PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES DEL CONTRATO DEL SERVICIO DE IDENTIFICACIÓN REMOTA

ÍNDICE

1 ANTECEDENTES

1.1 Introducción

A raíz de la grave situación de la crisis sanitaria provocada por el coronavirus SARS-Cov-2, se ha hecho evidente la extraordinaria importancia del canal electrónico para relacionarse con la Administración, que durante algunos meses ha sido el único medio de tramitación posible.

Para poder realizar trámites administrativos por medios electrónicos o acceder a servicios públicos digitales (como por ejemplo las carpetas ciudadanas), se requiere disponer de sistemas de identificación electrónica para acreditar la identidad. Desafortunadamente, la gran mayoría de la población no dispone actualmente de un sistema de identidad digital fácil y usable para relacionarse con el sector público. Aunque, casi todos los ciudadanos disponen de un DNI electrónico, la realidad es que su uso es absolutamente testimonial debido a su grave falta de usabilidad provocada por la complejidad de instalación, configuración, de requerir un lector especial y recordar la contraseña facilitada en su momento por la Dirección General de la Policía.

La pandemia que estamos sufriendo ha puesto de manifiesto las desigualdades digitales y las importantes dificultades de algunos colectivos para obtener un servicio de identificación digital fácil y usable por medios electrónicos, problemáticas que aún persisten en algunos casos, aunque ya se ha levantado el estado de alarma.

Concretamente, hay dificultades en la obtención de identidades digitales en oficinas presenciales porque no todas las oficinas están abiertas. Y, las que están abiertas, lo hacen mayoritariamente con cita previa con unos horarios reducidos, que a menudo está provocando que haya un colapso de peticiones que no permiten ofrecer el servicio a corto plazo, con el consiguiente potencial perjuicio a los ciudadanos que requieren hacer trámites con urgencia. Estas complicaciones afectan, tanto a la expedición de certificados digitales (que actualmente sólo se pueden emitir presencialmente), como la obtención del idCAT Móvil que para algunos colectivos sólo se puede conseguir con un acto presencial.

El registro telemático del idCAT Móvil (sin certificado digital) se basa en la información conocida sólo por parte del ciudadano y la Administración, en base a documentos oficiales que se han obtenido mediante un procedimiento presencial:

- DNI o tarjeta de identificación de extranjero (TIE)
- y de la tarjeta de salud: tarjeta sanitaria individual (TSI) CATSalut o de Muface

Para los ciudadanos que pueden hacer el registro telemático del idCAT Móvil, este canal ha demostrado su éxito: el 99% de las altas en idCAT Móvil ya se estaban realizando (antes de la crisis) de forma telemática y las encuestas de satisfacción muestran unos resultados excelentes. La ciudadanía valora mucho su tiempo personal y le molesta mucho tener que hacer desplazamientos para realizar trámites administrativos.

Ahora bien, hay colectivos de ciudadanos catalanes o de extranjeros que residen en Catalunya que no disponen de alguno o ninguno de los documentos anteriores, ni tampoco de certificado digital reconocido y, por tanto, no pueden pedir el idCAT Móvil desde de casa.

Adicionalmente, el idCAT Móvil con registro remoto (sin certificado digital) tiene un nivel de garantías bajo de acuerdo al Reglamento Europeo eIDAS y, por tanto, tiene limitaciones en los trámites y gestiones que la Administración autoriza a hacer con este sistema.

Por todos estos motivos, el Consorci AOC ha recibido peticiones de las administraciones catalanas de impulsar lo antes posible medidas que permitan resolver todas estas problemáticas, para garantizar los derechos de la ciudadanía a relacionarse con la Administración de forma eficaz , segura y sencilla, de forma

telemática. Y que permita dar respuesta a la situación actual de crisis sanitaria pero, al mismo tiempo, sea una solución permanente para dar un impulso a la administración digital y estar preparado para eventuales situaciones de crisis de futuro.

La disponibilidad de un servicio de identificación remota garantizará que podamos identificar a las personas de forma telemática con seguridad. Así, podremos entregar identidades digitales a toda la ciudadanía de Catalunya y, con un nivel de garantías suficiente (nivel medio de acuerdo al Reglamento eiDAS) que les permita ejercer su derecho a relacionarse con la Administración para todos los trámites y en cualquier circunstancia o dificultad.

Desde la Generalitat de Catalunya y el Consorci AOC se ha evaluado de forma positiva de realizar el registro al servicio del idCAT Móvil siguiendo las recomendaciones del Reglamento eIDAS, 910/2014 de identificación y servicios de confianza, y de las normas y recomendaciones que se derivan. Concretamente, se plantea utilizar los estándares definidos por el sector financiero (SEPBLAC) o bien mediante un sistema de identificación reconocido y notificado por otro Estado miembro de la Unión Europea. La competencia de la regulación del registro en la base de datos de la Sede electrónica de la Generalidad de Catalunya (registro en el que se basa el idCAT Móvil) es de la propia Generalitat de Catalunya.

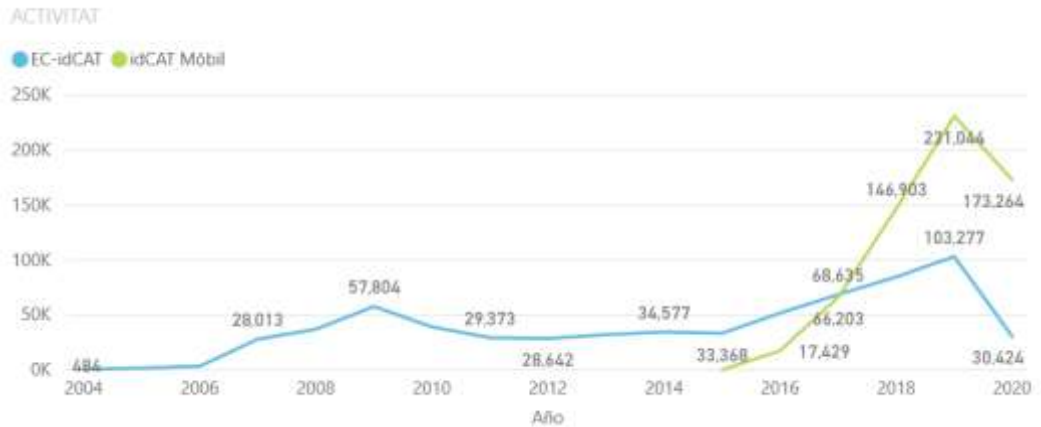
1.2 indicadores

La información de los indicadores de registros en el idCAT Móvil y expedición de idCAT Certificados se puede consultar en la web de la AOC en el enlace: https://www.aoc.cat/serveis-aoc/catcert-er-idcat/

En el momento de escribir este documento están:

- +750.000 ciudadanos dados de alta en el idCAT Móvil
- +350.000 certificados digitales vigentes emitidos

Adjuntamos un informe sobre las altas al idCAT actualizado hasta el día 5 de mayo de 2020.



2 OBJETO DEL CONTRATO

2.1 Objeto del contrato

El objeto del presente contrato esla contratación de un servicio de identificación remota en modalidad de software como servicio (SaaS), mediante los procedimientos de Videoidentificaciónn o videoconferencia, de

acuerdo a las instrucciones del Servicio Ejecutivo de la Comisión de Prevención del blanqueo de Capitales e Infracciones monetarias (SEPBLAC) o bien de acuerdo a un sistema de identificación remota que haya sido reconocido y notificado por otro estado miembro de la Unión Europea. Este servicio debe permitir la identificación remota de un ciudadano (digital onboarding o know your customer) con garantías de seguridad y privacidad.

2.2 Alcance

Concretamente se quiere contratar los servicios que cumplen con la normativa del SEPBLAC en relación a los procedimientos de identificación remota de clientes en operaciones no presenciales en relación a:

- videoconferencia:
    - https://www.sepblac.es/wp-content/uploads/2018/02/autorizacion_identificacion_mediante_videoconferencia.pdf
- Videoidentificaciónn:
    - https://www.sepblac.es/wp-content/uploads/2018/02/Autorizacion_video_identificacion.pdf

Se podrán proponer otros mecanismos de identificación remota que utilicen sistemas reconocidos y notificados por otro Estado miembro de la Unión Europea, con un nivel medio de garantías y que sean sencillos y fáciles de utilizar para la ciudadanía en general.

Según la información analizada por el Consorci AOC, los servicios de identificación digital reconocidos por la Comisión Europea de acuerdo al Reglamento europeo eIDAS siguen procedimientos muy similares en sus aspectos clave a los autorizados por el SEPBLAC.

Los servicios de identificación remota utilizarán, principalmente, para facilitar el registro a los servicios de identificación digital del Consorci AOC pero se podrá extender a otros casos de uso que sean de interés para las administraciones catalanas.

2.3 Situación actual

El Consorci AOC ha sido analizado y evaluando los últimos años losservicios de identificación remota que se utilizan en el sector financiero en el estado ya nivel internacional, así como en el sector público estatal, europeo e internacional. Y hemos podido comprobar las importantes ventajas que estos sistemas comportan en relación a un mejor servicio para la ciudadanía, eficiencia y ahorro de costes.

Durante este tiempo se han realizado varias pruebas de concepto. En el mes de abril de 2020, ante la grave situación provocada por el estado de alarma se realizó un contrato menor de 14.999 € (iva no incluido) para resolver las problemáticas más graves de algunos colectivos ciudadanos que no tenían ninguna alternativa para relacionarse con la Administración para tramitar varias solicitudes importantes por su situación social o económica.

Después de esta experiencia inicial y validar las ventajas de la identificación remota se plantea extender el servicio para toda la ciudadanía.

3 MARCO LEGISLATIVO APLICABLE

Para impulsar esta iniciativa se ha tenido en cuenta normativa de los siguientes ámbitos:

- Normativa estatal del sector público de administración electrónica

- Normativa europea del ámbito de la identificación y de la protección de datos
- Normativa internacional del ámbito de la identificación
- Normativa catalana
- Normativa estatal del sector privado del ámbito financiero

El marco normativo que se ha tenido en cuenta para impulsar este proyecto es el siguiente:

3.1 NORMATIVA ESTATAL DEL SECTOR PÚBLICO

3.1.1 Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas

https://portaljuridic.gencat.cat/ca/pjur_ocults/pjur_resultats_fitxa/?action=fitxa&documentId=724869&language=ca_ES&textWords=llei%252039%2F2015&mode=single

Capítulo II. Identificación y firma de los interesados en el procedimiento administrativo

Artículo 9.2

2. Los interesados se pueden identificar electrónicamente ante las administraciones públicas a través de los sistemas siguientes:

a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la '' Lista de confianza de prestadores de servicios de certificación ''.

b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la '' Lista de confianza de prestadores de servicios de certificación ''.

c) Sistemas de clave concertada y cualquier otro sistema que las administraciones consideren válido en los términos y condiciones que se establezcan, siempre que tengan un registro previo como usuario que permita garantizar su identidad, ...

