Expediente P.O.94.22

Pliego de Prescripciones Técnicas para la contratación del Servicio de una plataforma de autenticación multifactor y su puesta en marcha en la Autoridad Portuaria de Baleares

Índice

1 Antecedentes y justificación

De acuerdo con la medida control de acceso (op.acc) del marco operacional del Esquema Nacional de Seguridad (ENS) el control de acceso comprende el conjunto de actividades preparatorias y ejecutivas tendentes a permitir o denegar a una entidad, usuario o proceso, el acceso a un recurso del sistema para la realización de una acción concreta. Los mecanismos de control de acceso deberán equilibrar la facilidad de uso y la protección de la información y los servicios, primando una u otra característica atendiendo a la categoría de seguridad del sistema.

Uno de los aspectos que más preocupa a los responsables de seguridad de las diferentes organizaciones es la alta capacidad que tienen los atacantes de obtener credenciales de accesos a los sistemas de información, aspecto que adquiere más importancia en un entorno de trabajo remoto generalizado.

Por todo ello, se considera primordial el establecimiento de sistemas de autenticación multifactor, entendido como la exigencia de dos o más factores de autenticación para ratificar una autenticación como válida, para proteger los sistemas de información.

El pasado 17 de mayo de 2022, la APB contrató el servicio de "ASISTENCIA TÉCNICA PARA EL ANÁLISIS PRELIMINAR DE LA IMPLANTACIÓN DE UN SISTEMA DE AUTENTIFICACIÓN MULTIFACTOR EN LA AUTORIDAD PORTUARIA DE BALEARES" expediente nº P.O.19.22. Con este contrato se pretendía una prueba de concepto para obtener los requerimientos necesarios del sistema de autenticación multifactor a implementar y que mejor se adaptara a la infraestructura de sistemas de la información de la APB. De este análisis se obtuvo el listado de requerimientos necesarios que se enumeran en el Anexo I de este documento: REQUISITOS DE LA SOLUCIÓN AUTENTICACIÓN MULTIFACTOR.

Se pretende ahora, con la redacción de este expediente la implementación de un sistema de autenticación multifactor en la APB.

2 Objeto del contrato

El objeto del contrato es la contratación del servicio de una plataforma de autenticación multifactor en la APB.

El objetivo es incorporar funcionalidades de autenticación multifactor mediante una plataforma fácil de implementar y que permita establecer una política y control sobre qué usuarios, dispositivos y redes pueden acceder a las aplicaciones de la APB.

A continuación, se resumen las características principales que se pretenden obtener con el despliegue de dicha solución en la APB:

- Protección de servicios y aplicaciones. Debe permitir proteger tanto servicios y aplicaciones locales o SaaS (Google Workspace, Citrix...).
- Identificación robusta del usuario. Confirmar la identidad de los usuarios con políticas de autenticación de dos factores y acceso contextual para usuarios.

- Identificación y control del dispositivo. Visibilidad completa de los dispositivos administrados y no administrados que se autentican en sus servicios/aplicaciones y sus configuraciones de seguridad para identificar los dispositivos que se conectan a sus aplicaciones y servicios sin necesidad de agentes.
- Experiencia de usuario. El usuario debe poder elegir su método de autenticación preferido de una lista de autorizados durante el inicio de sesión, lo que les permite la flexibilidad de usar un teléfono inteligente, tableta o token de hardware en cualquier momento. Se deberá proporcionar una aplicación disponible en todas las plataformas de teléfonos inteligentes (iPhone, iPad y Android) que permita un inicio de sesión con la aprobación de un solo toque.
- Administración simplificada. Capacite a los usuarios con la facilidad de administrar sus propios dispositivos de autenticación a través un portal de autoservicio que elimine la necesidad de contactar con el personal de soporte TI para los cambios de dispositivo de autenticación.
- Fácil despliegue. Debe permitir el proceso de autoinscripción en el sistema, que facilite el registro del teléfono inteligente en el sistema por parte de cada usuario, así como los posibles cambios de dispositivo (tanto si son personales como corporativos).
- Integración de aplicaciones. El sistema debe permitir proteger fácilmente cualquier servicio/aplicación, especialmente las aplicaciones SaaS y de los fabricantes más importantes: autenticación de Windows (por ejemplo mediante SAML), Google Workspace, Citrix Netscaler, etc.
- Securización simplificada. Debe permitir definir fácilmente las políticas de acceso adecuadas para los usuarios y las aplicaciones. Se debe poder elegir entre permitir, denegar o requerir la autenticación de dos factores para cada intento de autenticación, dependiendo de ciertas condiciones y cómo se configuran por aplicación y grupo de usuarios.

3 Descripción de los servicios. Requerimientos y especificaciones de los servicios

Las prescripciones técnicas que se marcan a continuación son requisitos mínimos, de tal modo que su incumplimiento determinará la desestimación de la oferta presentada.

Con el objetivo de clarificar la solución a suministrar y teniendo en cuenta la exigencia de su compatibilidad con los múltiples sistemas que actualmente dispone la APB y dado que no siempre es posible realizar una descripción lo bastante precisa e inteligible que contemple todas las características técnicas y exigencias funcionales requeridas, se agrega al final de la descripción técnica de cada elemento la referencia de un producto concreto comercial. No obstante, las referencias a marcas y modelos que aparecen en estas características técnicas y en las mediciones **no son en ningún caso excluyentes**, sino que pretenden establecer los criterios de diseño, los niveles de calidad y las prestaciones mínimas que se exigirán a la plataforma de autenticación multifactor, por lo que las empresas licitadoras podrán presentar

ofertas con productos equivalentes, siempre y cuando acrediten perfectamente que las características ofertadas son equivalentes técnicamente con las especificadas en el Pliego. Todas ellas serán tomadas en consideración, siempre que:

- No se aparten sustancialmente de las funcionalidades especificadas y operación del sistema, según se describen en este Pliego.
- Sean equivalentes o superiores en prestaciones y calidad a los referenciados en el Pliego, o aporten alguna ventaja funcional importante.
- Queden suficientemente justificadas desde el punto de vista técnico.

