Resolució
PRE/ /2025, per la qual es fa públic l'Acord del Consell d'Administració de l'Agència de Ciberseguretat de Catalunya, de 13 de novembre de 2025, pel qual s'aprova la convocatòria per a la concessió de subvencions per acompanyar les petites i mitjanes empreses tecnològiques de Catalunya en el procés d'adequació a l'ENS o de certificació en l'ENS

Atès que el Consell d'Administració de l'Agència de Ciberseguretat de Catalunya, en la sessió de 13 de novembre de 2025, ha adoptat l'acord d'aprovació de la convocatòria per la concessió de subvencions per acompanyar les petites i mitjanes empreses tecnològiques de Catalunya en el procés d'adequació a l'ENS o de certificació en l'ENS,

Atès que, en la mateixa sessió, el Consell d'Administració de l'Agència ha autoritzat la directora a signar la resolució corresponent,

D'acord amb el que s'ha exposat, i en virtut de les facultats que m'han estat conferides,

Resolc:

—1.Que es publiqui en el *Diari Oficial de la Generalitat de Catalunya* l'Acord del Consell d'Administració de l'Agència de Ciberseguretat de Catalunya, adoptat en la sessió de 13 de novembre de 2025, d'aprovació de la convocatòria per la concessió de subvencions per acompanyar les petites i mitjanes empreses tecnològiques de Catalunya en el procés d'adequació a l'ENS o de certificació en l'ENS, que s'incorpora com a annex a aquesta Resolució.

—2. Que, contra aquest Acord, que no exhaureix la via administrativa, es pot interposar un recurs d'alçada davant la persona titular del Departament de la Presidència en el termini d'un mes a comptar de la publicació al *Diari Oficial de la Generalitat de Catalunya.*

Barcelona,

Laura Caballero Nadales
Directora de l'Agència de Ciberseguretat de Catalunya

Annex

ACORD DE 13 DE NOVEMBRE DE 2025 DEL CONSELL D'ADMINISTRACIÓ DE L'AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA D'APROVACIÓ DE LA CONVOCATÒRIA PER A LA CONCESSIÓ DE SUBVENCIONS PER ACOMPANYAR LES PETITES I MITJANES EMPRESES TECNOLÒGIQUES DE CATALUNYA EN EL PROCÉS D'ADEQUACIÓ A L'ENS O DE CERTIFICACIÓ EN L'ENS

Actualment, la ciberseguretat és una de les qüestions més desafiants a les quals han de fer front governs, empreses i ciutadans. El seu principal objectiu és protegir els sistemes tecnològics i les dades privades que contenen davant de qualsevol tipus d'amenaça.

Per aquest motiu, el paper de la ciberseguretat en la societat actual és fonamental, ja que proporciona les eines i mecanismes necessaris per augmentar la confiança i la seguretat en l'àmbit digital.

A causa de la seva rellevància i creixent, tant a escala europea com espanyola, s'estan impulsant diversos plans i accions destinats a fomentar el desenvolupament i l'aplicació de mesures de ciberseguretat que garanteixin un entorn digital més protegit i fiable per a tothom.

A nivell estatal, l'Estratègia Nacional de Ciberseguretat, en el seu "Objectiu IV: Cultura i compromís amb la ciberseguretat i millora de les capacitats humanes i tecnològiques", inclou, dins de la seva "Línia d'Acció 7: Desenvolupar una cultura de la ciberseguretat", una sèrie de mesures orientades a consolidar la confiança digital tant de la ciutadania com de les empreses.

A més, l'Agenda 2026 de l'Espanya Digital, en el marc del Pla de Recuperació, Transformació i Resiliència (PRTR) d'Espanya i del context europeu del Mecanisme de Recuperació i Resiliència - "NextGenerationEU" (MRR), constitueix el marc estratègic global i el motor per accelerar la transformació digital d'Espanya. Aquesta agenda subratlla la importància del desenvolupament de les capacitats en matèria de ciberseguretat per part de ciutadans, empreses i Administracions Públiques, alhora que posa l'accent en la necessitat de generar confiança mitjançant una cultura de ciberseguretat que arribi a totes les capes de la societat.

