PLIEGO DE PRESCRIPCIONES TÉCNICAS
QUE RIGE LA CONTRATACIÓN DEL SUMINISTRO DE NUEVO SISTEMA DE CONTROL DE ACCESO BASADO EN CERRADURAS ELECTRONICAS

Donostia / San Sebastián, septiembre de 2026

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE RIGE LA CONTRATACIÓN DEL SUMINISTRO DE NUEVO SISTEMA DE CONTROL DE ACCESO BASADO EN CERRADURAS ELECTRONICAS

Índice

1. ANTECEDENTES 1
2. OBJETO DEL CONTRATO 2
3. REQUISITOS TÉCNICOS GENERALES 2
3.1 Componentes principales del sistema 2
3.1.1 Sistema de Gestión (Software) 3
3.1.2 Llaves Inteligentes 4
3.1.3 Dispositivos de Cierre (Cilindros y Candados) 5
3.1.4 Dispositivos de sincronización y actualización de derechos 6
4. ALCANCE 6
4.1 Dispositivos de cierre (Cilindros y candados) 6
4.2 Llaves inteligentes 7
4.3 Sistema de gestión 7
4.4 Dispositivos de actualización 8
4.5 Maletin para modificar los cilindros modulares 8
4.6 Suministro complementario mediante partida alzada a justificar **¡Error! Marcador no definido.**
4.7 Formación 8
5. PLAZO DE GARANTÍA ..... ¡Error! Marcador no definido.
6. REQUISITOS PARAR LA PRESTACIÓN DEL SUMINISTRO 9

SUMINISTRO DE NUEVO SISTEMA DE CONTROL DE ACCESO BASADO EN CERRADURAS ELECTRONICAS

1. ANTECEDENTES

Históricamente, la seguridad física de nuestra infraestructura de aguas ha descansado sobre sistemas de cerrajería mecánica y planes de amaestramiento complejos. Dada la naturaleza dispersa de nuestros activos, la gestión de multitud de llaves físicas se ha convertido en un desafío logístico insostenible.

Nuestras infraestructuras presentan una serie de características operativas específicas que condicionan de forma determinante el diseño de los sistemas de acceso físico:

- Red extensa de instalaciones distribuidas (estaciones de tratamiento, depósitos en zonas rurales, arquetas urbanas y plantas de bombeo, etc.).
- Ubicaciones frecuentemente no atendidas y de difícil acceso.
- Intervención recurrente de personal externo (mantenimiento, obras, inspección, emergencias).
- Entornos expuestos a intemperie, humedad, corrosión, vandalismo y condiciones climáticas severas.
- Necesidad de cumplir con requisitos de seguridad, prevención de riesgos laborales, coordinación de actividades empresariales (CAE) y auditorías internas o regulatorias.

En este contexto, los sistemas tradicionales basados en el sistema de amaestramiento mecánico presentan limitaciones estructurales. En un entorno de agua, considerado infraestructura sensible, el extravío o la duplicación no autorizada de una llave maestra representa una amenaza de alto nivel; la única solución ante un compromiso de este tipo es la sustitución física de decenas de bombillos y el re-troquelado de todo el parque de llaves, un proceso extremadamente costoso y lento. Además, el sistema mecánico es "mudo": no existe un registro de quién ha accedido a una instalación o cuánto tiempo ha permanecido en ella dejando un vacío de información que dificulta las auditorías de seguridad y salud laboral.

Frente a estas limitaciones, la transición hacia un ecosistema de cerraduras electrónicas inteligentes se presenta no como una opción, sino como una evolución estratégica necesaria. Esta solución permite la sustitución de la llave física por credenciales digitales llaves mecatrónicas programables que pueden ser habilitadas o revocadas desde una consola central. La capacidad de otorgar permisos de acceso temporales o condicionados a horarios específicos elimina de raíz el riesgo de llaves perdidas y optimiza la coordinación con empresas colaboradoras.

