CONSORCI AOC

Administració Oberta de Catalunya

Administració
Oberta de
Catalunya

Plec de prescripcions tècniques particulars per la prestació del Servei d'Identificació Remota

AOC-2026-7

Generalitat de Catalunya

Localret

CONSORCI AOC

Administració Oberta de Catalunya

Control documental

Estat formal	
Elaborat per	
Aprovat per	
Data de creació	04/10/2012
Nivell accés informació	Pública
Títol	Plec de prescripcions tècniques particulars per la prestació del Servei d'Identificació Remota
Fitxer	2026 Contracte Servei Video-identificació– Plec Tècnic.docx
Control de còpies	Només les còpies disponibles a la Seu electrònica del Consorci AOC garanteixen l'actualització dels documents. Tota còpia impresa o desada en ubicacions diferents es consideraran còpies no controlades.
Drets d'autor	Aquesta obra està subjecta a una llicència Reconeixement - No comercial- Sense obres derivades 3.0 Espanya de Creative Commons. Per veure'n una còpia, visiteu http://creativecommons.org/licenses/by-nc-sa/3.0/deed.ca o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.

Control de versions

Data:	24/10/2025
Descripció:	Versió final

Administració Oberta de Catalunya

Índex

Administració Oberta de Catalunya

1 Objecte del contracte

1.1 Introducció

La identitat digital ha emergit amb força els darrers anys, degut al desenvolupament de l'economia digital, dels serveis de l'administració electrònica i de la seva utilització de forma quotidiana per la gran majoria de la ciutadania. Actualment, més del 80% dels ciutadans de Catalunya són internautes habituals que accedeixen periòdicament a Internet i a serveis en línia. I la majoria d'interaccions entre els ciutadans, les empreses i les Administracions requereixen de disposar d'una identitat digital. Els governs i els negocis enfronten la necessitat d'identificar a les persones amb suficients garanties, de forma fiable i correcta, per a realitzar les transaccions de processos de negoci amb seguretat.

En desenvolupament del pacte institucional signat el 23 de juliol del 2001 pels grups parlamentaris del Parlament de Catalunya, la Generalitat de Catalunya i el Consorci d'Ens Locals de Catalunya (Localret), es va decidir establir sistemes d'interrelació entre les esmentades administracions, i entre les administracions i els ciutadans, per via telemàtica i electrònica, en les condicions de seguretat necessàries i, especialment, fent ús de certificats digitals d'identitat i signatura electrònica.

L'Agència Catalana de Certificació (CATCert) es va crear per acord de la Comissió Executiva del Consorci de l'Administració Oberta Electrònica de Catalunya (AOC), de 29 d'abril de 2002, com a organisme autònom de caràcter comercial, els estatuts de la qual van ser publicats al Diari Oficial de la Generalitat de Catalunya el 30 de maig de 2003, per Resolució PRE/1574/2003, de 15 de maig.

D'aquesta forma, CATCert es va constituir en l'entitat principal del sistema públic català de certificació que regula l'emissió i la gestió dels certificats que s'emetin per a les entitats que integren el sector públic català; així com l'admissió i l'ús dels certificats emesos a ciutadans i empreses per a altres prestadors de serveis de certificació qualificats.

D'acord a la Llei 29/2010, del 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya, CATCert té la competència de prestar serveis de signatura electrònica al sector públic de Catalunya per a garantir la confidencialitat, la integritat, la identitat i el no-rebuig en les comunicacions electròniques que duen a terme les entitats del sector públic de Catalunya, i qualsevol altra tasca que se li encomani. Posteriorment aquestes funcions van ser assumides pel Consorci AOC directament, en virtut de l'absorció del CATCert.

En compliment d'aquestes funcions, el Consorci AOC es va establir l'any 2016 com a Prestador Qualificat de Serveis de Confiança, amb acord al que estableixen el Reglament (UE) 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014 relatiu a la identificació electrònica i els serveis de confiança (en endavant RelDAS) i la Llei 6/2020, de 11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança. Com a tal és que emet els certificats electrònics qualificats idCAT per a la ciutadania, els certificats TCAT per al personal al servei de les Administracions Públiques Catalanes i segells electrònics pel seu ús en l'àmbit de l'actuació administrativa automatitzada.

Val a dir que la Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis de confiança, al seu article 7, obre la porta a acceptar mecanismes de verificació de la identitat a distància com a alternativa als ja especificats a l'article 24 punt 1 del ReIDAS. L'Ordre ETD/465/2021, de 6 de maig, que regula els mètodes de identificació remota per vídeo per l'expedició de certificats electrònics qualificats, per la seva banda, és la que defineix els requisits que han de complir aquests mecanismes i els prestadors de serveis de confiança per poder-los acceptar.

Addicionalment, més enllà de la seva funció com a prestador de serveis de confiança qualificat, el Consorci AOC ofereix el servei d'identitat digital per a la ciutadania idCAT Mòbil, que permet a la ciutadania identificar-se davant les Administracions Públiques Catalanes per Internet de forma fàcil i usable.

1.2 Situació actual

Per poder realitzar tràmits administratius per mitjans electrònics o accedir a serveis públics digitals, es requereix disposar de sistemes d'identificació i signatura electrònica que acreditin la identitat i la voluntat d'actuació. D'acord al que estableix la normativa tècnica i jurídica que regula l'ús d'aquests tipus de mecanismes en l'àmbit de les administracions públiques, és necessari un registre previ a l'emissió de les credencials que els possibiliten, que aporti garantia total sobre la identitat de les persones que els utilitzen, i que hauria de ser presencial.

Arran de la greu situació de la crisis sanitària provocada pel coronavirus SARS-Cov-2, es va posar de manifest l'extraordinària importància del canal electrònic per relacionar-se amb l'Administració, que durant alguns mesos va ser l'únic mitjà de tramitació possible. En el cas del registre per a l'obtenció de certificats electrònics i credencials d'identitat digital, les administracions van haver d'adoptar mesures tècniques i legislatives per adoptar mecanismes remots basats en vídeo amb nivells de seguretat i fiabilitat equivalents als que dona la presencialitat. És en aquest sentit que la Llei 6/2020 i l'Ordre ETD/465/2021 obren la porta a fer-ho per a l'emissió de certificats qualificats.

Aplicant les mesures establertes per aquestes normes, el Consorci AOC va habilitar la possibilitat de dur a terme el registre per a l'obtenció de idCAT Mòbil i del certificat electrònic qualificat de signatura avançada idCAT mitjançant un procés de video-identificació, supervisat per operadors amb la pertinent formació per fer-ho, complint sempre amb la normativa aplicable.

1.3 Objecte

L'objecte del present plec és el **subministrament dels serveis necessaris per realitzarla verificació d'identitat per video-identificació,** per a l'obtenció del certificat electrònic qualificat idCAT i del sistema d'identificació electrònica idCAT Mòbil.

2 Requisits

2.1 Requisits generals

Amb caràcter general, els serveis objecte de la present licitació hauran de permetre al Consorci Administració Oberta de Catalunya poder portar a terme processos de verificació de la identitat per video-identificació com a mecanisme de registre per a l'obtenció de credencials d'identitat digital i signatura electrònica.

És, per tant, objecte de la present licitació la contractació d'un servei d'identificació remota en modalitat de programari com a servei (SaaS), mitjançant el procediment de video-identificació o videoconferència, que haurà de complir amb la normativa vigent, tècnica i jurídica, en matèria d'identificació i signatura electrònica, així com els serveis professionals de suport i consultoria associats al propi servei d'identificació remota.

Concretament es vol contractar un servei de identificació remota que permeti la verificació de la identitat a distància, en compliment amb el que estableix l'article 7 punt 2 de la Llei 6/2020, i que, per tant, disposi de les funcionalitats per complir amb els requisits establerts per l'Ordre ETD/465/2021, de 6 de maig, reguladora dels mètodes d'identificació remota per vídeo per a l'expedició de certificats electrònics qualificats.

Els serveis d'identificació remota s'utilitzaran, principalment, per facilitar el registre als serveis d'identificació digital del Consorci AOC , i per a l'obtenció de certificats electrònics qualificats per part de la ciutadania, tot i que es podrà estendre el seu ús a altres casos que siguin d'interès per a les administracions catalanes.

2.2 idCAT Mòbil i idCAT Certificat

Els serveis de verificació de la identitat per vídeo objecte de la present licitació s'aplicaranen la fase de registre dels següents serveis que el Consorci AOC ofereix a la ciutadania :

- **idCAT Certificat.** És un certificat qualificat de signatura avançada d'acord amb el reglament eIdAS. És, per tant, un certificat en programari que els ciutadans poden obtenir adreçant-se, presencialment, a qualsevol dels ens que s'han establert com a entitat de registre del servei.
- **idCAT Mòbil.** És un mecanisme d'autenticació de dos factors basat en l'enviament de paraules de pas d'un sol ús per SMS al dispositiu mòbil del ciutadà. Per ser-ne usuari, cal que el ciutadà s'enregistri a la Base de Dades de la Seu Electrònica de la Generalitat de Catalunya. Aquest registre es pot portar a terme:
  - Presencialment, tant des de les entitats de registre del Consorci AOC com des de les OAC de la Generalitat de Catalunya.
  - Telemàticament:
    - emprant un certificat qualificat,
    - per video-identificació, o

- introduint dues dades conegudes i que el Consorci AOC pot verificar, com són la data de caducitat del DNI i el número TIS de targeta sanitària.

