecer un servicio de calidad y optimizar la gestión de las peticiones recibidas.

2.1 Servicio de Soporte Telefónico, Nivel Estándar

El servicio de asistencia telefónica es atendido por orden de entrada de llamadas, y según su nivel de mantenimiento. La primera vez que acceda deberá identificarse con su usuario y clave, que será ligada al teléfono desde que el que realiza la llamada, para sucesivas ocasiones.

1. Acceso

- Teléfonos de contacto: 955 283 621/ 934 864 601.
- Horario:

- Horario de verano (comprendido entre el 16 de junio y el 15 de septiembre, aproximadamente): De 8:00 a 15:00 horas, de lunes a viernes.

- Horario de invierno: De 8:00 a 15:00 horas, de lunes a viernes; y de 16:00 a 19:30 horas, de lunes a jueves.

2. Consultas e incidencias

A través del Servicio de Soporte de aytos Berger-Levrault podrá realizar consultas acerca del uso de los productos contratados, y/o reportar incidencias en su funcionamiento. Nuestros expertos en cada materia atenderán su llamada, para darle una solución específica adaptada a su solución. Cualquier cambio en la gestión de los asuntos reportados se comunicará vía correo electrónico.

3. Solicitud de modificaciones funcionales

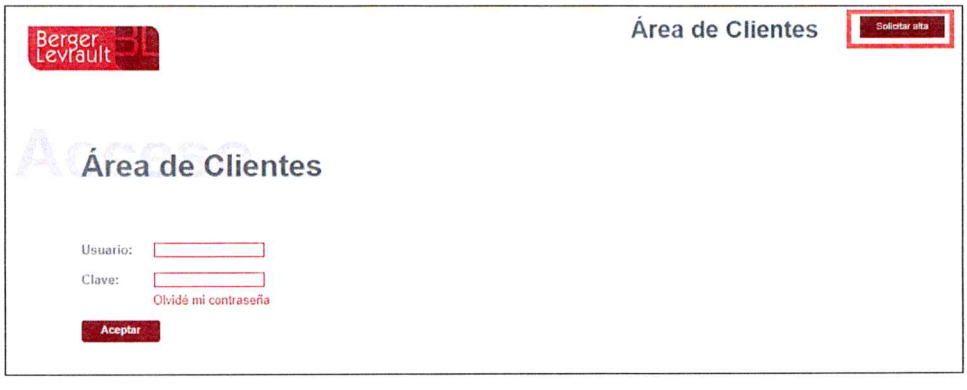
La Entidad podrá solicitar modificaciones y/o adaptaciones funcionales sobre las aplicaciones contratadas. El responsable producto analizará y valorará dichas modificaciones. En caso de ser aceptada, la petición será trasladada al equipo de desarrollo e incluida en el roadmap de producto; y, en caso de ser descartada, se informará a la Entidad, justificándose el motivo del rechazo.

2.2 Servicio de Soporte Telemático, Nivel Estándar

A través del Área de Clientes de la Web, se pueden realizar las mismas comunicaciones que se pueden hacer a través del Servicio de Soporte Telefónico, así como, consultar el estado de tramitación de cada una de las solicitudes realizadas con anterioridad, a través del teléfono o de la web. La plataforma web en la que pueden realizarse estas gestiones es: https://www.berger-levrault.com/es/areadeclientes/index.html

1. Acceso

Tanto el alta de acceso, como el alta de nuevos usuarios, se solicitarán a través del Área de Clientes de la web de aytos Berger-Levrault.



2. **Registro de consultas**
   Si prefiere no utilizar el teléfono, ponemos a su disposición la posibilidad de registrar sus consultas o incidencias con el grado de detalle que desee desde esta plataforma. Será atendida por un equipo especializado y con los mismos criterios que las llamadas telefónicas.
   Cualquier cambio en la gestión de los asuntos reportados se comunicará vía correo electrónico.

3. **Información del estado de las consultas registradas.**
   Podrá ver la información del estado de las incidencias registradas a través de la plataforma.

4. **Gestión de los datos de contacto de la Entidad y de los usuarios asociados a la Entidad.**
   Todos los usuarios que cuenten con acceso a esta área de Clientes podrán modificar y actualizar sus datos en cualquier momento. Solo el/los Administrador/es de la Entidad podrán cambiar o eliminar datos de todos los usuarios registrados para su organización.

2.3 Área de Clientes de la web

A través del Área de Clientes de la Web, la Entidad también tendrá a su disposición los siguientes servicios:

1. **Servicio de Asistencia Remota**
   A través del Servicio de Asistencia Remota los técnicos de aytos Berger-Levrault podrán conectarse a las instalaciones de su Entidad, y realizar la verificación de lo comunicado a través del Servicio de Soporte, o explicar de manera práctica el modo de operar cuando es compleja su explicación a través de otra vía.

2. **Formación on-line continuada**
   La Entidad dispondrá de formaciones on-line periódicas (webinars), de modo que se podrán acceder a ellas en el momento que sea de mayor conveniencia para el usuario. Los objetivos de la formación continuada son:

- Actualizar el conocimiento de los usuarios a las novedades incorporadas en la aplicación durante el último ejercicio.
- Extender las mejores prácticas de la aplicación que, a lo largo del tiempo, se identifican desde el propio servicio de Atención Clientes.
- Reunir a usuarios de distintos lugares para promover el intercambio de impresiones.

Las Formaciones Continuadas On-line se complementan con las presenciales desde un punto de vista geográfico, ya que son accesibles a todos los clientes, evitando

desplazamientos; y, desde el punto de vista de los contenidos de la formación, permite impartir sesiones más cortas y focalizadas en materias concretas.

3. **Documentación técnica**

En esta área también podrá acceder a actualizaciones y revisiones, comunicaciones, FAQ's, manuales, boletines, novedades de producto, y encuestas.

2.4 Actualización del software

1. **Actualización de producto**
   - **Mantenimiento funcional.** aytos Berger-Levrault trabaja para mejorar sus soluciones día a día, aportándole una imagen más moderna, funcionalidades más eficientes y mejorando la usabilidad. Su Entidad recibirá estas mejoras incluidas dentro de las actualizaciones, que podrá descargar desde el Área de Clientes.
   - **Mantenimiento legal.** Ante el cambio de nuevas disposiciones legales de obligado cumplimiento, aytos Berger-Levrault desarrollará las adaptaciones pertinentes en el producto y pondrá a disposición de la Entidad las versiones adaptadas.
   - **Mantenimiento correctivo.** Se corregirán las incidencias o errores en el producto, que impidan o afecten al uso normal del aplicativo. La prioridad será establecida en función de la importancia o gravedad de la incidencia.

1. **Revisiones y correcciones**

aytos Berger-Levrault realizará la revisión y corrección de posibles inconsistencias en los datos provocadas por un incorrecto funcionamiento de cualquiera de los módulos del producto, o en su caso, derivadas de la migración de datos.

2.5 Servicio de información periódica

Mediante correo electrónico se informará a la Entidad, sobre los siguientes ámbitos:

- Novedades y comunicaciones.
- Publicación y contenido de nuevas versiones.
- Cambios legales que están previstos incorporar y las soluciones que se adaptarán.

2.6 Servicios no incluidos

Quedan excluidos de la presente propuesta los siguientes servicios:

- La corrección de errores imputables a la manipulación del programa por personal no autorizado expresamente por aytos Berger-Levrault.
- La adaptación del producto a las circunstancias especiales del cliente, a su sistema informático o a las nuevas necesidades surgidas con el uso.