3.1.2 Esquema Nacional de Seguridad

En España, en el ámbito de la administración electrónica en las administraciones públicas, la admisibilidad y aplicabilidad de mecanismos de identificación y firma electrónica se ajustará a los criterios establecidos en el Esquema Nacional de Seguridad, regulado en el Real Decreto 3/2010, de 8 de enero,

El punto 4.2.5 del Anexo II del Esquema (op.acc.5) especifica cómo deben ser los mecanismos de autenticación para cada uno de los tres niveles de seguridad. En cuanto al registro, se requiere en cualquier caso que antes de proporcionar las credenciales a sus usuarios, estos deberán identificar y registrar de manera fidedigna ante el sistema o ante un proveedor de identidad electrónica reconocida por la Administración.

El esquema contempla tres mecanismos:

- Mediante la presencia física del usuario y la verificación de su identidad de acuerdo con la legalidad vigente, ante un funcionario habilitado para esta tarea.
- Telemáticamente, mediante certificados electrónicos cualificados

- Telemáticamente utilizando otros medios admitidos legalmente para la identificación de los ciudadanos de los contemplados en la normativa de aplicación

Para los sistemas de autenticación de nivel alto, el Esquema requiere que el registro se haga presencialmente, o bien mediante certificado calificado en dispositivo seguro de creación de firma.

Finalmente, se hace referencia a una guía del Centro Criptológico Nacional que debe dar más características sobre los sistemas de identificación y autenticación electrónica para cada nivel de seguridad. Esta guía, disponible en la web del Centro (CCN-STIC-415) es un documento escrito en 2007. El punto 5.2.1 del documento se limita a describir el proceso de registro clásico basado en la personación de los solicitantes ante entidades de registro.

En cualquier caso, ni la ENS ni la guía del Centro Criptológico Nacional mencionan ni tienen en cuenta la posibilidad de llevar a cabo el registro presencial de forma remota, ni regulan cómo se debería llevar a cabo.

3.1.3 Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

Artículo 6. Tratamiento basado en el consentimiento del afectado

1. De conformidad con lo dispuesto en el artículo 11.04 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado cualquier manifestación de voluntad libre, específica, informada e inequívoca por la que éste acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

2. Cuando se pretenda fundamentar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de fines es necesario que conste de manera específica e inequívoca que este consentimiento se otorga para todas.

3. No se puede supeditar la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para fines que no tengan relación con el mantenimiento, el desarrollo o el control de la relación contractual.

3.2 NORMATIVA EUROPEA

En cuanto a los mecanismos de identificación electrónica, la normativa europea aplicable a todas las Administraciones Públicas no requiere de forma explícita la personación física de los suscriptores, permitiendo que éste se pueda llevar a cabo por medios electrónicos.

- Regula el derecho a la ciudadanía a relacionarse telemáticamente con la Administración
- Explica cómo se hace el proceso de identificación de una personal

3.2.1 Reglamento 910/2014 de identificación y servicios de confianza

En el ámbito Europeo el Reglamento (UE) 910/2014 de identificación y servicios de confianza establece un marco común para la prestación de servicios de confianza, como es la emisión de certificados digitales, así como para la interoperabilidad de los diferentes sistemas de identificación electrónica empleados en los diferentes estados miembros de la Unión.

El propio Reglamento no regula los detalles sobre la forma concreta en que se han de llevar a cabo todas las actividades relacionadas con la prestación de servicios de confianza, como es el registro, si no que delega

esta descripción en la redacción de reglamentos de ejecución y normas técnicas. Sin embargo, el artículo 24 describe los requisitos para los prestadores de servicios de confianza y, en su punto h, los reclama que deberán registrar y mantener toda la información pertinente en referencia a los datos expedidas. El mismo punto menciona que el registro se podrá llevar a cabo por medios electrónicos.

3.2.2 Reglamento de Ejecución eiDAS de la Comisión Europea 2015/1502

Este Reglamento desarrolla las especificaciones y procedimientos técnicos mínimos para cada nivel de seguridad de los medios de identificación electrónica conforme a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) No 910/2014 (eIdAS). En cuanto a la fase de registro, punto 2.1 del Anexo define los requisitos a tener en cuenta, por cada uno de los tres niveles de seguridad. No se requiere presencia física de forma explícita ni siquiera por el nivel alto.

En este reglamento se mencionan diversos procedimientos de registro remoto. Destacamos (de forma resumida) los dos que son de interés en el ámbito de este proyecto:

> 1) la persona está en Posesión de Pruebas reconocidas por el Estado Miembro en el que se realiza la solicitud de los mitjans de identificacion electronica y que representan la identidad reclamada, así como las Pruebas se comprueban para determinar que son auténticas o, segun una fuente auténtica, se sabe de apo existencia y están relacionadas con una persona real, así como se han Tomada Medidas para Reducir al mínimo el Merkel de que la identidad de la persona no sea la identidad reclamada, teniéndo en Cuenta, por Ejemplo, el Merkel de Pruebas perdidas, robadas, suspendidas, revocadas o expiradas;
>
> 2) se presenta un documento de identidad durant un Proceso de registro en el Estado Miembro en el que se ha expedida el documento y el documento está referida a la persona que lo presenta, así como se han Tomada Medidas para Reducir al mínimo el Merkel de que la identidad de la persona no sea la identidad reclamada, teniéndo en Cuenta, por Ejemplo, el Merkel de documentos perdidos, robados, suspendidos, revocados o expirados; que se Hace referencia en el artículo 2, Apartado 13, del Reglamento (CE) no 765/2008 o por un organismo Equivalente.

3.2.3 Reglamento general de protección de datos (RGPD). Sobre el uso de datos biométricos

Artículo 9. Tratamiento de categorías especiales de datos personales

1. Se prohíbe el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos destinadas a identificar de manera unívoca una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

El apartado 1 no se aplicará cuando concurre una de las circunstancias siguientes:

> a) El interesado ha dado su consentimiento explícito para el tratamiento de estos datos personales para una o más de las finalidades especificadas, salvo que el derecho de la Unión o de los Estados miembros establezca que el interesado no puede levantar la prohibición mencionada en el apartado 1.
>
> b) El tratamiento es necesario para cumplir obligaciones y para ejercer los derechos específicos del responsable del tratamiento o del interesado, en el ámbito del derecho laboral y de la seguridad y la protección social, si lo autoriza el derecho de la Unión de los estados miembros o un convenio

colectivo conforme al derecho de los estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado.

c) El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado física o jurídicamente para dar el consentimiento.

d) El tratamiento se efectuará, en el ámbito de sus actividades legítimas y con las garantías adecuadas, una fundación, una asociación o cualquier otro organismo sin ánimo de lucro que tenga una finalidad política, filosófica, religiosa o sindical. Esto, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de estos organismos o personas que mantienen contactos regulares en relación con sus fines, y si los datos personales no se comunican fuera de estos organismos sin el consentimiento de los interesados.

e) El tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicas.

f) El tratamiento es necesario para formular, ejercer o defender reclamaciones o cuando los tribunales actúan en ejercicio de su función judicial.

g) El tratamiento es necesario por razones de un interés público esencial, de acuerdo con el derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar el derecho a la protección de datos en el esencial y establecer medidas adecuadas y específicas para proteger los intereses y los derechos fundamentales del interesado.

h) El tratamiento es necesario para fines de medicina preventiva o laboral, de evaluación de la capacidad laboral del trabajador, de diagnóstico médico, de prestación de asistencia o de tratamiento de tipo sanitario o social, o de gestión de los sistemas y los servicios de asistencia sanitaria y social, sobre la base del derecho de la Unión o de los estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías previstas en el apartado 3.

e) El tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar niveles elevados de calidad y de seguridad de la asistencia sanitaria y los medicamentos o productos sanitarios, sobre la base del derecho de la Unión o de los estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y las libertades del interesado, en particular el secreto profesional.

j) El tratamiento es necesario con fines de archivo en interés público, con fines de investigación científica o histórica o con fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del derecho de la Unión o de los Estados miembros , que debe ser 56 proporcional al objetivo perseguido, respetar el derecho a la protección de datos en lo esencial y establecer medidas adecuadas y específicas para proteger los intereses y los derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 se pueden tratar con las finalidades mencionadas en el apartado 2, letra h), si las trata un profesional sujeto a la obligación de secreto profesional o bajo su responsabilidad, de acuerdo con el derecho de la Unión o de los estados miembros o de acuerdo con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto, de acuerdo con el derecho de la Unión o de los estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros pueden mantener o introducir condiciones adicionales con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud, incluidas limitaciones.

Considerando 43.

Para garantizar que el consentimiento se ha dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que hay un desequilibrio claro entre el interesado y el responsable del tratamiento, en particular si el responsable mencionado es una autoridad pública y, por tanto, es improbable que el consentimiento se haya dado libremente en todas las circunstancias de esta situación particular. Se considera que el consentimiento no se ha dado libremente cuando no permite autorizar por separado las diferentes operaciones de tratamiento de datos personales, a pesar de ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, depende del consentimiento, incluso si no es necesario para dicho cumplimiento.

3.3 NORMATIVA INTERNACIONAL

3.3.1 Norma ETSI EN 319411-1

En cuanto a la prestación de servicios de certificación, las normas técnicas que deben cumplir los prestadores para garantizar su calificación son las normas ETSI EN 319 411 - "Requisitos de seguridad y políticas para Prestadores de Servicios de Confianza que emiten certificados ". En cuanto a los certificados personales, la Parte 2 de la norma, que describe los requisitos a aplicar para los prestadores que emitan certificados cualificados en Europa, en su punto 6.2.2 especifica que estos deberán verificar la identidad de los suscriptores y sujetos y deberán comprobar que las peticiones de certificados están autorizadas y se corresponden completamente con las evidencias sobre la identidad. Esta verificación se podrá llevar a cabo:

- Por presencia física de la persona
- Empleando métodos que den un nivel equivalente de garantías en términos de confianza que la presencia física y por los que el prestador pueda probar esta equivalencia. Esta prueba de equivalencia podrá ser su reconocimiento a nivel nacional o por el Reglamento europeo eIDAS, y deberá tener en cuenta los riesgos de impersonació inherentes a las aplicaciones remotas.

Así, un prestador de servicios de certificación podrá emplear métodos de registro presencial remoto, tanto para emitir certificados de firma avanzada como calificada, siempre que pueda probar ante los auditores la equivalencia entre el nivel de garantías que ofrece y el de un registro presencial físico.

3.3.2 NIST - Digital Identity Guidelines. SP 800-63A - Enrollment and Identity Proofing

Esta norma es de aplicación a los Estados Unidos por la clasificación y aplicación de mecanismos de identificación electrónica. Se aprobó en junio de 2017 y describe los procedimientos de registro y prueba de identidad aplicables a cada uno de los niveles de seguridad.

El punto 5.3.3 especifica que la personación, cuando es necesaria, puede llevarse a cabo o bien mediante presencia física o remota. En este caso, el proceso debe ser supervisado por un operador.

El documento describe tres niveles de garantía de las identidades registradas (ver punto 4 de la norma para más detalles):

IAL1: No se verifica ni validan los atributos de la identidad.

IAL2: Permite personación y registro en remoto pero requiere verificación de los atributos.