De fet, l'Eix Estratègic núm. 3 de l'Agenda 2026 de l'Espanya Digital està específicament dedicat a la ciberseguretat, amb objectius principals com augmentar les capacitats de ciberseguretat a Espanya, impulsar el desenvolupament de l'ecosistema empresarial del sector (indústria, R+D+i i talent) i millorar el lideratge internacional del país en aquest àmbit.

En aquesta línia, i en relació amb el PRTR, dins de les deu palanques polítiques de reforma estructural per a un creixement sostenible i inclusiu en què s'articula aquest pla, destaca la cinquena palanca: "Modernització i digitalització del teixit industrial i PIME, recuperació del turisme i impuls d'una Espanya Nació Emprenedora". Dins del seu component 15 (C15) s'inclou la iniciativa "Connectivitat digital, foment de la ciberseguretat i desplegament del 5G", que contempla una inversió específica (I7) titulada "Ciberseguretat: reforçar les capacitats de ciberseguretat dels ciutadans, PIME i professionals, potenciant l'ecosistema del sector". Aquesta inversió inclou actuacions

destinades a reforçar les infraestructures de seguretat digital i cibernètica, amb l'objectiu específic d'enfortir i millorar les capacitats de ciberseguretat, tal com s'estableix en el marc normatiu del PRTR en el Component 15.I07.

En aquest context, i amb la finalitat de continuar impulsant la transformació digital a tot el territori nacional, recentment s'ha inclòs un nou eix a l'Agenda 2026 de l'Espanya Digital. Mitjançant aquest nou eix, es va crear el Programa de Xarxes Territorials d'Especialització Tecnològica (en endavant, "Programa RETECH"), que té per objectiu impulsar xarxes territorials d'especialització tecnològica a través de projectes regionals centrats en la transformació i l'especialització digital. Aquest programa assegura la coordinació, col·laboració i complementarietat entre regions.

Emmarcat al programa RETECH, en particular, es llança una iniciativa estratègica, RETECH Ciberseguretat, inclosa dins del Component 15, Inversió 7, destinada al desenvolupament de l'ecosistema de ciberseguretat a Espanya, amb la coordinació de l'Institut Nacional de Ciberseguretat (en endavant, "INCIBE") i, com a conseqüència, es va llançar una invitació pública per establir aliances amb entitats, tant públiques com privades, que tinguin com a objectiu contribuir a la consecució del Component 15.I07 del PRTR i de l'Eix Estratègic 3 de l'Agenda 2026 de l'Espanya Digital.

En resposta a aquesta convocatòria pública, diverses Comunitats Autònomes, com Catalunya, la Comunitat Valenciana i Galícia, a través de diferents entitats, han presentat el projecte a gran escala denominat "Centre d'Innovació i Competència en Ciències de la Salut, Indústria Intel·ligent, Connectada i Excel·lència Operativa" (en endavant, "Projecte RETECH CCAA"). Aquest projecte, centrat en la ciberseguretat, s'alinea amb els objectius de l'Agenda 2026 de l'Espanya Digital i el PRTR.

Els sectors estratègics o pols específics sobre els quals versarà són: ciències de la salut, transport intel·ligent, indústria connectada i excel·lència operativa, amb la finalitat d'ampliar, desenvolupar i fomentar les capacitats tecnològiques i industrials cibernètiques necessàries per a garantir la seguretat digital en els sectors nomenats. En el Projecte es proposen, a més, cinc àmbits d'actuació transversals, els quals ajudaran a evolucionar els sectors comentats i treballar al voltant de l'àmbit formatiu i de desenvolupament de talent, d'innovació, potenciar la col·laboració públic-privada, desplegar solucions i serveis cibernètics i fomentar un espai de dades. El Projecte RETECH CCAA va ser avaluat i aprovat per la Comissió d'Avaluació de l'INCIBE el 7 de desembre de 2022. Posteriorment, el 18 de desembre de 2023, INCIBE i les comunitats autònomes de Catalunya, la Comunitat Valenciana i Galícia van formalitzar un conveni de col·laboració per a l'execució del projecte. En virtut d'aquest acord, conegut com a "Acord RETECH", les comunitats autònomes participants es van comprometre a desenvolupar diferents accions i projectes.