- La corrección de anomalías imputables exclusivamente al equipo informático utilizado, así como averías por causas de la red general o deficiencias del ambiente de trabajo y que no guarden ninguna relación de causalidad con el programa.
- La reparación causada por la acción de virus u otros agentes infecciosos, o por instalación de nuevos programes por parte del cliente y que sean ajenas a aytos Berger-Levrault.
- Sustitución del programa original por uno nuevo que sea objeto de una mejora de nivel que implique up-grade o cambio de plataforma (lenguaje, sistema operativo o base de datos).
- La adaptación de los productos de aytos Berger-Levrault a las circunstancias excepcionales del cliente, a nuevas necesidades derivadas del uso de sus productos o al cambio de su sistema informático, entendiendo como tal el sistema operativo de su servidor o clientes, el sistema de gestión de bases de datos, la topología e infraestructura de su red o la incorporación de nuevos dispositivos periféricos no contemplados en el proyecto inicial.
- Las consultas de tipo legal o de interpretación de la legislación o de su normativa.
- Las consultas de operaciones ajenas a las derivadas de la operatoria del producto.
- Las consultas sobre configuración de instalaciones informáticas o los problemas derivados de anomalías imputables exclusivamente al equipo informático utilizado, a deficiencias en las condiciones ambientales de trabajo, así como a averías de la red general de corriente alterna, o variaciones de la misma, que no guarden ninguna relación con la calidad de los productos.

3. Modificación del contrato

El contrato podrá ser modificado según lo establecido en la normativa vigente.

4. Propuesta Económica

4.1 Duración del Contrato

El contrato tendrá una duración de **UN AÑO**, comenzando el **01/01/2023** y finalizando el **31/12/2023.**

4.2 Importe

El importe de la propuesta económica, incluyendo todas las prestaciones a realizar por aytos Berger-Levrault, se establece en:

Descripción					
CONCEPTO	**Fecha Inicio**	**Fecha Fin**	**Base Imponible/ Anual**	**IVA 21%/ Anual**	**Total/ Anual**
Mantenimiento SICALWin	01/01/2023	31/12/2023	1.536,00 €	322,56 €	1.858,56 €

El IVA de la presente propuesta podrá modificarse según la legislación fiscal vigente en el momento de la emisión de la factura. En relación con el impuesto autonómico, IGIC, aytos Berger-Levrault está exento de pago del mismo, siendo el sujeto pasivo la propia Entidad.

5. Facturación

5.1 Periodicidad

De forma **trimestral al final del periodo**, aytos Berger-Levrault expedirá factura, con los requisitos reglamentariamente exigidos, por las prestaciones realizadas durante dicho período de tiempo.

5.2 Presentación de las Facturas

Portal telemático	FACE	
Códigos DIR 3	**Oficina contable**	LA0005919 CONSORCIO
	Órgano Gestor	LA0005919 CONSORCIO AGUAS DEL PONIENTE
	Unidad tramitadora	LA0005919 CONSORCIO

En Écija, a 13 de septiembre de 2022

Las condiciones económicas ofertadas solo serán válidas para aquellos contratos cuyo periodo de duración sea el indicado en el apartado "Duración del Contrato" de la presente propuesta, o superior. La baja del servicio deberá comunicarse formalmente con 30 días de antelación a su fecha fin. Esta propuesta tiene un período de validez de 60 días.

Contrato de Encargado de Tratamiento

Mantenimiento de las aplicaciones

Reunidas las siguientes partes,

De una parte, Don _____, mayor de edad y con DNI número _____, en nombre y representación de Consorcio Gestión del Ciclo Integral del Agua de Uso Urbano en el Poniente Almeriense, en adelante LA ENTIDAD, con NIF _____, y domicilio, en _____.

De otra parte, Don ***Juan Miguel Aguilar Martín,*** mayor de edad y con DNI número ***75.415.723-B***, en nombre y representación de **Aytos Soluciones Informáticas, S.L.U.**, con NIF **B-41.632.332,** en adelante **Aytos**, y con domicilio en **Écija (Sevilla), Avda. Blas Infante, nº 6 – 2ª planta, CP 41.400**.

Reconociéndose ambas partes la capacidad para contratar y manifestando el mutuo interés por suscribir el presente acuerdo, y en base a ello,

EXPONEN

PRIMERO.- Que LA ENTIDAD es una ADMINISTRACIÓN PÚBLICA de carácter territorial, con plenas competencias en asuntos reglamentarios y de autorregulación, asuntos tributarios y financieros, asuntos relacionados con la programación y planificación, así como con plena legitimidad en la aprobación de actos y su ejecutividad, entre otras, y pudiendo con carácter general, para el pleno cumplimiento de sus fines y con plena capacidad, celebrar contratos que permitan mantener el pleno cumplimiento de sus fines y dentro de sus correspondientes competencias.

SEGUNDO.- Que Aytos es una empresa de desarrollo de software, especializado para el sector público y con productos específicos para la gestión y administración electrónica en sus diferentes procesos públicos, tanto internos como destinados a la ciudadanía.

TERCERO.- Que Aytos como empresa especializada en el desarrollo e implantación de soluciones, procederá a desarrollar determinados servicios y actividades a LA ENTIDAD, para lo cual aquella, debe acceder a los datos personales de los que resulta responsable ésta, y actuando bajo sus instrucciones desarrollará el servicio, por lo que a todos los efectos, no se considerará comunicación de datos el acceso de Aytos a los datos, dado que dicho acceso es necesario para la prestación de un servicio al responsable del tratamiento, LA ENTIDAD; y en tal sentido .

CUARTO.- Que LA ENTIDAD cumple con el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y demás normativa aplicable en relación al tratamiento de datos de carácter personal y declara que los datos han sido recabados según lo dispuesto en dicha normativa y está autorizado por los afectados para otorgar a Aytos el tratamiento de los mismos de acuerdo con las estipulaciones del presente Contrato.

QUINTO.- Que en atención al artículo 28 del Reglamento general de protección de datos es necesario regular de forma escrita, mediante contrato, acuerdo o acto jurídico vinculante la relación entre ambas Entidades y que, entre otras cuestiones, establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable por lo que se establece el presente documento como medio de cumplir la obligación impuesta.

SEXTO.- Que Aytos, en calidad de prestador de servicios, realizará por encargo directo de LA ENTIDAD las siguientes acciones:

☐	**Servicio de consultoría para el asesoramiento personalizado.**
☐	**Implantación de productos /software**
	X Lanzamiento y toma de requisitos X Integración sistema interno. (análisis, pruebas, migración, producción) X Conexiones in situ/ en remoto X Cierre y aceptación
☐	**Servicio hosting** (gestionado)
	X Sistema de copias de seguridad y pruebas de restauración. X Acciones preventivas y reactivas sobre el hosting.
☐	**Formación.** (Usuarios del sistema)
☒	**Servicio de vigilancia (actualizaciones y versiones mejoradas)**
☒	**Actividades de soporte y mantenimiento.**

SÉPTIMO.- Que la relación que regirá entre las partes estará basada en la *buena fe y el respeto de la ley, actuando con la máxima diligencia debida y en especial, enmarcada en el deber de secreto y máxima reserva,* y extrema confidencialidad de toda la información suministrada y tratada por Aytos en relación al encargo, con especial referencia a los datos de los que siendo responsable LA ENTIDAD, debe acceder Aytos y gestionar, siempre bajo las indicaciones de aquel, y con las garantías y medidas de seguridad que se establecen en el presente contrato, de conformidad a las leyes aplicables.

OCTAVO.- Que este documento complementa a otro(s) que viene(n) a regular otra(s) prestación(es) de servicio(s), entre las partes, no siendo independientes y regulándose relación, en el presente contrato, así como en los pliegos correspondientes, contratos administrativos que pudieran corresponder y en cuantos documentos lo complementa como actas, informes, albaranes y otros.

NOVENO.- Que Aytos es corresponsable de los datos personales junto con las empresas BERGER-LEVRAULT ESPAÑA, ABS Informática, SLU, por lo que, de acuerdo a las estipulaciones del acuerdo entre las partes podrán también tratar los datos personales en el desarrollo de los trabajos contratados. Este acuerdo queda a disposición del RESPONSABLE.

DÉCIMO.- Por todo ello, reconociéndose las partes la capacidad de obrar necesaria para contratar y manifestando de mutuo interés por suscribir el presente contrato, en base a las siguientes;

CLÁUSULAS

I.- OBJETO DEL CONTRATO.