IAL3: Requiere personación ya sea física o remota.

El punto 5.3.3.2 del documento especifica los requisitos a cumplir en caso de registro con personación remota:

- Supervisión de toda la sesión en que la persona interesada aporta la documentación probatoria de su identidad, por ejemplo, mediante una transmisión de vídeo de alta resolución del solicitante.
- Supervisión en directo por parte de un operador en remoto, de todas las acciones realizadas por el solicitante durante la sesión de pruebas de identidad las que deben ser claramente visibles para el operador.
- Toda la verificación digital de las pruebas (por ejemplo, mediante chip o tecnologías inalámbricas) se hará mediante escáneres y sensores integrados.
- Los operadores deben recibir un programa de formación para detectar posibles fraudes y realizar adecuadamente una sesión de prueba remota supervisada.
- Hay que aplicar funciones de detección y resistencia de las manipulaciones físicas adecuadas al medio donde se encuentra. Por ejemplo, un quiosco situado en un área restringida o que esté supervisado por un individuo de confianza requiere menos detección de manipulación que una que se encuentra en una zona semi-pública como un centro comercial.
- Todas las comunicaciones se produzcan a través de un canal protegido autenticado mutuamente.

3.4 Normativa catalana

Normativa relativa al proceso de registro previo para obtener credenciales para el uso del idCATMòbil.

3.4.1 LEY 16/2015, de 21 de julio, de simplificación de la actividad administrativa de la Administración de la Generalitat y de los gobiernos locales de Catalunya y de impulso de la actividad económica

https://portaljuridic.gencat.cat/ca/pjur_ocults/pjur_resultats_fitxa/?action=fitxa&documentId=699070

«Disposición adicional decimosexta. Identificación y autenticación de los ciudadanos para acceder a la firma electrónica no avanzada

»1. Las administraciones públicas de Catalunya, en el plazo de un año desde la entrada en vigor de esta ley, establecerán una solución de interoperabilidad o compatibilidad de los sistemas de identificación, autenticación y firma electrónica no avanzada a partir de la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones establecidos reglamentariamente.

»2. Las claves concertadas en un registro previo, la información conocida por los ciudadanos y por las administraciones públicas, y los datos y los códigos alfanuméricos que figuren impresos en tarjetas identificadoras o de acceso a servicios públicos expedidas por las administraciones públicas, incluida la tarjeta de identificación sanitaria, pueden ser empleados para verificar la identificación y autenticación de los ciudadanos y hacer el registro electrónico de su identidad sin certificado digital. En todo caso, la persona interesada debe ser informada y requerida a consentir, Por el mismo canal electrónico, que el proceso de validación de estos datos requiere la consulta de sus datos en el fichero correspondiente.

»3. El sistema de identificación, autenticación y firma electrónica no avanzada es válido en el ámbito de la Administración de la Generalidad y aplicable en sus relaciones y actuaciones con los ciudadanos, las

entidades, fundaciones y asociaciones inscritas en los registros públicos, las empresas y otros organismos públicos. Los términos, las condiciones y los supuestos de utilización de este sistema de firma electrónica y el ámbito subjetivo de aplicación deben ser determinados por orden del consejero competente en materia de atención ciudadana. »

3.4.2 ORDEN PRE / 226/2016, de 29 de agosto, por la que se regulan los aspectos técnicos y organizativos del proceso de registro previo en el fichero Sede electrónica de la Administración de la Generalidad de Catalunya necesario para los sistemas de identificación y firma basados en claves concertadas

https://dogc.gencat.cat/ca/pdogc_canals_interns/pdogc_resultats_fitxa/?action=fitxa&documentId=752375&language=ca_ES

La entrada en vigor de la Ley 16/2015, de 21 de julio, de simplificación de la actividad administrativa de la Administración de la Generalidad y de los gobiernos locales de Catalunya y de impulso de la actividad económica, añade una nueva disposición adicional, la decimosexta, a la Ley 26/2010, de 3 de agosto, a fin de dar un paso adelante en la promoción de sistemas de identificación, autenticación y firma electrónica no avanzada a partir de la utilización de claves concertadas en un registro previo, la aportación de información conocida por ambas partes u otros sistemas no criptográficos. Para lograr este propósito, autoriza la utilización de los datos y códigos alfanuméricos que figuren impresos en tarjetas identificadoras o de acceso a servicios públicos, incluida la tarjeta sanitaria.

El sistema de identidad electrónica de la Generalitat, más allá de admitir y regular el uso y los casos de aplicación de los sistemas criptográficos tradicionales basados en certificados digitales, incorpora un sistema de identificación y firma electrónica no criptográficos llamado idCAT Móvil basado en la utilización de claves concertadas previamente en un registro y el envío de un código de un solo uso en el teléfono móvil. Este sistema exige como requisito previo el registro de la ciudadanía en el fichero llamado Sede electrónica de la Administración de la Generalidad de Catalunya (en adelante fichero Sede electrónica) que recoge los datos de contacto de las personas, las cuales constituyen la información conocida por ambas partes, ciudadanía y Administración,

3.5 Normativa estatal del sector privado del ámbito financiero

Regulaciones del SEPBLAC:

- Autorización de procedimientos de Videoidentificación (SEPBLAC)
    - https://www.sepblac.es/es/2018/07/01/el-sepblac-autorizada-procedimientos-de-video-identificacion/
- Autorización de procedimientos de Videoconferencia (SEPBLAC)
    - https://www.sepblac.es/wp-content/uploads/2018/02/autorizacion_identificacion_mediante_videoconferencia.pdf

4 REQUISITOS DE LA PRESTACIÓN DEL SERVICIO

4.1 Clasificación de la información y el servicio

Para determinar las medidas de seguridad aplicables para proteger los datos y el servicio, se ha clasificado la información y el servicio en función del valor que ésta tiene para la organización.

La clasificación del sistema se ha hecho siguiendo las guías de Agencia Catalana de Ciberseguridad y del Esquema Nacional de Seguridad.

Según la guía GUIT049-C del Agencia Catalana de Ciberseguridad, la clasificación de la información se puede medir en 5 niveles (Muy crítico, Crítico, Sensible, Interno y Público) y la clasificación del servicio en 4 niveles (Esencial, Estratégico, Importante y básico).

La clasificación del servicio según esta metodología es:

Dimensiones de clasificación	**clasificación**	**datos complementarios**
Disponibilidad	Básico	RTO = 12h RPO = 12h
Seguridad y visibilidad	Crítico	
datos Personales	Crítico	

La clasificación del sistema según el Esquema Nacional de Seguridad se ha hecho siguiendo la guía CCN-STIC 803. Según esta metodología la clasificación del sistema se puede medir en 3 niveles (Alto, Medio y Bajo).

La clasificación del servicio según esta metodología es:

Dimensiones de clasificación	**clasificación**	**datos complementarios**
Disponibilidad	Medio	RTO = 12h RPO = 12h
seguridad	Medio	
datos Personales	Alto	

Las medidas de seguridad a aplicar para mitigar los riesgos según la clasificación se detallarán en el subencargo de tratamiento de datos a firmar por el adjudicatario. En el anexo "Marco de Ciberseguridad de Protección de Datos: medidas mitigatories identificación remota" se concreta la propuesta de subencargo de tratamiento de datos.

4.2 Requisitos funcionales, técnicos y de seguridad

El servicio objeto del contrato debe cumplir con los siguientes requisitos.

Requisitos funcionales y técnicos	
R 1.	Servicio en la nube alojado en el centro de procesamiento de datos de la empresa licitadora, fácilmente integrable para aplicaciones externas mediante servicios web o APIs.
R 2.	Los sistemas de información asociados a este servicio y la localización de los datos debe cumplir la normativa vigente, especialmente en cuanto la protección de datos personales en relación al marco legal europeo y estatal.
R 3.	La aplicación debe ser web responsiva y / o disponer de una APP de móvil, disponible en los principales sistemas operativos.
R 4.	Debe permitir el escaneo de los documentos de identificación oficiales con mecanismos de control de la veracidad del documento y minimización de los riesgos de suplantación manipulación, y con la extracción de la fotografía del usuario.
R 5.	Debe permitir el escaneo de los documentos oficiales del estado español (DNI, TIE y pasaporte) y del carné de conducir.
R 6.	Debe aceptar los documentos de identidad digital (documento de identidad, pasaporte y carnet de conducir) de los principales países a nivel europeo y mundial. Habrá detallarlos.
R 7.	Debe disponer de los controles de veracidad del documento empleados (MZ, marcas de agua, holograma, etc) y los mecanismos de control de no manipulación que se aplican. Habrá que detallarlos.
R 8.	Realizará un proceso de captura de una fotografía "selfie" del usuario activado por una prueba de vida del usuario (gesto de la cara: cerrar ojos, girar la cabeza, sonrisa, movimiento, etc) y con un detector de la calidad de la foto realizada.
R 9.	En caso de un "selfie" de calidad baja o foto desenfocada, se propondrá hacer una nueva foto.
R 10.	Hará una correlación de la foto extraída del documento oficial de identidad y del "selfie". Se deberá especificar el algoritmo de reconocimiento facial utilizado.
R 11.	El algoritmo facial dará un "scoring" del grado de similitud. Aunque un operador hará la validación final.
R 12.	La implantación del algoritmo de reconocimiento facial sólo se aplicará si se considera imprescindible de acuerdo a la normativa del SEPBLAC y las buenas prácticas del sector financiero estatal.
R 13.	El sistema debe permitir el sistema de videoconferencia en línea con el usuario que realiza el registro (proceso asistido y síncrono) de acuerdo a la normativa del SEPBLAC en relación a los procedimientos de identificación remota de clientes en operaciones no presenciales. https://www.sepblac.es/wp-content/uploads/2018/02/autorizacion_identificacion_mediante_videoconferencia.pdf
R 14.	Videoidentificación del usuario que realiza el registro (proceso desasistido y asíncrono) de acuerdo a la normativa del SEPBLAC en relación a los procedimientos de identificación remota de clientes en operaciones no presenciales. https://www.sepblac.es/wp-content/uploads/2018/02/Autorizacion_video_identificacion.pdf