No se considerará equivalente y no se admitirá el producto ofertado si todas o alguna de las especificaciones no cumplen todos los requisitos de los referenciados en el presente Pliego.

Asimismo, dadas las características del servicio objeto del presente contrato, las empresas licitadoras deberán estar en posesión de, como mínimo, las siguientes certificaciones en vigor:

- Certificación ISO 20000 – Gestión del servicio de Tecnologías de la información
- Certificación del Esquema Nacional de Seguridad (ENS) nivel medio en sistemas de información para la prestación del servicio.

Este extremo se acreditará mediante declaración responsable del representante legal del licitador. En la fase de adjudicación, deberá aportar la correspondiente documentación acreditativa.

3.1 Servicio de software

Se debe ofrecer un servicio de software consistente en una plataforma de autenticación multifactor que se integre con los sistemas de información de la APB y que cumpla los requisitos definidos en el

ANEXO I. Requisitos de la solución de autenticación multifactor.

Los elementos principales que deben componer la solución son los siguientes:

- Servicio SaaS de autenticación multifactor.
- Plataforma de administración del servicio.
- Portal de gestión del proceso de autoinscripción y registro de dispositivos de usuarios.
- Componente de integración con el servicio que se implantará en los sistemas de la APB.

Concretamente se deberá suministrar:

- La suscripción para 400 usuarios durante 3 años al servicio de autenticación multifactor.

  En caso de necesidad se podrán contratar hasta un máximo de 150 suscripciones para usuarios adicionales.

3.2 Hardware

También se incluye el suministro de llaves de seguridad token que cumplan los requisitos definidos en el

ANEXO II. Requisitos llaves de seguridad.

- Llaves de seguridad que implementen los protocolos yubico OTP y FIDO2 (webAuthn) con interfaz USB/A y NFC.

Concretamente se deberán suministrar:

- 100 llaves de seguridad.

  No obstante, la cifra de llaves de seguridad finalmente a suministrar, será definida en la reunión de inicio de contrato, en función de las necesidades de la APB.

3.3 Servicios profesionales

Se deberán proveer los siguientes servicios profesionales:

- Servicios de despliegue, configuración y puesta en marcha de la solución. Mediante este servicio se deberán realizar las siguientes tareas:
  - Configuración de la plataforma.
  - Despliegue y configuración del componente local que se implantará sobre una máquina virtual que proveerá la APB.
  - Soporte a la integración del producto con los siguientes sistemas de información: Google Workspace, Citrix (Netscaler y acceso cloud), inicio de sesión local y remoto en los equipos Windows de la APB, etc.
  - Soporte a la integración con las aplicaciones de negocio de la APB que se consideren oportunas.
  - Generación de la documentación técnica del proyecto.
- Sesión de capacitación a los administradores de sistemas de la APB. La empresa adjudicataria deberá realizar la formación necesaria para posibilitar la gestión de la plataforma de autenticación multifactor en la APB. Para ello deberá elaborar un plan de formación que incluya al menos formación básica y avanzada en la plataforma de autenticación multifactor. Esta formación irá dirigida al personal de Sistemas de Información e Infraestructuras TIC. La estimación definitiva del número de sesiones formativas, su duración, contenidos, número y perfil de los asistentes, así como aquellos aspectos no especificados, se determinará en base a las necesidades detectadas por la APB para la correcta gestión de la plataforma. Como norma general, todas las sesiones de formación incluirán la entrega de documentación al inicio de las mismas para todos los participantes. La APB podrá grabar dichas sesiones para ponerlas a disposición de su personal.
- Bolsa de 36 horas (12 horas anuales) para soporte avanzado, evolutivos y tareas programadas.

Estas tareas se podrán realizar en remoto y en horario laborable 8x5.

Cuando ocurra cualquier tipo de incidencia relacionada con el objeto del contrato y atribuible a la empresa adjudicataria, la empresa adjudicataria deberá de resolver dicha incidencia en como máximo los sucesivos tiempos de respuesta y resolución reflejados en la siguiente tabla dependiendo de su nivel de gravedad.

Se considera tiempo de respuesta al tiempo que transcurre desde la comunicación de la incidencia (por la vía acordada con la empresa adjudicataria) hasta el inicio por parte del servicio de soporte de la empresa adjudicataria, de la actividad necesaria para la resolución de la incidencia, dando lugar a la conexión remota con el sistema afectado, o a la visita de un técnico experto, si esto fuera necesario.

Se considera tiempo de resolución al período de tiempo transcurrido desde que se detecta una incidencia de forma proactiva por parte de la empresa adjudicataria o la APB comunica a la empresa adjudicataria la incidencia, hasta el momento en que queda solucionada.

Para el entorno de producción se establecen los siguientes niveles de servicio. En caso de no cumplir con los tiempos de resolución establecidos se podrán derivar las siguientes penalizaciones. La penalización se refiere a cada incidencia cuyos tiempos de resolución no se cumplan.