Mediante el presente se fija el objeto, contenido y límites del acceso y tratamiento por parte de Aytos, a los datos de carácter personal cuyo responsable es LA ENTIDAD, en las diferentes fases del servicio acordado, y estableciéndose en este sentido:

1.- Que Aytos solo podrá acceder a los datos personales e información suministrada por LA ENTIDAD, con los límites y condiciones que se establecen en este documento. El presente contrato, queda alineado de manera estricta, a las obligaciones contenidas en:

a) Pliegos de carácter administrativo y técnicos afectados.

b) Contratos administrativos afectados.

2.- Este documento afectará a todo el proceso de gestión del servicio y a la documentación que se genere durante todo el proceso y de manera detallada en;

a) Anexos de mejora acordados entre las partes.

b) Requisitos técnicos expresos y excluyentes.

c) Documentos del proyecto: actas de reuniones, informes de seguimiento, documentación de gestión de proyecto, albaranes de entrega.

3.- En tal sentido, solo el personal de Aytos asignado previamente al proyecto e identificado, podrá acceder a la información de la responsable, para la prestación del servicio referenciado en este documento. La información a la que podrán accederá, será exclusivamente aquella implicada en el proyecto y necesaria para el correcto funcionamiento de la solución.

4. Que de conformidad con lo establecido en el artículo 28 y siguientes del RGPD, las partes someten a los requisitos de la normativa referenciada, la prestación de servicios y la aplicación de medidas técnicas y organizativas apropiadas, para garantizar la protección de los derechos del interesado.

5.- Que los datos a los que podrá acceder ENCARGADO para la prestación de los servicios encomendados por RESPONSABLE tiene la finalidad exclusiva de proporcionar a la última los servicios considerados en el contrato y en el EXPONENDO SEXTO del presente documento

6.- Que tratándose Aytos de una empresa especializada en la prestación de tales servicios y actuando bajo las circunstancias e instrucciones dadas por la ENTIDAD, este puede presentar garantías suficientes para la aplicación de las medidas técnicas y organizativas apropiadas, exigible a un prestador medio, de conformidad con los requisitos del sector y la industria.

7.- Que los datos a los que podrá acceder ENCARGADO para la prestación de los servicios encomendados por RESPONSABLE tienen la finalidad exclusiva de prestar los citados servicios, quedando prohibida cualquier utilización distinta a la finalidad prevista en este contrato.

8.- A todos los efectos se declara confidencial a la información implicada en el presente encargo, y por tanto sometida en su totalidad a las medidas declaradas.

II.- DESCRIPCIÓN DEL TRATAMIENTO

(Se puede añadir en un anexo)

DATOS PERSONALES OBJETO DE TRATAMIENTO

Para la prestación de los servicios, será necesario realizar acciones de tratamiento, sobre los siguientes datos personales;

DATOS IDENTIFICATIVOS			
☐ Nombre y apellidos	☐Correo electrónico	☐Firma electrónica	☐ Imagen / voz
☐Tarjeta sanitaria	☐Firma / rubrica	☐Nº SS /Mutua	☐Dirección
☐ Otros			
DATOS DE CATEGORIAS ESPECIALES			
☐Salud	☐Afiliación sindical	☐Dato biométrico (huellas y marcas físicas)	☐Vida sexual / Orientación sexual
☐Origen racial o etnia	☐Ideología	☐Datos genéticos	☐Origen racial o etnia
☐Convicciones religiosas o filosóficas	☐Creencias y opiniones políticas	☐ Otros	
DATOS INFRACCIONES			
☐Infracciones penales		☐Infracciones administrativas	
OTROS DATOS			

☐Características personales	☐Académicos y profesionales	☐IP, ubicación o movimientos	☐Datos comportamentales
☐Empleo y puestos de trabajo	☐Solvencia patrimonial y crédito	☐Rendimiento profesional	☐Económico-financieros
☐Situación económica	☐Transacciones	☐Evaluación de perfiles (personalidad y comportamiento)	☐*Otros datos relacionados con la idEntidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;*

Podrá anexionarse un listado completo de los datos personales implicados en el tratamiento.

CATEGORÍA DE LOS INTERESADOS

Los datos personales, provienen de los siguientes colectivos de interesados;

☐Empleados, personas el prácticas o candidatos.	☐Personas de contacto
☐Ciudadanos / Usuarios	☐Padres o tutores
☐Proveedores	☐Representantes legales
☐Asociados o miembros	☐Solicitantes
☐Propietarios o arrendatarios	☐Otros
☐Cargos públicos	
☐Beneficiarios	

ACCIONES DE TRATAMIENTO

El tratamiento de datos personales, requiere la ejecución de una serie de acciones, que comprenden;

☐Recogida	☐Difusión
☐Registro	☐Digitalización

☐Organización	☐Utilización
☐Estructuración	☐Cotejo
☐Modificación	☐Limitación
☒Conservación/Almacenamiento	☐Supresión
☐Extracción	☐Destrucción
☒Consulta	☐Otros (interconexión...):

Los datos personales objeto del tratamiento, pueden ser tratados por la empresa en modo automatizado y no automatizado.

Los medios empleados para el tratamiento serán:

FISICOS
INFORMATICOS
MIXTOS

TRANSMISIÓN / ACCESO A LOS DATOS

RESPONSABLE dará acceso a los datos personales a ENCARGADO mediante _____.

LOCALIZACIÓN DE LOS DATOS PERSONALES

Los datos personales son localizados /ubicados/almacenados en _____.

III.- OBLIGACIONES DERIVADAS DEL CARÁCTER CONFIDENCIAL DE LA INFORMACIÓN.

I. Aytos tratará con la máxima reserva todos y cada uno de los aspectos de la información implicada, no pudiendo comunicarlos o cederlos a terceros salvo que este previamente autorizado por el Responsable.

II. Aytos declara que el personal adscrito al presente proyecto, está sometido a un deber de secreto profesional, y han sido previamente informados respecto a la obligación de secreto inherente de la protección de los datos personales.

III. Todo el personal de Aytos, con acceso al servicio y a los datos personales, dispone de la formación, capacitación, y cualificación necesaria y precisa para efectuar los servicios de conformidad a los estándares del sector. Aytos ha formalizado contratos de confidencialidad con los trabajadores de su empresa que puedan tener acceso a información derivada del encargo de tratamiento Aytos acredita que su personal accederá solo a la información estrictamente necesaria y siempre en base a su puesto y funciones.

IV. Aytos dispone de acuerdos con todos los proveedores implicados, y específicamente mantiene encargos y contratos de confidencialidad, con los prestadores implicados en el presente servicio, y exige que el personal de estos con acceso a los datos, formalice contratos de confidencialidad, los cuales son requeridos y revisados.

V. Aytos tiene adoptadas todas las medidas de seguridad técnica y organizativa para asegurar la integridad, confidencialidad y protección de la información implicada en el servicio de LA ENTIDAD.

VI. A tales efectos, Aytos se somete en periodos definidos de al menos dos años, a auditorias de seguridad, que incluyen revisión y comprobación de las medidas de seguridad de la normativa de privacidad, y específicamente se somete al proceso de verificación de medidas de seguridad del Esquema Nacional de Seguridad –Real Decreto 3/2010-en conciliación con la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, de declaración de conformidad y/o auditorías de seguridad de la información basadas en la norma ISO 27001

VII. Aytos ha adoptado medidas específicas para la seguridad de la información del presente proyecto y específicamente, ha formado a su personal de manera precisa sobre la necesidad de mantener el secreto, y no revelar la información de la que pudiera ser conocedores con ocasión de los procesos relacionados con la solución., siendo advertidos

VIII. El personal adscrito al presente proyecto, ha sido advertido sobre la necesidad de seguir todas y cada una de las indicaciones que pudieran recibir del personal del LA ENTIDAD designados como interlocutores, con la advertencia de ser sancionados en caso de incumplimiento, o no seguir adecuadamente las instrucciones o indicaciones, o las medidas de seguridad.

IX. A tal efecto se acredita que la encargada se somete a auditorias de verificación y que sus procesos se desarrollan de conformidad a los estándares ISO de calidad –Versión vigente UNE-EN ISO 9001:2015. Sistemas de gestión de la calidad. Requisitos (ISO 9001:2015), pudiendo presentarse tal certificación a requerimiento de la administración.

