

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA CONTRATACIÓN DEL SUMINISTRO E INSTALACIÓN DE CERRADURAS ELECTRÓNICAS Y LECTORES DE ACCESO DEL FABRICANTE SALTO SYSTEMS EN LOS EDIFICIOS DE LA UPV/EHU, ASÍ COMO EL MANTENIMIENTO PREVENTIVO DEL SOFTWARE DE GESTIÓN DEL CONTROL DE ACCESOS SALTO PROACCESS SPACE Y CORRECTIVO PARA AVERÍAS GRAVES

0. ANTECEDENTES O CONTEXTO

La Universidad del País Vasco / Euskal Herriko Unibertsitatea dispone en sus edificios de un sistema de control de accesos mediante tarjeta Mifare, el cual está basado en lectores on-line y cerraduras electrónicas off-line del fabricante Salto Systems, todo ello gestionado de forma centralizada, unificada y homogénea mediante el software Salto ProAccess Space. En la actualidad existen 220 lectores on-line y 6.282 cerraduras electrónicas off-line de Salto Systems.

El correcto funcionamiento y plena operatividad del sistema de control de accesos, requiere la contratación del mantenimiento del software Salto ProAccess Space, así como el suministro e instalación de equipamiento de control de accesos adicional de Salto Systems para cubrir futuras necesidades de ampliación y mejoras.

1. OBJETO

El presente pliego tiene por objeto la definición de las características técnicas que rigen la prestación consistente en el suministro e instalación de cerraduras electrónicas y lectores de acceso del fabricante Salto Systems en los edificios de la UPV/EHU, así como el servicio de mantenimiento preventivo del software de gestión del control de accesos Salto ProAccess Space y el mantenimiento correctivo para averías graves de los controles de accesos instalados que requieran reparación con carácter de urgencia.

2. CARACTERÍSTICAS TÉCNICAS QUE DEBEN REUNIR LOS BIENES A SUMINISTRAR Y SU INSTALACION

2.1. Requerimientos técnicos

2.1.1.- Premisas iniciales.

2.1.1.1.- El sistema de cerraduras electrónicas estará basado en dispositivos lectores de tarjeta que se acoplarán al mecanismo de apertura de las puertas, de tal forma que se permita la apertura manual de la puerta al presentar una tarjeta con permiso de acceso autorizado.

2.1.1.2.- El dispositivo lector de tarjeta tratará de preservar las características mecánicas de la puerta en todo momento, p. ej. grosor de la puerta, mecanismo de apertura (manilla, pomo, tirador), etc., en la medida de lo posible, se acoplará a la puerta sin necesidad de realizar ningún tipo de mecanizado sobre la misma.

2.1.1.3.- Con carácter general, las cerraduras electrónicas a instalar en las puertas interiores serán de tipo off-line, es decir, funcionarán de forma autónoma y sin necesidad de conexión a cables de señalización ni eléctricos. No obstante, es posible que en ciertas puertas en las que se necesita un mayor grado de seguridad, se demande el uso de cerraduras electrónicas de tipo on-line, es decir, conectadas a la red de datos para monitorización del estado de la puerta y visualización en todo momento del personal que accede por dicha puerta, así como para la actualización inmediata de los permisos de acceso.

2.1.1.4.- Las cerraduras electrónicas on-line, podrán estar basadas en lectores de control de acceso convencionales de tipo mural, mientras que las cerraduras electrónicas off-line estarán basadas en cilindros electrónicos que sustituyan al bombillo de la llave convencional y/o en lectores de tipo escudo que actúen sobre la manilla de la puerta.

2.1.1.5.- Las instalaciones de cerraduras electrónicas a implantar en los edificios incluirán los materiales y mano de obra necesarios para proporcionar una solución completamente operativa "llave en mano", siendo a cuenta del contratista otro tipo de actividades complementarias como mecanizado de puertas, instalación de mecanismos de apertura y cierre de puertas, cableado de señalización, alimentación eléctrica, y cuantos elementos sean necesarios para el buen funcionamiento del sistema.