Nivel de gravedad	Tiempo de respuesta	Tiempo de resolución	Penalización en tiempo de resolución
Crítica	Antes de 1 hora	Antes de 3 horas	50€/hora retraso
Grave	Antes de 3 horas	Antes de 24 horas	25€/hora retraso
Normal	Antes de 6 horas	Antes de 72 horas	10€/hora retraso

Se considera la posibilidad de las incidencias siguientes, que se clasifican según el nivel de gravedad:

i. **Incidencia crítica:** el servicio o la aplicación no funciona. Implica una parada o una distorsión grave en la operativa normal de funcionamiento del sistema.

ii. **Incidencia grave:** el servicio o la aplicación o una de sus funcionalidades tiene una anomalía importante, pero no impide la operativa normal del resto de funcionalidades.

iii. **Incidencia normal:** el servicio o la aplicación o una de sus funcionalidades tiene una incidencia, pero se puede usar con normalidad.

Las incidencias se comunicarán por parte de la APB al Jefe/a de proyecto de la empresa adjudicataria al correo electrónico que se indique a tal efecto. En caso de incidencias críticas también se intentará contactar por teléfono, por lo que el Jefe/a de proyecto deberá indicar un número de teléfono en el que esté disponible en horario laboral (se establece el horario laboral en los días laborables en Palma en horario de 8:00 a 18:00).

La empresa adjudicataria propondrá el sistema y procedimientos de gestión de las incidencias en el marco de la presente asistencia técnica.

Las **tareas de soporte** se realizarán mediante los siguientes mecanismos:

- **Soporte por correo electrónico.** La empresa adjudicataria deberá proveer un correo electrónico de soporte, al cual responder y resolver las incidencias y dudas que se envíen por parte del personal de Sistemas de Información e Infraestructuras TIC.
- **Soporte telefónico.** La empresa adjudicataria deberá establecer un número de teléfono de soporte sin coste adicional asociado a la llamada (que no sea un teléfono tipo 902 o similar) **con un horario 24x7** para dar soporte al personal de Sistemas de Información e Infraestructuras TIC.
- **Soporte presencial o remoto.** La empresa adjudicataria proporcionará el soporte y asistencia técnica in situ en las instalaciones de la APB o en remoto, en caso necesario y siempre que la situación lo permita, para conseguir una atención inmediata y personalizada.

  La planificación y coordinación del soporte serán aprobadas por el Responsable del Contrato.

4 Entregables

Como resultado de los trabajos realizados, la empresa adjudicataria deberá entregar como mínimo la documentación indicada en los siguientes apartados.

La documentación generada durante la ejecución del contrato será de propiedad exclusiva de la APB sin que los adjudicatarios puedan conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización de la APB, que la daría en su caso previa petición formal de los adjudicatarios con expresión del fin.

La documentación se entregará en formato editable (LibreOffice o Microsoft Office) y en formato pdf.

Servicio software

i. Suscripción a los servicios de la plataforma para los usuarios contratados.

Hardware

ii. Llaves de seguridad.

Servicios profesionales

i. Manuales de instalación y configuración.

ii. Plan de formación detallado, que se deberá consensuar y aprobar por parte de la APB.

iii. Informes de las acciones de formación realizadas (sesiones, asistentes, contenido, incidencias, encuesta de satisfacción...).

iv. Documentación utilizada para realizar las acciones de formación.

v. Propuestas de consumo de las horas de la bolsa.

vi. Informes de consumo de las horas de la bolsa.

5 Requisitos de los licitadores

Como prestador del servicio, la empresa licitadora deberá estar en poder, como mínimo, de la certificación del Esquema Nacional de Seguridad (ENS) nivel medio o certificado de haber iniciado el proceso de certificación, teniendo que estar finalizado al menos en los 3 primeros meses del contrato, ya que la APB está en proceso de certificación del ENS nivel medio.

Este extremo se acreditará mediante declaración responsable del representante legal del licitador. En la fase de adjudicación, deberá aportar la correspondiente documentación acreditativa.

6 Plazo para la ejecución del contrato

El plazo de ejecución del contrato se establece en un plazo máximo de TREINTA Y SIETE (37) MESES desde la fecha del Acta de Inicio de los trabajos (reunión de kick-off).

La implantación, configuración y puesta en marcha de la plataforma de seguridad se realizará en un plazo máximo de UN (1) MES, correspondiendo el resto del plazo de TREINTA Y SEIS (36) MESES a la operación, soporte y mantenimiento de la plataforma de autenticación multifactor.

El desarrollo de los trabajos se realizará en los locales de la empresa adjudicataria con sus propios recursos físicos y lógicos. En caso necesario, la APB podrá autorizar la presencia de personal de la empresa adjudicataria en las oficinas de la APB sitas en Moll Vell nº5 de Palma de Mallorca o la conexión remota, para las reuniones y actividades propias para el desarrollo de los trabajos objeto del presente Pliego.

7 Presupuesto, recepción de los trabajos y forma de pago

7.1 Presupuesto máximo de licitación

Asciende el presupuesto de licitación excluido IVA a la cantidad de CIENTO TREINTA Y SIETE MIL VEINTISIETE EUROS CON CUARENTA Y OCHO CÉNTIMOS (137.027,48 €), resultando el IVA (21%) la cantidad de VEINTIOCHO MIL SETECIENTOS SETENTA Y CINCO EUROS CON SETENTA Y SIETE CÉNTIMOS (28.775,77 €) y el Presupuesto de Ejecución por Contrata la cantidad de CIENTO SESENTA Y CINCO MIL OCHOCIENTOS TRES EUROS CON VEINTICINCO CÉNTIMOS (165.803,25 €).