2.3 Normativa aplicable

Per impulsar aquesta iniciativa s'ha tingut en compte normativa dels següents àmbits:

- Normativa estatal del sector públic d'administració electrònica
- Normativa europea de l'àmbit de la identificació i de la protecció de dades
- Normativa internacional de l'àmbit de la identificació
- Normativa catalana

El marc normatiu que s'ha tingut en compte per impulsar aquest projecte és el següent:

- Reglament UE Nº 910/2014 del Parlament Europeu i el Consell, del 23 de juliol, relatiu a la identificació electrònica i els serveis de confiança per les transaccions electròniques en el mercat interior, modificat pel Reglament (UE) 2024/1183 del Parlament Europeu i del Consell, d'11 d'abril de 2024.
- Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança, en especial pel que fa al seu article 7 sobre la comprovació de la identitat i altres circumstàncies dels sol·licitants d'un certificat qualificat.
- Ordre ETD/465/2021, de 6 de maig, que regula els mètodes de identificació remota per vídeo per l'expedició de certificats electrònics qualificats.
- Especificació tècnica ETSI TS 119 461 - *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects*, pels que fa als mecanismes de verificació de la identitat remots.
- Reglament (UE) 2016/679 del Parlament Europeu i el Consell, del 27 d'abril, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades.
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.
- Reglament (UE) 2024/1689 del Parlament Europeu i del Consell, de 13 de juny de 2024, pel qual s'estableixen normes harmonitzades en matèria d'intel·ligència artificial.
- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques
- Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.
- Llei 16/2015, del 21 de juliol, de simplificació de l'activitat administrativa de l'Administració de la Generalitat i dels governs locals de Catalunya i d'impuls de l'activitat econòmica

Administració Oberta
de Catalunya

- ORDRE PRE/226/2016, de 29 d'agost, per la qual es regulen els aspectes tècnics i organitzatius del procés de registre previ en el fitxer Seu electrònica de l'Administració de la Generalitat de Catalunya necessari per als sistemes d'identificació i signatura basats en claus concertades

2.4 Requisits

Requisits funcionals i tècnics
1. Servei al núvol allotjat al centre de processament de dades de l'empresa licitadora, fàcilment integrable per aplicacions externes mitjançant serveis web o APIs.
2. Els sistemes d'informació associats a aquest servei i la localització de les dades ha de complir la normativa vigent, especialment pel que fa la protecció de dades personals en relació al marc legal europeu i estatal.
3. L'aplicació ha de ser web responsiva i/o disposar d'una APP de mòbil, disponible en els principals sistemes operatius.
4. Ha de permetre l'escaneig dels documents d'identificació oficials amb mecanismes de control de la veracitat del document i minimització dels riscos de suplantació manipulació, i amb l'extracció de la fotografia de l'usuari.
5. Ha de permetre l'escaneig dels documents oficials de l'estat espanyol (DNI, TIE i passaport) i del carnet de conduir.
6. Ha d'acceptar els documents d'identitat digital (document d'identitat, passaport i carnet de conduir) dels principals països a nivell europeu i mundial. Caldrà detallar-los.
7. Ha de disposar dels controls de veracitat del document emprats (MZ, marques d'aigua, holograma, etc) i els mecanismes de control de no manipulació que s'apliquen. Caldrà detallar-los.
8. Realitzarà un procés de captura d'una fotografia "selfie" de l'usuari activat per una prova de vida de l'usuari (gest de la cara: tancar ulls, girar el cap, somriure, moviment, etc) i amb un detector de la qualitat de la foto realitzada.
9. En cas d'un "selfie" de qualitat baixa o foto desenfocada, es proposarà fer una nova foto.
10. Farà una correlació de la foto extreta del document oficial d'identitat i del "selfie". S'haurà d'especificar l'algorisme de reconeixement facial utilitzat.
11. L'algorisme facial donarà un "scoring" del grau de similitud. Tot i que un operador farà la validació final.
12. La implantació de l'algorisme de reconeixement facial només s'aplicarà si es considera imprescindible amb acord al que estableix l'Ordre ETD/465/2021, de 6 de maig, que regula els mètodes de identificació remota per vídeo per l'expedició de certificats electrònics qualificats..

13. El sistema ha de permetre els sistema ha de permetre el procés de registre tant per Videoconferència (procés en línia) com per video-identificacióamb supervisió d'un operador (procés desassistit i asíncron) amb acord al que estableix l'Ordre ETD/465/2021, de 6 de maig, que regula els mètodes de identificació remota per vídeo per l'expedició de certificats electrònics qualificats.
14. El servei d'identificació remota per vídeo haurà de complir els requisits mínims de seguretat indicats a l'annex F.11 de la Guia de Seguretat de les TIC CCN-STIC-140, del Centre Criptològic Nacional de categoria alta. El prestador qualificat haurà de seguir les indicacions de configuració i ús segur del producte. El compliment de l'obligació esmentada haurà d'estar certificat seguint metodologies d'avaluació reconegudes per l'Organisme de Certificació de l'ENECSTI (Esquema Nacional d'Avaluació i Certificació de la Seguretat de les Tecnologies de la Informació), per un organisme acreditat segons la norma ISO/IEC 17065.
15. Enregistrarà amb vídeo en línia d'una part o tot el procés com a evidència per a facilitar les tasques de supervisió, validació i control.
16. No es permetrà pujar un vídeo pregravat o que es guardi en local que sigui susceptible de manipulació.
17. Verificarà el número de telèfon mòbil informat mitjançant l'enviament d'un codi d'un sol ús al telèfon mòbil.
18. Gaudirà d'una elevada usabilitat de tot el procés des de telèfons mòbils intel·ligents mitjançant una web responsiva.
19. La web responsive ha de accessible des d'algun dels principals navegadors des de Windows, MAC, iOS i Android: Chrome, Safari, IExplorer, Firefox
20. Lliurarà a l'AOC, durant el present contracte, de tots els documents, dades personals i evidències digitals recollides, mitjançant un servei d'integració.
21. Disposarà d'una aplicació de gestió per als operadors (back office) que faciliti la supervisió i/o validació dels registres realitzats per video-conferència o video-identificació. La validació del procés es realitzarà per un empleat públic adequadament format en pràctiques de certificació digital. El cost de personal associat no està inclòs en l'àmbit d'aquest contracte.
22. Es valorarà la usabilitat per a l'empleat públic que optimitzi el temps de validació.
23. Es facilitarà un entorn de proves, rèplica del de producció on es puguin fer les proves tècniques, funcionals i de seguretat que es considerin oportunes.
24. El termini de posada en marxa del servei a Producció, operatiu i disponible per a ser utilitzat pel Consorci AOC serà d'un màxim 10 dies hàbils a partir de l'inici d'execució.

25. En la fase inicial es reutilitzarà les solucions i plataformes estandarditzades ja disponibles pel licitador, minimitzant les integracions, per facilitar l'inici ràpid del projecte 26. La posada en marxa inicial inclou la creació d'una instància a Producció per al Consorci AOC, formació a formadors i una personalització bàsica de la imatge corporativa.
27. La solució de front office (adreçada a la ciutadania) i la de back-office (adreçada als operadors) permetrà una personalització de la imatge i estils d'acord als requisits del Consorci AOC.
28. El servei d'identificació remota ha d'estar disponible tècnicament 24x7 amb un nivell de disponibilitat mínim del 99%.
29. La aplicació de front-office ha d'estar disponible o s'ha de poder personalitzar en els idiomes cooficials a Catalunya: català i castellà
30. Serveis de suport de formació a formadors, implantació i integració: 100 h/any
31. Serveis de suport a la resolució d'incidències d'acord a l'acord de nivell de servei especificat
32. El suport de l'adjudicatari serà durant l'horari garantit del Consorci AOC
33. Compliment de l'acord de nivell de servei
Requisits de Seguretat
L'adjudicatari garantirà la continuïtat del servei amb el disseny i redundància de l'arquitectura de la solució que permeti assolir els requeriments de disponibilitat i continuïtat requerits • RTO (Recovery Time Objetive) temps sense servei: 12h • RPO (Recovery Point Objective) pèrdua de dades: 12h
35. L'adjudicatari haurà de garantir l'execució de proves de recuperació de desastres, com a mínim un cop a l'any, i disposar d'un pla de continuïtat per al personal i instal·lacions.
36. L'adjudicatari haurà d'identificar el país on es tracten i reposen les dades tant pel que fa a les ubicacions principals, com aquelles secundàries necessàries, per a donar suport als plans de contingència o recuperació de desastres.
37. L'adjudicatari haurà d'identificar els diversos proveïdors tecnològics on s'allotja la infraestructura que dona suport a l'aplicació i als seus diferents components. L'adjudicatari haurà d'identificar quin és l'abast i certificacions de seguretat que disposin els diversos proveïdors d'infraestructura contractats.
38. L'adjudicatari haurà d'identificar si la instància és dedicada o compartida amb altres clients, o si és possible optar per qualsevol de les dues modalitats.