En el cas de la Comunitat Autònoma de Catalunya l'Agència de Ciberseguretat és l'entitat responsable de la implementació del Projecte RETECH CCAA i de les actuacions derivades de l'Acord RETECH a Catalunya. Per tant, li correspon concretar els múltiples subprojectes i accions de ciberseguretat que promouran el desenvolupament tecnològic i incrementaran la confiança digital tant del govern autonòmic com dels ciutadans i empreses del territori Català. Aquesta tasca implica identificar les necessitats específiques del sector públic i privat a Catalunya, desenvolupar estratègies i projectes per a abordar-les, i garantir la coordinació entre els diferents actors implicats. Desde l'Agència de ciberseguretat de Catalunya, es busca impulsar els eixos estratègics d'Excel·lència operativa i Ciències de la salut.

Les bases reguladores per a la subvenció de l'acompanyament a la certificació de PIMEs del sector TIC, s'emmarca en l'eix d'Excel·lencia operativa, la qual té com a objectiu dotar de capacitats i coneixement en l'excel·lència tecnològica que es reflecteixi en excel·lència operativa i capacitats de sobirania digital.

Pel que fa la present actuació d'acompanyament a la certificació de PIMEs del sector TIC, sobre el programa RETECH, té la missió d'impulsar la ciberresiliència de les PIMEs del sector TIC a Catalunya mitjançant l'acompanyament a la certificació en l'Esquema Nacional de Seguretat (ENS).

Per aconseguir aquest propòsit, l'Agència de Ciberseguretat de Catalunya té previst fomentar la col·laboració amb entitats de certificació acreditades i assessors digitals especialitzats en ciberseguretat en l'àmbit de la gestió i l'assessorament per a l'adequació a l'ENS per potenciar la confiança digital de les PIMEs del sector TIC català i la seva capacitat per a prestar serveis amb garanties de seguretat. Aquesta col·laboració, per tant, busca garantir que les PIMEs del sector TIC a Catalunya compleixin amb els estàndards de seguretat necessaris per a operar amb confiança en el mercat i que puguin participar en projectes de major complexitat.

La transformació digital ha esdevingut cabdal per la nostra societat. L'Agenda Digital per a Europa de 2010, ja va assenyalar la importància de les TIC per a la consecució dels objectius de la Unió. El 2021, la Brúixola Digital va establir els objectius digitals de la Unió en matèria de capacitats, govern, empreses i infraestructures per al 2030.

La digitalització es va veure accelerada arran de la pandèmia de la COVID-19 i va suposar una oportunitat per les empreses i per les persones. Es va confirmar que es podia ser productiu sense haver de requerir la presència en el lloc de treball. Es van generar noves possibilitats de generar nous models de negoci basats en les tecnologies més avançades. També es va poder evolucionar la forma d'interactuar amb les administracions públiques, rebent serveis com els sanitaris a distància o gestionant tràmits, sense haver d'anar a les oficines.

Tanmateix, aquesta digitalització també va posar de manifest les problemàtiques d'aquest espai digital, com la dependència de tecnologies i empreses proveïdores d'aquestes, la desinformació o la bretxa digital entre qui pot accedir a una bona connectivitat o qui no. També la bretxa que va aparèixer per les empreses entre les quals van poder aprofitar tot el potencial d'aquest món digital i les que no van poder per manca de coneixements o recursos.

A aquestes problemàtiques s'afegeix també la inseguretat. Així, aquest pas d'un món analògic a un món digital ha implicat l'augment de les oportunitats per desenvolupar accions cibercriminals, que també s'han vist multiplicades en un context global de tensions i conflictes geopolítics.