El presupuesto de licitación se desglosa según el siguiente cuadro:

Presupuesto					
CAP.1	**Ud**	**SERVICIO DE SOFTWARE**	**Cantidad**	**Importe**	**Total**
1.1	**Ud**	Suscripción plataformade autenticación multifactor MFA	1200	73,44 €	88.128,00 €
1.1	**Ud**	Suscripción plataforma de autenticación multifactor MFA (opcional)	450	73,44 €	33.048,00 €
CAP.2	**Ud**	**HARDWARE**			
2.1	**Ud**	Llaves de seguridad Token	100	52,53 €	5.253,00 €
CAP.3	**Ud**	**SERVICIOS PROFESIONALES**			
3.1	**Ud**	Servicios de despliegue, configuración de la plataforma, soporte a la integración y generación de la documentación técnica del proyecto	1	7.130,48 €	7.130,48 €
3.2	**Ud**	Sesión de capacitación a los administradores de sistemas de la APB	1	696,00 €	696,00 €
3.3	**H**	Bolsa de horas para soporte avanzado, evolutivos y tareas programadas	36	77,00 €	2.772,00 €
		PRESUPUESTO BASE DE LICITACIÓN			**137.027,48 €**
		I.V.A. (21 %)			**28.775,77 €**
		PRESUPUESTO DE EJECUCIÓN POR CONTRATA			**165.803,25 €**

Están incluidos en los precios anteriores todos los costes derivados de la ejecución material de los servicios, los gastos generales de estructura y el beneficio industrial, además dichos precios incluyen todos los costes laborales, ajustándose al Convenio Colectivo vigente.

La recepción de los trabajos será parcialmente para cada uno de ellos, hasta que se hayan completado el total de los que se prevén en este contrato. Se podrán realizar actas de recepción parcial de los trabajos, recogiendo los entregables de la etapa recibida.

Los gastos de desplazamientos y dietas y otros costes complementarios por los distintos viajes y servicios que deberá realizar el personal de la empresa adjudicataria para la ejecución de los trabajos, así como el alquiler o amortización de oficinas o locales y demás bienes que sean necesarios para el desarrollo de los mismos, así como seguros, tributos, gravámenes, tasas y cualquier otro gasto necesario para llevar a cabo los servicios objeto del Contrato, no supondrán ningún incremento de coste.

7.2 Medición y abono de los trabajos

La unidad de medición de los trabajos será la indicada en la descripción de la partida económica. En caso de omisión o contradicción entre documentos o partes de documentos, será la indicada por el Responsable del Contrato.

Para el abono de los trabajos, **sólo se admitirán los precios unitarios del presente Pliego, a los que se les aplicará el coeficiente de adjudicación resultante** (cociente entre el importe ofertado y el de licitación).

El abono se realizará por unidad realmente ejecutada, siempre que exista conformidad por parte del Responsable del Contrato o en quien delegue. El importe a resarcir se obtendrá de la multiplicación de la medición los trabajos ejecutados por el precio unitario de dicho trabajo afectado por el coeficiente de adjudicación (cociente entre el importe ofertado y el de licitación).

Para ello se elaborará el documento "Relación valorada" que contendrá la relación de trabajos ejecutados, el precio unitario y el coeficiente de adjudicación a aplicar.

Dicha "Relación valorada" deberá ser **firmada electrónicamente** de conformidad, como mínimo por el representante de la empresa adjudicataria y por el Responsable del Contrato. Su cumplimentación será indispensable para el abono de los trabajos realizados.

El Responsable del Contrato elaborará el documento "Certificación" a partir de la información recogida en la "Relación valorada" y hará llegar al representante de la empresa adjudicataria el **ID de certificación asignado**.

7.3 Forma de pago

Una vez facilitado el número ID de certificación (nunca antes), la empresa adjudicataria podrá proceder a la emisión de la factura y su posterior remisión a la APB vía FACe.

Para que la factura sea válida deberá consignarse en el envío FACe:

- ID de certificación asignado.
- Datos identificativos del expediente.
- Importe de facturación, que deberá ser coincidente al segundo decimal con el de la "Relación valorada".

8 Garantía

De acuerdo con el artículo 120 del Real Decreto. Ley 7/2021 en vigor desde el 1 de enero de 2022, todo equipamiento físico en el marco del presente contrato contará con una garantía de TRES (3) AÑOS a partir de la fecha del documento Acta de Recepción, del mismo modo que los productos software y licencias suministrados, contarán con una garantía de DOS (2) AÑOS.

Según el artículo 127 bis del Real Decreto. Ley 7/2021, la empresa Contratista garantizará la existencia de un adecuado servicio técnico, así como repuestos durante el plazo mínimo de DIEZ (10) años a partir de la fecha en que el bien deje de fabricarse.

Transcurrido el plazo de garantía sin que se hayan formulado reparos a los suministros ejecutados, quedará extinguida la responsabilidad del contratista.

Durante el periodo de garantía el contratista estará obligado a subsanar, a su costa, todas las deficiencias que se puedan observar en los bienes suministrados, así como errores en el software, con independencia de la consecuencia que se pudieran derivar de las responsabilidades en que hubiese podido incurrir.

Si se acreditase la existencia de vicios o defectos en los bienes suministrados, la APB podrá exigir al contratista la reposición de los que resulten inadecuados, o la reparación de los mismos, si ésta fuese suficiente.

Si la APB, durante el plazo de garantía concluyera, que los bienes suministrados no son aptos para el fin pretendido, como consecuencia de los vicios o defectos observados en ellos e imputables al contratista, y exista la presunción de que la reposición o reparación de dichos

bienes no será bastante para lograr el fin podrá, antes de expirar dicho plazo, rechazar los bienes dejándolos de cuenta del contratista, quedando exento de la obligación de pago o teniendo derecho, en su caso, a la recuperación del precio satisfecho.