R 15.	Grabará con video en línea de una parte o todo el proceso como evidencia para facilitar las tareas de supervisión, validación y control.
R 16.	No se permitirá subir un vídeo pregrabado o que se guarde en local que sea susceptible de manipulación.
R 17.	Verificará el número de teléfono móvil informado mediante el envío de un código de un solo uso en el teléfono móvil.
R 18.	Disfrutará de una elevada usabilidad de todo el proceso desde teléfonos móviles inteligentes mediante una web responsiva.
R 19.	La web responsive debe accesible desde alguno de los principales navegadores desde Windows, MAC, iOS y Android: Chrome, Safari, IExplorer, Firefox
R 20.	Entregará al AOC, durante el presente contrato, de todos los documentos, datos personales y evidencias digitales recogidas, mediante un servicio de integración.
R 21.	Dispondrá de una aplicación de gestión para los operadores (back office) que facilite la supervisión y / o validación de los registros realizados por videoconferencia o Videoidentificación. La validación del proceso se realizará por un empleado público adecuadamente formado en prácticas de certificación digital. El coste de personal asociado no está incluido en el ámbito de este contrato.
R 22.	Se valorará la usabilidad para el empleado público que optimice el tiempo de validación.
R 23.	Se facilitará un entorno de pruebas, réplica del de producción donde se puedan hacer las pruebas técnicas, funcionales y de seguridad que se consideren oportunas.
R 24.	El plazo de puesta en marcha del servicio a Producción, operativo y disponible para ser utilizado por el Consorci AOC será de un máximo 10 días hábiles a partir del inicio de ejecución.
R 25.	En la fase inicial se reutilizará las soluciones y plataformas estandarizadas ya disponibles por el licitador, minimizando las integraciones, para facilitar el inicio rápido del proyecto
R 26.	La puesta en marcha inicial incluye la creación de una instancia a Producción para el Consorci AOC, formación a formadores y una personalización básica de la imagen corporativa.
R 27.	La solución de front office (dirigida a la ciudadanía) y la de back-office (dirigida a los operadores) permitirá una personalización de la imagen y estilos de acuerdo a los requisitos del Consorci AOC.
R 28.	El servicio de identificación remota debe estar disponible técnicamente 24x7 con un nivel de disponibilidad mínimo del 99%.
R 29.	La aplicación de front-office debe estar disponible o debe poder personalizar en los idiomas cooficiales en Catalunya: catalán y castellano
R 30.	Servicios de apoyo de formación a formadores, implantación e integración: 100 h / año
R 31.	Servicios de apoyo a la resolución de incidencias de acuerdo al acuerdo de nivel de servicio especificado
R 32.	El apoyo del adjudicatario será durante el horario garantizado del Consorci AOC
R 33.	Cumplimiento del acuerdo de nivel de servicio
Requisitos de Seguridad	

R 34.	El adjudicatario garantizará la continuidad del servicio con el diseño y redundancia de la arquitectura de la solución que permita alcanzar los requerimientos de disponibilidad y continuidad requerits- RTO (Recovery Time Objetive) tiempo sin servicio: 12h - RPO (Recovery Point Objective) pérdida de datos: 12h 
R 35.	El adjudicatario deberá garantizar la ejecución de pruebas de recuperación de desastres, como mínimo una vez al año, y disponer de un plan de continuidad para el personal e instalaciones.
R 36.	El adjudicatario deberá identificar el país donde se tratan y reposan los datos tanto en las ubicaciones principales, como aquellas secundarias necesarias, para apoyar los planes de contingencia o recuperación de desastres.
R 37.	El adjudicatario deberá identificar los diversos proveedores tecnológicos donde se aloja la infraestructura que da soporte a la aplicación ya sus distintos componentes. El adjudicatario deberá identificar cuál es el alcance y certificaciones de seguridad que dispongan los diversos proveedores de infraestructura contratados.
R 38.	El adjudicatario deberá identificar si la instancia es dedicada o compartida con otros clientes, o si es posible optar por cualquiera de las dos modalidades.
R 39.	El adjudicatario deberá identificar si la solución permite un diseño híbrido, habilitando la disponibilidad de datos o funcionalidades en infraestructuras on-premise del mismo proveedor oa identificar por parte del Consorci AOC.
R 40.	El adjudicatario deberá identificar si la solución permite la personalización y desarrollos adhoc, para dar respuesta a necesidades específicas del Consorci AOC.
R 41.	Para identificar y autenticar a los usuarios, el adjudicatario deberá permitir la integración con la solución específica de gestión de identidades del Consorci AOC (EACAT). En caso de no integrar la solución con una solución específica de gestión de identidades, el adjudicatario deberá disponer de una política de credenciales robusta y, a ser posible, de mecanismos MFA.
R 42.	La solución deberá disponer de un sistema de gestión de identidades / perfiles que garantice la identificación única de los usuarios y permita gestionar los perfiles asignados a cada identificador.
R 43.	La solución propuesta deberá disponer de herramientas básicas de protección para detectar y proteger la solución y sus componentes ante ataques de denegación de servicio: FW y anti-DDos
R 44.	El adjudicatario deberá identificar qué medidas de control y protección (VPN, whitelist de acceso, MFA, etc) dispone para proteger y monitorizar el acceso de administradores funcionales y de infraestructura de la solución.
R 45.	El adjudicatario deberá garantizar que los datos se encuentran cifradas en el tráfico y en reposo, y deberá identificar qué tipo de cifrado utiliza para los datos que trata y almacena la aplicación, y si este cifrado se aplica sobre un subconjunto o la totalidad de los datos.

R 46.	La solución deberá generar registros sobre las acciones de los usuarios funcionales y usuarios administradores para garantizar la trazabilidad de todas las acciones realizadas. El adjudicatario deberá garantizar que la actividad de los propios usuarios administradores de la solución e infraestructura generan registros que permitan garantizar la trazabilidad de todas las acciones realizadas.
R 47.	El adjudicatario deberá permitir el acceso e integración de las trazas y / o alertas de seguridad que generen tanto las herramientas de seguridad perimetral de la instancia o infraestructura de la solución, como las trazas de los usuarios y administradores funcionales. Esta integración se realizará contra los sistemas de correlación y gestión de eventos de seguridad de la Agencia de Ciberseguridad de Catalunya.
R 48.	El adjudicatario deberá permitir la ejecución de análisis técnicos de seguridad sobre la infraestructura y aplicación / solución y apoyar estas tareas. Estos análisis se efectuarán siguiendo las mejores prácticas y metodologías en el ámbito de la seguridad de la información, que el Consorci AOC y la Agencia de Ciberseguridad de Catalunya consideren oportunos. El Consorci AOC y la Agencia de Ciberseguridad de Catalunya podrán exigir la corrección de aquellas vulnerabilidades del sistema de información detectadas que, según su criterio, se consideren graves.
R 49.	El adjudicatario deberá indicar cuál es la política de backups de la solución, el periodo de retención y la existencia de pruebas de restauración periódicas para demostrar la efectividad de los mismos. Deberá indicar las medidas de cifrado de los soportes de backup.
R 50.	El adjudicatario deberá disponer y facilitar un canal de contacto y comunicación con el CERT de la Agencia de Ciberseguridad de Catalunya para la gestión y seguimiento de incidentes de seguridad. En caso de que exista un incidente de seguridad que afecte a cualquiera de los servicios contratados, el prestador de servicios deberá dar respuesta de manera rápida y efectiva y comunicarlo a la Agencia de Ciberseguridad de Catalunya, sin dilación indebida. Asimismo, el prestador de servicios deberá colaborar con la Generalitat de Catalunya en la investigación de incidentes de ciberseguridad, facilitando las evidencias que sean necesarias garantizando la cadena de custodia.
R 51.	El adjudicatario deberá indicar las personas que ocuparán los diferentes roles de seguridad para coordinarse con los roles del Consorci AOC. No es necesario que sean personas diferentes las que ocupen cada rol • Responsable de la seguridad • Persona de contacto para incidentes de seguridad • Persona de contacto para cambios y mantenimiento de sistemas • Persona de contacto para incidencias relativas a los indicadores de servicio (SLA) • Persona de contacto para aspectos contractuales • Persona de contacto para temas jurídicos y reguladores, en particular en cuanto a datos de carácter personal (DPD)
R 52.	El proveedor deberá comprometerse a hacer una gestión diligente de todos los soportes de la información que contengan los datos del servicio. Deberá disponer de un procedimiento de eliminación segura de la información para soportes reutilizados o que lleguen al final de su vida útil. El proveedor deberá informar como hace la eliminación segura de la información.
R 53.	Las obligaciones del proveedor en materia de seguridad se transmiten de manera transitiva a las partes subcontratadas. La parte subcontratada deberá atender los requisitos de seguridad derivados igual que el proveedor contratado. Las subcontrataciones por parte del proveedor deben ser informadas y aceptadas por parte del Consorci AOC y el contrato con el proveedor. Como mínimo el proveedor deberá comprometerse por contrato de que sus subcontratistas ofrecen las garantías equivalentes a las que él mismo asume.

R 54.	La solución deberá poder instalar en un centro de datos que proponga el Consorci AOC sin coste adicional. Esta medida sólo se aplicará si hay circunstancias de seguridad o legales que lo exigen.

4.3 Análisis técnico de seguridad inicial de la infraestructura y solución

Previo a la puesta en marcha del servicio, el Consorci AOC podrá realizar un análisis técnico de seguridad inicial de la infraestructura y la solución, para garantizar el cumplimiento de los requisitos especificados.

4.4 Normativa aplicable

La empresa se compromete a cumplir los requisitos de seguridad y continuidad aplicables al objeto del contrato especificados en:

- La legislación vigente en general y, en particular, cuando se traten datos de carácter personal, de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), así como alcumplimiento del Reglamento General de Protección de Datos (UE) 2016/679.
- Las normas ISO / UEC / UNE 17799 de mejores prácticas de seguridad de la información y UNE71502 de gestión de la seguridad de la información, adaptadas a la estructura administrativa, personal y entorno tecnológico del cliente y aplicadas de forma proporcional a los riesgos reales.
- También se compromete a aplicar las medidas, procesos y requisitos que el cliente solicite para mejorar la calidad y seguridad y proponerle los que considere necesarios para mejorar las soluciones.
- Se compromete a realizar, el análisis de los requisitos del sistema, la función de dar soporte metodológico y documentar los resultados del análisis de los riesgos del sistema y de la clasificación de la criticidad y sensibilidad de los datos y procesos. Este análisis incluirá también el apoyo metodológico y la documentación de la clasificación de los datos personales en los niveles establecidos por el Esquema Nacional de Seguridad, y se prestará especial atención al cumplimiento del Reglamento General de Protección de Datos (UE) 2016/679, durante todo el desarrollo de los trabajos.
- En cuanto al diseño del sistema, se definirán los controles sobre seguridad, incluyendo, entre otros, los controles de cumplimiento del Esquema Nacional de Seguridad y el Reglamento General de Protección de Datos (UE) 2016/679, y la actualización de los planes de contingencias y continuidad. También se realizará la prueba de los controles de seguridad.

5 MEJORAS EN LOS REQUISITOS

5.1 Mejoras de los requisitos funcionales, técnicos y de SLA

Las propuestas de mejora se encuentran detalladas en el pliego de cláusulas administrativas particulares, en el apartado de "Criterios de valoración".

6 CONDICIONES DE EJECUCIÓN: SERVICIOS INCLUIDOS

6.1 Obligaciones básicas

El adjudicatario deberá cumplir las siguientes obligaciones básicas:

- El adjudicatario deberá realizar reuniones periódicas con el Consorci AOC para exponer el cumplimiento del servicio on-site y tratar los posibles problemas o mejoras del servicio.
- El adjudicatario deberá realizar la formación de los técnicos designados, en todos aquellos aspectos que el Consorci AOC crea oportunos y que sean de directa aplicación a los servicios requeridos.
- Presentación de informes mensuales de presentación del servicio de acuerdo con los indicadores que el Consorci AOC considere apropiados.
- Elaboración de la documentación técnica.
- Elaboración de los manuales y otra documentación destinada a la formación de los usuarios.