Les empreses i, especialment les petites i mitjanes empreses (en endavant PIMEs) han hagut de fer front a aquest repte sense en moltes ocasions, tenir suficient preparació i capacitació digital. Aquesta capacitació també requereix tenir present que un procés de transformació digital implica també incorporar la seguretat en el seu disseny, per tal de protegir-se de les amenaces que van evolucionant a la mateixa velocitat que evolucionen les tecnologies.

Els ciberdelinqüents també milloren la seva capacitat per superar les proteccions i assolir els seus objectius i els sistemes d'informació de les PIMEs es veuen exposats de forma cada vegada més intensa a aquestes amenaces. Aquests ciberatacs cada vegada són més generalitzats i sofisticats i es produeixen en un context d'alta dependència de les tecnologies de la informació i de les comunicacions.

Però aquesta necessitat de capacitació encara és més rellevant en relació amb les PIMEs que proporcionen serveis tecnològics, ja que aquests han de prestar-se amb les degudes garanties de ciberseguretat. Així mateix, les PIMEs que proveeixin serveis de ciberseguretat han de ser clau per poder assolir un nivell adequat de protecció dels seus clients, per lluitar contra les amenaces creixents de ciberatacs. Un exemple d'aquesta rellevància és la consideració d'aquests prestadors de serveis tecnològics i de ciberseguretat com a sectors crítics per part de la Directiva (UE) 2022/2555 del Parlament Europeu i del Consell de 14 de desembre de 2022 relativa a les mesures destinades a garantir un elevat nivell comú de ciberseguretat a tota la Unió (Directiva NIS2).

Precisament, el marc regulador propugnat per la Unió Europea per tal d'impulsar i garantir un espai segur en el qual poder desenvolupar aquesta vida digital, s'ha convertit en una peça clau. La legislació que s'ha anat aprovant pretén que les empreses garanteixin la protecció mitjançant l'adopció de les mesures de seguretat adequades per fer front als riscos als quals estan exposats. D'aquesta manera, aquesta necessitat de protegir-se ja no rau només en la voluntat de les empreses sinó també en una obligació de complir amb aquestes lleis.

Per les PIMEs, evidenciar el compliment amb aquestes regulacions genera també la confiança de clients i socis comercials, facilitant la seva integració en mercats més amplis i competitius.

En Espanya, el 5 de maig de 2022 va entrar en vigor el Reial decret 311/2022 pel qual es regula l'Esquema Nacional de Seguretat (d'ara endavant, ENS) i que va derogar l'anterior Reial Decret 3/2010. L'ENS té com a objectiu assolir una protecció adequada de la informació i els serveis prestats per les Administracions Públiques.

Entre les novetats que va incorporar el nou text normatiu està l'extensió clara del seu àmbit d'aplicació. Així, a més d'aplicar-se a aquestes Administracions Públiques, definides a l'article 2 de la Llei 40/2015, també s'indica expressament que s'aplicarà als sistemes d'informació de les entitats del sector privat, quan, en virtut d'una relació contractual, prestin serveis o proveeixin solucions a les entitats del sector públic per a l'exercici d'aquestes de les seves competències i potestats administratives (art. 2.3 ENS).

I és que, com s'assenyala al preàmbul del mateix ENS, la transformació digital ha suposat un increment dels riscs associats als sistemes d'informació que sustenten els serveis públics i que també incorporen sistemes del sector privat. Per tant, sector públic i privat estan igualment exposats a les mateixes amenaces. Si no es protegeixen de forma equivalent els dos sectors, no es pot assolir una protecció completa. I això ja es va reflectir a la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia de Drets Digitals, que va establir a la seva disposició addicional primera que caldria implantar les mesures de seguretat de l'ENS a les entitats del sector públic i també a les entitats del sector privat que els hi poguessin prestar algun servei.