Finalmente, la implementación de esta tecnología dota a la empresa de una capacidad de monitorización en tiempo real antes inexistente. Cada interacción con un punto de acceso genera un rastro de datos auditable que permite supervisar el cumplimiento de las rondas de mantenimiento y garantizar que solo personal autorizado y debidamente formado acceda a áreas críticas. En definitiva, el paso a la cerrajería electrónica transforma un elemento pasivo de seguridad en una herramienta de gestión operativa inteligente, alineada con los objetivos de digitalización y eficiencia de la compañía.

2. OBJETO DEL CONTRATO

El objeto principal del presente pliego es el suministro de un nuevo sistema de control de acceso basado en cerraduras electrónicas, es decir, toda la infraestructura necesaria para la sustitución del sistema actual de cerraduras mecánicas amaestradas.

El licitador deberá cumplir con todas las leyes, reglamentos, ordenanzas, etc. aplicables a cualquier parte del proyecto. La implantación de los sistemas contemplados en el presente documento incluirá los servicios necesarios para minimizar los tiempos de implantación y garantizar los parámetros de calidad y servicio requeridos por cada una de las partes del sistema.

3. REQUISITOS TÉCNICOS GENERALES

La solución de gestión de accesos deberá estar fundamentada en una arquitectura distribuida y resiliente, adecuada para infraestructuras críticas caracterizadas por una amplia dispersión geográfica y condiciones operativas de alta exigencia.

La arquitectura propuesta debe facilitar la administración centralizada de políticas de acceso y garantizar un funcionamiento autónomo y seguro en campo, minimizando dependencias críticas relacionadas con la red, el suministro eléctrico local o las comunicaciones continuas.

3.1 Componentes principales del sistema

El sistema se compondrá, como mínimo, de los siguientes elementos funcionales:

- Sistema de Gestión (Software).
- Llaves Inteligentes de acceso.
- Dispositivos de Cierre (Cilindros y Candados).
- Dispositivos de sincronización y actualización de derechos.

Cada componente debe tener una función clara para asegurar coherencia y simplicidad en el sistema.

3.1.1 Sistema de Gestión (Software)

La plataforma de administración debe ser escalable y permitir modalidades de gestión SaaS/Nube o instalación local.

Para este contrato se solicita la modalidad de Software as a Service (SaaS) que ha de contemplar las siguientes funcionalidades:

- Acceso vía navegador web.
- Control Total: La solución debe tener capacidad para gestionar al menos 10.000 cilindros y emitir permisos dinámicos (quién puede entrar en cada puerta y en qué franja horaria).
- Integración: Debe ofrecer APIs para la integración con software de terceros (CCTV, sistemas de alarma o gestión de activos). **El uso de dichas APIs ha de estar incluido en el presupuesto.**
- Trazabilidad: Registro inmediato de auditoría de las llaves y posibilidad de bloquear llaves perdidas en el sistema.
- Alojamiento en centros de datos ubicados en la Unión Europea o en regiones que garanticen el cumplimiento de la normativa europea aplicable.
- Control de accesos al sistema basado en roles y perfiles diferenciados.
- Registro y trazabilidad de las acciones administrativas realizadas sobre la plataforma.
- Autenticación Multifactor (MFA): El acceso del personal administrador a la interfaz web de gestión del sistema requerirá obligatoriamente una autenticación reforzada.
- Todo acceso externo, integración o conexión de dispositivos remotos al servidor de gestión exigirá el uso de certificados de cliente firmados mediante algoritmo de cifrado. El sistema contará con la capacidad de revocar de forma inmediata cualquier certificado en caso de pérdida, robo del dispositivo o compromiso de seguridad.

La arquitectura SaaS debe estar diseñada de modo que:

- La indisponibilidad temporal del servicio central no impida el acceso autorizado en campo.
- Los dispositivos de cierre y las credenciales continúen operando conforme a los derechos previamente asignados.

- La sincronización de eventos y derechos se realice de forma diferida una vez restablecido el servicio.

- Tanto el equipo de desarrollo de la solución como los equipos encargados del soporte de segundo nivel y de las operaciones de la infraestructura Cloud (SaaS) deberán estar auditados y certificados bajo la norma ISO/IEC 27001.

- El entorno Cloud subyacente (proveedor de hosting) deberá disponer de las certificaciones ISO 27001, ISO 27017 (Seguridad en la nube), ISO 27018 (Privacidad en la nube).