2.1.1.6.- Para garantizar la apertura de las cerraduras electrónicas y elementos de control de acceso deben ser plenamente compatibles con las tarjetas corporativas de la UPV/EHU, que disponen de un aro de proximidad Mifare® o Desfire de lectura/escritura. La tarjeta dispone de un código identificativo grabado por la UPV/EHU en la memoria de lectura/escritura, el cual está asociado unívocamente a los datos del personal de la UPV/EHU, que debe ser utilizado para acceder al sistema de control de accesos con cerraduras electrónicas mediante la lectura de los permisos grabados en el aro de proximidad Mifare® y/o Desfire de dicha tarjeta.

Por otra parte, se destinarán 8 bloques de 64 bytes cada uno para el almacenamiento de los permisos de acceso, eventos de acceso, calendarios, modos de apertura de puerta, alarmas, etc.

2.1.1.7.- El método de acceso de las cerraduras off-line será variable en función del calendario definido para cada puerta, debiendo permitirse como mínimo los siguientes modos de apertura: modo estándar (cerrado en todo momento, realizándose la apertura al presentar tarjeta autorizada) y modo paso libre (la puerta puede abrirse accionando la manilla, sin necesidad de presentar la tarjeta).

2.1.1.8.- El método de acceso de las cerraduras on-line será variable en función del calendario definido para cada puerta, debiendo permitirse como mínimo los siguientes modos de apertura: acceso libre, acceso con sólo tarjeta y acceso con tarjeta y PIN de 4 dígitos. Al menos dos de las combinaciones anteriores podrán darse en un mismo día para cada lector (p. ej. acceso libre en horario laboral y acceso con tarjeta + PIN fuera del horario laboral).

2.1.1.9.- El colectivo susceptible de disponer de tarjeta universitaria asciende a 60.000 usuarios.

2.1.1.10.- Número de edificios con posibilidad de instalar cerraduras electrónicas: aproximadamente 60 edificios.

2.1.1.11.- Número de puertas a controlar: inicialmente, 6.502 puertas, sin embargo, el sistema deberá ser capaz de controlar un mínimo de 10.000 puertas.

2.1.1.12.- Número de clientes simultáneos con acceso al servidor para visualización y gestión de la aplicación: 200

2.1.1.13.- Las cerraduras electrónicas y lectoras a suministrar e instalar serán plenamente integrables a nivel operativo, funcional y de gestión con la siguiente aplicación de control de accesos existente: **Salto Pro Access Space** de la empresa SALTO Systems, que se podrá gestionar, de forma centralizada, desde los centros de control provinciales a través de la red de datos propia de la UPV/EHU.

2.1.2.- Funcionalidades y especificaciones de cerraduras electrónicas.

2.1.2.1.- Las cerraduras electrónicas deberán disponer de cabeza lectora del aro de proximidad de la tarjeta corporativa de la UPV/EHU, existiendo al menos los siguientes tipos de cerraduras y lectores de accesos:

- Cilindro electrónico off-line
- Escudo electrónico off-line con manilla
- Cilindro electrónico wireless
- Escudo electrónico wireless con manilla
- Lector mural on-line, sin teclado ni display.
- Lector mural on-line, con teclado numérico.

Se deben poder instalar en cualquier tipo de puerta, independientemente del grosor, material de la puerta, tipo de cerradura mecánica, mecanismo manual de apertura (manilla, pomo, tirador...), etc.

2.1.2.2.- Las cerraduras electrónicas y lectores dispondrán de al menos una señal luminosa y/o audible para indicar si el acceso se permite o no.

2.1.2.3.- Las cerraduras electrónicas y lectores se podrán instalar tanto en interior como en exteriores, por lo que serán resistentes a las inclemencias meteorológicas.

2.1.2.4.- Generalmente, las cerraduras electrónicas se instalarán para Entrar en un local, no obstante, debe ser posible instalar cerraduras electrónicas y lectores para Entrar y Salir de un local.