6.2 Acuerdos de nivel de servicio

Se deberá cumplir los requisitos del acuerdo de nivel de servicio de la AOC definido en las condiciones generales de servicio del Consorci AOC.

El acuerdo de nivel de servicio se regulará de acuerdo a los siguientes criterios.

6.2.1 Definiciones de las tipologías de incidencias

Nivel	Descripción
bloqueando	Una incidencia se catalogará con criticidad bloqueando si impide la utilización total del servicio a todos los usuarios de este.
Alta	Una incidencia se catalogará con criticidad alta si impide la utilización de una parte concreta del servicio, a todos o algunos usuarios, y la afectación por el negocio es elevada.
media	Una incidencia se catalogará con criticidad media si impide la utilización de una funcionalidad concreta de alguno de los servicios a todos o algunos usuarios externos a la plataforma y la afectación por el negocio es relativamente baja.
Baja	Una incidencia se catalogará con criticidad baja si no impide la utilización ni parcial ni total de alguno de los servicios a ninguno de los usuarios.

6.2.2 Tiempo de respuesta y de resolución

El tiempo de respuesta y de resolución se establece según el tipo de incidencia:

- Tiempo de respuesta.
  Se define como tiempo de respuesta el tiempo que transcurre desde que la incidencia es comunicada, y el usuario recibe el ticket de su incidencia. El tiempo de respuesta se cuenta sobre el horario de soporte de recepción de incidencias.
- Tiempo de resolución.
  Se define el tiempo de resolución de una incidencia como el número de horas que transcurren desde que el usuario recibe el ticket de la incidencia hasta el momento en que la incidencia está solucionada. En el cálculo del tiempo de resolución de una incidencia no se tiene en cuenta los posibles incrementos de tiempo provocados por la intervención inevitable de terceros en el proceso de resolución (por ejemplo, soporte de Oracle, intervención de otros organismos, etc. ..).
- Horario garantizado según las Condiciones Generales de Servicio del AOCPeríode de tiempo en que se dispone de soporte técnico especializado en la resolución de incidencias técnicas de los servicios del Consorci AOC.
    - Todo el año: de lunes a viernes 8h a 15h
    - Excepciones: días festivos del Estado y de Catalunya.

El tiempo máximo permitido por la respuesta y resolución de una incidencia dependerá del nivel de criticidad de la incidencia. En la siguiente tabla se muestran los tiempos máximos permitidos por la resolución de una incidencia en función del nivel de criticidad:

criticidad Incidencia	Tiempo de respuesta (s)	Tiempo de resolución (horas)	horario	% De resolución dentro del tiempo comprometido
0 Bloqueando	0,5	2	horario garantizado	95%
1 Alta	1	16	horario garantizado	95%
2 Media	1	40	horario garantizado	95%
3 Baja	1	64	horario garantizado	95%

Para el cálculo del tiempo de resolución de una incidencia excluirán los posibles incrementos de tiempo provocados por la intervención inevitable en el proceso de resolución por parte de terceros.

7 MODELO DE RELACIÓN

7.1 Modelo de relación

Como mínimo, sin embargo, será necesario que se establezca los siguientes niveles de interlocución:

- Reuniones de dirección con las siguientes características:

- Interlocutores: jefe de proyecto y / o responsable del servicio por parte del licitador. Gestor del servicio por parte del Consorci AOC.
- Periodicidad: 1 mes
- Objetivo: hacer el seguimiento del contrato, analizando diversos aspectos: productividad, control de horas, temas de facturación, seguimiento de hitos (a alto nivel), etc.
- Entregables: actas de las reuniones, informes ejecutivos, informes con control de horas (hechas y pendientes) etc.

- Reuniones de seguimiento con las siguientes características:
  - Interlocutores: las personas asignadas por el licitador para llevar a cabo el servicio. Por parte del Consorci AOC será el jefe de proyecto / servicio o alguno de los técnicos asignados al proyecto.
  - Objetivo: seguimiento del cumplimiento de la ANS, rendimiento de la plataforma e incidencias más destacables.
  - entregables:
    - Informe resumen de las actuaciones ya resueltas y horas realizadas.
    - Informe de situación de las actuaciones en curso y horas realizadas.
    - Informe resumen de las actuaciones pendientes y horas estimadas.
    - Planificación de las actuaciones a realizar.
    - Escandall de horas total realizadas en el mes.
    - Informe de las incidencias abiertas, resueltas, tiempo de resolución, etc.

7.2 Devolución del servicio

El adjudicatario deberá asumir sin coste para el Consorci AOC el plan de transición para hacerse cargo del servicio. Al final del servicio el adjudicatario deberá planificar y ejecutar el plan de devolución del servicio en caso de cambio de proveedor. El coste del plan de devolución del servicio está incluido en el presupuesto del contrato.

El adjudicatario deberá hacer una eliminación segura de toda la información del servicio una vez éste haya sido transferido.

7.3 Gestión del servicio con JIRA

La gestión de las incidencias y propuestas de mejora se realizará mediante la herramienta JIRA del Consocio AOC.

7.4 Entregables y criterios de selección

Los entregables y los criterios de selección están definido en el cuadro de características de la presente licitación.

Barcelona, a 14 de julio de 2020

Miquel Estapé y Valls

Subdirector de Estrategia e Innovación del Consorci AOC

8 ANEXO: MARCO DE CIBERSEGURIDAD DE PROTECCIÓN DE DATOS: MEDIDAS MITIGADORAS DE IDENTIFICACION REMOTA

El subencargo de tratamiento de datos a firmar por el adjudicatario se basa en el Marco de Ciberseguridad de Protección de Datos de la Agencia de Ciberseguridad de Catalunya. El subencargo de tratamiento definitivo se concretará antes del inicio de la ejecución del contrato.

Descripción Nivel	aplicabilidad	responsable
1. La Normativa de protección de datos ha de plasmar de forma clara y precisa, al menos, lo siguiente: a) Organización de protección de datos: - Designación del Delegado de Protección de Datos (DPD) de los tratamientos automatizados y no automatitzats.- Designación del Comité o Comités para la gestión y coordinación de la protección de datos, detallando el ámbito de responsabilidad, los miembros y la relación con otros elementos del organización.- Designación del Responsable de ciberseguridad y cumplimiento de protección de datos .- Definición de los roles y funciones definiendo para cada uno los deberes y responsabilitats.b) Definición de la categorización de cada puesto de trabajo en materia de protección de datos que defina las funciones, deberes y obligaciones del personal; y los criterios y reglas de uso encaminados a la correcta utilización de las herramientas de trabajo y los servicios. Debe incluir la responsabilidad de los usos indebidos y las medidas disciplinarias associades.c) Modelo de relación con la autoridad de control.d) Registro de Actividades de Tratamiento que deberá contener como mínimo los siguientes campos: - Nombre y datos de contacto del DPD, del Responsable del Tratamiento y, en su caso, del corresponsable y del representante del responsable.- Actividades y finalidades de los tractaments.- Descripción de las categorías de datos y los interessats.- categorías de los destinatarios a los que se le han comunicado o comunicarán los datos, incluidos los destinatarios en terceros países u organizaciones internacionales.- Transferencias internacionales de datos.- Cuando sea posible, información associats.g) Definición de los niveles de riesgo de las Actividades de Tratamiento y los criterios para la classificació.h) Metodología de Evaluación de Impacto relativa a la Protección de Datos (AIPD) i) Identificación de las medidas de ciberseguridad asociadas los diferentes niveles de risc.2. La normativa referida en este apartado deberá mantenerse en todo momento actualizada y será revisada siempre que se produzcan cambios rellevants.3. Cualquier incumplimiento o excepción de la normativa deberá ser correctamente documentado. La	aplica	Proveedor Servicio Identificación Remota (Subencargado)

normativa referida en este apartado deberá mantenerse en todo momento actualizada y será revisada siempre que se produzcan cambios rellevants.3. Cualquier incumplimiento o excepción de la normativa deberá ser correctamente documentado. La normativa referida en este apartado deberá mantenerse en todo momento actualizada y será revisada siempre que se produzcan cambios rellevants.3. Cualquier incumplimiento o excepción de la normativa deberá ser correctamente documentado.		
4. Se deberá disponer de la documentación de un sistema de gestión de seguridad de la información aprobada y actualizada.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Se dispondrá, como mínimo, los siguientes documentos que detallen de forma clara y precisa cómo llevar a cabo los tratamientos automatizados: a) Control de acceso lógico (gestión de usuarios). Debe incluir el control de acceso a los datos que tienen limitado el tractament.b) Identificación y autenticació.c) Gestión de suports.d) Copias de seguridad y restauración de dades.e) Control de acceso físic.f) tratamiento de ficheros temporals.g) Eliminación segura de información en la reutilización o destrucción de soportes y sistemes.h) Devolución de actius.i) Registro de accessos.j) Gestión de excepcions.k) Trabajo fuera de los locales del responsable de las Actividades de Tratamiento o encargados de los tractaments.l) Notificación, registro y gestión de incidències.m) Notificación de vulneraciones de seguretat.2. Los documentos referidos en este apartado se	aplica	Proveedor Servicio Identificación Remota (Subencargado)
3. Se dispondrá, como mínimo, los siguientes documentos que detallen de forma clara y precisa cómo llevar a cabo los tratamientos automatizados: a) Pseudonimització.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Se establecerá un proceso formal de autorizaciones que cubra, como mínimo, los siguientes aspectos: a) Uso de dispositivos móviles (ordenadores portátiles, dispositivos móviles inteligentes, tabletas, agendas electrónicas, etc.). b) Uso de soportes (dispositivos ópticos (CD, DVD), discos duros externos, cintas y discos de copias de seguridad, unidades USB o pendrives, tarjetas de memoria (SD, microSD, etc.)). c) Salida de dispositivos móviles y suports.d) Tratamiento fuera de los locales del Responsable del Tratamiento o Encargado del Tractament.e) Acceso remot.f) Ejecución de los procedimientos de recuperación de dades.g) Entrada en producción y mantenimiento de equipos y aplicacions.2. Los documentos referidos en este apartado se deberán mantener en todo momento actualizados y serán revisados siempre que se produzcan cambios relevantes.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
3. Se debe establecer un proceso formal de autorizaciones que cubra, como mínimo, los siguientes aspectos: a) Ejecución del Plan de Continuidad y pruebas periódicas.	aplica	Proveedor Servicio Identificación Remota (Subencargado)

