5. Anuncios

5.2. Otros anuncios oficiales

CONSEJERÍA DE LA PRESIDENCIA, INTERIOR, DIÁLOGO SOCIAL Y SIMPLIFICACIÓN ADMINISTRATIVA

Anuncio de 1 de julio de 2025, de la Agencia Digital de Andalucía, para la formalización de un convenio de colaboración con la Agencia Digital de Andalucía, para la puesta en marcha de un laboratorio de Ciberseguridad en Málaga en el marco del programa Retech y del Plan de recuperación, Transformación y Resiliencia-Next Generation EU.

1. INTRODUCCIÓN

La ciberseguridad constituye hoy uno de los pilares fundamentales para garantizar la estabilidad, competitividad y sostenibilidad de la economía digital. Gobiernos, empresas, instituciones públicas y ciudadanía se enfrentan a un contexto tecnológico interconectado, cada vez más complejo y vulnerable, donde la confianza digital se vuelve imprescindible para el funcionamiento de los servicios y la protección de los derechos fundamentales.

En este marco, la Estrategia Nacional de Ciberseguridad plantea, dentro de su Objetivo IV, la necesidad de fomentar una cultura sólida de ciberseguridad, impulsando el compromiso institucional y ciudadano, así como el desarrollo de capacidades tecnológicas y humanas. En concreto, a través de la Línea de Acción 7: Desarrollar una cultura de Ciberseguridad, se promueve la generación de conocimiento, formación especializada y redes de colaboración que fortalezcan el ecosistema nacional de ciberseguridad.

En coherencia con estos principios, la Agenda España Digital 2026, como uno de los ejes tractores del Plan de Recuperación, Transformación y Resiliencia (PRTR) financiado por la Unión Europea a través del instrumento NextGenerationEU, establece como una de sus prioridades estratégicas el impulso a la ciberseguridad. En particular, promueve el fortalecimiento de las capacidades de ciberseguridad de la ciudadanía, las pymes, las empresas tecnológicas y las administraciones públicas, así como la consolidación de una cultura digital segura e inclusiva.

En este contexto, la Agencia Digital de Andalucía (ADA), como entidad responsable de definir e implementar la estrategia digital del Gobierno andaluz y de desarrollar iniciativas en materia de transformación digital, TIC y ciberseguridad, lanza la presente Invitación Pública para promover la colaboración público-privada orientada a la creación y puesta en marcha de un Laboratorio de Evaluación de la Ciberseguridad de Productos y Servicios de IoT e Inteligencia Artificial, con especial enfoque en los sectores de la salud y las ciudades inteligentes (smart cities).

Esta actuación se enmarca dentro del programa estatal Retech-Redes Territoriales de Especialización Tecnológica, y específicamente dentro del proyecto interregional Red Argos, coordinado por INCIBE, que une a varias comunidades autónomas para construir una red nacional de nodos de especialización en ciberseguridad.

El laboratorio de ciberseguridad previsto actuará como nodo andaluz de excelencia, proporcionando servicios de validación técnica, certificación, evaluación y formación, así como facilitando la adopción de estándares de ciberseguridad por parte de empresas tecnológicas y administraciones públicas. Asimismo, servirá como espacio de experimentación, transferencia de conocimiento y apoyo a la innovación, en línea con los objetivos de la Estrategia Andaluza de Ciberseguridad 2022-2025.

Los proyectos derivados de esta invitación deben responder a una lógica de proyecto estratégico, entendido como una cartera de actuaciones tecnológicas y de innovación, orientadas a objetivos medibles, que no serían alcanzables mediante iniciativas individuales. Cada entidad colaboradora deberá disponer de capacidades técnicas,

00323330

operativas y organizativas que aseguren la ejecución del laboratorio, el cumplimiento de los principios del Mecanismo de Recuperación y Resiliencia, así como la sostenibilidad de los resultados más allá del periodo financiado.

Al convenio que se deriven de esta invitación les será aplicable la normativa nacional y europea relativa al Mecanismo de Recuperación y Resiliencia, incluyendo el Reglamento (UE) 2021/241, el Reglamento (UE) 2020/852, el Real Decreto-ley 36/2020, y la legislación española específica sobre gestión de fondos europeos, conflict of interest (DACI), sostenibilidad ambiental (DNSH) y etiquetado digital.