2.1.2.5.- Las cerraduras electrónicas off-line deben tener capacidad de memoria suficiente para almacenar un mínimo de 500 eventos de apertura, alarmas (p. ej. batería baja) y los calendarios y horarios de los modos de apertura.

2.1.2.6.- Las cerraduras electrónicas off-line deben utilizar pilas o baterías convencionales, con una duración suficiente para permitir 30.000 eventos de apertura de puerta.

2.1.2.7.- Las cerraduras electrónicas off-line deben disponer de un mecanismo o dispositivo electrónico de apertura de puerta de emergencia, en caso de fallo o agotamiento de las baterías.

2.1.2.8.- En cada edificio existirá al menos un lector on-line para actualización de los permisos de las tarjetas y para descarga de alarmas y eventos de apertura hacia el servidor de gestión de cerraduras, a través de la red de datos IP.

2.1.2.9.- Se utilizarán unidades de control para cerraduras y/o lectores on-line, las cuales dispondrán de todos los elementos de interfaz necesarios para su conexión y comunicación con los lectores y con los mecanismos de apertura de puerta.

2.1.2.10.- Cada unidad de control se conectará directamente a través de switch a la red de datos, utilizando una tarjeta de red ethernet a 10/100 Mbps.

2.1.2.11.- Las unidades de control serán capaces de funcionar de forma autónoma en caso de fallo de la conexión a la red de datos, de tal forma que mantengan su configuración (modo de funcionamiento, calendario, horario, etc.) y almacenen temporalmente los eventos que se produzcan (mínimo 500 eventos por puerta) hasta su transmisión al servidor de gestión, una vez restablecida la conexión de red de datos.

2.1.2.12.- En caso de funcionamiento autónomo, la unidad de control deberá leer la memoria en la tarjeta: permisos de acceso, calendario, identificación de tarjeta, PIN, etc.) para un mínimo de 5.000 tarjetas, de tal forma que, en caso de fallo de la conexión a la red de datos, el servicio de control de acceso esté operativo para al menos 5.000 tarjetas definidas por el administrador del edificio.

2.1.2.13.- La unidad de control se conectará en la medida de lo posible a un enchufe eléctrico protegido por SAI que permita el funcionamiento de la puerta durante un mínimo de 10 minutos en caso de fallo de corriente eléctrica.

2.1.2.14.- La unidad de control se encargará de la activación de la puerta de acceso mediante cerraderos eléctricos o similar y controlará el estado de la puerta, monitorizándose en tiempo real el estado de la puerta en el software de gestión y visualizándose los datos de la persona que accede. El tiempo de puerta abierta se podrá configurar de forma individual por cada puerta desde el sistema de gestión, y quedará registrada la fecha y hora de apertura de la puerta, así como si la apertura se ha realizado de forma manual desde el sistema de gestión.

2.1.2.15.- El estado de puerta abierta asociado a lectores on-line deberá notificarse en tiempo real al sistema de gestión y en los puestos cliente de los Centros de Control Provinciales mediante mensaje de texto y visualización gráfica de la puerta.

2.1.2.16.- En los accesos mediante tarjeta+PIN, únicamente se ofrecerá 3 intentos para introducir correctamente el PIN, tras los cuales se generará un mensaje de incidencia por PIN erróneo al Centro de Control Provincial, identificándose el lector de acceso, la tarjeta, fecha, hora, tipo de incidencia, etc.

2.1.2.17.- Posibilidad de habilitar exclusas, es decir, en caso de abrir una puerta no se podrá abrir otra hasta que la primera se haya cerrado.

2.1.2.18.- Posibilidad de habilitar antipassback, es decir, si una persona ha entrado en un local o recinto sin haber utilizado la tarjeta, no podrá salir del mismo utilizando la tarjeta.

2.1.2.19.- Como medida de seguridad, la apertura de la puerta desde el interior siempre se podrá realizar de forma manual, salvo en los casos en los que se defina disponer de un cerradero o lector para Salir. En estos casos puntuales, se instalará adicionalmente un pulsador de apertura de emergencia de tipo rearmable.

