Resolución

PRE/ /2025, por la cual se hace público el Acuerdo del Consejo de Administración de la Agencia de Ciberseguridad de Catalunya, de 13 de noviembre de 2025, por el cual se aprueba la convocatoria para la concesión de subvenciones para acompañar las pequeñas y medianas empresas tecnológicas de Cataluña en el proceso de adecuación al ENS o de certificación en el ENS

Dado que el Consejo de Administración de la Agencia de Ciberseguridad de Catalunya, en la sesión de 13 de noviembre de 2025, ha adoptado el acuerdo de aprobación de la convocatoria por la concesión de subvenciones para acompañar las pequeñas y medianas empresas tecnológicas de Cataluña en el proceso de adecuación al ENS o de certificación en el ENTS,

Dado que, en la misma sesión, el Consejo de Administración de la Agencia ha autorizado a la directora a firmar la resolución correspondiente,

De acuerdo con lo que se ha expuesto, y en virtud de las facultades que me han sido conferidas,

Resuelvo:

—1. Que se publique en el *Diari Oficial de la Generalitat de Catalunya* el Acuerdo del Consejo de Administración de la Agencia de Ciberseguridad de Catalunya, adoptado en la sesión de 13 de noviembre de 2025, de aprobación de la convocatoria para la concesión de subvenciones para acompañar las pequeñas y medianas empresas tecnológicas de Cataluña en el proceso de adecuación al ENS o de certificación en el ENS, que se incorpora como anexo a esta Resolución.

—2. Que, contra este Acuerdo, que no agota la vía administrativa, se puede interponer un recurso de alzada ante la persona titular del Departamento de la Presidencia en el plazo de un mes a contar de la publicación en el *Diari Oficial de la Generalitat de Catalunya*.

Barcelona,

Laura Caballero Nadales
Directora de la Agencia de Ciberseguridad de Cataluña

Anexo

ACUERDO DE 13 DE NOVIEMBRE DE 2025 DEL CONSEJO DE ADMINISTRACIÓN DE LA AGENCIA DE CIBERSEGURIDAD DE CATALUÑA DE APROBACIÓN DE LA CONVOCATORIA PARA LA CONCESIÓN DE SUBVENCIONES PARA ACOMPAÑAR LAS PEQUEÑAS Y MEDIANAS EMPRESAS TECNOLÓGICAS DE CATALUÑA EN EL PROCESO DE ADECUACIÓN AL ENS O DE CERTIFICACIÓN EN EL ENS

Actualmente, la ciberseguridad es una de las cuestiones más desafiantes a las que deben hacer frente gobiernos, empresas y ciudadanos. Su principal objetivo es proteger los sistemas tecnológicos y los datos privados que contienen ante cualquier tipo de amenaza.

Por este motivo, el papel de la ciberseguridad en la sociedad actual es fundamental, ya que proporciona las herramientas y mecanismos necesarios para aumentar la confianza y la seguridad en el ámbito digital.

Debido a su relevancia y crecimiento, tanto a nivel europeo como español, se están impulsando diversos planes y acciones destinados a fomentar el desarrollo y la aplicación de medidas de ciberseguridad que garanticen un entorno digital más protegido y fiable para todos.

A nivel estatal, la Estrategia Nacional de Ciberseguridad, en su "Objetivo IV: Cultura y compromiso con la ciberseguridad y mejora de las capacidades humanas y tecnológicas", incluye, dentro de su "Línea de Acción 7: Desarrollar una cultura de la ciberseguridad", una serie de medidas orientadas a consolidar la confianza digital tanto de la ciudadanía como de las empresas.

Además, la Agenda 2026 de la España Digital, en el marco del Plan de Recuperación, Transformación y Resiliencia (PRTR) de España y del contexto europeo del Mecanismo de Recuperación y Resiliencia - "NextGenerationEU" (MRR), constituye el marco estratégico global y el motor para acelerar la transformación digital de España. Esta agenda subraya la importancia del desarrollo de las capacidades en materia de ciberseguridad por parte de ciudadanos, empresas y Administraciones Públicas, a la vez que pone el acento en la necesidad de generar confianza mediante una cultura de ciberseguridad que llegue a todas las capas de la sociedad.