L'ENS també és utilitzat com a norma de referència a la legislació nacional actual que va transposar la Directiva NIS1, el Reial decret-llei 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació i el Reial decret 43/2021, de 26 de gener, pel qual es desenvolupa el Reial decret-llei 12/2018, de manera que s'havia d'utilitzar per establir les mesures de seguretat que havien d'adoptar els operadors de serveis essencials i els proveïdors de serveis digitals. Aquesta remissió a l'ENS és previsible que es mantingui en la legislació de transposició de la Directiva NIS2, que esdevingui aplicable als sectors considerats crítics establerts i que, com s'ha esmentat, incorporen el de les empreses que proveeixin serveis tecnològics o de ciberseguretat, tot i que la Directiva NIS2 no aplica en principi a les petites empreses, però sí que afectarà les mitjanes.

Sense perjudici de si resulta directament aplicable, en el cas que les PIMEs prestin serveis a les Administracions Públiques o si esdevé obligatori per l'aplicació de la legislació de transposició de la Directiva NIS2, l'ENS s'ha configurat com un estàndard normatiu de referència en ciberseguretat que ofereix un marc comú de principis bàsics, requisits i mesures de seguretat per a la protecció adequada de la informació i els serveis prestats.

Així doncs, a més de constituir un requisit legal, el compliment de l'ENS per part de les entitats proporciona beneficis que afecten tant la seguretat de la informació com a la confiança i reputació de les entitats percebuda per la ciutadania; ajudant a protegir la informació enfront de les ciberamenaces, proporcionant confiança als seus clients i un marc per a la gestió efectiva dels riscos de seguretat, promovent la revisió i millora contínua, proporcionant un avantatge competitiu i permetent implementar controls i processos de seguretat que poden ajudar a optimitzar les operacions de l'entitat.
Per evidenciar el compliment amb l'ENS dels sistemes d'informació de cada entitat, tal com s'identifica a l'article 38 del RD 311/2022, aquestes hauran de ser objecte d'un procés per determinar la seva conformitat amb l'ENS. A tal efecte, els sistemes de categoria MITJANA o ALTA requeriran una auditoria de certificació de la seva conformitat, que han de realitzar a través de l'una Entitat de Certificació acreditada, mentre que els sistemes de categoria BÀSICA només requeriran d'una autoavaluació per la seva declaració de conformitat, sens perjudici que també es puguin sotmetre a una auditoria de certificació de forma voluntària.

El compliment amb aquests processos de conformitat, tal com assenyala el mateix ENS a l'article 3, és un requeriment per tal que les empreses puguin presentar-se a processos de contractació de les Administracions Públiques.

Per tant, el compliment amb l'ENS i, especialment, poder evidenciar aquest compliment, proporciona a les PIMEs un benefici indubtable, permetent no només que puguin col·laborar amb les administracions públiques sinó que generin la confiança en la seva capacitat per protegir els productes i els serveis que proveeixen als seus clients.

En compliment de tots aquests objectius, el present programa té per objecte atorgar una subvenció per a la contractació de serveis (1) d'acompanyament a l'adequació de l'ENS i (2) de certificació en l'ENS per a impulsar la millora del compliment normatiu en ciberseguretat de les petites i mitjanes empreses tecnològiques de Catalunya. Aquest programa està inclòs en el Pla Estratègic de Subvencions 2024-2026 del Ministeri per a la Transformació Digital i de la Funció Pública.

La primera línia d'ajuts del programa té com a objectiu fomentar l'adequació a l'ENS de les PIMES a les categories BÀSICA, MITJANA o ALTA, dotant les empreses d'eines a curt i mig termini per ajudar-les a complir en l'ENS. Un cop la PIME s'ha adequat, es consolidarà l'objectiu del programa executant la segona línia d'ajuts que té per objecte fomentar la consecució del procés de certificació en l'ENS per part d'una Entitat de Certificació acreditada per ENAC.