Con esta iniciativa, la ADA pretende reforzar su compromiso con el desarrollo tecnológico de Andalucía, la protección del entorno digital y el fortalecimiento del tejido empresarial andaluz, contribuyendo así al objetivo común de convertir a España en un referente europeo en ciberseguridad.

2. OBJETO Y ALCANCE DE LA INVITACIÓN

En el marco del Plan de Recuperación, Transformación y Resiliencia (PRTR), financiado por la Unión Europea-NextGenerationEU, y en consonancia con el eje estratégico de transformación digital de la Agenda España Digital 2026, la Agencia Digital de Andalucía (ADA) lanza la presente invitación pública de colaboración dirigida a entidades con capacidades técnicas y estratégicas que desarrollen su actividad en el ámbito de la ciberseguridad, con el objeto de promover la creación de un Laboratorio de Evaluación de Ciberseguridad especializado en tecnologías IoT e Inteligencia Artificial aplicadas a los sectores de salud y smart cities.

Esta actuación se enmarca dentro de la iniciativa interregional Red Argos, integrada en el programa estatal Retech-Redes Territoriales de Especialización Tecnológica, coordinado por el Instituto Nacional de Ciberseguridad (INCIBE), y en la que participan de forma conjunta las comunidades autónomas de Andalucía, Castilla y León y País Vasco.

La presente invitación tiene como finalidad establecer un marco de colaboración estable con entidades del ecosistema tecnológico y de innovación andaluz para desarrollar un proyecto estratégico que contribuya a:

• Reforzar las capacidades de evaluación y certificación de ciberseguridad en productos y servicios tecnológicos en tecnologías innovadoras.

• Impulsar el desarrollo de una industria de ciberseguridad regional especializada, mediante infraestructuras físicas y lógicas al servicio del sector.

• Facilitar la adopción de medidas de seguridad por parte de empresas tecnológicas, administraciones públicas y universidades.

• Fomentar la transferencia de conocimiento y tecnologías desde centros de excelencia hacia el tejido empresarial.

• Proveer servicios de formación, experimentación y demostración tecnológica que potencien el talento especializado en ciberseguridad.

A través de la firma del convenio de colaboración, ADA apoyará la puesta en marcha de un proyecto que integre capacidades técnicas, operativas y de sostenibilidad a medio-largo plazo y que:

• Actúe como parte del nodo de la Red Argos en Andalucía.

• Genere un catálogo de servicios de ciberseguridad estructurado, accesible y alineado con las necesidades del mercado.

• Implante, gestione y mantenga un laboratorio de ciberseguridad especializado en tecnologías emergentes (IA, IoT) con sede en Málaga.

• Desarrolle capacidades formativas, demostrativas y de apoyo a proyectos de innovación empresarial.

• Promueva la colaboración interinstitucional y la creación de consorcios público-privados para el desarrollo de soluciones tecnológicas seguras.

• Preste servicios avanzados en evaluación técnica, certificación, auditorías, formación, experimentación y validación.

00323330

• Contribuya al fortalecimiento del ecosistema andaluz de ciberseguridad mediante la transferencia de conocimiento, colaboración con universidades y atención a empresas locales.

El proyecto seleccionado estará sujeto a las normas reguladoras del Mecanismo de Recuperación y Resiliencia, la legislación estatal y autonómica en materia de gestión de fondos europeos, y deberán cumplir con los principios de ausencia de conflicto de interés (DACI), no perjuicio significativo al medio ambiente (DNSH) y etiquetado digital, así como con los requisitos de visibilidad y publicidad institucional exigidos por el PRTR.

3. ENTIDADES DESTINATARIAS

La participación en esta invitación pública está abierta a entidades jurídicas, públicas o privadas sin ánimo de lucro, legalmente constituidas en España, que acrediten experiencia, medios y capacidades en el ámbito de la ciberseguridad, las tecnologías digitales, la inteligencia artificial y la innovación tecnológica, que puedan asumir los compromisos técnicos y administrativos del convenio y que cumplan los siguientes requisitos.