9 Normativa de aplicación

Por su carácter general se considerarán vigentes y de aplicación las siguientes disposiciones, normas e instrucciones, que complementan el presente Documento en lo referente a aquellos aspectos no mencionados expresamente en él, quedando a juicio del Director dirimir las posibles contradicciones habidas entre ellas.

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Normas N.T.E., normas UNE, normas DIN e ISO.
- Ley de Prevención de Riesgos Laborales, Ley 31/1995 (BOE nº 269 de 10 de noviembre) y todos los Reales Decretos que la regulan, en especial el 1627/1997.
- Normas UNE aplicables a equipos y materiales.

Así como cuanta normativa desarrolle, amplíe o sustituya a la antes citada. No obstante, deberá consultarse, las posibles actualizaciones de la mencionada normativa.

10 Seguridad

10.1 Acceso a los sistemas de la APB

En caso de que el personal de la empresa adjudicataria necesite conectarse a los sistemas de información de la APB, ya sea local o remotamente, la empresa adjudicataria deberá identificar a todos y cada uno de sus empleados que vayan a realizar el mencionado tipo de actividades, con el fin de asignarles a cada uno de ellos credenciales de acceso personalizadas.

La empresa adjudicataria se obliga a transmitir al personal mencionado anteriormente la necesidad de custodiar diligentemente sus credenciales, evitando compartirlas o revelarlas. En caso de que las credenciales sean reveladas, el adjudicatario deberá comunicar tal circunstancia de forma inmediata a la APB para que sean revocadas.

En caso de que algún empleado con acceso a los sistemas de la APB causara baja, la empresa adjudicataria deberá poner en conocimiento de la APB tal circunstancia de forma inmediata.

10.2 Cambios

Cualquier cambio que la empresa adjudicataria vaya a realizar en sus procesos, sus infraestructuras y, en general, en su entorno, y que pudiera afectar directa o indirectamente a la APB o al objeto del contrato, debe ser previamente comunicado y consensuado con la misma.

10.3 Incidentes de seguridad de la información

La empresa adjudicataria deberá comunicar de inmediato a la APB cualquier incidente de seguridad de la información que hubiera afectado al entorno de la empresa adjudicataria (malware, fugas de información, etc.) que pudiera afectar, a su vez, a la APB, ya sea a través de correos electrónicos, pendrives, equipos portátiles, el propio personal o por cualquier otro medio.

10.4 Derecho de auditoría

La empresa adjudicataria deberá admitir, y facilitará a la APB, la realización de auditorías que permitan comprobar que la empresa adjudicataria cumple con los requisitos de seguridad establecidos en el marco del contrato.

10.5 Subcontratación

En caso de que se subcontrate alguno de los servicios incluidos en el presente proyecto, la empresa adjudicataria deberá transmitir a los posibles subcontratistas todos los requisitos establecidos en los pliegos de condiciones administrativas y técnicas, y muy especialmente, aquellos requisitos relacionados con la disponibilidad, integridad y confidencialidad de la información y de los servicios de la APB.

10.6 Servicios críticos en disponibilidad o que afecten a servicios críticos en disponibilidad de la APB

La empresa adjudicataria deberá disponer de la suficiente redundancia en sus infraestructuras como para ofrecer un servicio con garantías de disponibilidad a la APB.

La empresa adjudicataria deberá disponer de un plan de continuidad de su negocio o un plan de recuperación de desastres que afecten a sus infraestructuras relacionadas con el objeto del contrato. Estos planes estarán a disposición de la APB para ser revisados en caso de que se estimara oportuno por parte de la APB.

10.7 Desarrollo software

Para el desarrollo de software objeto del contrato, la empresa adjudicataria deberá utilizar una metodología de desarrollo software y unas reglas de codificación segura para garantizar que el software desarrollado no contiene vulnerabilidades. Se deberá mencionar explícitamente:

- Cómo se tiene en cuenta la seguridad de la información durante todo el ciclo de vida del desarrollo.
- Cómo se utilizarán los datos de prueba en caso de ser datos reales.
- Si se utilizan lenguajes que permitan la inspección del código fuente en caso de ser necesario.

Previo a su entrega, el software desarrollado será objeto de pruebas funcionales y pruebas de seguridad por parte del adjudicatario, de forma que se verifique que los requisitos funcionales y de seguridad se cumplen satisfactoriamente. La empresa adjudicataria deberá realizar un

plan de pruebas formales, donde se describan los casos de prueba, las condiciones de la prueba, las entradas inyectadas, los resultados esperados y los resultados obtenidos. El plan de pruebas, junto con sus resultados, será entregado a la APB junto con las entregas de software a las que hace referencia.

11 Contraindicaciones y omisiones del presente documento

Las omisiones erróneas de los detalles que sean indispensables para llevar a cabo el espíritu e intención expuestos en estas especificaciones, o que, por uso y costumbre deban ser realizados, no sólo no exime al Contratista de la obligación de ejecutar estos detalles de omitidos o erróneamente descritos, sino que, por el contrario, deberán ser ejecutados como si hubieran sido completos y correctamente especificados en este documento.

12 Consideración final

Las condiciones del presente Documento prevalecen, en lo que pudiera ocurrir de oposición, sobre cualesquiera otros de carácter técnico o administrativo que pudiera tener establecidos la empresa adjudicataria para la prestación de servicios a personas físicas o jurídicas privadas, siendo en todo caso de aplicación al Contrato cuanto previene la normativa vigente.

El desconocimiento del Contrato o de cualquiera de sus términos, de los documentos anexos que forman parte del mismo, o de las instrucciones, pliegos o normas de toda índole aprobadas por la Administración que puedan ser de aplicación en la ejecución de los servicios objeto del Contrato, no eximirá a la empresa adjudicataria de la obligación de su cumplimiento.