- El diseño de la infraestructura SaaS deberá garantizar que, aun compartiendo entornos virtuales, los datos y los sistemas de amaestramiento de cada cliente estén separados lógicamente de forma estricta.

- Los respaldos completos de las bases de datos (diarios) y los registros de transacciones deberán almacenarse de forma aislada y cifrada en reposo mediante servicios de gestión de claves de hardware. El diseño técnico del servicio debe impedir que los propios administradores de la infraestructura de hosting puedan extraer las claves en formato de texto plano.

- Los centros de datos principales y de respaldo que alojen las bases de datos del sistema mecatrónico deberán estar situados obligatoriamente dentro del Territorio de la Unión Europea.

- El entorno SaaS dispondrá de cortafuegos, sistemas de monitorización continua de amenazas, detección de intrusiones (IDS) y prevención de intrusiones (IPS) capaces de reportar de forma automatizada alertas 24/7 ante actividad sospechosa o cambios en la configuración de los servidores.

3.1.2 Llaves Inteligentes

Las llaves deben funcionar como la credencial única de acceso y la fuente de energía del sistema.

Las llaves objeto de este contrato van a ser utilizadas por el personal operativo en infraestructuras hidráulicas y entornos industriales hostiles (tales como estaciones de bombeo, galerías subterráneas y plantas de tratamiento de aguas). En este tipo de emplazamientos, es habitual la presencia de humedad extrema, condensación constante, salpicaduras severas e incluso el riesgo real de caída accidental de los dispositivos al interior de arquetas, canales o depósitos de agua. Por lo que han de han de poseer las siguientes características:

- Seguridad y Encriptación: Deben utilizar chips de última generación con encriptación AES y alta velocidad de procesamiento.

- Características Físicas: Llave compacta, reversible, resistente al agua y polvo con certificación IP67 o superior.

- Señalización: Deben incluir indicadores LED y señales acústicas para informar sobre permisos de acceso, zonas horarias y estado de la batería.

- Tipologías de Llave:

    - Básica: se actualizará mediante validadores.
    - Conectividad Remota: Llave con módulo Bluetooth integrado para actualizar derechos de acceso y revalidar horarios en tiempo real a través de una aplicación móvil.

- Autonomía: **La batería** (pila de litio estándar) **debe permitir al menos 50.000 ciclos o 5 años de uso** para el modelo de llave básico, **siendo sustituible por el usuario sin herramientas**.

Todos los tipos de llaves han de tener la opción de integrar chips RFID (como MIFARE o DESFire) para control de accesos adicionales.

3.1.3 Dispositivos de Cierre (Cilindros y Candados)

Los cilindros han de estar diseñados para sustituir el sistema de cerraduras mecánicas existente. Los cilindros deben estar disponibles en diferentes diseños y longitudes de modo que puedan adaptarse a una amplia variedad de aplicaciones de bloqueo.

- **Alimentación y Conectividad:** Los cilindros y candados no deberán disponer de batería interna ni requerir cableado. La energía para la apertura y el intercambio de datos se suministrará exclusivamente a través de la llave.

- **Capacidad de Almacenamiento:** Cada dispositivo debe integrar un microchip con memoria integrada y no volátil para almacenar autorizaciones de acceso y registros de eventos detallados (quién, cuándo y dónde).

- **Durabilidad y Mantenimiento:** Deben ser libres de mantenimiento hasta los 200.000 ciclos de apertura.

- **Resistencia Ambiental:** El sistema debe operar en condiciones climáticas exigentes, con un rango de temperatura operativa de al menos -20º a +60ºC y un grado de protección de al menos IP54.

- **Seguridad:** Certificados VdS y DIN EN15684

- **Protección del Firmware y Hardware:** Los componentes electrónicos de los cilindros y llaves deberán estar integrados en un microchip propietario diseñado específicamente para la solución, con protecciones nativas que impidan la ingeniería inversa, el hackeo de componentes y los ataques por sustitución o réplica.

- **Algoritmos de Cifrado de Hardware:** Toda la comunicación entre los elementos físicos del sistema (llaves, cilindros y dispositivos de programación) deberá estar cifrada de extremo a extremo mediante algoritmos estándar avanzados.