De hecho, el Eje Estratégico núm. 3 de la Agenda 2026 de la España Digital está específicamente dedicado a la ciberseguridad, con objetivos principales como aumentar las capacidades de ciberseguridad en España, impulsar el desarrollo del ecosistema empresarial del sector (industria, I+D+i y talento) y mejorar el liderazgo internacional del país en este ámbito.

En esta línea, y en relación con el PRTR, dentro de las diez palancas políticas de reforma estructural para un crecimiento sostenible e inclusivo en el que se articula este plan, destaca la quinta palanca: "Modernización y digitalización del tejido industrial y PYME, recuperación del turismo e impulso de una España Nación Emprendedora". Dentro de su componente 15 (C15) se incluye la iniciativa "Conectividad digital, fomento de la ciberseguridad y despliegue del 5G", que contempla una inversión específica (I7) titulada "Ciberseguridad: reforzar las capacidades de ciberseguridad de los ciudadanos, PYME y profesionales, potenciando el ecosistema del sector". Esta inversión incluye actuaciones destinadas a reforzar las infraestructuras de seguridad digital y cibernética, con el objetivo específico de fortalecer y mejorar las capacidades de ciberseguridad, tal y como se establece en el marco normativo del PRTR en el Componente 15.I07.

En este contexto, y con el fin de continuar impulsando la transformación digital en todo el territorio nacional, recientemente se ha incluido un nuevo eje en la Agenda 2026 de la España Digital. Mediante este nuevo eje, se creó el Programa de Redes Territoriales de Especialización Tecnológica (en adelante, "Programa RETECH"), que tiene por objetivo impulsar redes territoriales de especialización tecnológica a través de proyectos regionales centrados en la transformación y la especialización digital. Este programa asegura la coordinación, colaboración y complementariedad entre regiones.

Enmarcado en el programa RETECH, en particular, se lanza una iniciativa estratégica, RETECH Ciberseguridad, incluida dentro del Componente 15, Inversión 7, destinada al desarrollo del ecosistema de ciberseguridad en España, con la coordinación del Instituto Nacional de Ciberseguridad (en adelante, "INCIBE") y, como consecuencia, se lanzó una invitación pública para establecer alianzas con entidades, tanto públicas como privadas, que tengan como objetivo contribuir a la consecución del Componente 15.I07 del PRTR y del Eje Estratégico 3 de la Agenda 2026 de la España Digital.

En respuesta a esta convocatoria pública, varias Comunidades Autónomas, como Cataluña, la Comunidad Valenciana y Galicia, a través de diferentes entidades, han presentado el proyecto a gran escala denominado "Centro de Innovación y Competencia en Ciencias de la Salud, Industria Inteligente, Conectada y Excelencia Operativa" (en adelante, "Proyecto RETECH CCAA"). Este proyecto, centrado en la ciberseguridad, se alinea con los objetivos de la Agenda 2026 de la España Digital y el PRTR.

Los sectores estratégicos o polos específicos sobre los que versará son: ciencias de la salud, transporte inteligente, industria conectada y excelencia operativa, con la finalidad de ampliar, desarrollar y fomentar las capacidades tecnológicas e industriales cibernéticas necesarias para garantizar la seguridad digital en los sectores nombrados. En el Proyecto se proponen, además, cinco ámbitos de actuación transversales, los cuales ayudarán a evolucionar los sectores comentados y trabajar en torno al ámbito formativo y de desarrollo de talento, de innovación, potenciar la colaboración público-privada, desarrollar soluciones y servicios cibernéticos y fomentar un espacio de datos. El Proyecto RETECH CCAA fue evaluado y aprobado por la Comisión de Evaluación del INCIBE el 7 de diciembre de 2022. Posteriormente, el 18 de diciembre de 2023, INCIBE y las comunidades autónomas de Cataluña, la Comunidad Valenciana y Galicia formalizaron un convenio de colaboración para la ejecución del proyecto. En virtud de este acuerdo, conocido como "Acuerdo RETECH", las comunidades autónomas participantes se comprometieron a desarrollar diferentes acciones y proyectos.