X. Aytos no copiará, ni reproducirá, ni comunicará o exhibirá, ningún elemento, información, documento y análogos, que le haya sido entregados para la prestación o que debiera generar para la ejecución correcta del encargo. Toda la documentación generada en el proyecto, está sometida a secreto y como tal, mantendrá las medidas de seguridad más altas en relación a información confidencial. A todos los efectos quedan

sometidos a confidencialidad, los datos personales de los que es responsable LA ENTIDAD, y cuanta información institucional y de carácter interno y organizativo, no sometida a publicidad actividad, se vea implicada en el proyecto.

XI. LA ENTIDAD podrá entregar un documento al personal de la encargada, en el que se informe de manera clara y directa de la obligación de secreto y sometimiento a las medidas de seguridad que la Responsable considere necesarias sobre los datos de su responsabilidad, así como la obligación de cumplimiento de las restantes obligaciones derivadas de protección de datos. LA ENTIDAD podrá mantener otras medidas de control y acreditación que le permitan comprobar el deber de secreto y las medidas de seguridad desarrolladas por la encargada.

XII. Se exceptúa cualquier sometimiento al deber de secreto o confidencialidad o reserva, a aquella información afectada por la Ley 19/2013, salvo que, de la misma, y específicamente por lo contenido en el Art. 14 y Art 15, se determine un límite a su necesaria transparencia –en sus dos modalidades; acceso o publicidad activa-.

SUBCONTRATACION

Queda terminantemente prohibido delegar en tercero(s) o entidades colaboradoras o subcontratas, la ejecución directa de este acuerdo, salvo que forme parte de la oferta contratada y se hubiera especificado propiamente en la memoria presentada. No obstante, se autoriza al encargado a subcontratar con las empresas del grupo (ABS Informática S.L.U. con CIF B-59383596, y BERGER LEVRAULT ESPAÑA con CIF A66024845) las prestaciones de servicios relacionados con el contratado y que comportan los mismos tratamientos de datos personales.

Se autoriza al encargado a subcontratar con la empresa..... las prestaciones que comporten los tratamientos siguientes: .....

Asimismo, se permite la subcontratación de aquellas entidades que sean mantenedoras o prestadoras de servicio de hosting, y en su caso de soporte de la encargada.

Por otra parte, cuando la encargada considere necesario, por razón del servicio, que se autorice el acceso de personal no autorizado o personal de un tercero diferente a los antes señalados, se realizará una comunicación previa a la Responsable, informándole de la empresa subcontratista, del personal de la misma autorizado al acceso, finalidad y obligaciones estipuladas. Indicando también el motivo, los datos personales afectados, así como, las medidas de seguridad que va a aplicar al tratamiento. Esta comunicación deberá realizarse con una antelación de 15 días hábiles. La subcontratación podrá llevarse a cabo si el Responsable no manifiesta su oposición en el plazo establecido. El régimen de contratación se regirá por los siguientes principios:

1. Para poder realizar una subcontratación a un tercero, el encargado deberá formalizar un contrato con el mismo, en el que se establezcan las condiciones de seguridad y las obligaciones de cada parte, poniendo a disposición del responsable, una copia del contrato y cuantas modificaciones posteriores se pudieran producir. Solo se podrá subcontratar a un tercero el alojamiento, cuando el mismo disponga de certificaciones de seguridad en vigor, tales como UNE ISO /IEC 27001: 2013. No obstante el encargado deberá desarrollar un análisis en profundidad de los requisitos necesarios, conforme a los requisitos establecidos en la medida op.pl.4 del Real Decreto 3/2010, y mantener una diligencia adecuada que permita garantizar las reglas de mínima funcionalidad y seguridad por defecto, así como el resto de elementos contenidos en la medida op.exp.2, op.exp.3 y op.expo.4 del citado. El encargado deberá asegurarse de que el servicio subcontratado cumple con los requisitos de denegación de servicio mp.s.8 del Real Decreto 3/2010. Las conexiones relacionadas con acciones de configuración y mantenimiento o cualquier otra acción operacional en el alojamiento, desde el exterior, deberán realizarse mediante VPN. Será necesario contar con un adecuado control de acceso y un proceso de identificación, existiendo una segregación de funciones y supervisión de tareas críticas y unos mecanismos de autenticación conforme a op.acc.5 del Real Decreto 3/2010. El encargado velara porque en el alojamiento, se mantengan todos aquellos elementos de seguridad, requeridos para la categoría declarada por el cliente para su sistema, conforme al Anexo I del Real Decreto 3/2010.

2. La responsabilidad por el incumplimiento o negligencia en el servicio del subcontratado, será del encargado inicial, quién en todo caso, será responsable del tratamiento y del servicio a los efectos de responder ante los posibles daños y perjuicios ocasionados a AAPP.

3. La empresa subcontratada, se deberá comprometer a adoptar al efecto, todas las medidas de índole organizativas, legales y técnicas. Asimismo, se comprometerá a que todo su personal, dependiente o vinculado, que tenga acceso a los datos personal cumpla con las obligaciones contenidas en la normativa. Aytos deberá realizar cuantas labores de vigilancia considere precisas o encomendar la ejecución de las mismas a fin de corroborar el cumplimiento de las obligaciones emanadas de la normativa de protección de datos por parte de la empresa subcontratada.

4. Cualquier modificación, sustitución o rescisión de los acuerdos con el subcontratista deberán ser notificados a la AAPP, debiendo constar por escrito la autorización para poder llevar a cabo los citados cambios.

5. Finalizada la relación, la empresa subcontratada deberá proceder a la devolución de los soportes, documentos y análogos en que constasen los datos de carácter personal a los que hubiera accedido por razón de la subcontratación, no pudiendo mantener más datos de aquellos a los que quede legalmente obligado.

PROHIBICIÓN DE CESIÓN DE DATOS A TERCEROS, A EXCEPCIÓN DE QUE EXISTA HABILITACIÓN LEGAL

La ENTIDAD no autoriza la cesión de los datos personales objeto del presente contrato, salvo que exista una obligación legal.

La ENTIDAD podrá dar instrucciones por escrito al Encargado del tratamiento en el supuesto de que sea necesaria una cesión de datos personales durante el desarrollo del presente contrato, incluyendo la cesión a otros Encargados del tratamiento del Responsable del tratamiento. En las instrucciones se identificará la Entidad, los datos personales que deben ser transmitidos y las medidas de seguridad de la citada comunicación.

Aytos deberá trasferir los datos personales para el cumplimiento de una obligación legal a las autoridades u organismos competentes, incluyendo terceros países de la Unión Europea si así lo indicase una norma de Derecho Comunitario o de la normativa de cada país integrante. La transmisión de estos datos a terceros países será comunicada al Responsable, con carácter previo a su envío indicando los datos personales a transmitir, autoridad u organismo y base legal, salvo que la normativa aplicable lo prohíba expresamente o la autoridad competente así lo comunique al Encargado del tratamiento de forma fehaciente.

TRANSFERENCIAS INTERNACIONALES

Se declara la prohibición de transmisión internacional de datos, por lo que Aytos, no podrá transferir datos a terceros países ajenos al marco de la Unión Europea, incluyéndose en esta prohibición el almacenamiento de los datos en terceros países ajenos al ámbito de aplicación del RGPD.

No obstante, si Aytos debiera transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, deberá recabar, salvo prohibición legal o comunicada por la autoridad competente, la autorización previa y por escrito la ENTIDAD, facilitando la información necesaria en relación con las garantías adecuadas.

En caso de que la transferencia internacional se encuentre sometida a autorización expresa de la autoridad de control, Aytos, se abstendrá de efectuar la misma hasta que la ENTIDAD comunique la obtención de dicha autorización.

IV.- FINALIDAD DEL ACCESO

1.- El acceso por parte del Encargado del Tratamiento Aytos, a los datos de carácter personal facilitados por el Responsable LA ENTIDAD, tiene la exclusiva finalidad de llevar a cabo la gestión de los servicios relacionados con las soluciones de la encargada, descritos en **Exponendo VI y Clausula I del presente**.