3.1. Requisitos.

Podrán presentar solicitudes las entidades que cumplan con los siguientes requisitos:

• Ser Entidades adscritas en el Sistema Andaluz del Conocimiento.

• Acreditar experiencia en proyectos de ciberseguridad, valorándose otros proyectos tecnológicos y de innovación.

• Contar con capacidad técnica, operativa y financiera para desarrollar las actuaciones objeto del convenio.

• Encontrarse al corriente en el cumplimiento de sus obligaciones tributarias y frente a la Seguridad Social, tanto con la Administración General del Estado como con la Hacienda Autonómica de la Junta de Andalucía.

4. DOTACIÓN PRESUPUESTARIA Y CONDICIONES DE FINANCIACIÓN

La presente Invitación Pública cuenta con una dotación presupuestaria estimada de un millon setecientos cincuenta mil euros (1.750.000 €), que será gestionada por la Agencia Digital de Andalucía (ADA) con cargo a los fondos europeos del Mecanismo de Recuperación y Resiliencia (MRR) en el marco del Plan de Recuperación, Transformación y Resiliencia (PRTR), financiado por la Unión Europea-NextGenerationEU.

Este presupuesto estará destinado a la formalización de un solo convenio de colaboración con la entidad que, conforme a los criterios establecidos en esta convocatoria, participe y resulte seleccionada para el desarrollo y puesta en marcha de un laboratorio de ciberseguridad con sede en Málaga, especializado en soluciones de IoT e Inteligencia Artificial orientadas a los sectores de la salud y las smart cities, en el marco del proyecto interregional Red Argos dentro del programa Retech.

La justificación presupuestaria de esta iniciativa se enmarca en las siguientes referencias del PRTR:

Línea directriz del Plan: Transformación Digital.

Componente 15: Conectividad Digital, impulso de la ciberseguridad y despliegue del 5G.

Inversión C15.I7: Ciberseguridad: Fortalecimiento de las capacidades de ciudadanos, pymes y profesionales; e impulso del ecosistema del sector, orientada al desarrollo de capacidades técnicas, generación de conocimiento aplicado y consolidación del ecosistema nacional de ciberseguridad.

Condiciones de financiación.

La ADA aportará hasta un máximo de 875.000 € correspondiente al 50% en concepto de anticipo para la financiación de las operaciones preparatorias que resulten necesarias para realizar las actuaciones objeto de este proyecto, incluyendo:

- Pago inicial de alquiler de espacios.
- Reformas del espacio, incluyendo cableado de laboratorio.

00323330

- Diseño, despliegue, instalación y puesta en funcionamiento del laboratorio.
- Mobiliario.
- Compra y/o alquiler de equipamiento.
- Puesta en marcha de servicios y costes indirectos asociados.

Durante la fase 1 del proyecto, que se extenderá hasta el 31 de mayo de 2026.

A partir del momento en que el Laboratorio comience a prestar servicios, y hasta la finalización de la fase 1 o, en su caso, hasta que la ADA abone el total de su aporte a la entidad colaboradora, la ADA abonará cada mes a dicha entidad colaboradora el importe correspondiente a los servicios prestados y los costes soportados durante el mes anterior, conforme a lo establecido en el presupuesto, siempre que estos no hayan sido objeto de anticipo según el párrafo anterior.

Durante la fase 2, posterior a mayo de 2026, la entidad colaboradora asumirá la financiación y sostenibilidad del laboratorio, bien a través de ingresos propios derivados de la prestación de servicios, bien mediante esquemas complementarios de financiación de I+D similares a los (European) Digital Innovation Hubs (eDIH) u otros programas, cumpliendo la normativa que aplique. Esta financiación auxiliar será valorable única y exclusivamente a partir del inicio de la fase 2, una vez finalizada la fase 1 (financiada con fondos MRR). Esta financiación no superará el 25% del importe del convenio (437.500 €).