39. L'adjudicatari haurà d'identificar si la solució permet un disseny híbrid, habilitant la disponibilitat de dades o funcionalitats en infraestructures on-premise del mateix proveïdor o a identificar per part del Consorci AOC.
40. L'adjudicatari haurà d'identificar si la solució permet la personalització i desenvolupaments adhoc, per a donar resposta a necessitats específiques del Consorci AOC.
41. Per identificar i autenticar els usuaris, l'adjudicatari haurà de permetre la integració amb la solució específica de gestió d'identitats del Consorci AOC (EACAT). En cas de no integrar la solució amb una solució específica de gestió d'identitats, l'adjudicatari haurà de disposar d'una política de credencials robusta i, a ser possible, de mecanismes MFA.
42. La solució haurà de disposar d'un sistema de gestió d'identitats/perfils que en garanteixi la identificació única dels usuaris i permeti gestionar els perfils assignats a cada identificador.
43. La solució proposada haurà de disposar d'eines bàsiques de protecció per detectar i protegir la solució i els seus components davant d'atacs de denegació de servei: FW i anti-DDos
44. L'adjudicatari haurà d'identificar quines mesures de control i protecció (VPN, whitelist d'accés, MFA, etc) disposa per protegir i monitorar l'accés d'administradors funcionals i d'infraestructura de la solució.
45. L'adjudicatari haurà de garantir que les dades es troben xifrades en el trànsit i en repòs, i haurà d'identificar quin tipus de xifrat utilitza per les dades que tracta i emmagatzema l'aplicació, i si aquest xifrat s'aplica sobre un subconjunt o la totalitat de les dades.
46. La solució haurà de generar registres sobre les accions dels usuaris funcionals i usuaris administradors per garantir la traçabilitat de totes les accions realitzades. L'adjudicatari haurà de garantir que l'activitat dels propis usuaris administradors de la solució i infraestructura generen registres que permetin garantir la traçabilitat de totes les accions realitzades.
47. L'adjudicatari haurà de permetre l'accés i integració de les traces i/o alertes de seguretat que generin tant les eines de seguretat perimetral de la instància o infraestructura de la solució, com les traces dels usuaris i administradors funcionals. Aquesta integració es realitzarà contra els sistemes de correlació i gestió d'esdeveniments de seguretat de l'Agència de Ciberseguretat de Catalunya.
48. L'adjudicatari haurà permetre l'execució d'anàlisis tècniques de seguretat sobre la infraestructura i aplicació/solució i donar suport a aquestes tasques. Aquestes anàlisis s'efectuaran seguint les millors pràctiques i metodologies en l'àmbit de la seguretat de la informació, que el Consorci AOC i l'Agència de Ciberseguretat de Catalunya considerin oportuns. El Consorci AOC i l'Agència de Ciberseguretat de Catalunya podran exigir la correcció d'aquelles vulnerabilitats

del sistema d'informació detectades que, segons el seu criteri, es considerin greus.
49. L'adjudicatari haurà d'indicar quina és la política de backups de la solució, el període de retenció i l'existència de proves de restauració periòdiques per demostrar-ne l'efectivitat dels mateixos. Haurà d'indicar les mesures de xifrat dels suports de backup.
50. L'adjudicatari haurà de disposar i facilitar un canal de contacte i comunicació amb el CERT de l'Agència de Ciberseguretat de Catalunya per la gestió i seguiment d'incidents de seguretat. En cas que existeixi un incident de seguretat que afecti a qualsevol dels serveis contractats, el prestador de serveis haurà de donar resposta de manera ràpida i efectiva i comunicar-ho a l'Agència de Ciberseguretat de Catalunya, sense dilació indeguda. Així mateix, el prestador de serveis haurà de col·laborar amb la Generalitat de Catalunya en la investigació d'incidents de ciberseguretat, facilitant les evidències que siguin necessàries garantint la cadena de custòdia.
51. L'adjudicatari haurà de indicar les persones que ocuparan els diferents rols de seguretat per coordinar-se amb els rols del Consorci AOC. No és necessari que siguin persones diferents les que ocupin cada rol • Responsable de la seguretat • Persona de contacte per a incidents de seguretat • Persona de contacte per a canvis i manteniment de sistemes • Persona de contacte per a incidències relatives als indicadors de servei (SLA) • Persona de contacte per a aspectes contractuals • Persona de contacte per a temes jurídics i reguladors, en particular quant a dades de caràcter personal (DPD)
52. El proveïdor s'haurà de comprometre a fer una gestió diligent de tots el suports de la informació que continguin les dades del servei. Haurà de disposar d'un procediment d'eliminació segura de la informació per suports reutilitzats o que arribin al final de la seva vida útil. El proveïdor haurà d'informar com fa la eliminació segura de la informació.
53. Les obligacions del proveïdor en matèria de seguretat es transmeten de manera transitiva a les parts subcontractades. La part subcontractada haurà d'atendre els requisits de seguretat derivats igual que el proveïdor contractat. Les subcontractacions per part del proveïdor han de ser informades i acceptades per part del Consorci AOC i el contracte amb el proveïdor. Com a mínim el proveïdor s'haurà de comprometre per contracte de que els seus subcontractistes ofereixen les garanties equivalents a les que ell mateix assumeix.
54. La solució s'haurà de poder instal·lar en un centre de dades que proposi el Consorci AOC sense cap cost addicional. Aquesta mesura només s'aplicarà si hi ha circumstàncies de seguretat o legals que ho exigeixen.

2.5 Protecció de dades de caràcter personal

El licitador, en la seva oferta, haurà de detallar les mesures de seguretat i les mesures de privacitat des del disseny i per defecte que s'estableixen per donar compliment als requeriments establerts al Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de dades de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i a Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals. En aquest sentit, caldrà estar a les guies aprovades per l'Autoritat Catalana de Protecció de Dades, l'Agencia Española de Protección de Datos i el Comitè Europeu de Protecció de Dades (CEPD).

L'adjudicatari haurà de revisar anualment, i quan es produeixi alguna modificació en el tractament de les dades, l'Anàlisi de Riscos pels drets i llibertats dels titulars de les dades i adoptar les mesures de seguretat que, si s'escau, calgui implantar per preservar-los.

Sent l'objecte de la present licitació un servei de tractament de dades de caràcter personalque inclouen dades biomètriques, sent aquestes de categoria especial, caldrà que el servei ofert per les empreses licitadores pugui recavar el consentiment explícit de les persones interessades amb acord al que estableix l'article 9 del RGPD en els termes que estableix el propi reglament.

3 Requisits de seguretat

3.1 Requisits normatius

L'empresa es compromet a complir els requisits de seguretat i continuïtat aplicables a l'objecte del contracte especificats a:

- La legislació vigent en general i, en particular, quan es tractin dades de caràcter personal, de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD), així com al compliment del Reglament General de Protecció de Dades (UE) 2016/679.
- Les normes ISO/UEC/UNE 17799 de millors pràctiques de seguretat de la informació i UNE71502 de gestió de la seguretat de la informació, adaptades a l'estructura administrativa, personal i entorn tecnològic del client i aplicades de forma proporcional als riscos reals.
- També es compromet a aplicar les mesures, processos i requisits que el client sol·liciti per millorar la qualitat i seguretat i proposar-li els que consideri necessaris per millorar les solucions.
- Es compromet a a que durant els temps d'execució del contracte, el sistema des del qual es presta el servei, estigui certificat conforme a l'Esquema Nacional de Seguretat, com a mínim en el nivell de categorització que el Consorci AOC ha mesurat per les dades i el servei. Es prestarà especial atenció al compliment del Reglament General de Protecció de Dades (UE) 2016/679, durant tot el desenvolupament dels treballs.

- Pel que fa al disseny del sistema, es definiran els controls sobre seguretat, incloent-hi, entre d'altres, els controls de compliment del l'Esquema Nacional de Seguretat i el Reglament General de Protecció de Dades (UE) 2016/679, i l'actualització dels plans de contingències i continuïtat. També es realitzarà la prova dels controls de seguretat.

3.2 Classificació de la informació i el servei

Per determinar les mesures de seguretat aplicables per protegir les dades i el servei, s'ha classificat la informació i el servei en funció del valor que aquesta té per a l'organització.

La classificació del sistema s'ha fet seguint les guies de Agència Catalana de Ciberseguretat i del Esquema Nacional de Seguridad.

Segons la guia GUIT049-C del Agència Catalana de Ciberseguretat, la classificació de la informació es pot mesurar en 5 nivells (Molt crític, Crític, Sensible, Intern i Públic) i la classificació del servei en 4 nivells (Essencial, Estratègic, Important i Bàsic).

La classificació del servei segons aquesta metodologia és:

Dimensions de classificació	**Classificació**	**Dades complementàries**
Disponibilitat	Mig	RTO = 12h RPO = 12h
Seguretat i visibilitat	Crític	
Dades Personals	Crític	

La classificació del sistema segons el Esquema Nacional de Seguridad s'ha fet seguint la guia CCN-STIC 803. Segons aquesta metodologia la classificació del sistema es pot mesurar en 3 nivells (Alt, Mig i Baix).

La classificació del servei segons aquesta metodologia és:

Dimensions de classificació	**Classificació**	**Dades complementàries**
Disponibilitat	Mig	RTO = 12h RPO = 12h
Confidencialitat	Mig	

Integritat	Mig
Autenticitat	Mig
Traçabilitat	Mig
Dades Personals	Alt

Les mesures de seguretat a aplicar per mitigar els riscos segons la classificació es detallaran en el subencàrrec de tractament de dades a signar per l'adjudicatari. En l'annex "Marc de Ciberseguretat de Protecció de Dades: mesures mitigatories identificacio remota" es concreta la proposta de subencàrrec de tractament de dades.

3.3 Anàlisis tècnic de seguretat inicial de la infraestructura i solució

Previ a la posada en marxa del servei, el Consorci AOC podrà realitzar un anàlisi tècnic de seguretat inicial de la infraestructura i la solució, per a garantir el compliment dels requisits especificats.

4 Condicions d'execució: serveis inclosos

4.1 Obligacions bàsiques

L'adjudicatari haurà de complir les següents obligacions bàsiques:

- L'adjudicatari haurà de realitzar reunions periòdiques amb el Consorci AOC per tal d'exposar el compliment del servei on-site i tractar els possibles problemes o millores del servei.
- L'adjudicatari haurà de realitzar la formació dels tècnics designats, en tots aquells aspectes que el Consorci AOC cregui oportuns i que siguin de directa aplicació als serveis requerits.
- Presentació d'informes mensuals de presentació del servei d'acord amb els indicadors que el Consorci AOC consideri apropiats.
- Elaboració de la documentació tècnica.
- Elaboració dels manuals i altra documentació destinada a la formació dels usuaris.

4.2 Acords de nivell del servei

S'haurà de complir els requisits de l'acord de nivell de servei de l'AOC definit a les condicions generals de servei del Consorci AOC.

L'acord de nivell de servei es regularà d'acord als següents criteris.