2.2. Requerimientos de la instalación

2.2.1.- Premisas iniciales

2.2.1.1.- En el Centro de Control Provincial se deberá configurar el software de gestión de acceso para monitorizar, controlar y gestionar las unidades de control de acceso del edificio. Adicionalmente, desde el Centro de Control se podrá activar la apertura remota de puertas dotadas de lector on-line.

2.2.2.- Infraestructura de cableado de señalización y eléctrico

2.2.2.1.- Los tendidos de cableado eléctrico para alimentación de los equipos, así como los tendidos de cableado de señalización necesarios para la plena operatividad de las soluciones de cerraduras electrónicas y lectores a implantar serán los adecuados para garantizar la comunicación vía Web del sistema con los equipos on-line instalados.

2.2.2.2.- Los tendidos de cableado de señalización podrán instalarse a través de las canalizaciones de la Red de cableado estructurado de voz/datos de la UPV/EHU, siempre y cuando dichas señales no produzcan interferencias sobre las comunicaciones telefónicas y/o de datos.

2.2.2.3.- En los casos en los que no exista canalización, o bien, la señal pueda producir interferencias, el cableado discurrirá a través de nuevas canalizaciones, debiéndose utilizar canaleta o tubo de PVC en instalaciones vistas y tubo corrugado en instalaciones ocultas.

2.2.2.4.- Adicionalmente, el cableado eléctrico se instalará a través de las canalizaciones eléctricas existentes, independientes de las canalizaciones de voz/datos.

2.2.2.5.- La instalación del cableado de señalización, control y eléctrico en el entorno de las puertas se deberá ejecutar de forma oculta en la medida de lo posible, a fin de preservar la seguridad del cableado y minimizar el impacto visual.

2.2.2.6.- El cableado del interior del edificio deberá disponer de cubierta ignífuga y libre de halógenos.

3. OTROS ASPECTOS RELATIVOS AL ALCANCE DEL CONTRATO

3.1 Documentación de inicio y fin de proyecto.

La contratista deberá entregar PREVIAMENTE A LA EJECUCIÓN DE LA INSTALACIÓN asignada un Proyecto Técnico-Económico con el siguiente contenido:

- Plan de implantación (fases, fechas, horarios, descripción de actividades y personal a emplear).

- Documentación de los materiales a instalar.
- Presupuesto desglosado en las unidades de obra a emplear, expresando las cantidades, precios unitarios de materiales (incluyendo mano de obra, completamente instalado y funcionando) y los importes de cada partida y del Proyecto en su conjunto.

AL FINALIZAR LA INSTALACIÓN, la contratista entregará la documentación de fin de proyecto, que constará de lo siguiente:

- Descripción técnica de la solución implantada, configuración de los sistemas, así como identificación fotográfica del cuadro eléctrico y de la ubicación de los elementos cableados.
- Planos de la instalación, en los que se especificarán la ubicación de los escudos electrónicos, lectores murales, controladoras de acceso (CU), y cuadro eléctrico al que se han conectado.
- Plan de pruebas, en el que se especificarán las pruebas realizadas, que permitan certificar que la instalación está plenamente operativa y cumple las funcionalidades solicitadas.
- Factura desglosada en las unidades de obra empleadas, expresando las cantidades, precios unitarios de materiales (incluyendo mano de obra, completamente instalado y funcionando), importes de cada partida y centro donde se ha ejecutado el proyecto o instalación.

Toda la documentación se entregará en soporte informático (pendrive USB o DVD). Los planos digitalizados en soporte informático, se entregarán a su escala real.

Para la elaboración de la documentación se sugiere emplear el siguiente entorno:

- Ficheros de texto tipo Microsoft Word 2016 o compatible
- Ficheros de hoja de cálculo tipo Microsoft Excel 2016 o compatible
- Ficheros de planos en AutoCAD versión 2020 o compatible

La documentación indicada será entregada por la contratista en el Servicio de Seguridad de la UPV/EHU.

3.2.- Plazos para el suministro e instalación.