Així, el present programa compta amb la participació de quatre tipus d'actors:

1.l'Agència de Ciberseguretat de Catalunya com a responsable de la subvenció;

2.les empreses beneficiàries de les subvencions, és a dir, les PIMEs que rebran la prestació dels serveis operatius d'adequació i/o certificació en l'ENS, objecte de subvenció;

3.les entitats col·laboradores de l'Agència de Ciberseguretat de Catalunya en el procés d'atorgament de les subvencions, essent agents de representació empresarial de Catalunya, encarregats de la dinamització i gestió de la subvenció;

Foment del Treball és la confederació que representa als empresaris i a la indústria catalana en tots els centres de decisió i de poder. Es tracta d'una de les patronals més antigues d'Europa i fundadora de la CEOE, una organització independent, privada i sense ànim de lucre, que es regeix per òrgans de govern democràticament escollits i renovats cada quatre anys. La seva Assemblea General, òrgan sobirà de la institució, està integrada per més de 600 representants d'empreses, moltes d'elles PIMEs. Foment del Treball agrupa a 25 organitzacions territorials i 95 sectorials, el que suposa al voltant de 250.000 empreses i el 75% del PIB català.

Foment del Treball és una organització empresarial sense ànim de lucre, legalment constituïda, que, d'acord amb l'article 5.1 dels seus estatuts, té entre els seus objectius, entre d'altres, el d'ajudar el desenvolupament de les empreses amb les seves polítiques i prestant els serveis necessaris, coordinadament amb les organitzacions afiliades, i el de promoure i coordinar les actuacions de les organitzacions afiliades, en benefici de les empreses.

Foment del Treball té reconeguda la condició d'organització empresarial més representativa en l'àmbit territorial de Catalunya, d'acord amb el que preveu el Decret llei 9/2020, de 24 de març, pel qual es regula la participació institucional, el diàleg social permanent i la concertació social de les organitzacions sindicals i empresarials més representatives a Catalunya.

PIMEC és una confederació patronal de les micro, petites i mitjanes empreses de Catalunya.

Fundada l'any 1974, PIMEC és una confederació empresarial multisectorial, independent i autònoma de qualsevol organisme, poder o entitat tercera, que compta amb una xarxa de seus, delegacions i oficines d'atenció a les PIMEs arreu de Catalunya, i amb representació a Madrid i Brussel·les.

Actualment, PIMEC està formada per més de 300 gremis i associacions, així com negocis individuals.

PIMEC promou activament el creixement d'empreses i professionals autònoms, creant més oportunitats de futur, contribuint activament al seu creixement i a la seva competitivitat, viabilitat i productivitat, i oferint serveis i eines que ajudin a fer les PIMEs més fortes.
PIMEC té reconeguda la condició d'organització empresarial més representativa en l'àmbit territorial de Catalunya, d'acord amb el que preveu el Decret llei 9/2020, de 24 de març, pel qual es regula la participació institucional, el diàleg social permanent i la concertació social de les organitzacions sindicals i empresarials més representatives a Catalunya.

4.els proveïdors de servei, que executaran els serveis operatius dels projectes a les entitats beneficiàries finals, les PIMEs.

El projecte s'ha conceptualitzat incorporant el rol de les entitats col·laboradores com a promotors i facilitadors de la subvenció, ja que constitueixen un actor imprescindible per a l'èxit del projecte, essent els agents empresarials més representatius de Catalunya. Disposen de la competència, la capacitat, la presència territorial, la relació estratègica amb els beneficiaris finals i el posicionament necessari per a desplegar amb garanties el projecte.

Per la naturalesa de les activitats a subvencionar, el seu volum i les característiques dels beneficiaris finals, les entitats col·laboradores es constitueixen doncs, com un actor completament necessari per a l'èxit del projecte.

Per tot això exposat,

S'ha ACORDAT:

—1 Obrir la convocatòria única, en règim de concurrència no competitiva, del procediment de concessió de les subvencions per acompanyar a les petites i mitjans empreses tecnològiques de Catalunya en el procés d'adequació a l'ENS i de certificació de l'ENS, finançades amb càrrec a la Inversió 7 del Component 15 del Pla de Recuperació, Transformació i resiliència – finançat per la Unió Europea-Next Generation EU.