Administració Oberta de Catalunya

4.2.1 Definicions de les tipologies d'incidències

Nivell	Descgripció
Bloquejant	Una incidència es catalogarà amb criticitat bloquejant si impedeix la utilització total del servei a tots els usuaris d'aquest.
Alta	Una incidència es catalogarà amb criticitat alta si impedeix la utilització d'una part concreta del servei, a tots o alguns usuaris, i l'afectació pel negoci és elevada.
Mitja	Una incidència es catalogarà amb criticitat mitja si impedeix la utilització d'una funcionalitat concreta d'algun dels serveis a tots o alguns usuaris externs a la plataforma i l'afectació pel negoci és relativament baixa.
Baixa	Una incidència es catalogarà amb criticitat baixa si no impedeix la utilització ni parcial ni total d'algun dels serveis a cap dels usuaris.

4.2.2 Temps de resposta i de resolució

El temps de resposta i de resolució s'estableix segons el tipus d'incidència:

- **Temps de resposta**. Es defineix com a temps de resposta el temps que transcorre des de que la incidència es comunicada, i l'usuari rep el tiquet de la seva incidència. El temps de resposta es compta sobre l'horari de suport de recepció d'incidències.
- **Temps de resolució**. Es defineix el temps de resolució d'una incidència com el nombre d'hores que transcorren des de que l'usuari rep el tiquet de la incidència fins el moment en que la incidència està solucionada. En el càlcul del temps de resolució d'una incidència no es té en compte els possibles increments de temps provocats per la intervenció inevitable de tercers en el procés de resolució (per exemple, suport d'Oracle, intervenció d'altres organismes, etc...).
- **Horari garantit segons les Condicions Generals de Servei de l'AOC**. Període de temps en que es disposa de suport tècnic especialitzat en la resolució d'incidències tècniques dels serveis del Consorci AOC.
    - Tot l'any: de dilluns a divendres 8h a 15h
    - Excepcions: dies festius de l'Estat i de Catalunya.

El temps màxim permès per la resposta i resolució d'una incidència dependrà del nivell de criticitat de la incidència. En la següent taula es mostren els temps màxims permesos per la resolució d'una incidència en funció del nivell de criticitat:

Criticitat Incidència	Temps de resposta (hores)	Temps de resolució (hores)	Horari	% de resolució dins del temps compromès
0 Bloquejant	0,5	2	horari garantit	95 %
1 Alta	1	16	horari garantit	95 %
2 Mitja	1	40	horari garantit	95 %
3 Baixa	1	64	horari garantit	95 %

Pel càlcul del temps de resolució d'una incidència s'exclouran els possibles increments de temps provocats per la intervenció inevitable en el procés de resolució per part de tercers.

5 Model de relació

Com a mínim, però, caldrà que s'estableixi els següents nivells d'interlocució:

- Reunions de direcció amb les següents característiques:
  - Interlocutors: cap de projecte i/o responsable del servei per part del licitador. Gestor del servei per part del Consorci AOC.
  - Periodicitat: 1 mes
  - Objectiu: fer el seguiment del contracte, analitzant diversos aspectes: productivitat, control d'hores, temes de facturació, seguiment de fites (a alt nivell), etc.
  - Lliurables: actes de les reunions, informes executius, informes amb control d'hores (fetes i pendents) etc.
- Reunions de seguiment amb les següents característiques:
  - Interlocutors: les persones assignades pel licitador per dur a terme el servei. Per part del Consorci AOC serà el cap de projecte/servei o algun dels tècnics assignats al projecte.
  - Objectiu: seguiment del compliment de l'ANS, rendiment de la plataforma i incidències més destacables.
  - Lliurables:
    - Informe resum de les actuacions ja resoltes i hores realitzades.
    - Informe de situació de les actuacions en curs i hores realitzades.
    - Informe resum de les actuacions pendents i hores estimades.
    - Planificació de les actuacions a realitzar.
    - Escandall d'hores total realitzades en el mes.

- Informe de les incidències obertes, resoltes, temps de resolució, etc.

6 Devolució del servei

L'adjudicatari haurà d'assumir sense cost per al Consorci AOC el pla de transició per fer-se càrrec del servei. Al final del servei l'adjudicatari haurà de planificar i executar el pla de devolució del servei en cas de canvi de proveïdor. El cost del pla de devolució del servei està inclòs en el pressupost del contracte.

L'adjudicatari haurà de fer una eliminació segura de tota la informació del servei una vegada aquest hagi sigut transferit.

7 Gestió del servei amb JIRA

La gestió de les incidències i propostes de millora es realitzarà mitjançant l'eina JIRA del Consoci AOC.

8 Lliurables i criteris de selecció

Els lliurables i els criteris de selecció estan definit en el quadre de característiques de la present licitació.

Barcelona, a 14 de juliol de 2020

Xavier Llebaria Seoane

Cap de l'Àrea de Serveis del Consorci AOC

Annex: Marc de Ciberseguretat de Protecció de Dades: mesures mitigatories Identificació Remota

El subencàrrec de tractament de dades a signar per l'adjudicatari es basa en el Marc de Ciberseguretat de Protecció de Dades de l'Agència de Ciberseguretat de Catalunya. El subencàrrec de tractament definitiu es concretarà abans de l'inici de l'execució del contracte.

Descripció Nivell	Aplicabilitat	Responsable
1. La Normativa de protecció de dades ha de plasmar de forma clara i precisa, almenys, el següent: a) Organització de protecció de dades: - Designació del Delegat de Protecció de Dades (DPD) dels tractaments automatitzats i no automatitzats. - Designació del Comitè o Comitès per a la gestió i coordinació de la protecció de dades, detallant-ne l'àmbit de responsabilitat, els membres i la relació amb altres elements de l'organització. - Designació del Responsable de ciberseguretat i compliment de protecció de dades. - Definició dels rols i funcions definint per a cadascun els deures i responsabilitats. b) Definició de la categorització de cada lloc de treball en matèria de protecció de dades que defineixi les funcions, deures i obligacions del personal; i els criteris i regles d'ús encaminats a la correcta utilització de les eines de treball i els serveis. Ha d'incloure la responsabilitat dels usos indeguts i les mesures disciplinàries associades. c) Model de relació amb l'autoritat de control. d) Registre d'Activitats de Tractament que haurà de contenir com a mínim els següents camps: - Nom i dades de contacte del DPD, del Responsable del Tractament i, si s'escau, del corresponsable i del representant del responsable. - Activitats i finalitats dels tractaments. - Descripció de les categories de dades i dels interessats. - Categories dels destinataris a qui se li han comunicat o comunicaran les dades, inclosos els destinataris en tercers països o organitzacions internacionals. - Transferències internacionals de dades. - Quan sigui possible, els terminis previstos per a la supressió de les diferents categories de dades. - Quan sigui possible, una descripció general de les mesures tècniques i organitzatives de seguretat. e) Si s'actua com encarregat del tractament, haurà de	Aplica	Proveïdor Servei Identificació Remota (subencarregat)

portar un registre de les categories d'activitats de tractament que porta a terme per compte d'un responsable que haurà de contenir la següent informació: - Nom i dades de contacte del encarregat i de cada responsable per compte del que actuï i, si s'escau, del representant del responsable o del encarregat i del DPD. - Categories de tractaments efectuats per compte de cada responsable. - Transferències internacionals de dades. - Quan sigui possible, una descripció general de les mesures tècniques i organitzatives de seguretat. f) Identificació de les Activitats de Tractament i sistemes d'informació associats. g) Definició dels nivells de risc de les Activitats de Tractament i els criteris per la classificació. h) Metodologia d'Avaluació d'Impacte relativa a la Protecció de Dades (AIPD). i) Identificació de les mesures de ciberseguretat associades als diferents nivells de risc. 2. La normativa referida en aquest apartat haurà de mantenir-se en tot moment actualitzada i serà revisada sempre que es produeixin canvis rellevants. 3. Qualsevol incompliment o excepció de la normativa haurà de ser correctament documentat.		
4. S'haurà de disposar de la documentació d'un sistema de gestió de seguretat de la informació aprovada i actualitzada.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. S'ha de disposar, com a mínim, dels següents documents que detallin de forma clara i precisa com portar a terme els tractaments automatitzats: a) Control d'accés lògic (gestió d'usuaris). Ha d'incloure el control d'accés a les dades que tenen limitat el tractament. b) Identificació i autenticació. c) Gestió de suports. d) Còpies de seguretat i restauració de dades. e) Control d'accés físic. f) Tractament de fitxers temporals. g) Eliminació segura d'informació en la reutilització o destrucció de suports i sistemes. h) Devolució d'actius. i) Registre d'accessos. j) Gestió d'excepcions.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)

k) Treball fora dels locals del responsable de les Activitats de Tractament o encarregats dels tractaments. l) Notificació, registre i gestió d'incidències. m) Notificació de vulneracions de seguretat. 2. Els documents referits en aquest apartat s'hauran de mantenir en tot moment actualitzats i seran revisats sempre que es produeixin canvis rellevants.		
3. S'ha de disposar, com a mínim, dels següents documents que detallin de forma clara i precisa com portar a terme els tractaments automatitzats: a) Pseudonimització.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. S'ha d'establir un procés formal d'autoritzacions que cobreixi, com a mínim, els següents aspectes: a) Ús de dispositius mòbils (ordinadors portàtils, dispositius mòbils intel·ligents, tauletes, agendes electròniques, etc.). b) Ús de suports (dispositius òptics (CD's, DVD's), discs durs externs, cintes i discs de còpies de seguretat, unitats USB o pendrives, targetes de memòria (SD, microSD, etc.)). c) Sortida de dispositius mòbils i suports. d) Tractament fora dels locals del Responsable del Tractament o Encarregat del Tractament. e) Accés remot. f) Execució dels procediments de recuperació de dades. g) Entrada en producció i manteniment d'equips i aplicacions. 2. Els documents referits en aquest apartat s'hauran de mantenir en tot moment actualitzats i seran revisats sempre que es produeixin canvis rellevants.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
3. S'ha d'establir un procés formal d'autoritzacions que cobreixi, com a mínim, els següents aspectes: a) Execució del Pla de Continuïtat i les proves periòdiques.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. S'ha d'informar al personal de: a) Les funcions, deures i obligacions tant durant el període el qual exerceix el lloc de treball com en cas de finalització de l'assignació o trasllat a un altre lloc de treball. b) Els requisits a complir respecte les dades a les que ha tingut accés, en particular, en termes de confidencialitat, tant durant el període en el qual ha estat	Aplica	Proveïdor Servei Identificació Remota (subencarregat)