3.2.1.- Plazo de entrega del Proyecto Técnico-Económico de la instalación, considerado a partir de la fecha de Replanteo Inicial de cada instalación a efectuar conjuntamente entre el contratista y la UPV/EHU. Este plazo no deberá superar los **10 días laborales**.

La Dirección de Proyecto de la UPV/EHU, constituida por el Director de Seguridad y el Responsable del Servicio de Telecomunicaciones, revisará el Proyecto Técnico-Económico y solicitará a la empresa contratista los replanteos necesarios hasta que el Proyecto sea de conformidad para la UPV/EHU. Una vez verificada la conformidad, la UPV/EHU definirá la fecha de inicio de la instalación.

3.2.2.- Plazo máximo del suministro de materiales e inicio de la instalación. Este plazo no deberá superar **los 15 días laborales**, considerados a partir de notificarse a la empresa la fecha de inicio.

3.2.3.- Plazos máximos de ejecución de instalaciones:

3.2.3.1.- Instalación de escudos electrónicos, lectores murales y controladoras de acceso en un edificio, incluida integración en la base de datos: máximo **18 días laborales desde el suministro de los materiales**. El contratista especificará orientativamente, cuando presente el proyecto, los plazos en función del número de equipos a instalar.

3.2.3.2.- Importante: Los plazos que establezca el contratista en su propuesta (Proyecto Técnico-Económico de la instalación), según los baremos anteriores, deberán garantizarse y cumplirse expresamente en todos los casos, siendo responsabilidad del contratista la incorporación de mayor cantidad de personal del previsto inicialmente, e incluso el realizar trabajos en horario extra, sin suponer en ningún caso sobrecoste alguno para la UPV/EHU.

En su caso, el plazo máximo de entrega de suministro e instalación de un edificio completo, será de **60 días naturales**.

3.3.- Formación.

Según lo presentado por la contratista en su oferta, teniendo que contar con lo siguiente:

Contenido de los cursos de formación para supervisores del sistema:

- Programación y configuración de escudos electrónicos, lectores murales y controladoras de acceso.
- Funcionalidades de las actualizaciones del software de gestión.
- Conexión de equipos al sistema.
- Gestión y asignación de perfiles de acceso para los diferentes niveles de operador.

Documentación formativa:

- Catálogo/Manual para resolución de averías de primer nivel, por parte de los vigilantes.
- Manuales de uso para vigilantes.
- Manuales de configuración para supervisores con las actualizaciones del software.

3.4.- Garantía.

La garantía incluirá durante todo el periodo, la sustitución de componentes y la mano de obra "in situ", con el mismo tiempo de respuesta que el especificado para el mantenimiento.

Las instalaciones tendrán una garantía mínima de DOS AÑOS, a partir del pago de la factura correspondiente, mientras que las reparaciones tendrán una garantía mínima de 6 meses. Se entiende por garantía la cobertura, tanto de los componentes que fuera preciso cambiar como el transporte, desplazamiento y mano de obra incluida de cuantos

técnicos y otros profesionales tuvieran que intervenir durante el citado periodo, pudiendo el contratista incrementarla en el plazo en que sea conveniente.

La garantía consistirá en la intervención de personal técnico in-situ en la UPV/EHU para la reparación o sustitución del material afectado en menos de 24 horas o en el siguiente día laborable.

La notificación de las averías por parte de UPV/EHU podrá cursarse telefónicamente y por correo electrónico, por lo que el contratista, una vez formalizado el contrato, deberá indicar en las condiciones del servicio de la garantía, el procedimiento de atención de averías y el horario de atención y de intervención.

La empresa contratista se comprometerá a garantizar durante el periodo de vida útil de los elementos, que no será menor de 4 años, el **suministro de recambios idénticos o compatibles** de todos y cada uno de los componentes que formen parte de la instalación original.

3.5.- Lugar de ejecución de la prestación.

Las prestaciones del servicio de mantenimiento y el suministro de materiales y sus instalaciones se realizarán en los Centros de la Universidad del País Vasco / Euskal Herriko Unibertsitatea, distribuidos en las 3 provincias de la Comunidad Autónoma Vasca.