En el caso de la Comunidad Autónoma de Cataluña la Agencia de Ciberseguridad es la entidad responsable de la implementación del Proyecto RETECH CCAA y de las actuaciones derivadas del Acuerdo RETECH en Cataluña. Por lo tanto, le corresponde concretar los múltiples subproyectos y acciones de ciberseguridad que promoverán el desarrollo tecnológico e incrementarán la confianza digital tanto del gobierno autonómico como de los ciudadanos y empresas del territorio catalán. Esta tarea implica identificar las necesidades específicas del sector público y privado en Cataluña, desarrollar estrategias y proyectos para abordarlas, y garantizar la coordinación entre los diferentes actores implicados. Desde la Agencia de Ciberseguridad de Cataluña, se busca impulsar los ejes estratégicos de Excelencia operativa y Ciencias de la Salud.

Las bases reguladoras para la subvención del acompañamiento a la certificación de PYMEs del sector TIC, se enmarca en el eje de Excelencia operativa, la cual tiene como objetivo dotar de capacidades y conocimiento en la excelencia tecnológica que se refleje en excelencia operativa y capacidades de soberanía digital.

En cuanto a la presente actuación de acompañamiento a la certificación de PYMEs del sector TIC, sobre el programa RETECH, tiene la misión de impulsar la ciberresiliencia de las PYMEs del sector TIC en Cataluña mediante el acompañamiento a la certificación en el Esquema Nacional de Seguridad (ENS).

Para conseguir este propósito, la Agencia de Ciberseguridad de Cataluña tiene previsto fomentar la colaboración con entidades de certificación acreditadas y asesores digitales especializados en ciberseguridad en el ámbito de la gestión y el asesoramiento para la adecuación al ENS para potenciar la confianza digital de las PYMEs del sector TIC catalán y su capacidad para prestar servicios con garantías de

seguridad. Esta colaboración, por tanto, busca garantizar que las PYMEs del sector TIC en Cataluña cumplan con los estándares de seguridad necesarios para operar con confianza en el mercado y que puedan participar en proyectos de mayor complejidad.

La transformación digital se ha convertido en crucial para nuestra sociedad. La Agenda Digital para Europa de 2010, ya señaló la importancia de las TIC para la consecución de los objetivos de la Unión. En 2021, la Brújula Digital estableció los objetivos digitales de la Unión en materia de capacidades, gobierno, empresas e infraestructuras para 2030.

La digitalización se vio acelerada a raíz de la pandemia de la COVID-19 y supuso una oportunidad para las empresas y por las personas. Se confirmó que se podía ser productivo sin tener que requerir la presencia en el puesto de trabajo. Se generaron nuevas posibilidades de generar nuevos modelos de negocio basados en las tecnologías más avanzadas. También se pudo evolucionar la forma de interactuar con las administraciones públicas, recibiendo servicios como los sanitarios a distancia o gestionando trámites, sin tener que ir a las oficinas.

Sin embargo, esta digitalización también puso de manifiesto las problemáticas de este espacio digital, como la dependencia de tecnologías y empresas proveedoras de las mismas, la desinformación o la brecha digital entre quien puede acceder a una buena conectividad o quién no. También la brecha que apareció por las empresas entre las que pudieron aprovechar todo el potencial de este mundo digital y las que no pudieron por falta de conocimientos o recursos.

A estas problemáticas se añade también la inseguridad. Así, este paso de un mundo analógico a un mundo digital ha implicado el aumento de las oportunidades para desarrollar acciones cibercriminales, que también se han visto multiplicadas en un contexto global de tensiones y conflictos geopolíticos.