—2 Les subvencions objecte d'aquesta convocatòria es regulen per la Resolució PRE/4784/2025, de 19 de desembre, per la qual es fa públic l'Acord del Consell d'Administració de l'Agència de Ciberseguretat de Catalunya, de 13 de novembre de 2025, d'aprovació de les bases reguladores per a la concessió de subvencions per acompanyar les petites i mitjanes empreses tecnològiques de Catalunya en el procés d'adequació a l'ENS o de certificació en l'ENS (DOGC, núm. 9572; 29.12.2025), finançades amb càrrec a la Inversió 7 del Component 15 del Pla de Recuperació, Transformació i resiliència – finançat per la Unió Europea-Next Generation EU.

—3 La dotació de les subvencions que preveu aquesta convocatòria és de 840.000,00 euros i la seva concessió s'imputa amb càrrec a la posició pressupostària capítol 4 de despesa del pressupost de l'Agència de Ciberseguretat de Catalunya partida 470.0001.

—4 El termini de presentació de les sol·licituds és des de l'endemà de la publicació d'aquesta Resolució al *Diari Oficial de la Generalitat de Catalunya* i fins el 16 de febrer de 2026.

—5 Les sol·licituds, juntament amb la documentació prevista a les bases reguladores s'han de presentar per mitjans electrònics a través de Tràmits gencat, a l'adreça web.gencat.cat/ca/tramits/24404 Els models específics habilitats per a aquesta subvenció són d'ús obligatori i el formulari de sol·licitud ha d'anar signat pel representant legal en el cas de persones jurídiques i per la persona sol·licitant de la subvenció en el cas de persones físiques.

—6 El procediment de concessió de les subvencions, que és de concurrència no competitiva.

La resolució de concessió o denegació de les subvencions, degudament motivada, s'ha de dictar i notificar mitjançant la seva publicació al **Tauler electrònic de l'Administració de la Generalitat de Catalunya (e-Tauler),** tauler.gencat.cat sens perjudici d'utilitzar addicionalment altres mitjans electrònics, dins del termini màxim de dos mesos des de la finalització del termini de presentació. Aquesta publicació substitueix la notificació individual i té els mateixos efectes.

Contra la resolució dictada, que no exhaureix la via administrativa, es pot interposar recurs d'alçada, de conformitat amb el que preveuen l'article 76 de la Llei 26/2010, del 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya, i els articles 112, 121 i 122 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, en el termini d'un mes comptador a partir de l'endemà de la notificació, davant l'òrgan que ha dictat l'acte impugnat o davant el titular Departament de la Presidència mitjançant la Secretaria de Telecomunicacions i Transformació Digital

—7 S'ha de donar publicitat a les subvencions concedides, amb indicació del seu import, objectiu o finalitat i els beneficiaris, al **Tauler electrònic de l'Administració de la Generalitat de Catalunya (e-Tauler),** tauler.gencat.cat .

A més, s'ha de donar publicitat de les subvencions d'acord amb el que preveuen les bases reguladores.

—8 D'acord amb el que estableix la base reguladora, el termini màxim per executar les actuacions subvencionades abans del 30 de juliol de 2026.

—9 El pagament de la subvenció s'efectua un cop la entitat beneficiària ha justificat, d'acord amb els terminis establerts, el compliment de la finalitat per a la qual se li va atorgar la subvenció, tal com preveu les bases reguladores.

—10 La Resolució de convocatòria produeixi efectes el mateix dia de la seva publicació al DOGC.

Contra la resolució dictada, que no exhaureix la via administrativa, es pot interposar recurs d'alçada, de conformitat amb el que preveuen l'article 76 de la Llei 26/2010, del 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya, i els articles 112, 121 i 122 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, en el termini d'un

mes comptador a partir de l'endemà de la notificació, davant l'òrgan que ha dictat l'acte impugnat o davant el titular Departament de la Presidència mitjançant la Secretaria de Telecomunicacions i Transformació Digital