La ayuda aportada por ADA estará sujeta a las siguientes condiciones:

• No podrá destinarse a costes ya cubiertos por otros instrumentos europeos, en cumplimiento del artículo 9 del Reglamento (UE) 2021/241.

• La financiación pública deberá aplicarse a costes elegibles y justificados, asociados a la ejecución técnica del proyecto y conforme a los criterios definidos en el convenio.

• No se permite la doble financiación con otros instrumentos del mismo ámbito o finalidad.

La ejecución de las actividades deberá ajustarse a los plazos, hitos y objetivos definidos en el convenio específico que se formalice con la entidad colaboradora, en línea con los principios de ejecución del PRTR.

El convenio de colaboración no estará sujeto al Impuesto sobre el Valor Añadido (IVA), al no constituir una prestación de servicios realizada a título oneroso.

4.1. Actuaciones de trabajo.

Las actuaciones que deberán desarrollarse se agrupan en las siguientes líneas:

1. Actuaciones de supervisión y control del desarrollo de las actividades objeto del convenio.

• Supervisión y control del proyecto.
• Seguimiento del cumplimiento de los hitos y objetivos definidos en el convenio.
• Revisión y validación de los informes de progreso y resultados obtenidos.
• Identificación y resolución de posibles incidencias o desviaciones en la ejecución del proyecto.
• Identificación de áreas de mejora y de líneas de evolución futura del proyecto.

2. Por su parte, las actuaciones a desarrollar por la entidad colaboradora serán las relativas a:

1. Implantación, gestión y mantenimiento del laboratorio de ciberseguridad

a) Diseñar el laboratorio de ciberseguridad con sede en Málaga.
b) Desplegar, instalar y poner en marcha el laboratorio de ciberseguridad.
c) Coordinar el funcionamiento operativo del laboratorio.
d) Velar por el mantenimiento y actualización del equipamiento.
e) Gestionar los procesos administrativos y de soporte necesarios.

2. Prestar servicios de ciberseguridad mediante el uso del laboratorio:

Los servicios de ciberseguridad a ofrecer serán:

• Servicios de Certificación ENS (Esquema Nacional de Seguridad)
• Auditorías técnicas
• Evaluación de servicios y certificaciones técnicas.

00323330

• Evaluación de sistemas microinformáticos
• Formación en ciberseguridad relacionada con las pruebas y resultados del laboratorio.

En las metodologías de trabajo de los servicios se contemplarán las directrices y recomendaciones derivadas de otras actuaciones del Proyecto Red Argos, en particular, las de elaboración de guías de ciberseguridad sobre la aplicación de tecnologías de IoT e Inteligencia artificial en los ámbitos de la salud y las Smart Cities.

Finalmente, ambas entidades llevarán a cabo actividades conjuntas en materia de:

1. Identificación de potenciales entidades usuarias del laboratorio y comunicación y promoción de las actividades de éste.
2. Comunicación y difusión del proyecto.
3. Establecimiento de condiciones y normas aplicables al desarrollo del programa.
4. Diseño de pruebas y casos de uso.
5. Y otras actuaciones objeto de implementación en el laboratorio susceptibles de aplicación en el ámbito de la ciberseguridad.

La financiación contemplada en el marco de esta Invitación Pública será canalizada mediante convenio de colaboración suscrito entre la Agencia Digital de Andalucía (ADA) y la entidad seleccionada. Los importes financiables se destinarán exclusivamente a cubrir actuaciones directamente vinculadas al objeto del convenio, y los costes elegibles serán aquellos que cumplan con lo establecido en la normativa nacional y europea aplicable, en especial la relacionada con el Plan de Recuperación, Transformación y Resiliencia (PRTR), el Mecanismo de Recuperación y Resiliencia (MRR) y la Orden HFP/1030/2021, de 29 de septiembre.

4.2. Condiciones de la prestación de los servicios de ciberseguridad.

Durante la vigencia del convenio a celebrar se establecerán dos fases:

La «fase 1», que durará desde la firma del convenio hasta final de mayo de 2026. Esta fase podrá prorrogarse si las condiciones del PRTR lo permiten.

La «fase 2», que se iniciará a la finalización de la fase 1 y se prolongará hasta la finalización del convenio.