3.6.- Mantenimiento preventivo del software de gestion y correctivo para la resolucion de averias graves

Actualmente el número de puertas instaladas a controlar es de 6.502 puertas. Sin embargo, el sistema deberá ser capaz de controlar un mínimo de 10.000 puertas. El número de clientes que de forma simultanea pueden acceder al servidor para visualización y gestión de la aplicación será de 200.

A continuación, se describen las condiciones, plazos y forma en la que se prestarán los servicios de mantenimiento preventivo en el servidor de la aplicación informática SALTO Pro Access Space y correctivo para la resolución de averías graves en los equipos y terminales de acceso en los edificios de la UPV/EHU.

3.6.1.- Mantenimiento Preventivo

3.6.1.1.- La empresa contratista realizará una revisión semestral de mantenimiento preventivo del software. La estimación de tiempo destinado a cada revisión será de 16 horas.

3.6.1.2.- Los puntos a revisar en la BBDD, actualizar en el sistema y, en su caso, con la propuesta de mejora para optimizar la eficiencia del Plan de Cierre son los que siguen:

- Depuración de la lista negra
- Revisar la carga de datos coincidiendo con la carga de alumnos durante el periodo de matrícula (15 – 30 de julio).
- Actualizaciones a la última versión de software previo consenso con la UPV/EHU.

- Actualización firmware de elementos online.
- Purgar y eliminar eventos con antigüedad superior a 4 años.

3.6.1.3.- Consulta telefónica sobre el funcionamiento y prestaciones del software y elementos de control de accesos. Máximo 16 horas anuales.

3.6.2.- Mantenimiento Correctivo para averías que no pueda resolver el cliente (UPV/EHU) (9 horas x 7 días de la semana)

3.6.2.1.- Servicio de Asistencia Técnica Telefónica Preferente, por Control Remoto y/o Servicio de Asistencia Técnica "in situ" en jornada laboral con horario de 8:00 a 17:00 de lunes a viernes laborables. Fuera de ese horario, solo para avisos considerados como urgentes. Desde la recepción de la incidencia por parte de la empresa contratista hasta la primera valoración no se excederá los siguientes tiempos de respuesta:

- Tiempo de respuesta no presencial (telefónica o control remoto): 2 horas laborables para averías urgentes y 8 horas laborables para las que no revistan carácter de urgencia.

- Tiempo de respuesta presencial (desde la recepción del aviso hasta la llegada al cliente): entre 8 y 48 horas naturales (NBD); una vez diagnosticado y evaluado por parte del Departamento Técnico el nivel de gravedad de la incidencia:

Leve: avería en un terminal que no sea de un acceso principal por fallo de batería o mecánico/ fallo de comunicación con un terminal on line de un acceso principal pero que permita el acceso off line, conservando en su memoria el registro de accesos.

Grave. Avería en un terminal de acceso principal a algún edificio, impidiendo la entrada de las personas autorizadas. Bloqueo del software del sistema cancelando, de forma generalizada, los permisos en las tarjetas de acceso al presentarlas en un lector actualizador.

. Tiempo máximo de solución de avería grave: máximo 8 horas naturales, independientemente de la fecha y horario. En cualquier caso, la resolución definitiva de cualquier avería no podrá superar el tiempo máximo de solución establecido para las averías leves.

Tiempo máximo de solución de avería leve: máximo 12 horas laborables. En función de la hora de notificación de la avería, la intervención debe ser dentro del mismo día laboral o el siguiente, por lo que a efectos de cálculo se considerará como tiempo máximo de solución 12 horas laborables.

El tiempo máximo de solución de una avería es el intervalo de tiempo considerado desde el momento de la comunicación de la avería hasta que dicha avería ha sido resuelta, ya sea de forma definitiva o provisional.

Se considera que la avería está resuelta cuando el servicio afectado ha quedado restablecido y funcionando.

El tiempo de solución dejará de contabilizarse en caso de que la demora en el acceso al sistema averiado sea atribuible a la UPV/EHU.