Las empresas y, especialmente las pequeñas y medianas empresas (en adelante PYMEs) han tenido que hacer frente a este reto sin en muchas ocasiones, tener suficiente preparación y capacitación digital. Esta capacitación también requiere tener presente que un proceso de transformación digital implica también incorporar la seguridad en su diseño, con el fin de protegerse de las amenazas que van evolucionando a la misma velocidad que evolucionan las tecnologías.

Los ciberdelincuentes también mejoran su capacidad para superar las protecciones y alcanzar sus objetivos y los sistemas de información de las PYMEs se ven expuestos de forma cada vez más intensa a estas amenazas. Estos ciberataques cada vez son

más generalizados y sofisticados y se producen en un contexto de alta dependencia de las tecnologías de la información y de las comunicaciones.

Pero esta necesidad de capacitación aún es más relevante en relación con las PYMEs que proporcionan servicios tecnológicos, ya que estos deben prestarse con las debidas garantías de ciberseguridad. Asimismo, las PYMEs que provean servicios de ciberseguridad deben ser clave para poder alcanzar un nivel adecuado de protección de sus clientes, para luchar contra las amenazas crecientes de ciberataques. Un ejemplo de esta relevancia es la consideración de estos prestadores de servicios tecnológicos y de ciberseguridad como sectores críticos por parte de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS2).

Precisamente, el marco regulador propugnado por la Unión Europea con el fin de impulsar y garantizar un espacio seguro en el que poder desarrollar esta vida digital, se ha convertido en una pieza clave. La legislación que se ha ido aprobando pretende que las empresas garanticen la protección mediante la adopción de las medidas de seguridad adecuadas para hacer frente a los riesgos a los que están expuestos. De esta manera, esta necesidad de protegerse ya no radica sólo en la voluntad de las empresas sino también en una obligación de cumplir con estas leyes.

Para las PYMEs, evidenciar el cumplimiento con estas regulaciones genera también la confianza de clientes y socios comerciales, facilitando su integración en mercados más amplios y competitivos.

En España, el 5 de mayo de 2022 entró en vigor el Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS) y que derogó el anterior Real Decreto 3/2010. El ENS tiene como objetivo alcanzar una protección adecuada de la información y los servicios prestados por las Administraciones Públicas.

Entre las novedades que incorporó el nuevo texto normativo está la extensión clara de su ámbito de aplicación. Así, además de aplicarse a estas Administraciones Públicas, definidas en el artículo 2 de la Ley 40/2015, también se indica expresamente que se aplicará a los sistemas de información de las entidades del sector privado, cuando, en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio de las mismas, de sus competencias y potestades administrativas (art. 2.3 ENS).

Y es que, como se señala en el preámbulo del propio ENS, la transformación digital ha supuesto un incremento de los riesgos asociados a los sistemas de información que sustentan los servicios públicos y que también incorporan sistemas del sector privado. Por lo tanto, sector público y privado están igualmente expuestos a las mismas amenazas. Si no se protegen de forma equivalente los dos sectores, no se puede alcanzar una protección completa. Y eso ya se reflejó en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de Derechos Digitales, que estableció en su disposición adicional primera que habría que implantar las medidas de seguridad de la ENS a las entidades del sector público y también a las entidades del sector privado que les pudieran prestar algún servicio.

El ENS también es utilizado como norma de referencia a la legislación nacional actual que transpuso la Directiva NIS1, el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de manera que debía utilizarse para establecer las medidas de seguridad que debían adoptar los operadores de servicios esenciales y los proveedores de servicios digitales. Esta remisión al ENS es previsible que se mantenga en la legislación de transposición de la Directiva NIS2, que sea aplicable a los sectores considerados críticos establecidos y que, como se ha mencionado, incorporan el de las empresas que provean servicios tecnológicos o de ciberseguridad, aunque la Directiva NIS2 no aplica en principio a las pequeñas empresas, pero sí afectará a las medias.