2.- Al ser necesario el citado acceso a los datos, para la ejecución de los servicios contratados, no tendrá la consideración de "comunicación o cesión de datos".

Por ello, LA ENTIDAD será considerado a todos los efectos **RESPONSABLE DEL tratamiento** según el artículo 24 y siguientes del Reglamento General de Protección de Datos Personales.

Bajo ningún concepto se considerará que existe relación –laboral-, entre el personal de la encargada y el personal de la responsable, que deberán mantener plena independencia.

V.- MEDIDAS TECNICAS Y ORGANIZATIVAS

De conformidad con los Arts 28 y 32 del RGPD, Aytos deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. Todas las medidas de seguridad se han desarrollado, considerando las medidas detalladas en el análisis de riesgos y, en su caso, la Evaluación del Impacto realizada por la ENTIDAD, todas ellas en referencia al Esquema Nacional de Seguridad –Real Decreto 3/2010-en conciliación con la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, de declaración de conformidad.

Las medidas de seguridad, serán aquellas medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo derivado del tratamiento, que, en su caso, incluya los apartados que se van detallando a continuación.

MEDIDAS DE DILIGENCIA DEBIDA

La ENTIDAD considera necesario que Aytos, ponga a su disposición elementos que evidencien el nivel de cumplimiento de la normativa, y en general, que puede garantizar un tratamiento adecuado, conforme a los estándares del mercado.

I. Aytos podrá establecer un periodo específico en el que acepte procesos de auditoria y revisiones por la ENTIDAD.
II. Aytos, pondrá a disposición de la ENTIDAD los elementos que evidencien el deber de diligencia exigible, las medidas de seguridad establecidas y las garantías de protección de los datos personales.
III. Aytos impone como principios transversales en sus medidas de seguridad, la protección desde el diseño y por defecto, desarrollando los medios más adecuados para el tratamiento, y de manera efectiva la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos de la normativa de protección de datos vigente y proteger los derechos de los interesados.
IV. Aytos ha establecido como principio general de trabajo, que, por defecto, solo serán objeto de tratamiento, los datos personales que sean estrictamente necesarios para cada uno de los fines específicos del tratamiento, por lo que no se accederá, tratara o conservaran, datos personales no implicados o innecesarios en el proyecto.
V. Cualquier acceso a datos personales, será por personas implicadas en el proyecto y con acciones detalladas, que precisen el acceso a cada dato personal implicado. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.
VI. Aytos colaborará, de acuerdo con las instrucciones dadas por la ENTIDAD en el cumplimiento de las prescripciones contenidas en el RGPD y, en concreto, si así le fuese requerido:
    - En el procedimiento para la respuesta eficaz a los derechos ARSOLP de los interesados de acuerdo a los principios y plazos del RGPD

- Al cumplimiento de las medidas de seguridad contenidas en los artículos 32 a 36 del RGPD, con diligencia especial en el procedimiento de notificación de las brechas de seguridad y la realización, en su caso, de las Evaluaciones de Impacto por parte del Responsable del tratamiento

REGISTRO DE ACTIVIDAD DEL TRATAMIENTO

Aytos, deberá poner a disposición de la ENTIDAD cuando así le sea requerido, el registro de actividad del tratamiento descrito en el artículo 30.2 del RGPD, que deberá tener forma escrita, pudiendo ser en formato electrónico.

Este registro deberá contener;

- Nombre y los datos de contacto del encargado y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del delegado de protección de datos;
- Finalidad del tratamiento
- categorías de tratamientos efectuados por cuenta de cada responsable;
- Transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
- Descripción general de las medidas técnicas y organizativas de seguridad, de conformidad con el RGPD.

La ENTIDAD considera necesario que Aytos, disponga de este registro, ya que el tratamiento que se debe realizar puede entrañar un riesgo para los derechos y libertades de los interesados, y puede afectar categorías especiales de datos.

DELEGADO DE PROTECCIÓN DE DATOS

Aytos, comunicará a La ENTIDAD la designación del Delegado de Protección de Datos de acuerdo con el Art. 37 del RGPD, así como las funciones y medios de contacto con el mismo.

MEDIDAS DE SEGURIDAD

Privacidad en el diseño y por defecto

Aytos, desarrollara por defecto, desde el mismo momento del diseño, medios y medidas de seguridad, tanto en sus instalaciones y equipos, como en los del cliente que se vean afectados por los servicios que debe desarrollar, con acceso a los datos personales responsabilidad de LA ENTIDAD.

1.- Protección Preventiva y Proactiva.

Todos productos y soluciones empleados en la prestación de servicios, estará concebida y diseñada considerando los riesgos a la privacidad. A mayor abundamiento, las aplicaciones propietarias serán certificadas por personal diferente al que las hubiera diseñado y desarrollado, y podrán ser auditadas a efectos de la privacidad.

2.- Privacidad "por Defecto"

El personal de la encargada, tendrá la instrucción clara de desarrollar una configuración por defecto, y esta será la más segura posible en términos de protección de los datos personales. No se deben recoger, almacenar ni tratar datos personales, salvo que sea imprescindible para la finalidad perseguida.

3.- Privacidad integrada en el Diseño

El servicio a desarrollar en todas sus fases, integrara como elemento central la protección de los datos personales, generando la misma importancia que la propia funcionalidad. En consecuencia, el encargado desarrollara cuando sea preciso revisiones, propias o de terceros, y desarrollara evaluaciones de impacto tanto a sus procesos y desarrollos como aquellos en los que intervenga un tercero implicado en el servicio.

Las evaluaciones de impacto se desarrollarán en el diseño e inicio de nuevos servicios, como mecanismos de análisis de los riesgos potenciales y elaboración de medidas de tratamiento adecuadas.

4.- Funcionalidad Plena

El servicio ha sido diseñado y se desarrollara en el cliente, siguiendo la premisa de eficacia y funcionalidad, con el máximo respeto privacidad.

5.- Protección durante todo el Ciclo de Vida

La privacidad integrara todo el proceso y el servicio desde el diseño y será un estándar durante la ejecución de los servicios, de manera que se desarrollaran como medidas preferentes durante los servicios, la *seudoniminzación* y la *encriptación*-siguiendo los estándares adecuados, la custodia de las claves, a la autenticación segura y la no generación de datos no cifrados-.

6.- Visibilidad y Transparencia:

Las políticas de seguridad, las medidas desarrolladas y los protocolos que los usuarios deben desarrollar en el proyecto están entregados a cada usuario afectado y se mantendrán a su disposición como mecanismo de refuerzo. Los usuarios disponen de un responsable de proyecto que podrá resolver cualquier duda relativa a la seguridad de los datos y a la funcionalidad del servicio. Se ha considerado la descripción completa de las medidas aplicadas y las recomendaciones de parametrización, disponibles para la Responsable.

7.- Respeto del Usuario.

El usuario final del sistema dispone de información valiosa para el personal de la encargada y sobre los principales riesgos que pueden materializarse por lo que se consideraran en las acciones de consultoría y de implantación, así como en la formación, cuanta información pudiera resultarles relevante.

1. MEDIDAS DE SEGURIDAD ADECUADAS AL RGPD

Aytos garantiza que las medidas de seguridad son adecuadas al nivel de riesgo de las operaciones de tratamiento de acuerdo a lo establecido en el artículo 32 y siguientes del Reglamento General de Protección de Datos Personales.

2. SEGREGACIÓN

Identificación inequívoca y personalizada del usuario autorizado a la ejecución de los trabajos. Todos los usuarios podrán ser individualizados.

3. REGISTRO DE INCIDENCIAS

La encargada dispone de un procedimiento de gestión de incidencias y reclamaciones, que generara un registro efectivo de cada comunicación y de cada acción desarrollada al efecto.

Se ha establecido un procedimiento para notificar y gestionar las incidencias relativas al servicio y que son asociadas al cliente y al servicio.