3.6.2.2.- La empresa contratada, en el mismo día de la formalización del contrato, deberá indicar los medios de contacto para la notificación de averías.

3.6.2.3.- Para la resolución de las averías se dispondrá de un stock de repuestos en la UPV/EHU con los elementos recomendados por la empresa contratista. En caso de no disponer de material en stock, la empresa contratista enviará un equipo o módulo de sustitución en el plazo más breve posible, de parecidas características al equipo averiado.

3.6.2.4.- La asistencia telefónica, para atender las consultas técnicas, se estima en 16 horas anuales.

3.6.3.- Condiciones particulares de la UPV/EHU

La UPV/EHU proporcionará el máximo de información y cooperación al personal de asistencia técnica de la empresa contratista cuando se produzca una avería, en los diferentes niveles de intervención que se pudieran dar: telefónica, control remoto e "in situ".

Facilitará al personal de la empresa contratista las condiciones necesarias para un correcto desempeño de la revisión de mantenimiento objeto de este contrato.

Dedicará una persona para el mantenimiento básico de los elementos que componen el sistema instalado por parte de la empresa contratista.

Proporcionará conectividad vía VPN al servidor de control de accesos utilizando los mecanismos de seguridad informática establecidos por la UPV/EHU. Todo ello sin el detrimento para la seguridad de las redes del cliente y siempre utilizando en primer lugar los medios promovidos por el mismo.

La UPV/EHU será la responsable de los ficheros en los que se almacenen los datos de carácter personal. En este sentido, se delega a la empresa contratista el tratamiento de la información con carácter general y, especialmente, de los datos personales y/o imágenes, y/o equipos, y/o ficheros, con la autorización expresa de la UPV/EHU.

4. OTRAS CLÁUSULAS

4.1- Normativa

El presente contrato y las actividades derivadas del mismo, sin perjuicio del cumplimiento de las normas generales que le sean de aplicación, se regirá igualmente por la Ley de seguridad privada vigente.

4.2.- Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales

La empresa contratista se compromete a adoptar las medidas técnicas y organizativas que garanticen la seguridad de la información a la que tenga acceso, directa o indirectamente, como consecuencia de la prestación de los servicios, especialmente la relativa a datos de carácter personal. Así mismo, se compromete a no ceder, y/o hacer uso y/o comunicar a terceras personas la información a la que haya tenido acceso por razón de su relación con la UPV/EHU.

Firma:

ALEJANDRO
ZARRAGA
LARRONDO
- 14600072V

Firmado digitalmente por
ALEJANDRO
ZARRAGA
LARRONDO -
14600072V
Fecha: 2024.12.11
16:23:44 +01'00'

Álex Zarraga Larrondo
Director en Materia de Seguridad de UPV/EHU

Listado de Materiales (Anexo sin precios)

Listado de cantidades a adquirir y sus precios máximos

Listado orientativo de elementos a suministrar e instalar.

El listado global de equipamiento estimado a instalar durante el periodo de vigencia del contrato, en la totalidad de los edificios de la UPV/EHU se resume a continuación:

Concepto	Uds.
Cerraduras electrónicas off-line	654
Lectores murales on-line	16
Unidades de Control (C.U.)	16

Observación: debe tenerse en cuenta que, una vez realizados los replanteos en cada edificio, la cantidad de equipamiento estimado puede variar al alza o a la baja y siempre teniendo en cuenta las posibilidades presupuestarias.

Horas estimadas de Mantenimiento:

Los servicios recogidos en el presente contrato serán los que se detallan a continuación:

PREVENTIVO + BOLSA CORRECTIVO + ASISTENCIA PREFERENTE	Nº HORAS
ACTUALIZACION BBD + SOFTWARE + FIRMWARE	32 HORAS / SEMESTRAL
BOLSA DE HORAS MANO DE OBRA ANUAL	80 HORAS / ANUAL
ASISTENCIA TECNICA TELEFONICA ANUAL	16 HORAS / ANUAL