Una vez se encuentre completamente operativo el laboratorio de ciberseguridad (se estima aproximadamente 6 meses tras el inicio del Convenio), la entidad colaboradora se encargará de la prestación de servicios avanzados de ciberseguridad asociados al mismo, entre los que se incluyen: auditorías de certificación, auditorías técnicas y servicios de formación y concienciación en el ámbito de la ciberseguridad, entre otros. Estos servicios están orientados principalmente a incorporar nuevos recursos para las empresas y entidades públicas con sede social en Andalucía o fuera de la Comunidad Autónoma, siempre que las actividades a realizar en el laboratorio repercutan en centros de trabajo radicados en el ámbito territorial de la Comunidad Autónoma de Andalucía que permitan una mejora de sus capacidades en el ámbito de la ciberseguridad, incrementar la adopción global de medidas de ciberseguridad e impulsar la inversión en ciberseguridad y desarrollo de conocimientos en este ámbito en la Comunidad.

Dentro de este ámbito, la entidad colaboradora se comprometerá a:

• Planificar y prestar servicios de ciberseguridad a empresas y entidades públicas que cumplan los requisitos del párrafo anterior.
• Promocionar los servicios de ciberseguridad entre las administraciones públicas y empresas que cumplan los requisitos del párrafo anterior.
• Aportar hasta un máximo del 25% del importe del convenio de sus fondos propios para seguir prestando los servicios una vez finalizada la fase 1.
• La prestación de estos servicios se realizará conforme a la programación, demanda y requisitos de acceso que en cada caso establezca la Agencia Digital de Andalucía y, en su caso, a las normas y directrices que se determine en la Comisión de Seguimiento.

El valor unitario y las jornadas necesarias para la ejecución de cada servicio se fijarán en base a criterios de referencia técnica y económica, a la aplicación de las guías CCN-CERT IC-01/19 «ENS: Criterios Generales de Auditoría y Certificación» y CCN-CERT

00323330

IC-02/20 «Guía para la contratación de auditorías de certificación del ENS», en las cuales la unidad básica de coste corresponde a la jornada de auditoría, y a la Instrucción 1/2024, de 4 de mayo, de la Agencia Digital de Andalucía sobre perfiles, precios de referencia y desglose de costes en contratos de bienes y servicios TIC. El número de jornadas es estimatorio, puesto que cada sistema auditable tendrá sus propias parti cularidades y condicionantes que pueden hacer variar al alza o a la baja la cantidad de jornadas necesarias.

6. VENTAJAS Y REQUISITOS DE LAS ENTIDADES PARTICIPANTES

A través de la presente Invitación Pública, la Agencia Digital de Andalucía (ADA) ofrece a las entidades interesadas la oportunidad de integrarse en un proyecto de alto impacto estratégico, contribuyendo de manera activa a la consolidación del ecosistema regional y nacional de ciberseguridad. Esta convocatoria promueve la creación de capacidades estructurales, la transferencia de tecnología, la generación de conocimiento y la innovación aplicada, mediante la puesta en marcha de un laboratorio de ciberseguridad especializado en soluciones de IoT e Inteligencia Artificial orientadas a los sectores de la salud y las smart cities.

Las entidades participantes seleccionadas en esta invitación pública se beneficiarán de las siguientes ventajas:

• Participar en una infraestructura de vanguardia para la experimentación, evaluación y certificación en ciberseguridad de productos y servicios emergentes.

• Acceso preferente a un ecosistema de innovación colaborativo público-privado en torno a tecnologías clave como IoT y la IA.

• Refuerzo de capacidades para el diseño, validación y despliegue de soluciones en sectores críticos, especialmente salud y ciudades inteligentes.

• Oportunidad de colaborar en el desarrollo de servicios avanzados de ciberseguridad y su transferencia al tejido empresarial andaluz y nacional.

• Visibilidad institucional y posicionamiento como nodo estratégico de innovación en ciberseguridad dentro del espacio nacional e internacional.

• Participación en actividades de formación especializada, experimentación tecnológica, programas de aceleración y red de centros de excelencia en ciberseguridad vinculados al proyecto Red Argos.