Palma, a fecha de firma del documento

Autor del Documento

Francesc Piris Pons
Responsable de Sistemas de Información e Infraestructuras TIC

VºBº,

Javier Segovia Mascaró
Jefe de División de Sistemas de Información e Infraestructuras TIC

VºBº,

Antonio Ginard López
Jefe de Área de Planificación e Infraestructuras

VºBº,

Jorge Nasarre López
Director

ANEXO I. Requisitos de la solución de autenticación multifactor

I.1. Autenticación e inscripción

La plataforma deberá cumplir los siguientes requisitos en cuanto al proceso de autenticación e inscripción:

Requisito	**Descripción**
REQ-1-01	Debe permitir a los usuarios inscribir varios dispositivos para autenticación.
REQ-1-02	Debe permitir a los usuarios seleccionar un dispositivo preferido para la autenticación
REQ-1-03	Debe permitir seleccionar un dispositivo alternativo si el dispositivo principal no está disponible.
REQ-1-04	Debe permitir a los usuarios administrar de forma segura sus dispositivos para reducir la carga de trabajo administrativo. Se debe poder administrar a nivel de grupo/usuario y/o aplicación.
REQ-1-05	Debe permitir autenticarse con una notificación automática en un teléfono móvil inteligente. Esta debe ser push y utilizar claves asimétricas.
REQ-1-06	Debe permitir autenticación mediante mensajes SMS.
REQ-1-07	Debe permitir autenticación mediante teléfonos con iOS, Android, Windows Mobile y teléfonos no inteligentes
REQ-1-08	Debe permitir autenticación con llamada telefónica tanto para teléfonos móviles como líneas fijas con extensiones, sin dejar un OTP pero requiriendo la interacción del usuario.
REQ-1-09	Debe permitir autenticación con llaves de seguridad, concretamente con las suministradas en este contrato
REQ-1-10	Debe permitir autenticarse con un código de acceso de un solo uso generado desde una aplicación móvil
REQ-1-11	Debe proporcionar códigos *bypass* para la autenticación
REQ-1-12	No debe tener ningún tipo de coste adicional para aplicaciones móviles
REQ-1-13	Debe proveer métodos de autenticación que no impliquen costes adicionales ni cargos telefónicos para el usuario.
REQ-1-14	Debe proporcionar un método de autenticación de segundo factor que pueda funcionar sin datos ni conectividad a la red.
REQ-1-15	Se debe poder aprovisionar la aplicación móvil mediante un código QR
REQ-1-16	La aplicación móvil no debe requerir un escáner de código QR de terceros.
REQ-1-17	La plataforma debe ser compatible con lista blanca de IP. Se debe poder basar en usuario/grupo y/o el tipo de aplicación.

REQ-1-18	La plataforma debe ser compatible con dispositivos de confianza en función de las horas y los días. Se debe poder basar en usuario/grupo y/o el tipo de aplicación.
REQ-1-19	Debe solicitar de manera intuitiva a los usuarios todas las opciones disponibles al iniciar sesión a través de un portal web. Se debe poder basar en usuario/grupo y/o el tipo de aplicación.
REQ-1-20	Debe ser compatible con usuarios que tienen dispositivos de autenticación redundantes.
REQ-1-21	La plataforma debe admitir tokens U2F para la autenticación en aplicaciones basadas en navegador.
REQ-1-22	Debe permitir que las políticas personalizadas bloqueen a los usuarios con un software de navegador desactualizado para controlar el riesgo, según el grupo o la aplicación.
REQ-1-23	Debe permitir políticas personalizadas para advertir/alertar (pero no bloquear) a los usuarios con un software de navegación desactualizado para controlar el riesgo, según el grupo y/o la aplicación. Estos controles se deben realizar con un enfoque sin agentes.
REQ-1-24	Debe ayudar a los usuarios a corregir por sí mismos los navegadores desactualizados para controlar el riesgo, según el grupo o la aplicación.
REQ-1-25	Debe permitir que las políticas personalizadas bloqueen o aumenten la autenticación para los usuarios dentro de ubicaciones geográficas específicas para controlar el riesgo, según el grupo o la aplicación. Estos controles se deben proporcionar con un enfoque sin agentes.
REQ-1-26	Debe permitir que las políticas personalizadas bloqueen a los usuarios con dispositivos rooteados o liberados para controlar el riesgo, según el grupo o la aplicación. Estos controles se deben proporcionar con un enfoque sin agentes.
REQ-1-27	Debe permitir políticas personalizadas para evitar intentos de autenticación originados en direcciones IP anónimas conocidas, como las proporcionadas por TOR e I2P, proxies HTTP/HTTPS o VPN anónimas. Se debe poder definir en función de un grupo de usuarios o una aplicación y proporcionar los controles con un enfoque sin agentes.
REQ-1-28	Debe permitir que las políticas personalizadas requieran un bloqueo de pantalla activo en los dispositivos móviles al aprobar las autenticaciones en estos dispositivos para controlar el riesgo, según el grupo o la aplicación. Estos controles se deben proporcionar con un enfoque sin agentes.
REQ-1-29	Debe permitir que las políticas personalizadas requieran el uso de autenticación de huellas dactilares/touchID en dispositivos móviles cuando se aprueban autenticaciones en estos dispositivos para controlar el riesgo, según el grupo o la aplicación. Estos controles se deben proporcionar con un enfoque sin agentes.
REQ-1-30	Debe permitir que las políticas personalizadas requieran el cifrado de disco completo en los dispositivos móviles al aprobar las autenticaciones en estos

	dispositivos para controlar el riesgo, según el grupo o la aplicación. Estos controles se deben proporcionar con un enfoque sin agentes.
REQ-1-31	Debe permitir que las políticas personalizadas requieran parches de seguridad actualizados para la aplicación de autenticación en dispositivos móviles al aprobar autenticaciones en estos dispositivos para controlar el riesgo, según el grupo o la aplicación. Estos controles se deben proporcionar con un enfoque sin agentes.
REQ-1-32	Debe permitir que las políticas personalizadas restrinjan los métodos de autenticación disponibles para la autenticación para controlar el riesgo, según el grupo o la aplicación. Estos controles se deben proporcionar con un enfoque sin agentes.
Producto de referencia	CISCO DUO