Sin perjuicio de si resulta directamente aplicable, en el caso de que las PYMEs presten servicios en las Administraciones Públicas o si resulta obligatorio para la aplicación de la legislación de transposición de la Directiva NIS2, el ENS se ha configurado como un estándar normativo de referencia en ciberseguridad que ofrece un marco común de principios básicos, requisitos y medidas de seguridad para la protección adecuada de la información y los servicios prestados.

Así pues, además de constituir un requisito legal, el cumplimiento del ENS por parte de las entidades proporciona beneficios que afectan tanto a la seguridad de la información como a la confianza y reputación de las entidades percibida por la ciudadanía; ayudando a proteger la información frente a las ciberamenazas, proporcionando confianza a sus clientes y un marco para la gestión efectiva de los riesgos de seguridad, promoviendo la revisión y mejora continua, proporcionando una ventaja competitiva y permitiendo implementar controles y procesos de seguridad que pueden ayudar a optimizar las operaciones de la entidad.

Para evidenciar el cumplimiento con el ENS de los sistemas de información de cada entidad, tal como se identifica en el artículo 38 del RD 311/2022, éstas deberán ser objeto de un proceso para determinar su conformidad con el ENS. A tal efecto, los sistemas de categoría MEDIA o ALTA requerirán una auditoría de certificación de su

conformidad, que deben realizar a través de la Entidad de Certificación acreditada, mientras que los sistemas de categoría BÁSICA sólo requerirán de una autoevaluación para su declaración de conformidad, sin perjuicio de que también se puedan someter a una auditoría de certificación de forma voluntaria.

El cumplimiento con estos procesos de conformidad, tal y como señala el propio ENS en el artículo 3, es un requerimiento para que las empresas puedan presentarse a procesos de contratación de las Administraciones Públicas.

Por tanto, el cumplimiento con el ENS y, especialmente, poder evidenciar este cumplimiento, proporciona a las PYMEs un beneficio indudable, permitiendo no sólo que puedan colaborar con las administraciones públicas, sino que generen la confianza en su capacidad para proteger los productos y los servicios que proveen a sus clientes.

En cumplimiento de todos estos objetivos, el presente programa tiene por objeto otorgar una subvención para la contratación de servicios (1) de acompañamiento a la adecuación del ENS y (2) de certificación en el ENS para impulsar la mejora del cumplimiento normativo en ciberseguridad de las pequeñas y medianas empresas tecnológicas de Cataluña. Este programa está incluido en el Plan Estratégico de Subvenciones 2024-2026 del Ministerio para la Transformación Digital y de la Función Pública.

La primera línea de ayudas del programa tiene como objetivo fomentar la adecuación al ENS de las PYMES a las categorías BÁSICA, MEDIA o ALTA, dotando a las empresas de herramientas a corto y medio plazo para ayudarlas a cumplir en el ENS. Una vez la PYME se ha adecuado, se consolidará el objetivo del programa ejecutando la segunda línea de ayudas que tiene por objeto fomentar la consecución del proceso de certificación en el ENS por parte de una Entidad de Certificación acreditada por ENAC.

Así, el presente programa cuenta con la participación de cuatro tipos de actores:

1.la Agencia de Ciberseguridad de Cataluña como responsable de la subvención;

2.las empresas beneficiarias de las subvenciones, es decir, las PYMEs que recibirán la prestación de los servicios operativos de adecuación y/o certificación en el ENS, objeto de subvención;

3.las entidades colaboradoras de la Agencia de Ciberseguridad de Cataluña en el proceso de otorgamiento de las subvenciones, siendo agentes de representación empresarial de Cataluña, encargados de la dinamización y gestión de la subvención;

Foment del Treball es la confederación que representa a los empresarios y a la industria catalana en todos los centros de decisión y de poder. Se trata de una de las patronales más antiguas de Europa y fundadora de la CEOE, una organización independiente, privada y sin ánimo de lucro, que se rige por órganos de gobierno democráticamente escogidos y renovados cada cuatro años. Su Asamblea General, órgano soberano de la institución, está integrada por más de 600 representantes de empresas, muchas de ellas PYMEs. Foment del Treball agrupa a 25 organizaciones territoriales y 95 sectoriales, lo que supone alrededor de 250.000 empresas y el 75% del PIB catalán.