Se considerará incidencia todo supuesto acaecido de manera repentina que ponga en riesgo los datos personales o la información que se encuentra presente en los servicios prestados, incluyéndose daños en la confidencialidad, integridad y disponibilidad bien por acción propia o por acciones de terceros, por fallos en equipos o dispositivos o por accidentes o casos fortuitos o fuerza mayor. Las incidencias podrán ser detectadas por el personal de la encargada de modo activo o por el Responsable / usuario final del servicio. Cualquier suceso que sea considerado incidencia será registrado en la aplicación interna de la encargada.

Las incidencias comunicadas por la Responsable, se podrán efectuar mediante llamada de telefónica al número de soporte establecido o a través de la página web. Cuando así se haya acordado se podrá realizar una comunicación de incidencia mediante chat.

Ante cualquier incidencia presentada, LA ENTIDAD podrá requerir al proveedor para que emita un informe que contendrá al menos los siguientes puntos; fecha de detección y fecha de solución, personal encargado de resolución de la incidencia, causas de la incidencia, medidas paliativas, medidas definitivas de corrección, perdida de disponibilidad del servicio, datos e información afectados, medidas establecidas para evitar una nueva incidencia.

La gestión de incidencias queda sometida a las medidas de seguridad de la responsable. En todo caso, LA ENTIDAD se reserva el derecho a reclamar a su proveedor el registro de incidencias en el que se haya incluido la incidencia acaecida y que verse sobre sus datos personales.

El registro de la incidencia, podrá dar lugar al inicio del cómputo de los plazos establecidos en los acuerdos de servicio, cuando se hubieran previsto en el servicio. El registro de incidencia deberá incluir todas las fases de resolución efectuadas y deberá permitir trazas las tareas efectuadas por el personal asignado. No se cerrará una incidencia sin aceptación expresa o tácita del comunicante.

4. PROCEDIMIENTO DE NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

Aytos ha establecido un procedimiento para notificar y gestionar las violaciones de seguridad relativas al servicio y que son asociadas al cliente y al servicio, que pueden afectar a datos personales, siguiendo los requisitos señalados en el Art. 33.2 del RGPD.

Las incidencias de seguridad deberán ser comunicadas al Responsable por si pudieran suponer una violación de seguridad en los datos personales de obligada notificación a la Agencia Española de Protección de datos. Aytos deberá comunicar sin dilaciones a la ENTIDAD las incidencias de seguridad detectadas en el plazo máximo de 24 horas, por el canal establecido por el Responsable a tales efectos, debiendo colaborar en todo momento, aportando toda la información que sea necesaria para el cumplimiento del deber de comunicación. La información a comunicar por parte de Aytos será, como mínimo, la siguiente:

- Descripción del evento o incidente de seguridad de los datos personales, valoración de la afectación, gravedad y riesgo para los interesados. Incluirá necesariamente fecha, personal implicado en la gestión de la incidencia, causas, y pérdida de disponibilidad.
- Descripción de la naturaleza de la violación de seguridad, número de afectados, categorías de datos, registros afectados y formato (papel o electrónico) que ha sufrido la brecha de seguridad.
- El nombre y los apellidos del Delegado de Protección de Datos, en su caso, o de la persona designada a los efectos de seguridad.
- Descripción de las medidas paliativas, medidas definitivas adoptadas, o en su caso, las propuestas por el encargado del tratamiento tras la detección de la violación de seguridad para paliar los daños producidos o, en su caso, los potenciales riesgos o efectos perjudiciales para los afectados.

La ENTIDAD podrá comunicar las incidencias de seguridad a Aytos mediante llamada de telefónica al número de soporte establecido o a través de la página web. Cuando así se haya acordado se podrá realizar una comunicación de incidencia mediante chat.

5. IDENTIFICACIÓN DEL PERSONAL DE SOPORTE

Existirá un procedimiento de autenticación y un control de los accesos. El sistema deberá permitir la identificación de forma inequívoca y personalizada, verificando la autorización.

Durante el inicio del proyecto se generará necesariamente asistencias in situ, que no estarán sometidas a los principios de requerimiento previo, pero si al control de accesos. Se podrán emplear registros-albaranes para que permitan mantener un adecuado control de las acciones ejecutadas por el personal del proyecto.

6. COPIAS DE SEGURIDAD.

Durante las primeras fases del proyecto, y en concreto durante la implantación de la solución, la encargada desarrollara procedimientos de actuación para la realización como mínimo semanal, de copias de respaldo, salvo que en dicho período no se hubiera producido, ninguna actualización de los datos.

Las pruebas desarrolladas antes de entrar en producción, anteriores a la implantación, no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado. En todo caso, quedara constancia en la documentación del proyecto, y en concreto en la aplicación de gestión interna de la encargada, con la adecuada trazabilidad y registro de personal autorizado a su acceso. Toda base de datos, queda sometida a las medidas de seguridad de la normativa de protección de datos.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad. Las copias de seguridad servirán para retrotraer el proceso de implantación, y proceder a la marcha atrás. Existirá un procedimiento de cambios que integrará la seguridad por defecto en la planificación.

Se mantendrá un acceso controlado y restringido a las ubicaciones en las que se encuentren las copias de seguridad.

Cuando deban eliminarse copias de seguridad, se procederá a su borrado de manera segura. Cuando fuera posible, se emplearán productos con su funcionalidad certificada.

Cuando el proyecto haya entrado en fase de producción, la encargada mantendrá el proceso de copias de seguridad, si la responsable concertara el servicio Cloud. La gestión del servicio deberá incorporar los correspondientes niveles de servicio y deberán ser controlados y medidos. El sistema de alojamiento deberá asegurar que los accesos son controlados y se dispone de una correcta gestión y trazabilidad de acciones.

Cuando no fuera así, la Responsable será la única obligada a mantener el proceso de copias de seguridad y restauración, debiendo dar acceso a la encargada a su sistema, y desarrollando medidas de seguridad relacionadas con acceso controlado, identificación remote login y registro de actividad de los usuarios.

7. PRUEBAS DE RESTAURACIÓN

Cada 6 meses deberá procederse a realizar una prueba de restauración que verifique el procedimiento de copia de seguridad. Dicha prueba de restauración podrá efectuarse en procesos diferentes a la propia prueba siempre que acredite la restauración.

Cuando el hosting dependa de la Responsable, la misma será la encargada de proceder a las pruebas de restauración.

8. REVISIONES

Procesos de auditoria que incluyan en el alcance, las medidas técnicas implantadas y en ejecución. Dichos procesos serán realizados por personal capacitado y cualificado, que evalúe el grado de cumplimiento con respecto a la normativa de protección de datos y normas conexas.

Cuando se considere pertinente, se podrán realizar auditorías sectoriales del software considerado o de un prestador implicado en el servicio.

Se considerarán las auditorias de calidad, en las que se vean implicados los procesos de gestión de incidencias, reclamaciones, soporte técnico y satisfacción de cliente, así como los procesos de implantación. De la información suministrada por el tercero certificador, se podrá segregar aquella que afecta al cliente y presentar para acreditar el cumplimiento.

9. RESPONSABLE DE SEGURIDAD

Existe un responsable designado a los efectos de mantener las medidas determinadas por la normativa. Este responsable podrá ser requerido por el contratante para presentar las correspondientes evidencias que acrediten que el prestador del servicio cumple con las medidas legales.

10. REGISTRO DE ACCESO

El prestado deberá mantener un registro relativo a los accesos al sistema de información que afecte al servicio concertado. Se gestionará el acceso al servidor de manera correcta, permitiendo un control de acceso completo durante al menos, 24 meses.

11. DERECHOS DE ACCESO, RECTIFICACIÓN, SUPRESIÓN, OPOSICIÓN LIMITACIÓN Y PORTABILIDAD.

En el caso de que los afectados, ejercitasen sus derechos ante Aytos con relación a los datos objeto del presente Contrato, ésta deberá dar traslado de la solicitud de forma inmediata a LA ENTIDAD y, a no más tardar, dentro del plazo de tres (3) días naturales a contar desde su recepción.