- **Versatilidad de Formatos:** Se debe garantizar una amplia gama de cilindros, incluyendo perfil europeo, medios cilindros, candados para exteriores, cerraduras para mobiliario, cilindros de conmutación para ascensores o equipos eléctricos y cilindros roscados.

3.1.4 Dispositivos de sincronización y actualización de derechos

Para la actualización de las llaves, se deben prever al menos estos tipos de dispositivos:

- **De Pared:** El dispositivo ha de estar diseñado como un ***único módulo*** compacto para ubicaciones remotas o entradas principales, con alimentación PoE o red (12-24V), permitiendo la actualización de validez temporal (ej. permisos válidos por 24h).

  Deben existir versiones resistentes al vandalismo (IK09) e intemperie (IP65).

- **Móviles/App:** Actualización independiente de la ubicación mediante Bluetooth a través de smartphone.

4. ALCANCE

En este apartado se presenta la relación de todos los elementos que serán suministrados, detallando sus características técnicas y funcionales. De este modo, se garantiza que el listado cubre tanto las especificaciones requeridas como la variedad de formatos necesarios para cumplir con las exigencias del proyecto.

4.1 Dispositivos de cierre (Cilindros y candados)

Se suministrará la siguiente lista de cilindros:

Medida	Tipo Bombillo	Tipo Leva	Unidades
30x30	electrónico electrónico	leva corta	9
30x30	electrónico electrónico	leva larga	2
50x50	electrónico electrónico	leva larga	1
30x30	electrónico mecánico	leva larga	72
30x30	electrónico mecánico	leva corta	62
60x30	electrónico mecánico	leva larga	18
50x30	electrónico mecánico	leva larga	15
40x40	electrónico mecánico	leva larga	12
50x40	electrónico mecánico	leva larga	7

30x40	electrónico mecánico	leva larga	6
40x40	electrónico mecánico	leva corta	5
50x50	electrónico mecánico	leva larga	3
60x60	electrónico mecánico	leva larga	3
30x50	electrónico mecánico	leva corta	2
30x90	electrónico mecánico	leva corta	1
40x40	electrónico mecánico	leva larga	1
60x60	electrónico mecánico	leva corta	1
30x40	electrónico mecánico	leva corta	1
30x60	electrónico mecánico	leva larga	1
30x50	electrónico mecánico	leva larga	1
35x35	electrónico mecánico	leva larga	1
35x40	electrónico mecánico	leva larga	1
40x30	electrónico mecánico	leva corta	1
65x30	electrónico mecánico	leva corta	1
60x30	electrónico mecánico	leva dentada	1
40x30	electrónico mecánico	leva larga	1
30x10	medio cilindro electrónico	leva larga	19
30x10	medio cilindro electrónico	leva corta	9
30x30	medio cilindro electrónico	leva corta	3
40x10	medio cilindro electrónico	leva larga	1
30x30	medio cilindro electrónico	leva larga	1
40x40	medio cilindro electrónico	leva larga	1
50x10	medio cilindro electrónico	leva larga	1
30x20	medio cilindro electrónico	leva larga	1
40x10	medio cilindro electrónico	leva larga	1
30x30	electrónico electrónico	leva larga	15

En cuanto los ***candados*** se solicitan ***200 unidades de candados*** con un arco de 10 mm de grosor y 50 mm de arco y con retención de llave.

4.2 Llaves inteligentes

Se suministrarán ***130 llaves de modelo básico*** actualizable mediante validadores de pared y ***20 llaves bluetooth*** con posibilidad de actualización mediante app móvil. Ambos modelos de llave han de tener integrado un tag RFID compatible con el sistema de control de accesos basado en tarjetas Mifare.

4.3 Sistema de gestión

La licencia de software (SaaS) asociada al presente contrato deberá cubrir, como mínimo, ***1.500 elementos***, e incluir en el importe del contrato los ***tres primeros años de licencia***.

Asimismo, deberá permitir la gestión de, al menos, 3 usuarios administradores y 300 usuarios de llaves.