I.2. Administración

En cuanto a la administración del sistema, la plataforma deberá cumplir los siguientes requisitos:

Requisito	**Descripción**
REQ-2-1	Requiere autenticación de dos factores para los inicios de sesión de administrador.
REQ-2-2	Permite a los administradores tener control sobre qué usuarios/grupos tienen acceso a ciertos factores de autenticación (es decir, push, llamada telefónica, SMS, etc.)
REQ-2-3	Proporciona herramientas de aprovisionamiento automático para sincronizar los usuarios existentes de Active Directory.
REQ-2-4	Permite agregar usuarios a través de una importación de CSV.
REQ-2-5	Es compatible con los administradores que aprovisionan a los usuarios mediante programación a través de las API de Restful.
REQ-2-6	Permite a los administradores habilitar un proceso de autoinscripción para que los usuarios finales reduzcan los plazos de implementación. Se puede configurar esto en grupos/usuarios y/o aplicaciones específicas.
REQ-2-7	Admite administradores para inscribir y aprovisionar usuarios a través de un correo electrónico.
REQ-2-8	Permite que los administradores creen un mensaje de correo electrónico de inscripción personalizado si inscriben a los usuarios a través de correos electrónicos.
REQ-2-9	Permite a los administradores crear grupos para organizar y administrar

	usuarios.
REQ-2-10	Permite a los administradores limitar el acceso a determinadas integraciones/aplicaciones en función de la pertenencia de los usuarios a los grupos.
REQ-2-11	Permite a los administradores reactivar dispositivos para los usuarios.
REQ-2-12	Permite a los administradores generar un código de omisión de un solo uso basado en los derechos apropiados.
REQ-2-13	Permite a los administradores limitar los factores/tipos de autenticación para todos los usuarios a nivel mundial.
REQ-2-14	Permite a los administradores limitar los factores/tipos de autenticación para ciertos grupos de usuarios.
REQ-2-15	Permite a los administradores configurar un identificador de llamadas salientes para la autenticación de llamadas telefónicas.
REQ-2-16	Permite a los administradores controlar la configuración de los códigos de acceso de SMS con respecto al número de códigos de acceso enviados por solicitud.
REQ-2-17	Permite a los administradores controlar la configuración de los códigos de acceso de SMS con respecto a la caducidad.
REQ-2-18	Admite la normalización de nombres de usuario para controlar la cantidad de ID de usuario en el sistema y optimizar las licencias (es decir, tratar a qwer@acme.com, acme/qwer y qwer como el mismo usuario).
REQ-2-19	Admite nombres de usuario con formato UPN o NTLM.
REQ-2-20	Es compatible con usuarios que pueden ser parte de múltiples dominios.
REQ-2-21	Brinda la capacidad de exportar registros a un SEIM de terceros.
REQ-2-22	Registra la dirección IP de inicio de sesión.
REQ-2-23	Proporciona API Restful para funciones de administración.
REQ-2-24	Es compatible con los controles de administración basados en roles para los administradores.
REQ-2-25	Proporciona una descripción general del panel de control de los dispositivos en riesgo según los sistemas operativos, navegadores o complementos obsoletos.
REQ-2-26	Brinda a los administradores la capacidad de ver qué dispositivos de autenticación están rooteados o liberados, incluida la opción de ver la lista de usuarios provistos para esos dispositivos.
REQ-2-27	Brinda a los administradores la capacidad de ver el sistema operativo de los dispositivos de autenticación, incluida la opción de ver la lista de usuarios previstos para esos dispositivos.
REQ-2-28	Brinda a los administradores la capacidad de ver qué dispositivos de autenticación no están protegidos con bloqueo de pantalla, incluida la opción