adscrit com posteriorment a la seva finalització. c) Les mesures disciplinàries en cas d'incompliment.		
1. En coordinació amb el DPD, s'han de dur a terme les accions necessàries per formar i conscienciar regularment el personal sobre el seu paper i responsabilitat en matèria de protecció de dades perquè la seguretat dels tractaments automatitzats i no automatitzats assoleixi els nivells exigits. En particular, pel que fa a: a) La normativa, procediments i estàndards de seguretat relativa al bon ús dels sistemes i els tractaments en paper. b) La detecció i reacció a incidents de seguretat, activitats o comportaments sospitosos. c) El procediment de notificació d'incidents i vulneracions de seguretat. d) La gestió de la informació en qualsevol format en què es trobi. S'han de cobrir almenys les activitats següents: llocs de treball endreçats, emmagatzematge, transferència, còpies, distribució, destrucció i ús de fitxers temporals.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. S'han de dissenyar i configurar els sistemes i xarxes aplicant la regla de mínima funcionalitat i la seguretat per defecte. 2. El disseny d'arquitectura de seguretat ha de contemplar les instal·lacions, els sistemes, l'esquema de línies de defensa i els sistemes d'identificació i autenticació. 3. S'han de configurar de forma segura els equips, prèviament a al seva entrada en producció de forma que s'apliquin mesures tècniques i organitzatives que garanteixin, per defecte: a) la limitació del tractament de dades per part dels usuaris dels diferents sistemes d'informació d'acord amb les funcions que l'usuari ha de desenvolupar. b) la retirada de comptes i contrasenyes per defecte. c) que no es proporcionin funcions innecessàries, ni d'operació, ni d'administració, ni d'auditoria, de manera que es redueixi el seu perímetre al mínim imprescindible. d) que no es proporcionin funcions que no siguin d'interès , ni siguin necessàries i, fins i tot, les que siguin inadequades al fi que es persegueix. 4. S'ha de mantenir documentació tant del disseny d'arquitectura com de la configuració dels equips. 5. De manera prèvia a l'entrada en producció s'ha de	Aplica	Proveïdor Servei Identificació Remota (subencarregat)

realitzar un anàlisi de vulnerabilitats. 6. S'ha de demanar autorització relativa a l'entrada en producció i manteniment d'equips i aplicacions.		
7. S'ha de formalitzar i documentar el disseny de l'arquitectura de seguretat i la configuració dels equips. 8. La descripció del disseny i configuració ha de contemplar: a) Instal·lacions: nombre, ubicació, àrees existents i detall dels punts d'accés. b) Sistemes: inventari dels sistemes d'informació que, com a mínim, contingui: - Els actius dels sistemes (servidor de correu, robot de backup...). - Les xarxes existents, així com els elements de connexió a l'exterior (p.ex. la xarxa local està separada d'Internet mitjançant un tallafocs). - Els punts d'accés als sistemes (llocs de treball, consoles d'administració, web de la intranet, etc.). c) Esquema de línies de defensa: - Inventari dels sistemes de seguretat (tallafocs, DMZ, antivirus, antispam, etc.). - Elements d'interconnexió a altres sistemes o a altres xarxes. - Elements de defensa en les connexions a altres xarxes (per exemple, la connexió amb Internet es realitza a través d'un tallafocs). - Utilització de tecnologies diferents per prevenir vulnerabilitats que puguin perforar simultàniament diverses línies de defensa. d) Sistema d'identificació i autenticació d'usuaris per a cada sistema o servei: - Ús de claus concertades, contrasenyes, targetes d'identificació, biometria, o altres de naturalesa anàloga. - Ús de fitxers o directoris per autenticar l'usuari i determinar els seus drets d'accés. e) Sistema de gestió, relatiu a la planificació, l'organització i el control dels recursos relatius a la seguretat de la informació. 9. El disseny de l'arquitectura ha d'estar aprovada per la unitat competent del CTTI i assessorat per l'equip d'especialistes en ciberseguretat de l'organisme competent en la matèria de la Generalitat de Catalunya (actualment, el CESICAT) o àrees equivalents de l'organització responsable o encarregada del tractament.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)

Administració Oberta de Catalunya

1. El desenvolupament d'aplicacions s'ha de fer sobre un sistema diferent i separat del de producció i no hi ha d'haver eines o dades de desenvolupament en l'entorn de producció. 2. S'ha d'aplicar una metodologia de desenvolupament reconeguda que: a) Prengui en consideració els aspectes de seguretat en tot el cicle de vida. b) Utilitzi algoritmes, programari i biblioteques reconegudes. c) Contempli la generació i el tractament de pistes d'auditoria que permeti registrar les activitats dels usuaris tal i com s'especifica a la mesura Id 20 "Registre i protecció de l'activitat dels usuaris". 3. De manera prèvia a l'entrada en producció s'ha de realitzar: a) Comprovació del funcionament correcte de l'aplicació. b) Anàlisi de vulnerabilitats.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
4. S'ha d'aplicar una metodologia de desenvolupament reconeguda que: a) Permeti la inspecció del codi font. b) Permeti comprovar que les dades d'entrada d'un usuari es corresponen a l'esperat (validació de dades d'entrada, sortida i dades intermèdies). 5. De manera prèvia a l'entrada en producció s'ha de realitzar: a) Proves de penetració. b) Anàlisi del codi font.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. Les proves s'han de fer en un entorn aïllat del de producció. 2. Les proves anteriors a l'entrada en producció o modificació no s'han de fer amb dades reals, llevat que s'asseguri que l'entorn en el que es facin les proves tingui implementades les mesures de ciberseguretat establertes pel nivell de seguretat del tractament de les dades.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. Els requisits d'accés s'han d'atenir al que s'indica a continuació: a) Tot sistema d'informació ha de disposar de mecanismes d'autenticació per a validar la identitat dels usuaris que hi accedeixen. b) Els recursos del sistema s'han de protegir amb algun mecanisme que n'impedeixi la utilització, llevat de les entitats, usuaris o persones que gaudeixin de drets	Aplica	Proveïdor Servei Identificació Remota (subencarregat)

d'accés suficients. c) Els drets d'accés de cada recurs s'han d'establir segons les decisions de la persona responsable del recurs, i s'han d'atenir a la normativa de seguretat del sistema. d) Particularment, s'ha de controlar l'accés als components del sistema i als seus fitxers o registres de configuració.		
2. El sistema de control d'accés s'ha d'organitzar de forma que s'exigeixi la concurrència de dues o més persones (o bé dos rols diferenciats per a cadascuna de les funcions que es duguin a terme) per realitzar tasques crítiques, i que anul·li la possibilitat que un sol individu autoritzat pugui abusar dels seus drets per cometre alguna acció il·lícita. En concret, s'han de separar almenys les funcions següents en diferents rols per evitar que una sola persona pugui dur a terme ambdues funcions en relació a un sistema: a) Desenvolupament d'operació. b) Configuració i manteniment del sistema d'operació. c) Auditoria o supervisió de qualsevol altra funció. En especial, es verificarà aquesta separació de rols i funcions en casos d'usuaris administradors i es garantirà que cap administrador ostenta en aquesta condició dues de les funcions definides anteriorment.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. Abans de proporcionar les credencials d'autenticació als usuaris, aquests s'han d'haver identificat i registrat de manera fidedigna davant el sistema o davant un proveïdor d'identitat electrònica reconegut per l'Administració. Es preveuen diverses possibilitats de registre dels usuaris: - Mitjançant la presentació física de l'usuari i la verificació de la seva identitat d'acord amb la legalitat vigent, davant un funcionari habilitat per a això. - De manera telemàtica, mitjançant DNI electrònic o un certificat electrònic qualificat. - De manera telemàtica, utilitzant altres sistemes admesos legalment per a la identificació dels ciutadans dels que prevegi la normativa aplicable. 2. Els mecanismes d'autenticació emprats a cada sistema s'han d'adequar al nivell del sistema i respondre als mecanismes autoritzats al Reglament Europeu 910/2014 (eIDAS) i reglaments d'execució del mateix, així com el Protocol d'Identificació i Signatura Electrònica, aprovat per l'Ordre GRI/233/2015, de 20 de	Aplica	Proveïdor Servei Identificació Remota (subencarregat)