12. RESPONSABILIDAD.

Ambas Partes se comprometen a respetar, en el cumplimiento de las obligaciones que se derivan del presente Contrato, toda la legislación y normativa que resulte aplicable, muy en particular, las obligaciones impuestas y determinadas por la normativa de protección de datos. Cada parte deberá hacer frente a la responsabilidad que se derive de su propio incumplimiento de dicha legislación y normativa.

Asimismo, LA ENTIDAD asume, y a su vez exime a Aytos, toda responsabilidad que pueda surgir en el supuesto que los Datos no hayan sido recogidos de conformidad con lo estipulado en la normativa de protección de datos, así como aquella que pueda ser producto de algún vicio en la autorización de los titulares de los datos para el tratamiento a éstos por parte de terceros, en este caso de Aytos, o la ausencia de la misma.

VI.- PARTICULARIDADES DEL SERVICIO

Como consecuencia de este Encargo de Tratamiento, Aytos gestionará parte del sistema automatizado de la Responsable, pudiendo acceder a las instalaciones de la citada–LA ENTIDAD-, a los servidores, a los equipos de los usuarios y a sus zonas de trabajo, Y a las correspondientes bases de datos. La encargada podrá acceder a la información en modo local o mediante acceso remoto, para lo cual empleará aplicaciones con mecanismos de protección suficiente

Se considerarán accesos remotos, los realizados desde fuera de las propias instalaciones de la organización, a través de redes de terceros. Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad de la responsable, y se podrá emplear cualquier mecanismo de autenticación con protección media, ataque de adivinación, diccionario o fuerza bruta.

Para el desarrollo de las actuaciones LA ENTIDAD se compromete a permitir el acceso a sus instalaciones al personal previamente identificado de Aytos, con la exclusiva finalidad de desarrollar los servicios necesarios. Solo se autorizará el acceso a las instalaciones, de aquel personal que haya sido previamente comunicado a la responsable. Aquellos que no se encuentren en estas circunstancias, pero cuya presencia y asistencia fuera requerida por necesidad del soporte, deberán ser previamente autorizados por la Responsable de Ficheros, salvo que se encuentren pre-autorizados previamente en modo individual.

1. Particularidades de accesos

A modo general se considerarán las siguientes medidas de seguridad, en los accesos permitidos:

1. El personal de Aytos y aquellos otros previamente autorizados, serán identificados en su acceso y se someterán a las medidas de control establecidas en las dependencias de la organización.

2. LA ENTIDAD controlará las actuaciones que la empresa lleve a cabo en sus instalaciones no permitiendo su libre acceso ni actuación, sin control en las instalaciones.

3. Cuando deban realizarse accesos en remoto a los equipos de usuario, se realizará mediante aplicaciones que requieran la autorización del usuario. El sistema inicialmente seleccionado será el sistema en modo atendido. En todo caso el citado sistema requiere de una acción directa del usuario, para permitir el acceso del personal de la encargada.

4. Cuando deban desarrollarse accesos a la base de datos se desarrollará con un control de identificación y de accesos. Cuando se produzcan copias de la base de datos se emplearán medios seguros, tanto para su copiado, como para su transmisión-traslado, y específicamente para su conservación, ejecución de pruebas y borrado de la información cuando ya no fuera necesaria.

5. Los accesos a la información serán en las instalaciones y equipos de la responsable, salvo el proceso propio de pruebas e integraciones. Deberán consultarse la memoria detallada del proyecto y los requerimientos presentes en la licitación.

6. Con carácter general se autoriza el uso de copia de bases de datos implicadas en el proyecto con la finalidad de ajustar los parámetros requeridos.

7. Con carácter general, las acciones de soporte y de resolución de incidencias se desarrollarán mediante aplicación de acceso remoto.

8. Cuando alguna de las partes lo requiera, la encargada y/o la Responsable, se podrá realizar una grabación de los accesos en remoto. No obstante, dicho proceso de grabación deberá ser previamente informado al usuario final, y no haberse opuesto al proceso.

9. Cuando la encargada lo considere pertinente o cuando la Responsable lo solicitará, podrán realizarse grabaciones de las llamadas de soporte. No obstante, dicho proceso de grabación deberá ser previamente informado al usuario final, y no haberse opuesto al proceso.

2. Particularidades actividades en locales de la responsable

Para el proceso de consultoría e implantación, será necesario desplazar a una personal o un equipo, a las instalaciones de la Responsable, por lo que se establece a modo general, las siguientes medidas:

a) El personal designado dispondrá de su propio equipo y dispositivos móviles o asimilados- que podrán requerir ser conectados a la red local y dominio – en su caso-, de la Entidad. Aytos mantendrá las más estrictas medidas de seguridad y no se permitirá el acceso al equipo o dispositivo, a personal ajeno al servicio. Todos los recursos empleados en el servicio, dispondrán de todas las medidas de seguridad y específicamente, medidas de autenticación y registros de logs.

b) Aytos en el marco de sus actuaciones, deberá adoptar las medidas necesarias para no interferir el desarrollo normal de las actividades llevadas a cabo por LA ENTIDAD para lo cual, cuando se deban realizar paradas técnicas o de mantenimiento, se procederá en horario pre-pactado o en fuera del horario establecido en la Responsable.

c) Aytos cuando actúe como empresa de alojamiento, desarrollará una monitorización del tráfico y mantendrá la correspondiente trazabilidad y seguimiento de las acciones de los usuarios finales.

d) Aytos cuando actué como mantenedor y empresa de soporte, integrara en el servicio cuando sea parte del objeto del servicio, los dispositivos móviles de la Responsable, pudiendo monitorizar el tráfico pero no el posicionamiento o usabilidad del dispositivo, salvo expresa petición del Responsable de Ficheros y siempre que se disponga de las aplicaciones necesarias o del acceso a la configuración de los citados dispositivos.

e) No son objeto del presente la regulación de los niveles de servicio por parte del mantenedor. No obstante, de las incidencias podrán derivarse informes relativos a los niveles de servicio y de los niveles de servicios podrán considerarse mejoras en el servicio.

f) LA ENTIDAD podrá requerir excepciones expresas o generales a la configuración del Firewall o herramientas asimiladas implicadas en la conexión (incluidos los puertos), y especialmente podrá requerir la monitorización del tráfico de manera individual.

3. Particularidades sistemas

Aytos como mantenedor desarrollará además las siguientes acciones, en aras a mantener la seguridad de la información y de los equipos y dispositivos implicados:

a) Para garantizar la correcta protección de los sistemas de información de la organización, las aplicaciones implicadas en el servicio, deberán disponer siempre de una correcta gestión de actualizaciones y parches de seguridad.

b) Garantizará que la instalación en los sistemas y aplicaciones –integración-, se realizan conforme a los requisitos de seguridad de la organización, previo asesoramiento técnico de los requisitos y riesgos potenciales. En concreto, la encargada procurará la instalación segura mediante diferentes entornos aislados entre sí, y específicamente el entorno de producción y pruebas.

c) Será necesario una adecuada gestión de contraseñas y un almacenamiento de las claves de manera segura, siendo potestad del Responsable ambas acciones.

d) Para el correcto funcionamiento de los servicios, deberá gestionarse adecuadamente la capacidad de las comunicaciones y de los sistemas, mediante monitorizaciones. Será responsabilidad de Aytos cuando se hubiera concertado con la misma, el servicio Cloud.

e) El personal de Aytos gestionará las incidencias relacionadas con datos personales como recogida de evidencias, si las mismas pudiera generar la necesidad de una cadena de custodia o una acreditación para posibles acciones de régimen disciplinario, reclamaciones o estudios de responsabilidad.

f) Desarrollará y gestionará, bajo demanda, la documentación relativa a la gestión de la configuración, entregable a la Responsable.

g) Generará un borrado seguro cuando sea legalmente requerido.

h) Gestionará de conectividades VPN para accesos desde el exterior al sistema de información de la Responsable, a usuarios previamente determinados. Todos los usuarios deberán ser nominativos.

i) Cuando sea necesaria la asistencia presencial, se cumplimentará el correspondiente registro o albarán documental.