	de ver la lista de usuarios provistos para esos dispositivos.
REQ-2-29	Brinda a los administradores la capacidad de ver qué dispositivos de autenticación no están protegidos con cifrado de disco completo, incluida la opción de ver la lista de usuarios provistos para esos dispositivos.
REQ-2-30	Brinda a los administradores la capacidad de ver qué dispositivos de autenticación no están protegidos con biometría de huella digital/TouchID (alternativa al código de acceso en el dispositivo), incluida la opción de ver la lista de usuarios provistos para esos dispositivos.
REQ-2-31	Brinda a los administradores la capacidad de ver qué *endpoints* se utilizan para acceder a las aplicaciones protegidas, incluida la opción de ver la lista de usuarios que se autentican con esos dispositivos. Brinda contexto sobre cuán desactualizados están y el riesgo para los dispositivos.
REQ-2-32	Brinda a los administradores la capacidad de ver las versiones del sistema operativo en estos dispositivos de punto final para identificar riesgos potenciales, incluida la opción de ver la lista de usuarios que se autentican con esos dispositivos. Brinda contexto sobre cuán desactualizados están y el riesgo para los dispositivos.
REQ-2-33	Brinda a los administradores la capacidad de ver las versiones del navegador en estos dispositivos de punto final para identificar riesgos potenciales, incluida la opción de ver la lista de usuarios que se autentican con esos dispositivos. Brinda contexto sobre cuán desactualizados están y el riesgo para los dispositivos.
REQ-2-34	Brinda a los administradores la capacidad de ver las versiones del complemento del navegador en estos dispositivos de punto final para identificar riesgos potenciales, incluida la opción de ver la lista de usuarios que se autentican con esos dispositivos. Brinda contexto sobre cuán desactualizados están y el riesgo para los dispositivos.
REQ-2-35	Muestra informes para todas las autenticaciones de los usuarios con detalles sobre el dispositivo de acceso y el dispositivo de autenticación, incluidos: sistema operativo, versión del navegador, versiones del complemento, ubicación geográfica/IP, tipo de dispositivo y resultado/estado.
REQ-2-36	Registra todas las acciones de administración.
REQ-2-37	Permite una marca personalizada con el logotipo corporativo.
REQ-2-38	El panel de administración está disponible en al menos uno de estos idiomas: catalán, español o inglés.
REQ-2-39	Admite un umbral de bloqueo para las autenticaciones. Este umbral debe ser configurable. Admite esto una caducidad de bloqueo automático durante un tiempo configurable.
REQ-2-40	Admite informes proactivos sobre intentos de inicio de sesión fraudulentos. Se puede configurar para que se envíe a todos los administradores o a un grupo de distribución de correo electrónico.

REQ-2-41	El sistema puede retener registros de forma indefinida y/o durante un período de tiempo predefinido.
Producto de referencia	CISCO DUO

I.3. *Zero trust*

La plataforma deberá cumplir los siguientes requisitos:

Requisito	**Descripción**
REQ-3-1	Identifica dispositivos no administrados que acceden a sus aplicaciones internas.
REQ-3-2	Identifica dispositivos no administrados que acceden a las aplicaciones en la nube.
REQ-3-3	Proporciona informes sobre dispositivos administrados y no administrados que acceden a aplicaciones locales y basadas en la nube.
REQ-3-4	Identifica dispositivos administrados y no administrados para los siguientes dispositivos/sistemas operativos: Windows, Mac, iOS, Android.
REQ-3-5	Permite crear políticas de seguridad para dispositivos no administrados que acceden a aplicaciones específicas.
REQ-3-6	Permite crear políticas de seguridad para dispositivos no administrados en función de los usuarios o grupos de usuarios que acceden a las aplicaciones.
REQ-3-7	Permite notificar a los usuarios finales si no pueden acceder a las aplicaciones desde un dispositivo no administrado.
REQ-3-8	Permite probar un grupo piloto de usuarios y evitar que accedan a las aplicaciones desde sus dispositivos no administrados sin afectar al resto de la organización,
REQ-3-9	Permite verificar la identidad del usuario remoto y la postura de seguridad del dispositivo sin una VPN.
Producto de referencia	CISCO DUO

I.4. SaaS e infraestructura

Los requisitos que deberá cumplir la plataforma SaaS son los siguientes:

Requisito	**Descripción**
REQ-4-1	Se proporciona un SLA para la confiabilidad de la solución.

REQ-4-2	La seguridad y la arquitectura de la solución han sido revisadas y auditadas por terceros independientes.
REQ-4-3	La solución está basada en SaaS.
REQ-4-4	La plataforma está alojada en un proveedor de servicios certificado por ISO 27001 y auditado por SSAE 16.
REQ-4-5	La solución escala fácilmente para crecer con integraciones y usuarios.
REQ-4-6	La solución está configurada para alta disponibilidad dentro de múltiples ubicaciones geográficas y proveedores de servicios.
REQ-4-7	La solución utiliza criptografía asimétrica para la autenticación remota.
REQ-4-8	La solución NO recopila información de identificación personal sobre los usuarios.
REQ-4-9	La solución es independiente de la autenticación primaria.
REQ-4-10	La solución requiere servidores dedicados en las instalaciones.
Producto de referencia	CISCO DUO

I.5. Integraciones

Los requisitos que deberá cumplir la solución propuesta respecto a las integraciones son los siguientes:

Requisito	**Descripción**
REQ-5-1	Se debe integrar con Citrix Netscaler
REQ-5-2	Se debe integrar con Microsoft Local Login y RDP, soportando los sistemas operativos Windows.
REQ-5-3	La solución permite la integración con aplicaciones personalizadas a través de SDK o API.
REQ-5-4	Se debe integrar con el protocolo RADIUS para autenticación.
REQ-5-5	Se debe integrar con el protocolo LDAP para autenticación.
REQ-5-6	Se debe integrar con SAML 2.0 para autenticación.
REQ-5-7	Se debe integrar con JIRA
Producto de referencia	CISCO DUO

I.6. Licenciamiento

Los requisitos de licenciamiento de la plataforma son:

Requisito	**Descripción**
REQ-6-1	El coste de la plataforma deberá estar basado únicamente en el número de usuarios dados de alta.
REQ-6-2	No habrá ningún coste adicional dependiente de los dispositivos de autenticación
REQ-6-3	No habrá ningún coste adicional asociado al número de autenticaciones.
REQ-6-4	No habrá ningún coste adicional asociado a integraciones
REQ-6-5	No habrá ningún coste adicional de mantenimiento
Producto de referencia	CISCO DUO

ANEXO II. Requisitos llaves de seguridad

Las llaves de seguridad deberán cumplir los siguientes requisitos:

Requisito	**Descripción**
REQ-1	Implementar los protocolos yubico OTP y FIDO2 (webAuthn).
REQ-2	Interfaz USB/A y NFC
Producto de referencia	YubiKey 5 NFC