Administració Oberta de Catalunya

juliol, i la Política d'Identificació i Signatura Electrònica del Marc Normatiu de Seguretat de la Informació de la Generalitat de Catalunya. Els mecanismes poden utilitzar els factors d'autenticació següents: - "Factors de coneixement": contrasenyes o claus concertades. Han de disposar de regles bàsiques de qualitat (extensió, tipus de caràcters, etc.). - "Factors de possessió": components lògics (com ara certificats de programari) o dispositius físics (tokens, telèfons mòbils, dispositius). - "Factors inherents o propis de l'usuari": elements biomètrics. 3. En l'àmbit bàsic es requerirà com a mínim un factor d'autenticació. Els factors anteriors es poden utilitzar de manera aïllada o combinar-se per generar mecanismes d'autenticació forta (veure nivells superiors). 4. La identificació dels usuaris del sistema s'ha de fer d'acord amb el que s'indica a continuació: a) Els identificadors d'usuari han de complir amb el MCPD i el Marc Normatiu de la Seguretat de la Informació de la Generalitat de Catalunya. b) Es poden utilitzar com a identificador únic els sistemes d'identificació que prevegi la normativa aplicable. c) Quan l'usuari tingui diferents rols davant del sistema (p.ex. com a ciutadà, com a treballador intern de l'organisme i com a administrador dels sistemes), ha de rebre identificadors singulars per a cadascun dels casos de manera que sempre quedin delimitats privilegis i registres d'activitat. d) Cada entitat (usuari o procés) que accedeix al sistema ha de disposar d'un identificador únic de manera que: - Es pot saber qui rep i quins drets d'accés rep. - Es pot saber qui ha fet alguna cosa i què ha fet. 5. Les credencials s'han de gestionar de la manera següent: a) S'han d'activar una vegada estiguin sota el control efectiu de l'usuari. b) Han d'estar sota el control exclusiu de l'usuari. c) L'usuari ha de reconèixer que les ha rebut i que coneix i accepta les obligacions que implica la seva tinença, en particular, el deure de custòdia diligent, protecció de la seva confidencialitat i informació immediata en cas de pèrdua. d) Han de ser inhabilitats en els casos següents: quan l'usuari deixa l'organització per qualsevol causa; quan l'usuari cessa en la funció per a la qual es requeria el		

compte d'usuari; o quan la persona que el va autoritzar dóna ordre en sentit contrari. En definitiva, quan s'acaba la relació amb el sistema. e) S'han de retenir durant el període necessari per atendre les necessitats de traçabilitat dels registres d'activitat que hi estan associats. A aquest període se'l denomina període de retenció. f) S'han de revisar periòdicament els identificadors i verificar si és necessari que accedeixin als sistemes d'informació. g) En el cas que siguin contrasenyes, s'han de configurar segons l'estàndard de contrasenyes del Marc Normatiu de Seguretat de la Informació de la Generalitat de Catalunya. Concretament, en allò referent a la complexitat, longitud, caducitat, limitació del nombre d'intents fallits, reutilització i emmagatzematge. En cas d'utilitzar OTPs aquests no tindran una duració superior a 24 hores.		
6. S'exigeix l'ús d'almenys dos factors d'autenticació de diferent tipologia. En el cas d'utilització de factors de coneixement, s'ha de donar compliment a les exigències de qualitat i renovació establertes al Marc Normatiu de Seguretat de la Informació de la Generalitat de Catalunya, atenent a la tipologia de perfil a què correspon la credencial. 7. Les credencials utilitzades s'han d'haver obtingut després d'una registre previ: a) Mitjançant la presentació física de l'usuari i la verificació de la seva identitat d'acord amb la legalitat vigent, davant un funcionari habilitat per a això. b) De manera telemàtica, mitjançant la utilització d'un certificat electrònic qualificat. c) De manera telemàtica, mitjançant la utilització d'un certificat electrònic qualificat en un dispositiu de creació de signatura.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. L'assignació i l'ús dels privilegis d'accés ha d'estar restringida i controlada. L'assignació de drets d'accés privilegiats ha d'estar recollida en un procés formal d'autorització, d'acord amb la normativa de control d'accés aplicable. Només el personal autoritzat pot concedir, alterar o anul·lar l'autorització d'accés als recursos, de conformitat amb els criteris establerts pel seu propietari. 2. Els drets d'accés de cada usuari s'han de limitar atenent els principis següents: a) Mínim privilegi. Els privilegis de cada usuari s'han de	Aplica	Proveïdor Servei Identificació Remota (subencarregat)

reduir al mínim estrictament necessari per complir les seves obligacions. b) Necessitat de conèixer. Els privilegis s'han de limitar de forma que els usuaris només accedeixin al coneixement d'aquella informació requerida per complir les seves obligacions. 3. L'assignació de drets ha de tenir en compte el següent: a) Haurien d'identificar-se els drets d'accés privilegiats associats a cada sistema o procés (p.ex. sistema operatiu, sistema de gestió de BBDD, aplicacions) juntament amb els usuaris als que s'han d'assignar. b) S'ha d'autoritzar l'assignació de privilegis i s'han de registrar tots els privilegis assignats. Els drets d'accés no s'han de fer efectius fins que es completi el procés d'autorització. c) Han de definir-se els requisits per al venciment dels drets d'accés privilegiats. d) Els drets d'accés han d'assignar-se a un identificador d'usuari. e) S'han de revisar periòdicament els permisos assignats als usuaris i, verificar que es corresponen a les seves funcions. f) En cas que sigui recomanable per criteris d'eficiència i no generi riscos de seguretat, l'assignació de permisos d'usuari es podrà realitzar en base a la definició i parametrització de rols, d'acord amb allò establert al Marc Normatiu de Seguretat de la Informació de la Generalitat de Catalunya. g) S'han d'establir i mantenir procediments per a evitar l'ús no autoritzat de l'identificador d'usuari, en especial pel que fa a aquelles credencials amb permisos d'administrador.		
Es considera accés local el realitzat des de llocs de treball dins de les mateixes instal·lacions de l'organització i des dels recursos propis ubicats en dites instal·lacions. Es considera accés remot el realitzat des de fora de les mateixes instal·lacions de l'organització, a través de xarxes o recursos de tercers que no estiguin posats a disposició específicament com a recursos locals o propis de la Generalitat de Catalunya. 1. S'ha de garantir la seguretat del sistema quan hi accedeixin remotament usuaris o altres entitats, cosa que implica protegir tant l'accés en si mateix com el canal d'accés remot. La concepció d'accés remot s'haurà d'aplicar a les formes establertes de Teletreball	Aplica	Proveïdor Servei Identificació Remota (subencarregat)

al Marc Normatiu de Seguretat de la Informació de la Generalitat de Catalunya. 2. Els accessos hauran de complir amb les següents mesures segons el nivell dels tractaments: a) S'han de prevenir atacs que puguin revelar informació del sistema sense arribar a accedir-hi. La informació revelada a qui intenta accedir-hi ha de ser la mínima imprescindible (els diàlegs d'accés només han de proporcionar la informació indispensable). b) El sistema ha d'informar l'usuari de les seves obligacions, si fossin específiques, immediatament després d'obtenir l'accés. Aquesta informació en relació amb les obligacions generals aplicables als sistemes de la Generalitat es mostrarà la primera vegada que l'usuari accedeixi al sistema. c) Passat un cert temps d'inactivitat en la sessió de l'usuari, ja sigui amb el sistema o amb una aplicació en particular, s'han de cancel·lar les sessions obertes des de l'esmentat lloc de treball. 3. S'aplicaran a les connexions en remot les mesures de seguretat establertes per a l'accés local, sempre i quan resultin adients. En cas contrari es definiran mesures equivalents per a assolir un nivell de seguretat equiparable.		
4. S'ha d'informar l'usuari de l'últim accés efectuat amb la seva identitat. 5. S'ha d'establir una política específica del que es pot fer remotament, per a la qual cosa es requereix autorització positiva. 6. Quan un equipament es connecti remotament a través de xarxes que no estan sota el control estricte de l'organització, l'àmbit d'operació del servidor ha de limitar la informació i els serveis accessibles als mínims imprescindibles i, s'ha de requerir una autorització prèvia dels responsables dels tractaments de dades afectats. Aquest punt és aplicable a connexions a través d'Internet i altres xarxes que no siguin de confiança.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. S'han de subscriure, si són d'aplicació els escenaris descrits, els següents contractes o altres actes jurídics amb els següents actors: a) Encarregats del Tractament. Aquests han d'establir de forma clara i concisa, com a mínim: - Objecte. - Durada. - Naturalesa i finalitat del tractament (característiques del servei prestat).	Aplica	Proveïdor Servei Identificació Remota (subencarregat)

- Tipus de dades personals. - Categoria dels interessats. - Obligacions, responsabilitats i drets del Responsable. - Obligacions, responsabilitats i drets de l'Encarregat segons el clausulat de l'article 28.3 RGPD. - Mesures tècniques i organitzatives que ofereixin unes garanties suficients d'acord amb el nivell de risc de les dades. - Nivells de servei (temps de resposta en cas de violacions de seguretat, resolució d'incompliments, etc.). - Conseqüències de l'incompliment. - Devolució o destrucció de les dades a la finalització de l'encàrrec. b) Prestadors de serveis sense accés a dades. Aquests han d'establir de forma clara i concisa, com a mínim: - Naturalesa i finalitat del servei. - Prohibició d'accedir a les dades personals. - Obligació de deure de secret respecte a les dades que el personal hagués pogut conèixer amb motiu de la prestació de servei. - Conseqüències de l'incompliment. 2. Els Encarregats del Tractament han de subscriure contractes o altres actes jurídics amb els subencarregats que utilitzin per a dur a terme determinades activitats de tractament. Aquests hauran d'establir, com a mínim, les mateixes obligacions de protecció que les estipulades en el contracte o altre acte jurídic entre el responsable i l'encarregat. Les subcontractacions han d'estar autoritzades pel Responsable del Tractament. 3. El Responsable del tractament ha d'identificar les activitats dels tractaments i sistemes d'informació tractats per compte de tercers amb referència expressa a l'encarregat, al contracte o document que reguli les condicions i la vigència de l'encàrrec. 4. Si s'actua com Encarregat del Tractament s'ha d'identificar i registrar les activitats de tractament i sistemes d'informació que tracta per compte de tercers, si és el cas, amb referència expressa al Responsable del tractament, al contracte o document que reguli les condicions i la vigència de l'encàrrec. 5. En cas de disposar d'encarregats de tractament el Responsable haurà d'establir un sistema de garanties per acreditar la qualitat i adequació professional de l'encarregat de tractament. Aquest s'haurà d'introduir en els models d'acreditació de la solvència tècnica en els		