1. Se debe informar al personal de: a) Las funciones, deberes y obligaciones tanto durante el período el cual ejerce el puesto de trabajo como en caso de finalización de la asignación o traslado a otro lugar de treball.b) Los requisitos a cumplir respecto los datos a los que ha tenido acceso, en particular, en términos de confidencialidad, tanto durante el periodo en el que ha sido adscrito como posteriormente a su finalització.c) las medidas disciplinarias en caso de incumplimiento .	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. En coordinación con el DPD, se deben llevar a cabo las acciones necesarias para formar y concienciar regularmente el personal sobre su papel y responsabilidad en materia de protección de datos para que la seguridad de los tratamientos automatizados y no automatizados alcance los niveles exigidos . En particular, con respecto a: a) La normativa, procedimientos y estándares de seguridad relativa al buen uso de los sistemas y los tratamientos en paper.b) La detección y reacción a incidentes de seguridad, actividades o comportamientos sospitosos.c) El procedimiento de notificación de incidentes y vulneraciones de seguretat.d) la gestión de la información en cualquier formato en que se encuentre. Se deben cubrir al menos las siguientes actividades: empleos ordenados, almacenamiento, transferencia, copias, distribución, destrucción y uso de archivos temporales.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Se deben diseñar y configurar los sistemas y redes aplicando la regla de mínima funcionalidad y la seguridad por defecto. 2. El diseño de arquitectura de seguridad debe contemplar las instalaciones, los sistemas, el esquema de líneas de defensa y los sistemas de identificación y autenticación. 3. Se deben configurar de forma segura los equipos, previamente a al su entrada en producción de forma que se apliquen medidas técnicas y organizativas que garanticen, por defecto: a) la limitación del tratamiento de datos por parte de los usuarios de los diferentes sistemas de información de acuerdo con las funciones que el usuario debe desenvolupar.b) la retirada de cuentas y contraseñas para defecte.c) que no se proporcionen funciones innecesarias, ni de operación, ni de administración, ni de auditoría, de manera que se reduzca su perímetro al mínimo imprescindible.d) que no se proporcionen funciones que no sean de interés, ni sean necesarias y, incluso, las que sean inadecuadas al fin que se persegueix.4. Se debe mantener documentación tanto del diseño de arquitectura como de la configuración de los equipos. 5. De manera previa a la entrada en producción se debe realizar un análisis de vulnerabilidades. 6. Se debe pedir autorización relativa a la entrada en producción y mantenimiento de equipos y aplicaciones. De manera previa a la entrada en producción se debe realizar un análisis de vulnerabilidades. 6. Se debe pedir autorización relativa a la entrada en producción y mantenimiento de equipos y aplicaciones. De manera previa a la entrada en producción se debe realizar un análisis de vulnerabilidades. 6. Se debe pedir autorización relativa a la entrada en producción y mantenimiento de equipos y aplicaciones.	aplica	Proveedor Servicio Identificación Remota (Subencargado)

7. Se debe formalizar y documentar el diseño de la arquitectura de seguridad y la configuración de los equips.8. La descripción del diseño y configuración debe contemplar: a) Instalaciones: número, ubicación, áreas existentes y detalle de los puntos de accés.b) Sistemas: inventario de los sistemas de información que, como mínimo, contenga: - Los activos de los sistemas (servidor de correo, robot de backup ...) .- Las redes existentes, así como los elementos de conexión en el exterior (por ejemplo la red local está separada de Internet mediante un cortafuegos). - Los puntos de acceso a los sistemas (puestos de trabajo, consolas de administración, web de la intranet, etc.). C) Esquema de líneas de defensa: - Inventario de los sistemas de seguridad (cortafuegos, DMZ, antivirus, antispam, etc.) .- Elementos de interconexión a otros sistemas o en otras redes. - Elementos de defensa en las conexiones a otras redes (por ejemplo, la conexión con Internet se realiza a través de un cortafuegos) .- Utilización de tecnologías diferentes para prevenir vulnerabilidades que puedan perforar simultáneamente varias líneas de defensa.d) Sistema de identificación y autenticación de usuarios para cada sistema o servicio: - Uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otros de naturaleza anàloga.- Uso de archivos o directorios para autenticar al usuario y determinar sus derechos de acceso. e) Sistema de gestión, relativo a la planificación, la organización y el control de los recursos relativos a la seguridad de la información. 9. El diseño de la arquitectura debe estar aprobada por la unidad competente del CTTI y asesorado por el equipo de especialistas en ciberseguridad del	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. El desarrollo de aplicaciones debe hacerse sobre un sistema diferente y separado del de producción y no debe haber herramientas o datos de desarrollo en el entorno de producció.2. Se aplicará una metodología de desarrollo reconocida que: a) Tome en consideración los aspectos de seguridad en todo el ciclo de vida.b) Utilice algoritmos, software y bibliotecas reconegudes.c) Contemple la generación y el tratamiento de pistas de auditoría que permita registrar las actividades de los usuarios tal y como se especifica en la medida Id 20 "Registro y protección de la actividad de los usuarios" .3. De manera previa a la entrada en producción se realizará: a) Comprobación del funcionamiento correcto del aplicació.b) Análisis de vulnerabilidades.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
4. Se aplicará una metodología de desarrollo reconocida que: a) Permita la inspección del código font.b) Permita comprobar que los datos de entrada de un usuario se corresponden al esperado (validación de datos de entrada, salida y datos intermedias) .5. De manera previa a la entrada en producción se realizará: a) Pruebas de penetració.b) Análisis del código fuente.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Las pruebas se realizarán en un entorno aislado del de producción. 2. Las pruebas anteriores a la entrada en producción o modificación no se deben hacer con datos reales, a menos que se asegure que el entorno en el que se hagan las pruebas tenga implementadas las medidas de ciberseguridad establecidas por el nivel de seguridad del tratamiento de los datos.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Los requisitos de acceso deben atenerse a lo que se indica a continuación: a) Todo sistema de información debe disponer de mecanismos de autenticación para validar la identidad de los usuarios que accedeixen.b) Los recursos del sistema deben protegerse con algún mecanismo que impida su utilización, salvo las entidades, usuarios o personas que disfruten de derechos de acceso suficients.c) Los derechos de acceso de cada recurso han de establecer según las decisiones de la persona responsable del recurso, y se atendrán a la normativa de seguridad del sistema.d) Particularmente, se debe controlar el acceso a los componentes del sistema y sus archivos o registros de configuración .	aplica	Proveedor Servicio Identificación Remota (Subencargado)

2. El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas (o bien dos roles diferenciados para cada una de las funciones que se lleven a cabo) para realizar tareas críticas , y que anule la posibilidad de que un solo individuo autorizado pueda abusar de sus derechos para cometer alguna acción il·lícita.En concreto, se deben separar al menos las siguientes funciones en diferentes roles para evitar que una sola persona pueda llevar a cabo ambas funciones en relación a un sistema: a) Desarrollo de operació.b) Configuración y mantenimiento del sistema de operació.c) Auditoría o supervisión de cualquier otra funció.En especial, se verificará esta separación de roles y funciones en casos deusuarios administradores y se garantizará que ningún administrador ostenta en esta condición dos de las funciones definidas anteriormente.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Antes de proporcionar las credenciales de autenticación a los usuarios, éstos deben haber identificado y registrado de manera fidedigna ante el sistema o ante un proveedor de identidad electrónica reconocido por la Administración. Se prevén varias posibilidades de registro de los usuarios: - Mediante la presentación física del usuario y la verificación de su identidad de acuerdo con la legalidad vigente, ante un funcionario habilitado para ello.- De manera telemática, mediante DNI electrónico o un certificado electrónico qualificat.- de manera telemática, utilizando otros sistemas admitidos legalmente para la identificación de los ciudadanos de los que prevea la normativa aplicable.2. Los mecanismos de autenticación empleados en cada sistema deben adecuarse al nivel del sistema y responder a los mecanismos autorizados en el Reglamento Europeo 910/2014 (eIDAS) y reglamentos de ejecución del mismo, así como el Protocolo de Identificación y Firma Electrónica, aprobado por la Orden GRI / 233/2015, de 20 de julio, y la Política de Identificación y Firma Electrónica del Marco Normativo de Seguridad de la Información de la Generalitat de Catalunya. Los mecanismos pueden utilizar los factores de autenticación siguientes: - "Factores de conocimiento": contraseñas o claves concertadas. Deben disponer de reglas básicas de calidad (extensión, tipo de caracteres, etc.) .- "Factores de posesión": componentes lógicos (tales como certificados de software) o dispositivos físicos (tokens, teléfonos móviles, dispositivos) .- "Factores inherentes o propios del usuario ": elementos biomètrics.3. En el ámbito básico se requerirá como mínimo un factor de autenticación. Los factores anteriores se pueden utilizar de manera aislada o combinarse para generar mecanismos de autenticación fuerte (ver niveles superiores). 4. La identificación de los usuarios del sistema se hará de acuerdo con lo que se indica a continuación: a) Los identificadores de usuario deben cumplir con el MCPD y el Marco Normativo de la Seguridad de la Información de la Generalidad de Catalunya.b) Se pueden utilizar como identificador único los sistemas de identificación que prevea la normativa aplicable.c) Cuando el usuario tenga diferentes roles ante el sistema (por ejemplo como ciudadano, como trabajador interno de el organismo y como administrador de los sistemas), debe recibir identificadores singulares para cada uno de los casos de manera que siempre queden delimitados privilegios y registros de activitat.d) Cada entidad (usuario o proceso) que accede al sistema debe disponer de un identificador único de forma que: - Se puede saber quién recibe y qué derechos de acceso rep.- Se puede saber quién ha hecho algo y que ha fet.5. Las credenciales se gestionar de la manera siguiente: a) Se deben activar una vez estén bajo el control efectivo del usuari.b) Deben estar bajo el control exclusivo del usuari.c) El el usuario debe reconocer que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pèrdua.d) Deben ser inhabilitados en los casos siguientes: cuando el usuario deja la organización por cualquier causa; cuando el usuario cesa en la función para la que se requería la cuenta de usuario; o cuando la persona que lo autorizó da orden en sentido contrario. En definitiva, cuando se termina la	aplica	Proveedor Servicio Identificación Remota (Subencargado)

relación con el sistema.e) Se retener durante el periodo necesario para atender las necesidades de trazabilidad de los registros de actividad asociados. A este periodo se le denomina período de retenció.f) deben revisar periódicamente los identificadores y verificar si es necesario que accedan a los sistemas de informació.g) En el caso de que sean contraseñas deben ser configurados según estándar de contraseñas del Marco Normativo de Seguridad de la Información de la Generalitat de Catalunya. Concretamente, en lo referente a la complejidad, longitud, caducidad, limitación del número de intentos fallidos, reutilización y almacenamiento. En caso de utilizar OTPs éstos no tendrán una duración superior a 24 horas.		
6. Se exige el uso de al menos dos factores de autenticación de diferente tipología. En el caso de utilización de factores de conocimiento, se debe dar cumplimiento a las exigencias de calidad y renovación establecidas en el Marco Normativo de Seguridad de la Información de la Generalitat de Catalunya, atendiendo a la tipología de perfil a la que corresponde la credencial .7. Las credenciales utilizadas deben haberse obtenido tras una registro previo: a) Mediante la presentación física del usuario y la verificación de su identidad de acuerdo con la legalidad vigente, ante un funcionario habilitado para ello. b) de manera telemática, mediante la utilización de un certificado electrónico qualificat.c) de manera telemática, mediante la utilización de un certificado electrónico cualificado en un dispositivo de creación de firma.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. La asignación y el uso de los privilegios de acceso debe estar restringida y controlada. La asignación de derechos de acceso privilegiados debe estar recogida en un proceso formal de autorización, de acuerdo con la normativa de control de acceso aplicable. Sólo el personal autorizado puede conceder, alterar o anular la autorización de acceso a los recursos, de conformidad con los criterios establecidos por su propietari.2. Los derechos de acceso de cada usuario se limitarán atendiendo a los principios siguientes: a) Mínimo privilegio. Los privilegios de cada usuario se deben reducir al mínimo estrictamente necesario para cumplir sus obligacions.b) Necesidad de conocer. Los privilegios deben limitarse de forma que los usuarios sólo accedan al conocimiento de aquella información requerida para cumplir sus obligacions.3. El b) Se autorizará la asignación de privilegios y se registrarán todos los privilegios asignados. Los derechos de acceso no se harán efectivos hasta que se complete el proceso de autorització.c) Deben definirse los requisitos para el vencimiento de los derechos de acceso privilegiats.d) Los derechos de acceso deben 'asignarse a un identificador de usuari.e) deben revisar periódicamente los permisos asignados a los usuarios y, verificar que se corresponden a sus funcions.f) en caso de que sea recomendable por criterios de eficiencia y no genere riesgos de seguridad, la asignación de permisos de usuario se podrá realizar en base a la definición y parametrización de roles, de acuerdo con lo establecido en el Marco Normativo de seguridad de la Información de la Generalitat de Catalunya.g) han de	aplica	Proveedor Servicio Identificación Remota (Subencargado)