Foment del Treball es una organización empresarial sin ánimo de lucro, legalmente constituida, que, de acuerdo con el artículo 5.1 de sus estatutos, tiene entre sus objetivos, entre otros, el de ayudar al desarrollo de las empresas con sus políticas y prestando los servicios necesarios, coordinadamente con las organizaciones afiliadas, y el de promover y coordinar las actuaciones de las organizaciones afiliadas, en beneficio de las empresas.

Foment del Treball tiene reconocida la condición de organización empresarial más representativa en el ámbito territorial de Cataluña, de acuerdo con lo previsto en el Decreto-ley 9/2020, de 24 de marzo, por el que se regula la participación institucional, el diálogo social permanente y la concertación social de las organizaciones sindicales y empresariales más representativas en Cataluña.

PIMEC es una confederación patronal de las micro, pequeñas y medianas empresas de Cataluña.

Fundada en el año 1974, PIMEC es una confederación empresarial multisectorial, independiente y autónoma de cualquier organismo, poder o entidad tercera, que cuenta con una red de sedes, delegaciones y oficinas de atención en las PYMEs por toda Cataluña, y con representación en Madrid y Bruselas.

Actualmente, PIMEC está formada por más de 300 gremios y asociaciones, así como negocios individuales.

PIMEC promueve activamente el crecimiento de empresas y profesionales autónomos, creando más oportunidades de futuro, contribuyendo activamente a su crecimiento y a

su competitividad, viabilidad y productividad, y ofreciendo servicios y herramientas que ayuden a hacer las PYMEs más fuertes.

PIMEC tiene reconocida la condición de organización empresarial más representativa en el ámbito territorial de Cataluña, de acuerdo con lo previsto en el Decreto-ley 9/2020, de 24 de marzo, por el que se regula la participación institucional, el diálogo social permanente y la concertación social de las organizaciones sindicales y empresariales más representativas en Cataluña.

4.los proveedores de servicio, que ejecutarán los servicios operativos de los proyectos a las entidades beneficiarias finales, las PYMEs.

El proyecto se ha conceptualizado incorporando el rol de las entidades colaboradoras como promotores y facilitadores de la subvención, ya que constituyen un actor imprescindible para el éxito del proyecto, siendo los agentes empresariales más representativos de Cataluña. Disponen de la competencia, la capacidad, la presencia territorial, la relación estratégica con los beneficiarios finales y el posicionamiento necesario para desarrollar con garantías el proyecto.

Por la naturaleza de las actividades a subvencionar, su volumen y las características de los beneficiarios finales, las entidades colaboradoras se constituyen pues, como un actor completamente necesario para el éxito del proyecto.

Por otra parte, la Agencia de Ciberseguridad de Cataluña, como responsable de las subvenciones, aprueba las presentes bases y los requisitos necesarios para convertirse en beneficiario, el papel que deben jugar las entidades colaboradoras y la tipología de servicios que son objeto de subvención.

Por todo lo expuesto,

Se ha ACORDADO:

—1 Abrir la convocatoria única, en régimen de concurrencia no competitiva, del procedimiento de concesión de las subvenciones para acompañar a las pequeñas y medianas empresas tecnológicas de Cataluña en el proceso de adecuación al ENS y de certificación del ENS, financiadas con cargo a la Inversión 7 del Componente 15 del Plan de Recuperación, Transformación y resiliencia – financiado por la Unión Europea-Next Generation EU.