procediments de contractació i es podrà basar en l'acreditació professional mitjançant certificats i models de compliment voluntaris (com per exemple codis de conducta) reconeguts a nivell nacional i/o internacional.		
6. Els contractes o actes jurídics hauran de preveure l'auditabilitat dels sistemes d'informació per a verificar el nivell de compliment de les mesures de ciberseguretat. 7. Els contractes hauran de preveure la revisió de les condicions de tractament. 8. Establiment d'un sistema rutinari per mesurar el compliment de les obligacions de servei que inclogui un procediment per neutralitzar qualsevol desviació respecte el contracte.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. S'ha de desenvolupar un pla de continuïtat que estableixi les accions a executar en cas d'interrupció dels serveis prestats amb els mitjans habituals. Aquest pla ha de preveure els aspectes següents: a) S'han d'identificar funcions, responsabilitats i activitats a realitzar. b) Hi ha d'haver una previsió dels mitjans alternatius que es conjugaran per poder seguir prestant els serveis. c) Tots els mitjans alternatius han d'estar planificats i materialitzats en acords o contractes amb els proveïdors corresponents. d) Els serveis i mitjans alternatius de comunicació han de: - Tenir les mateixes garanties de seguretat que els habituals. - Garantir temps màxim d'entrada en funcionament segons els terminis determinats a l'anàlisi d'impacte i/o acordats en el Pla de Continuïtat. e) Les persones afectades pel pla han de rebre formació específica relativa al seu paper en l'esmentat pla. f) El pla de continuïtat ha de ser part integral i harmònica dels plans de continuïtat de l'organització en altres matèries alienes a la seguretat. 2. L'execució del Pla de Continuïtat, així com qualsevol procediment de recuperació dins el mateix, haurà de ser prèviament autoritzat per la Generalitat de Catalunya.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. S'han de fer proves periòdiques per localitzar i corregir, si s'escau, els errors o deficiències que hi pugui haver en el pla de continuïtat. 2. L'execució del pla de proves haurà de ser prèviament aprovat per la Generalitat de Catalunya.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)

1. Els locals on s'ubiquin els sistemes d'informació i els seus components han de disposar d'elements adequats per al funcionament eficaç de l'equipament instal·lat allà. I, especialment: a) Condicions de temperatura i humitat. b) Energia elèctrica, i les seves preses corresponents, necessària per a funcionar, de forma que es garanteixi el subministrament de potència elèctrica i el funcionament correcte dels llums d'emergència. c) Protecció contra les amenaces identificades a l'anàlisi de riscos. d) Protecció del cablatge contra incidents fortuïts o deliberats. 2. S'ha de garantir el subministrament elèctric als sistemes en cas de fallada del subministrament general i garantir el temps suficient perquè finalitzin ordenadament els processos, salvaguardant la informació.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
L'equipament s'ha d'instal·lar en àrees específiques per a la seva funció (àrees de CPDs o sales tècniques, edificis o ubicacions on es trobi ubicat aquest equipament). S'han de controlar els accessos a les àrees indicades de manera que només s'hi pugui accedir per les entrades previstes i vigilades. 1. Han de quedar registrades l'entrada i sortida de les persones a les àrees separades i concretament la identificació de la persona, la data i hora d'entrada i sortida. 2. El registre d'accessos ha d'estar controlat per una persona autoritzada.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
S'ha de garantir que l'equipament i els suports estan sota control i que satisfan els seus requisits de seguretat mentre estan sent desplaçats d'un lloc a un altre. A aquest efecte: 1. S'ha de portar un registre detallat de qualsevol entrada i sortida d'equipament i suports dels CPDs, sales tècniques, edificis o ubicacions on es trobin aquests equipaments o suports, incloent-hi la identificació de la persona que autoritza el moviment. El registre ha de reflectir: data i hora, identificació inequívoca de l'equipament, persona que realitza l'entrada o sortida, persona que autoritza l'entrada o sortida i persona que realitza el registre. 2. S'ha d'elaborar una llista de serveis autoritzats de transport o missatgeria a emprar. 3. S'ha de disposar d'un procediment informal que	Aplica	Proveïdor Servei Identificació Remota (subencarregat)

compari les sortides amb les arribades per tal de detectar algun incident.		
4. El procediment previst en nivell bàsic que compari semestralment les sortides amb les arribades ha de ser rutinari, formal i que dispari les alarmes pertinents quan es detecti algun incident.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. S'han de registrar les activitats dels usuaris en el sistema, de manera que: a) El registre ha d'indicar qui fa l'activitat, quan la fa i sobre quina informació i les activitats efectuades amb èxit i els intents fallits. b) S'ha d'incloure l'activitat dels usuaris i, especialment, la dels operadors i administradors quan puguin accedir a la configuració i actuar en el manteniment del sistema. c) La determinació de quines activitats s'han de registrar i amb quins nivells de detall s'han d'adoptar en vista de l'anàlisi de riscos feta sobre el sistema i les capacitats del mateix. 2. S'han d'activar els registres d'activitat en els servidors. 3. El període de conservació de la informació es regirà per la normativa de gestió de traces del Marc Normatiu de Seguretat de la Informació de la Generalitat de Catalunya (18 mesos). 4. En cas de produir-se incidents o un increment de risc en relació amb amenaces o bé es produeix un requeriment de caràcter legal, es podrà recuperar, revisar i analitzar la informació associada a aquesta activitat sempre aplicant criteris de necessitat, idoneïtat i proporcionalitat.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
5. S'han de revisar informalment els registres d'activitat per buscar patrons anormals. A aquest efecte, es podrà disposar d'eines específiques automàtiques destinades a l'anàlisi d'aquests patrons per tal de determinar potencials incompliments. En cas de detectar-se podran analitzar-se en detall les dades que han generat la detecció d'aquests patrons atenent a l'amenaça i al nivell de risc. Aquestes eines podran ser transversals i/o operades per organismes específics dedicats a la ciberseguretat.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
6. S'ha de revisar formalment i s'ha de disposar d'un sistema automàtic de recol·lecció de registres i correlació d'esdeveniments. Els esdeveniments s'hauran de recollir en aquest sistema automàtic,	Aplica	Proveïdor Servei Identificació Remota (subencarregat)

d'acord amb el model TIC de la Generalitat de Catalunya. Aquest sistema podrà ser transversal i/o operat per organismes competents en matèria de ciberseguretat, com el CESICAT.		
1. S'ha d'establir un registre d'incidents en què es faci constar el tipus d'incidència, el moment en què s'ha produït, o si s'escau, detectat, la persona que fa la notificació, a qui se li comunica, els efectes derivats i les mesures correctores aplicades. A més, s'hauran de registrar les restauracions de còpies de seguretat, indicant la persona que realitza el procés, les dades restaurades i les dades que s'hagin hagut de gravar manualment en el procés de recuperació.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
2. S'han de registrar totes les actuacions relacionades amb la gestió d'incidents, de manera que: a) S'han de registrar el report inicial, les actuacions d'emergència i les modificacions del sistema derivades de l'incident. b) S'ha de registrar l'evidència que pugui sostenir, posteriorment, una actuació legal (administrativa o judicial), o fer-hi front, quan l'incident pugui portar a actuacions disciplinàries sobre el personal intern, sobre proveïdors externs o a la persecució de delictes. En la determinació de la composició, detall i gestió d'aquestes evidències, s'ha de recórrer a assessorament legal especialitzat. c) Com a conseqüència de l'anàlisi dels incidents, s'ha de revisar la determinació dels esdeveniments. 3. S'ha d'assegurar que es disposi de la informació necessària per fer la notificació d'informació en els termes previstos al Reglament General de Protecció de Dades. És a dir, s'haurà de poder facilitar la següent informació referent a les vulneracions de seguretat de les dades personals: a) Descripció de la naturalesa de la vulneració de la seguretat de les dades personals, incloent-hi, si és possible, les categories i el nombre aproximat d'interessats afectats i les categories i el nombre aproximat de registres de dades personals afectats. b) Descripció de les possibles conseqüències de la vulneració de la seguretat de les dades personals. c) Descripció de les mesures adoptades o proposades pel responsable del tractament per fer front a la vulneració de la seguretat de les dades personals,	Aplica	Proveïdor Servei Identificació Remota (subencarregat)

incloses, si escau, les mesures adoptades per mitigar-ne els possibles efectes negatius.		
1. S'han de mantenir inventaris actualitzats de tots els elements del sistema (informació, programari, maquinari, serveis, tercers, persones, instal·lacions, suports d'informació), detallant-ne com a mínim: a) El responsable. b) Tipus d'actiu (servidor, ordinador, router, etc.). c) Identificador, fabricant i model. d) Ubicació. 2. Els inventaris s'actualitzaran en funció dels terminis establerts a la normativa.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. Els fitxers temporals que s'haguessin creat exclusivament per la realització de treballs temporals auxiliars hauran de complir amb les mesures establertes que s'apliquin als fitxers considerats definitius. 2. Tot fitxer temporal així creat serà esborrat una vegada hagi deixat de ser necessari per la finalitat que va motivar la seva creació.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. El lloc de treball s'ha de bloquejar al cap d'un temps prudencial d'inactivitat i ha de requerir una nova autenticació de l'usuari per reprendre l'activitat en curs. 2. Els equips han de disposar de protecció antivirus i antimalware. 3. Els equips que siguin susceptibles de sortir de les instal·lacions de l'organització i no es puguin beneficiar de la protecció física corresponent, amb un risc manifest de pèrdua o robatori, s'han de protegir adequadament. Sense perjudici de les mesures generals que els afectin, s'ha d'evitar, en la mesura del possible, que l'equip contingui claus d'accés remot a l'organització. Es consideren claus d'accés remot les que siguin capaces d'habilitar un accés a altres equips de l'organització, o altres de naturalesa anàloga.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
En relació amb els equips que siguin susceptibles de sortir de les instal·lacions de l'organització: 4. S'ha de dotar el dispositiu de detectors de vulneracions que permetin saber si l'equip ha estat manipulat i activin els procediments previstos de gestió de l'incident. 5. Les dades dels tractaments de nivell alt emmagatzemades s'han de protegir mitjançant xifratge. 6. S'han d'establir mesures de protecció en llocs públics com filtres de confidencialitat o cadenat de seguretat.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)