VII.- ACEPTACION Y PUESTA EN SERVICIO

El encargado declara, que la(s) solución(es) implicada(s) en el proyecto ha pasado por un proceso de desarrollo documentado y sometido a una metodología, que integra la seguridad en sus diferentes fases. Se han considerado en el proceso del diseño, los mecanismos de identificación y autenticación, protección de la información tratada, y la generación y tratamiento de pistas de auditoria.

Con carácter general, se establece que antes de pasar a producción, la(s) solución(es) han sido comprobadas con respecto a la funcionalidad y la seguridad. Todo el proceso de desarrollo se realiza en un sistema diferenciado al de producción.

Se han evidenciado que se han cumplido las medidas de seguridad establecidas por la normativa de referencia –Reglamento General de protección de datos personales y Real Decreto 3/2010- y/o norma ISO 27001.

El personal encargado del proceso de consultoría e implantación, comprobara siempre, que la solución cumple los requisitos de seguridad y se integra de manera adecuada en el sistema de información de la Responsable. Será requisito para cerrar la implantación, el mantenimiento o la mejora de la seguridad del sistema, cuando la(s) solución(es) se encuentre en producción.

No se realizarán pruebas en entornos de producción ni con datos reales. No obstante, cuando la Responsable considere necesario el uso de datos reales, bajo un entorno aislado, se desarrollaran copias de seguridad y se empleara una copia controlada y sometida al mismo nivel de seguridad que el sistema origen de los datos.

La encargada acredita que se han desarrollado procesos de certificación interno por personal diferente al encargado del desarrollo de la(s) solución(es), y que se han desarrollado pruebas de penetración.

El diseño y pruebas de la(s) solución(es), incluye necesariamente un análisis de las vulnerabilidades y un proceso de corrección y tratamiento adecuado.

Cuando así se haya acordado, se podrán generar análisis de coherencia en la integración en los procesos. Cuando se haya acordado de manera expresa, podrá requerirse una auditoria de código fuente, siendo repercutido en el servicio el coste de la misma.

VIII.- MEDIDAS DE CONTROL DE LA RESPONSABLE.

Para mantener el pleno cumplimiento de las medidas de seguridad que afectan a los usuarios del sistema de la Responsable, la encargada pondrá en marcha un registro de actividad, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen, y a la protección de datos personales y a los derechos de carácter laboral, y demás disposiciones que resulten de aplicación, donde se registrarán las actividades de personal adscrito al proyecto por parte de Aytos -y en su caso terceros autorizados-, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar cuantas actividades se han desarrollado, incluyendo las que pudieran ser indebidas o no autorizadas, y permitiendo identificar en cada momento, a la persona ejecutante.

LA ENTIDAD podrá solicitar a la encargada, el establecimiento complementario de una cláusula que junto con la relativa al deber de secreto y confidencialidad, informe al personal de la encargada de las medidas de control que pudieran llevarse a cabo por parte de la Responsable.

Aytos dará a conocer al personal adscrito al proyecto, las medidas de control que pudieran llevarse a cabo por parte de la Responsable.

LA ENTIDAD podrá desarrollar las siguientes medidas de control:

1º.	**Control de personal en los accesos a las instalaciones**
2º.	**Control de accesos al sistema de información.**
3º.	**Comprobación de los accesos y/o cambios ejecutados.**
4º.	**Limitación de accesos a la información de la Responsable en base al principio de segregación de funciones.**

El Responsable del tratamiento, LA ENTIDAD, ostenta todas las facultades de dirección respecto a los datos personales que trata Aytos, por lo que se reserva el derecho a realizar **acciones de verificación del grado de cumplimiento** de las obligaciones impuestas y dictar las instrucciones que sean necesarias, asumiendo también todas las obligaciones que le atribuye el RGPD y en todo caso,

1. Obligación de entregar los datos personales en los formatos acordados y con la antelación suficiente para el inicio de la prestación de los servicios objeto del contrato.

2. Comunicar en la debida forma y con antelación al inicio de la prestación de los servicios, el contacto con el Delegado del Protección de Datos o en su caso, de la personal que asume las funciones necesarias y descritas en este contrato.

3. Remitir las actualizaciones de los datos personales que pueda conocer, así como el ejercicio de los derechos en materia de protección de datos que puedan afectar al encargado del tratamiento, en el menor tiempo posible.

4. Realizar los análisis de riesgo y evaluaciones de impacto de los tratamientos de datos personales que lleva a cabo el encargado del tratamiento, en su caso.

5. Colaborar con el encargado del tratamiento en la ejecución de las estipulaciones contenidas en el presente contrato.

6. Verificar y controlar la ejecución de las estipulaciones del presente contrato, de otras instrucciones que puedan comunicarse al encargado durante la ejecución del contrato y de las medidas contenidas en el RGPD. Entre estas medidas de verificación, se encuentra la de solicitar acreditaciones documentales o certificaciones (incluidas de organismos públicos) para verificar el cumplimiento de la legislación vigente.

7. Mantener el adecuado cumplimiento de la normativa implicada, incluyendo la de protección de datos, informando debidamente a los titulares de datos personales, de sus derechos y obligaciones.

IX.- PROPIEDAD INTELECTUAL

LA ENTIDAD reconoce que Aytos es el autor de la(s) solución(es) implicada(s) en el presente o legítimo propietario de los correspondientes derechos de explotación de la(s) solución(es), así como de la información generada para el programa, como de las imágenes, folletos, textos, métodos, videos, y en general todos los elementos asociados, incluido el diseño de la interfaz del programa o de versión móvil del programa o versión web y aplicación, objeto del presente encargo y que será empleada por LA ENTIDAD .

Aytos cuenta en régimen de autoría o licenciamiento con derechos de explotación y otorga a LA ENTIDAD los derechos de explotación del proyecto formalizado, excluyéndose la posibilidad de explotación de los mismos para proyectos futuros.

Aytos podrá realizar actos de protección jurídica respecto a los resultados tangibles que resulten del proyecto, respetando siempre los derechos de LA ENTIDAD y de los usuarios.

Se ceden con carácter general, los derechos que se derivan de la instalación y uso de las soluciones implicadas en el proyecto y de las sucesivas versiones o mejoras que pudieran verse afectadas.

X.- DEVOLUCIÓN DE LOS DATOS

Una vez cumplida la prestación, y en el momento en que, se den por cumplidas las condiciones pactadas o legalmente previstas, y/o finalice la relación entre ambas partes, los datos de carácter personal utilizados por el Encargado del Tratamiento deberán ser devueltos al responsable del mismo, siempre bajo las indicaciones que éste especifique, excepto cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando LA ENTIDAD dicha conservación..

Esto mismo será de aplicación respecto de cualquier soporte, documentos escrito o electrónico, o cualquier objeto en que conste algún dato de carácter personal objeto de tratamiento.

No obstante, cuando del servicio y específicamente, cuando del proceso de implantación o en la gestión de las incidencias se procesen datos reales y se disponga de copia en las instalaciones / infraestructura de la encargada, esta procederá a un borrado seguro, y cuando fuera posible, se realizará empleando una herramienta certificada –Common Criteria-, en el plazo máximo de 30 días naturales.

XI.- PLAZO Y VIGENCIA DEL ACUERDO

Se considerará que entra en vigor el presente, el día siguiente a la firma del mismo por las partes, teniendo una vigencia ligada a la duración del contrato de prestación de servicios que ha dado lugar a la suscripción del mismo.

Sin embargo, en lo relativo a las obligaciones de confidencialidad y no revelación, la vigencia del presente acuerdo se prolongará durante un plazo indefinido y permanente extendiéndose sus efectos más allá de la finalización de la prestación de servicios.

Y para que así conste, y en prueba de conformidad y aceptación del contenido de este escrito, ambas partes lo firman por duplicado y a un solo efectos en la fecha y lugar indicados en el encabezamientos y finalización.

Por LA ENTIDAD:	Por Aytos:
Fdo:	Fdo: ***Juan Miguel Aguilar Martín***
D.N.I	D.N.I ***75.415.723-B***