—2 Las subvenciones objeto de esta convocatoria se regulan por la Resolución PRE/4784/2025, de 19 de diciembre, por la que se hace público el Acuerdo del Consejo de Administración de la Agencia de Ciberseguridad de Cataluña, de 13 de noviembre de 2025, de aprobación de las bases reguladoras para la concesión de subvenciones para acompañar a las pequeñas y medianas empresas tecnológicas de Cataluña en el proceso de adecuación al ENS o de certificación en el ENS (DOGC, núm. 9752; de 29.12.2025), financiadas con cargo a la Inversión 7 del Componente 15 del Plan de Recuperación, Transformación y resiliencia – financiado por la Unión Europea-Next Generation EU.

—3 La dotación de las subvenciones que prevé esta convocatoria es de 840.000,00 euros y su concesión se imputa con cargo a la posición presupuestaria capítulo 4 de gasto del presupuesto de la Agencia de Ciberseguridad de Cataluña partida 470.0001.

—4 El plazo de presentación de las solicitudes es desde el día siguiente a la publicación de esta Resolución en el *Diari Oficial de la Generalitat de Catalunya* y hasta el 16 de febrero de 2026.

—5 Las solicitudes, junto con la documentación prevista en las bases reguladoras deben presentarse por medios electrónicos a través de Trámites gencat, en la dirección web.gencat.cat/ca/tramits/24404 Los modelos específicos habilitados para esta subvención son de uso obligatorio y el formulario de solicitud debe ir firmado por el representante legal en el caso de personas jurídicas y por la persona solicitante de la subvención en el caso de personas físicas.

—6 El procedimiento de concesión de las subvenciones, que es de concurrencia no competitiva.

La resolución de concesión o denegación de las subvenciones, debidamente motivada, debe dictarse y notificarse mediante su publicación en el **Tablero electrónico de la Administración de la Generalidad de Cataluña (e-Tauler), tauler.gencat.cat** sin perjuicio de utilizar adicionalmente otros medios electrónicos, dentro del plazo máximo de dos meses desde la finalización del plazo de presentación. Esta publicación sustituye la notificación individual y tiene los mismos efectos.

Contra la resolución dictada, que no agota la vía administrativa, se puede interponer recurso de alzada, de conformidad con lo previsto en el artículo 76 de la Ley 26/2010, de 3 de agosto, de Régimen Jurídico y de Procedimiento de las Administraciones Públicas de Cataluña, y los artículos 112, 121 y 122 de la Ley 39/2015, de 1 de

octubre, del procedimiento administrativo común de las administraciones públicas, en el plazo de un mes contando a partir del día siguiente al de la notificación, ante el órgano que ha dictado el acto impugnado o ante el titular Departamento de la Presidencia mediante la Secretaría de Telecomunicaciones y Transformación Digital.

—7 Se debe dar publicidad a las subvenciones concedidas, con indicación de su importe, objetivo o finalidad y los beneficiarios, en **el Tablero electrónico de la Administración de la Generalidad de Cataluña (e-Tauler),** tauler.gencat.cat

Además, se debe dar publicidad de las subvenciones de acuerdo con lo previsto en las bases reguladoras.

—8 De acuerdo con lo establecido en la base reguladora, el plazo máximo para ejecutar las actuaciones subvencionadas antes del 30 de julio de 2026.

—9 El pago de la subvención se efectúa una vez la entidad beneficiaria ha justificado, de acuerdo con los plazos establecidos, el cumplimiento de la finalidad para la que se le otorgó la subvención, tal y como prevé las bases reguladoras.

—10 La Resolución de convocatoria produce efectos el mismo día de su publicación en el DOGC.

Contra la resolución dictada, que no agota la vía administrativa, se puede interponer recurso de alzada, de conformidad con lo previsto en el artículo 76 de la Ley 26/2010, de 3 de agosto, de Régimen Jurídico y de Procedimiento de las Administraciones Públicas de Cataluña, y los artículos 112, 121 y 122 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas, en el plazo de un mes contando a partir del día siguiente al de la notificación, ante el órgano que ha dictado el acto impugnado o ante el titular Departamento de la Presidencia mediante la Secretaría de Telecomunicaciones y Transformación Digital.