Las condiciones específicas de colaboración serán detalladas en el convenio individualizado que se suscribirá con la entidad seleccionada tras el análisis técnico de la propuesta y su validación por parte de la Comisión de Evaluación y Seguimiento correspondiente.

7. OBLIGACIONES DE LAS PARTES

7.1. Agencia Digital de Andalucía (ADA).

La Agencia Digital de Andalucía, en su calidad de impulsora del proyecto en el marco del Plan de Recuperación, Transformación y Resiliencia (PRTR) y como órgano ejecutor del Componente 15.I7 «Ciberseguridad: Fortalecimiento de capacidades de ciudadanos, PYMES y profesionales; e impulso del ecosistema del sector», se compromete a:

• Aportar, durante la fase 1, la inversión necesaria para el diseño, despliegue, puesta en marcha y mantenimiento del laboratorio de ciberseguridad, así como a la prestación de servicios de ciberseguridad a empresas y entidades públicas andaluzas, conforme se detalle en el convenio de colaboración objeto de firma.

• Llevar a cabo, durante todo el periodo de vigencia del convenio, las actuaciones de supervisión y control.

• Proporcionar información y recursos que permitan coordinar la operación y el funcionamiento del labora-torio con otros proyectos relevantes con los que pudiera establecer relación y, en particular, con los derivados del programa Red Argos.

• Organizar y realizar actividades de formación para el personal que la entidad ponga al servicio del labora-torio sobre materias relacionadas con el ámbito de actuación del

00323330

mismo y con otros proyectos del pro-grama Red Argos o afines con los que pudiera mantener relación.

• Colaborar en las actividades de formación impartidas como parte de los servicios del laboratorio en la forma en que, en cada caso, se determine.

• Poner a disposición del proyecto la sede del Centro de Ciberseguridad de Andalucía para actividades de difusión del laboratorio y relacionadas con el funcionamiento de este.

7.2. Entidad colaboradora.

La entidad colaboradora seleccionada en el marco de esta invitación pública, en su papel de ejecutora del proyecto técnico y operadora del laboratorio de ciberseguridad, se compromete a:

• Implantar, gestionar y mantener el laboratorio. Para ello, asumirá las siguientes tareas:

- Diseñar el laboratorio de ciberseguridad.

- Desplegar, instalar y poner en marcha el laboratorio de ciberseguridad.

- Coordinar el funcionamiento operativo del laboratorio de ciberseguridad y el mantenimiento de la infraestructura.

- Velar por el adecuado mantenimiento del equipamiento del laboratorio de ciberseguridad y, en caso de necesidad, proceder al reemplazo o actualización de los equipos.

- Realizar los procesos administrativos, de soporte y de gestión necesarios para el funcionamiento del laboratorio y un aprovechamiento óptimo del mismo.

• Prestar servicios de ciberseguridad, utilizando para ello el laboratorio.

• Aportar, durante la fase 2, la inversión necesaria para continuar la prestación de servicios de ciberseguridad a empresas y entidades públicas andaluzas, conforme se detalle en el convenio de colaboración objeto de firma.

• Proporcionar a la ADA la información necesaria para el control y el seguimiento del convenio, así como aquella que sea precisa para la justificación de las actividades y los gastos realizados, así como del cumplimiento de objetivos fijados. Esta información se deberá entregar con el contenido y los formatos que a tal efecto establezca la Agencia Digital de Andalucía.

• Poner a disposición de la Agencia Digital de Andalucía las aulas de que dispone, para la realización de actividades formativas y de difusión en materias relacionadas, conforme se detalle en el convenio de colaboración objeto de firma.

• Contratar con cargo al convenio y presentar un informe de auditoría que verifique que los conceptos de gastos y cantidades que incluya, se adecúen a la memoria del proyecto cerrada entre ambas entidades y aprobada por la Comisión de Seguimiento

• Aceptar las condiciones, obligaciones y requisitos que conlleva la financiación mediante el Mecanismo de Recuperación y Resiliencia de la Unión Europea, conforme a lo establecido en la normativa europea y nacional aplicable.