S'han d'aplicar les mesures preventives i correctives necessàries per a mantenir l'equipament físic i lògic assegurant la confidencialitat, integritat i disponibilitat continua dels equips i sistemes. D'acord amb això, s'ha de disposar de: 1. Les especificacions dels fabricants pel que fa a la instal·lació i manteniment dels sistemes. 2. Un seguiment continu dels anuncis de defectes, utilitzant mecanismes, com per exemple, la subscripció de correu d'avisos de defectes per part del fabricant. 3. Un procediment per analitzar, prioritzar i determinar quan aplicar les actualitzacions de seguretat, pedaços, millores i noves versions.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. Els suports d'informació s'han d'identificar mitjançant etiquetatge o mecanisme equivalent de forma que, sense revelar el seu contingut, s'indiqui el nivell de seguretat de la informació continguda de més qualificació. 2. Les etiquetes o mecanismes equivalents haurien de ser fàcilment identificables. S'informarà als usuaris sobre aquests mecanismes d'identificació per tal que, o bé mitjançant simple inspecció, o bé mitjançant el recurs a un repositori, puguin entendre el significat. 3. Es podrà excloure, per previsió a la normativa, l'obligació d'etiquetatge en cas de suports en que no es pogués complir per les seves característiques físiques, establint mesures alternatives per assegurar la seva identificació i localització. 4. Els suports d'informació que s'hagin de reutilitzar per a una altra informació o lliurar a una altra organització han de ser objecte d'un esborrament segur del seu contingut.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
5. S'han de destruir de manera segura els suports d'informació, en els casos següents: a) Quan la naturalesa del suport no permeti un esborrat segur. b) Quan així ho requereixi el procediment associat al tipus d'informació continguda. 6. S'han d'aplicar mecanismes de xifrat que garanteixin la confidencialitat i la integritat de la informació continguda en tots els suports.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
El personal intern o extern haurà de retornar tots els actius de l'organització que estiguin en el seu poder al finalitzar la relació laboral, el contracte o acord.	Aplica	Proveïdor Servei Identificació

		Remota (subencarregat)
1. S'ha d'exigir que els llocs de treball estiguin endreçats, sense més material damunt la taula que el requerit per a l'activitat que es realitza en cada moment.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
2. El material s'ha de guardar en un lloc tancat quan no s'utilitzi. S'haurà de disposar de llocs tancats a disposició dels usuaris.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
Un cop finalitzi el tractament de dades i quan el Responsable del tractament hagi establert que les dades personals s'han de conservar pels motius establerts al RGPD o a la legislació aplicable, que impliquin una limitació d'ús de les mateixes, s'hauran d'adoptar mesures tècniques per protegir les dades d'acord amb aquest nou estat, com les següents: 1. Control d'accés. 2. Ubicació de les dades en un sistema diferent. 3. Xifrat.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. S'han de fer còpies de seguretat que permetin recuperar dades perdudes, accidentalment o intencionadament amb una antiguitat determinada. En particular, s'ha de considerar la conveniència o necessitat, segons que correspongui, que les còpies de seguretat estiguin xifrades. 2. Aquestes còpies han de tenir el mateix nivell de seguretat que les dades originals. 3. Les còpies de seguretat han d'incloure: a) Informació de treball de l'organització que es refereixi a dades personals. b) Aplicacions en explotació, incloent-hi els sistemes operatius mitjançant les que es tractin dades personals. c) Claus utilitzades per preservar la confidencialitat de les dades. 4. Semestralment es verificarà la correcta definició, funcionament i aplicació dels procediments de realització de les còpies i dels procediments de recuperació. 5. La recuperació de còpies haurà de ser autoritzada pel Responsable del tractament.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
6. Les còpies de seguretat i els procediments de recuperació han d'estar emmagatzemats en una	Aplica	Proveïdor Servei Identificació

ubicació diferent d'aquella en la que es trobin els equips que tracten les dades.		Remota (subencarregat)
1. En cas de transmissió de dades tant a nivell intern de l'organització com quan sigui a entitats externes a la mateixa o en situacions i contexts de tractament que es considerin sensibles, s'utilitzaran tècniques de pseudonimització o d'altres mesures anàlogues, com el xifrat. 2. Les tècniques de pseudonimització han d'incloure com a mínim: a) Que els atributs estiguin lligats a àlies aleatoris i que no siguin suficients per identificar l'interessat a qui es refereixen. b) L'assignació d'àlies és tal que no es pot revertir sense esforços desproporcionats de les parts interessades.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
La informació s'ha de xifrar tant durant l'emmagatzematge com durant la transmissió. Només pot estar en clar mentre se n'està fent ús.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. S'ha de disposar de mesures físiques o lògiques, o ambdues, que obstaculitzin la obertura dels dispositius d'emmagatzematge que continguin dades de caràcter personal. Si no és possible adoptar aquesta mesura el responsable del tractament haurà d'adoptar mesures que impedeixin l'accés de persones no autoritzades. 2. Si, per trobar-se en procés de tramitació o revisió, la documentació no es troba arxivada als dispositius d'emmagatzematge escaients, la persona que es trobi al càrrec de la mateixa haurà de custodiar la documentació impedint l'accés a qualsevol persona no autoritzada. 3. S'ha d'exigir que els llocs de treball estiguin endreçats, sense més documentació damunt la taula que la requerida per a l'activitat que es realitza en cada moment. 4. S'ha de destruir qualsevol document que contingui dades de caràcter personal que sigui rebutjat. 5. La destrucció es durà a terme mitjançant l'adopció de mesures dirigides a evitar l'accés a la informació continguda en els mateixos o la seva recuperació posterior per a eliminar el risc d'accés indegut.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. S'han de destruir les còpies o reproduccions rebutjades de manera que s'eviti l'accés a la informació continguda en les mateixes o la seva recuperació posterior.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)

2. S'ha de limitar únicament al personal autoritzat pel responsable del tractament la generació de còpies o la reproducció de documents.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. Quan el tractament de dades es realitzi fora dels locals del responsable o de l'encarregat del tractament el responsable del tractament ho haurà d'autoritzar prèviament. 2. S'ha de portar un registre detallat de qualsevol entrada i sortida de documentació. El registre ha de reflectir: data i hora, identificació de la documentació, el nombre de documents, el tipus d'informació que contenen, persona que realitza l'entrada o sortida, la forma d'enviament, la persona que autoritza l'entrada o sortida i la persona que realitza el registre.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
3. S'han d'adoptar mesures dirigides a impedir l'accés a la informació objecte del trasllat o a la seva manipulació.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. S'ha de garantir la correcta conservació dels documents, la localització i consulta de la informació de conformitat amb els criteris previstos a la legislació vigent sobre arxivística. Aquests criteris han possibilitar l'exercici dels drets previstos a la normativa de protecció de dades. En aquells casos en els quals no existeixi normativa aplicable, el responsable del tractament haurà d'establir els criteris i procediments d'actuació que hauran de seguir-se en matèria d'arxiu.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
1. S'ha d'establir un registre d'incidents en què es faci constar el tipus d'incidència, el moment en què s'ha produït, o si s'escau, detectat, la persona que fa la notificació, a qui se li comunica, els efectes derivats i les mesures correctores aplicades.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
2. S'han de registrar totes les actuacions relacionades amb la gestió d'incidents, de manera que: a) S'han de registrar el report inicial, les actuacions d'emergència i les modificacions del sistema derivades de l'incident. b) S'ha de registrar l'evidència que pugui sostenir, posteriorment, una actuació legal (administrativa o judicial), o fer-hi front, quan l'incident pugui portar a actuacions disciplinàries sobre el personal intern, sobre proveïdors externs o a la persecució de delictes. En la	Aplica	Proveïdor Servei Identificació Remota (subencarregat)

determinació de la composició, detall i gestió d'aquestes evidències, s'ha de recórrer a assessorament legal especialitzat. c) Com a conseqüència de l'anàlisi dels incidents, s'ha de revisar la determinació dels esdeveniments. 3. S'ha d'assegurar que es disposi de la informació necessària per fer la notificació d'informació en els termes previstos al Reglament General de Protecció de Dades. És a dir, s'haurà de poder facilitar la següent informació referent a les vulneracions de seguretat de les dades personals: a) Descripció de la naturalesa de la vulneració de la seguretat de les dades personals, incloent-hi, si és possible, les categories i el nombre aproximat d'interessats afectats i les categories i el nombre aproximat de registres de dades personals afectats. b) Descripció de les possibles conseqüències de la vulneració de la seguretat de les dades personals. c) Descripció de les mesures adoptades o proposades pel responsable del tractament per fer front a la vulneració de la seguretat de les dades personals, incloses, si escau, les mesures adoptades per mitigar-ne els possibles efectes negatius.		
1. S'ha de disposar dels següents procediments pels tractaments no automatitzats: a) Treball fora dels locals del responsable de les activitats dels tractaments o encarregats dels tractaments. b) Notificació, registre i gestió d'incidències. c) Control d'accés. d) Criteris d'arxiu. e) Dispositius d'emmagatzematge. f) Custòdia. g) Còpia o reproducció. h) Trasllat. i) Destrucció paper.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)
j) Registre accés.	Aplica	Proveïdor Servei Identificació Remota (subencarregat)