4.4 Dispositivos de actualización

Para la actualización de los permisos de suministrarán ***5 dispositivos murales de interior*** con todos los elementos de conexión necesarios.

4.5 Maletin para modificar los cilindros modulares

El adjudicatario deberá suministrar un maletín específico para la modificación y adaptación de cilindros modulares, que incluirá todos los módulos, componentes, accesorios y herramientas necesarias para configurar en campo las longitudes y formatos requeridos, sin necesidad de recurrir a material adicional no previsto en el suministro. El maletín deberá incorporar, como mínimo, módulos de extensión, alargadores o separadores de cuerpo y rotor, barras, tornillería, adaptadores para medios cilindros, llaves o útiles específicos de montaje y desmontaje, así como cualquier otro elemento necesario para realizar el ensamblaje, ajuste y verificación de los cilindros modulares de forma segura y ordenada.

4.6 Formación

El contratista deberá proporcionar un programa de formación diseñado para capacitar a los diferentes perfiles de la organización en el manejo autónomo del sistema de gestión de accesos.

Esta formación se dividirá en los siguientes bloques técnicos:

- **Administración del Software de Gestión:** Instrucción detallada para el personal de seguridad y administración sobre el control de permisos de acceso, la creación de horarios y la gestión de la validez temporal de las credenciales. Se incluirá formación específica en la interpretación de los registros de auditoría para monitorizar quién, cuándo y dónde ha accedido a las instalaciones.

- **Gestión de Dispositivos de Programación:** Capacitación operativa sobre el uso de dispositivos de pared y aplicaciones móviles para la transferencia segura de derechos de acceso y la recuperación de pistas de auditoría de las llaves.

- **Operativa para Usuarios Finales:** Sesiones prácticas para el personal de campo sobre el uso de las llaves inteligentes, incluyendo la interpretación de las señales ópticas/acústicas que indican los estados de acceso y el nivel de batería. Se instruirá también en el uso de la tecnología Bluetooth para la revalidación remota de permisos a través de dispositivos móviles, evitando desplazamientos innecesarios.

- **Mantenimiento Básico y Soporte:** Formación técnica para el equipo de mantenimiento sobre la sustitución de bombillos mecánicos por electrónicos sin necesidad de cableado o perforaciones adicionales. Se incluirá un módulo práctico

sobre el cambio de baterías en las llaves, el cual debe poder realizarse de forma sencilla y sin herramientas.

5. REQUISITOS PARAR LA PRESTACIÓN DEL SUMINISTRO

Serán por cuenta del contratista todos los gastos de manipulación y transporte que conlleve la entrega de los materiales hasta las dependencias de Aguas del Añarbe- Añarbeko Urak S.A., incluida la carga y descarga de los mismos. Dichas entregas se realizarán dentro de la franja horaria acordada previamente.

El contratista dispondrá de los medios de transporte y personal que sean precisos para atender adecuadamente las entregas, de manera que quede siempre garantizada la puntual recepción del material.

La mercancía se entregará en la siguiente ubicación:

- Aguas del Añarbe – Añarbeko Urak S.A.
  Paseo de Errotaburu nº 1 6ª planta
  20.018 Donostia

Condiciones de entrega:

- Empaquetado en paquetes uniformes con indicación de cantidad y contenido.

No se considerará recepcionado el suministro por parte de AGASA hasta que no se haya inspeccionado y aceptado su coincidencia con el pedido, para lo cual se firmará el acta de entrega entre las partes. En el supuesto de que AGASA no estime aceptable la mercancía, por defecto en la calidad, el estado del material, el empacado, etc., podrá reclamar al adjudicatario dentro de los 7 días hábiles posteriores a la recepción de la misma. En el supuesto que se trate de vicios ocultos, AGASA dispondrá de 2 meses de plazo para la reclamación. Las mercancías rechazadas serán reexpedidas a portes debidos al proveedor.

Durante el periodo de garantía deberá proveerse un servicio de atención telefónica técnica en jornada laboral y un Acuerdo de Nivel de Servicio (SLA) presencial o de envío de sustitución ante fallos críticos de hardware en campo en un plazo máximo de 72 horas hábiles.