Se considera acceso local al realizado desde puestos de trabajo dentro de las mismas instalaciones de la organización y desde los recursos propios ubicados en dichas instalaciones. Se considera acceso remoto al realizado desde fuera de las mismas instalaciones de la organización, a través de redes o recursos de terceros que no estén puestos a disposición específicamente como recursos locales o propios de la Generalidad de Catalunya.1. Se debe garantizar la seguridad del sistema cuando accedan remotamente usuarios u otras entidades, lo que implica proteger tanto el acceso en sí mismo como el canal de acceso remoto. La concepción de acceso remoto se deberá aplicar a las formas establecidas de Teletrabajo en el Marco Normativo de Seguridad de la Información de la Generalitat de Catalunya.2. Los accesos deberán cumplir con las siguientes medidas según el nivel de los tratamientos: a) Se prevendrán ataques que puedan revelar información del sistema sin llegar a acceder. La información revelada a quien intenta acceder debe ser la mínima imprescindible (los diálogos de acceso sólo deben proporcionar la información indispensable) .b) El sistema informará al usuario de sus obligaciones, si fueran específicas, inmediatamente después de obtener el acceso. Esta información en relación con las obligaciones generales aplicables a los sistemas de la Generalidad se mostrará la primera vez que el usuario acceda al sistema.c) Pasado un cierto tiempo de inactividad en la sesión del usuario, ya sea con el sistema o con una aplicación en particular, se cancelarán las sesiones abiertas desde dicho lugar de trabajo.3. Se aplicarán a las conexiones en remoto las medidas de seguridad establecidas para el acceso local, siempre y cuando resulten adecuadas. En caso contrario se definirán medidas equivalentes para alcanzar un nivel de seguridad comparable.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
4. Se informará al usuario del último acceso efectuado con su identitat.5. Se debe establecer una política específica de lo que se puede hacer remotamente, para lo cual se requiere autorización positiva.6. Cuando un equipo se conecte remotamente a través de redes que no están bajo el control estricto de la organización, el ámbito de operación del servidor debe limitar la información y los servicios accesibles a los mínimos imprescindibles y, se requerirá una autorización previa de los responsables de los tratamientos de datos afectados. Este punto es aplicable a conexiones a través de Internet y otras redes que no sean de confianza.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Se suscribir, si son de aplicación los escenarios descritos, los siguientes contratos u otros actos jurídicos con los siguientes actores: a) Encargados del Tratamiento. Estos deben establecer de forma clara y concisa, como mínimo: - Objeto.- Duración. - Naturaleza y finalidad del tratamiento (características del servicio prestado) .- Tipo de datos personales.- Categoría de los interessats.- Obligaciones, responsabilidades y derechos del Responsable.- Obligaciones, responsabilidades y derechos del Encargado según el clausulado del artículo 28.3 RGPD.- Medidas técnicas y organizativas que ofrezcan unas garantías suficientes de acuerdo con el nivel de riesgo de las datos.- Niveles de servicio (tiempo de respuesta en caso de violaciones de seguridad, resolución de incumplimientos, etc.) .- consecuencias del incumplimiento.- Devolución o destrucción de los datos a la finalización de la encàrrec.b) Prestadores de servicios sin acceso a datos. Estos deben establecer de forma clara y concisa, como mínimo: - Naturaleza y finalidad del servicio.- Prohibición de acceder a los datos personales. - Obligación de deber de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación de servicio.- Consecuencias del incompliment.2. Los Encargados del Tratamiento suscribirán contratos u otros actos jurídicos con los subencarregats que utilicen para llevar a cabo determinadas actividades de tratamiento. Estos deberán establecer, como mínimo, las mismas obligaciones de protección que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado. Las subcontrataciones deben estar autorizadas por el Responsable del	aplica	Proveedor Servicio Identificación Remota (Subencargado)

Tractament.3. El Responsable del tratamiento debe identificar las actividades de los tratamientos y sistemas de información tratados por cuenta de terceros con referencia expresa al encargado, al contrato o documento que regule las condiciones y la vigencia de la encàrrec.4. Si se actúa como Encargado del Tratamiento se debe identificar y registrar las actividades de tratamiento y sistemas de información que trata por cuenta de terceros, en su caso, con referencia expresa al Responsable del tratamiento, al contrato o documento que regule las condiciones y la vigencia de la encàrrec.5. En caso de disponer de encargados de tratamiento el Responsable deberá establecer un sistema de garantías para acreditar la calidad y adecuación profesional del encargado de tratamiento. Este deberá introducir en los modelos de acreditación de la solvencia técnica en los procedimientos de contratación y se podrá basar en el		
6. Los contratos o actos jurídicos deberán prever la auditabilidad de los sistemas de información para verificar el nivel de cumplimiento de las medidas de ciberseguretat.7. Los contratos deberán prever la revisión de las condiciones de tratamiento. 8. Establecimiento de un sistema rutinario para medir el cumplimiento de las obligaciones de servicio que incluya un procedimiento para neutralizar cualquier desviación respecto al contrato.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Se debe desarrollar un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Este plan debe contemplar los siguientes aspectos: a) Se identificarán funciones, responsabilidades y actividades a realitzar.b) Tiene que haber una previsión de los medios alternativos que se conjugarán para poder seguir prestando serveis.c) Todos los medios alternativos deben estar planificados y materializados en acuerdos o contratos con los proveedores corresponents.d) los servicios y medios alternativos de comunicación deben: - Tener las mismas garantías de seguridad que los habituals.- Garantizar tiempo máximo de entrada en funcionamiento según los plazos determinados en el análisis de impacto y / o acordados en el Plan de Continuidad. e) Las personas afectadas por el plan deben recibir formación específica relativa a su papel en dicho pla.f) El plan de continuidad debe ser parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad .2. La ejecución del Plan de Continuidad, así como cualquier procedimiento de recuperación dentro del mismo, deberá ser previamente autorizado por la Generalidad de Catalunya.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Se realizarán pruebas periódicas para localizar y corregir, en su caso, los errores o deficiencias que pueda haber en el plan de continuïtat.2. La ejecución del plan de pruebas deberá ser previamente aprobado por la Generalidad de Catalunya.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Los locales donde se ubiquen los sistemas de información y sus componentes deben disponer de elementos adecuados para el funcionamiento eficaz del equipamiento instalado allí. Y, especialmente: a) Condiciones de temperatura y humitat.b) Energía eléctrica, y sus presas correspondientes, necesaria para funcionar, de forma que se garantice el suministro de potencia eléctrica y el funcionamiento correcto de las luces de emergència.c) protección contra las amenazas identificadas en el análisis de riscos.d) protección del cableado contra incidentes fortuitos o deliberats.2. Se debe garantizar el suministro eléctrico a los sistemas en caso de fallo del suministro general y garantizar el tiempo suficiente para que finalicen ordenadamente los procesos, salvaguardando la información.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
El equipamiento se instalará en áreas específicas para su función (áreas de CPDs o salas técnicas, edificios o ubicaciones donde se encuentre ubicado este equipamiento). Se deben controlar los accesos a las áreas indicadas de forma que sólo se pueda acceder las entradas previstas y vigilades.1. Deben quedar registradas la entrada y salida de las personas en las áreas separadas y concretamente la identificación de la persona, la fecha y hora de entrada y	aplica	Proveedor Servicio Identificación Remota (Subencargado)

sortida.2. El registro de accesos debe estar controlado por una persona autorizada.		
Se debe garantizar que el equipamiento y los soportes están bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro. A tal efecto: 1. Se debe llevar un registro detallado de cualquier entrada y salida de equipamiento y soportes de los CPDs, salas técnicas, edificios o ubicaciones donde se encuentren estos equipamientos o soportes, incluyendo la identificación de la persona que autoriza el movimiento. El registro debe reflejar: fecha y hora, identificación inequívoca del equipamiento, persona que realiza la entrada o salida, persona que autoriza la entrada o salida y persona que realiza el registre.2. Se elaborará una lista de servicios autorizados de transporte o mensajería a emprar.3.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
4. El procedimiento previsto en nivel básico que compare semestralmente las salidas con las llegadas debe ser rutinario, formal y que dispare las alarmas pertinentes cuando se detecte algún incidente.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Se registrarán las actividades de los usuarios en el sistema, de forma que: a) El registro debe indicar quien hace la actividad, cuando la hace y sobre qué información y las actividades efectuadas con éxito y los intentos fallidos .b) se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores cuando puedan acceder a la configuración y actuar en el mantenimiento del sistema.c) la determinación de qué actividades se deben registrar y con qué niveles de detalle se deben adoptar en vista del análisis de riesgos hecha sobre el sistema y las capacidades del mateix.2. Se deben activar los registros de actividad en los servidors.3. El período de conservación de la información se regirá por la normativa de gestión de trazas del Marco Normativo de Seguridad de la Información de la Generalidad de Catalunya (18 meses). 4.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
5. Se deben revisar informalmente los registros de actividad para buscar patrones anormales. A tal efecto, se podrá disponer de herramientas específicas automáticas destinadas al análisis de estos patrones para determinar potenciales incumplimientos. En caso de detectarse podrán analizarse en detalle los datos que han generado la detección de estos patrones atendiendo a la amenaza y al nivel de riesgo. Estas herramientas podrán ser transversales y / o operadas por organismos específicos dedicados a la ciberseguridad.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
6. Se debe revisar formalmente y se debe disponer de un sistema automático de recolección de registros y correlación de eventos. Los acontecimientos se recogerán en este sistema automático, de acuerdo con el modelo TIC de la Generalidad de Catalunya. Este sistema podrá ser transversal y / o operado por organismos competentes en materia de ciberseguridad, como el CESICAT.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Se establecerá un registro de incidentes en los que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que hace la notificación, a quien se le comunica, los efectos derivados y las medidas correctoras aplicadas. Además, deberán registrarse las restauraciones de copias de seguridad, indicando la persona que realiza el proceso, los datos restaurados y los datos que se hayan tenido que grabar manualmente en el proceso de recuperación.	aplica	Proveedor Servicio Identificación Remota (Subencargado)

2. Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que: a) Se registrarán el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incident.b) se registrará la evidencia que pueda sostener, posteriormente, una actuación legal (administrativa o judicial), o hacerle frente, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos oa la persecución de delitos. En la determinación de la composición, detalle y gestión de estas evidencias, se debe recurrir a asesoramiento legal especialitzat.c) Como consecuencia del análisis de los incidentes, se debe revisar la determinación de los esdeveniments.3. Se debe asegurar que se disponga de la información necesaria para hacer la notificación de información en los términos previstos en el Reglamento General de Protección de Datos. Es decir, se deberá poder facilitar la siguiente información referente a las vulneraciones de seguridad de los datos personales: a) Descripción de la naturaleza de la vulneración de la seguridad de los datos personales, incluyendo, si es posible, las categorías y el número aproximado de interesados afectados y las categorías y el número aproximado de registros de datos personales afectats.b) Descripción de las posibles consecuencias de la vulneración de la seguridad de los datos personals.c) Descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para hacer frente a la vulneración de la seguridad de los datos personales, incluidas, en su caso, las medidas adoptadas para mitigar sus posibles efectos negativos.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Se deben mantener inventarios actualizados de todos los elementos del sistema (información, software, hardware, servicios, terceros, personas, instalaciones, soportes de información), detallando como mínimo: a) El responsable. b) Tipo de activo (servidor, ordenador, router, etc.). c) Identificador, fabricante y model.d) Ubicació.2. Los inventarios se actualizarán en función de los plazos establecidos en la normativa.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Los ficheros temporales que se hubieran creado exclusivamente para la realización de trabajos temporales auxiliares deberán cumplir con las medidas establecidas que se apliquen a los ficheros considerados definitius.2. Todo fichero temporal así creado será borrado una vez haya dejado de ser necesario para la finalidad que motivó su creación.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad y debe requerir una nueva autenticación del usuario para reanudar la actividad en curs.2. Los equipos deben disponer de protección antivirus y antimalware.3. Los equipos que sean susceptibles de salir de las instalaciones de la organización y no se puedan beneficiar de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, se deben proteger adecuadamente. Sin perjuicio de las medidas generales que les afecten, se debe evitar, en la medida de lo posible, que el equipo contenga claves de acceso remoto a la organización. Se consideran claves de acceso remoto las que sean capaces de habilitar un acceso a otros equipos de la organización, u otros de naturaleza análoga.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
En relación con los equipos que sean susceptibles de salir de las instalaciones de la organización: 4. Se debe dotar al dispositivo de detectores de vulneraciones que permitan saber si el equipo ha sido manipulado y activen los procedimientos previstos de gestión del incident.5. Los datos de los tratamientos de nivel alto almacenadas deben protegerse mediante xifratge.6. Se establecerán medidas de protección en lugares públicos como filtros de confidencialidad o candado de seguridad.	aplica	Proveedor Servicio Identificación Remota (Subencargado)

Se aplicarán las medidas preventivas y correctivas necesarias para mantener el equipamiento físico y lógico asegurando la confidencialidad, integridad y disponibilidad continua de los equipos y sistemas. De acuerdo con ello, se dispondrá de: 1. Las especificaciones de los fabricantes en cuanto a la instalación y mantenimiento de los sistemes.2. Un seguimiento continuo de los anuncios de defectos, utilizando mecanismos, como por ejemplo, la suscripción de correo de avisos de defectos por parte del fabricant.3. Un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Los soportes de información se identificarán mediante etiquetado o mecanismo equivalente de forma que, sin revelar su contenido, indique el nivel de seguridad de la información contenida de más qualificació.2. Las etiquetas o mecanismos equivalentes deberían ser fácilmente identificables. Se informará a los usuarios sobre estos mecanismos de identificación para que, o bien mediante simple inspección, o bien mediante el recurso a un repositorio, puedan entender el significado. 3. Se podrá excluir, por previsión a la normativa, la obligación de etiquetado en caso de soportes en que no se pudiera cumplir por sus características físicas, estableciendo medidas alternativas para asegurar su identificación y localització.4.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
5. Se deben destruir de manera segura los soportes de información, en los siguientes casos: a) Cuando la naturaleza del soporte no permita un borrado segur.b) Cuando así lo requiera el procedimiento asociado al tipo de información contenida. 6. Se aplicarán mecanismos de cifrado que garanticen la confidencialidad y la integridad de la información contenida en todos los soportes.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
El personal interno o externo deberá devolver todos los activos de la organización que estén en su poder al finalizar la relación laboral, el contrato o acuerdo.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Se exigirá que los puestos de trabajo permanezcan despejados, sin más material sobre la mesa que el requerido para la actividad que se realiza en cada momento.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
2. El material debe guardarse en un lugar cerrado cuando no se utilice. Se deberá disponer de lugares cerrados a disposición de los usuarios.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
Una vez finalice el tratamiento de datos y cuando el Responsable del tratamiento haya establecido que los datos personales deben conservarse por los motivos establecidos en el RGPD oa la legislación aplicable, que impliquen una limitación de uso de las mismas, se deberán adoptar medidas técnicas para proteger los datos de acuerdo con este nuevo estado, como las siguientes: 1. Control de accés.2. Ubicación de los datos en un sistema diferent.3. Cifrado.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidentalmente o intencionadamente con una antigüedad determinada. En particular, se debe considerar la conveniencia o necesidad, según corresponda, que las copias de seguridad estén xifrades.2. Estas copias deben tener el mismo nivel de seguridad que los datos originales. 3. Las copias de seguridad deben incluir: a) Información de trabajo de la organización que se refiera a datos personals.b) Aplicaciones en explotación, incluyendo los sistemas operativos mediante las que se traten datos personals.c) Claves utilizadas para preservar la confidencialidad de las dades.4. Semestralmente se verificará la correcta definición, funcionamiento y aplicación de los procedimientos de realización de las copias y de los procedimientos de recuperació.5.	aplica	Proveedor Servicio Identificación Remota (Subencargado)

6. Las copias de seguridad y los procedimientos de recuperación deben estar almacenados en una ubicación distinta de aquella en la que se encuentren los equipos que tratan los datos.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. En caso de transmisión de datos tanto a nivel interno de la organización como cuando sea a entidades externas a la misma o en situaciones y contextos de tratamiento que se consideren sensibles, se utilizarán técnicas de pseudonimització u otras medidas análogas, como el cifrado. 2. Las técnicas de pseudonimització deben incluir como mínimo: a) Que los atributos estén ligados a alias aleatorios y que no sean suficientes para identificar el interesado a quien se refereixen.b) La asignación de alias es tal que no se puede revertir sin esfuerzos desproporcionados de las partes interesadas.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
La información se cifrar tanto durante el almacenamiento como durante la transmisión. Sólo puede estar en claro mientras se esté haciendo.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Se debe disponer de medidas físicas o lógicas, o ambas, que obstaculicen la apertura de los dispositivos de almacenamiento que contengan datos de carácter personal. Si no es posible adoptar esta medida el responsable del tratamiento deberá adoptar medidas que impidan el acceso de personas no autorizadas. 2. Si, por encontrarse en proceso de tramitación o revisión, la documentación no se encuentra archivada en los dispositivos de almacenamiento adecuados, la persona que se encuentre al cargo de la misma deberá custodiar la documentación impidiendo el acceso a cualquier persona no autoritzada.3. Se exigirá que los puestos de trabajo permanezcan despejados, sin más documentación sobre la mesa que la requerida para la actividad que se realiza en cada moment.4. Se debe destruir cualquier documento que contenga datos de carácter personal que sea rebutjat.5. La destrucción se llevará a cabo mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en los mismos o su recuperación posterior para eliminar el riesgo de acceso indebido.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Deben destruir las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
2. Se debe limitar únicamente al personal autorizado por el responsable del tratamiento la generación de copias o la reproducción de documentos.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Cuando el tratamiento de datos se realice fuera de los locales del responsable o del encargado del tratamiento el responsable del tratamiento lo deberá autorizar prèviament.2. Se debe llevar un registro detallado de cualquier entrada y salida de documentación. El registro debe reflejar: fecha y hora, identificación de la documentación, el número de documentos, el tipo de información que contienen, persona que realiza la entrada o salida, la forma de envío, la persona que autoriza la entrada o salida y la persona que realiza el registro.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
3. Se deben adoptar medidas dirigidas a impedir el acceso a la información objeto del traslado o su manipulación.	aplica	Proveedor Servicio Identificación Remota (Subencargado)

1. Se debe garantizar la correcta conservación de los documentos, la localización y consulta de la información de conformidad con los criterios previstos en la legislación vigente sobre archivística. Estos criterios han posibilitar el ejercicio de los derechos previstos en la normativa de protección de datos. En aquellos casos en los que no exista normativa aplicable, el responsable del tratamiento deberá establecer los criterios y procedimientos de actuación que deberán seguirse en materia de archivo.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Se establecerá un registro de incidentes en los que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que hace la notificación, a quien se le comunica, los efectos derivados y las medidas correctoras aplicadas.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
2. Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que: a) Se registrarán el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incident.b) se registrará la evidencia que pueda sostener, posteriormente, una actuación legal (administrativa o judicial), o hacerle frente, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos oa la persecución de delitos. En la determinación de la composición, detalle y gestión de estas evidencias, se debe recurrir a asesoramiento legal especialitzat.c) Como consecuencia del análisis de los incidentes, se debe revisar la determinación de los esdeveniments.3. Se debe asegurar que se disponga de la información necesaria para hacer la notificación de información en los términos previstos en el Reglamento General de Protección de Datos. Es decir, se deberá poder facilitar la siguiente información referente a las vulneraciones de seguridad de los datos personales: a) Descripción de la naturaleza de la vulneración de la seguridad de los datos personales, incluyendo, si es posible, las categorías y el número aproximado de interesados afectados y las categorías y el número aproximado de registros de datos personales afectats.b) Descripción de las posibles consecuencias de la vulneración de la seguridad de los datos personals.c) Descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para hacer frente a la vulneración de la seguridad de los datos personales, incluidas, en su caso, las medidas adoptadas para mitigar sus posibles efectos negativos.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
1. Se dispondrá de los siguientes procedimientos por los tratamientos no automatizados: a) Trabajo fuera de los locales del responsable de las actividades de los tratamientos o encargados de los tratamientos .b) Notificación, registro y gestión de incidències.c) Control de acceso .d) Criterios de arxiu.e) Dispositivos de emmagatzematge.f) Custòdia.g) Copia o reproducció.h) Trasllat.i) Destrucción papel.	aplica	Proveedor Servicio Identificación Remota (Subencargado)
j) Registro acceso.	aplica	Proveedor Servicio Identificación Remota (Subencargado)