• Garantizar los derechos de acceso y supervisión por parte de la Comisión Europea, OLAF, el Tribunal de Cuentas Europeo, la Fiscalía Europea y las autoridades nacionales competentes.

Finalmente, ambas partes se comprometen, asimismo, a:

• Identificar potenciales entidades usuarias del mismo.

• Comunicar y difundir el programa, favoreciendo su promoción y difusión.

• Mencionar el origen de la financiación y darle visibilidad, cuando las actuaciones estén financiadas con fondos MRR, en particular cuando se haga promoción de las acciones y sus resultados.

• Colaborar en el establecimiento de las condiciones y normas aplicables al desarrollo el programa.

• Colaborar en el diseño de pruebas y casos de uso del laboratorio para atender a necesidades específicas, como las que pudieran derivarse de la publicación de una norma, un estándar o una guía aplicable al ámbito de aplicación del laboratorio.

00323330

Además de las obligaciones relacionadas en este apartado, las partes deberán cumplir las obligaciones, europeas y nacionales, relativas a la financiación del Mecanismo de Recuperación y Resiliencia de la Unión Europea, y especialmente la Orden HPF/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del PRTR, la Orden HFP/1031/2021, de 29 de septiembre, por la que se establece el procedimiento y formato de la información a proporcionar por las Entidades del Sector Público Estatal, Autonómico y Local para el seguimiento del cumplimiento de hitos y objetivos, y la Orden HFP/55/2023, de 24 de enero, relativa a la análisis sistemático del riesgo de conflicto de interés en los procedimientos que ejecutan el PRTR.

8. JUSTIFICACIÓN

La justificación de las actuaciones se desarrollará en los términos que se concreten en el Convenio de colaboración, e incluirá, al menos, los siguientes mecanismos:

a) Justificación mensual: mediante la presentación de un informe de seguimiento que permita evaluar el desarrollo del proyecto y el cumplimiento de los hitos establecidos.

b) Justificación anual: Mediante la entrega de una memoria de actuación que detalle las actividades realizadas durante el ejercicio, así como los resultados obtenidos en relación con los compromisos asumidos.

c) Justificación final de cada fase: al término de la fase 1 y de la fase 2, la entidad colaboradora deberá pre-sentar una memoria económico-financiera que recoja todos los gastos ejecutados y actividades realizadas. Esta memoria irá acompañada de:

- Una auditoría externa independiente de las cuentas justificativas, que garantice la veracidad, trazabilidad y conformidad de los gastos con la normativa aplicable.
- Cualquier otra documentación adicional que pudiera requerirse para la correcta justificación de los fondos europeos, en cumplimiento de los principios de gestión, auditoría, control y transparencia del Mecanismo de Recuperación y Resiliencia.

La entidad colaboradora mantendrá la custodia de los justificantes de gastos y pagos realizados y se compromete a ponerlos a disposición de la Comisión y de los órganos de control y auditoría competentes durante el periodo legal regulado en las normas nacionales y comunitarias.

La Comisión verificará que los gastos realizados en ejecución del convenio resulten de acuerdo con las normas y criterios previstos y acordados, pudiendo solicitar el reintegro a la entidad colaboradora de aquellas cantidades que no se hayan ejecutado conforme a las mismas, sobre cualquier pago anticipado.

Asimismo, se comprometen a facilitar, en cualquier momento, el acceso a dicha documentación por parte de:

- La Agencia Digital de Andalucía.
- El Instituto Nacional de Ciberseguridad (INCIBE), en su función de coordinación técnica.
- La Intervención General de la Junta de Andalucía.
- La Cámara de Cuentas de Andalucía.
- El Tribunal de Cuentas de España.
- El Tribunal de Cuentas de la Unión Europea.
- La Comisión Europea.
- La Oficina Europea de Lucha contra el Fraude (OLAF).
- La Fiscalía Europea.
- Cualquier otra autoridad, entidad u órgano nacional o europea habilitada.

La verificación de la elegibilidad de los gastos corresponderá a ADA, que podrá rechazar aquellos que no se ajusten a los criterios establecidos, requiriendo el reintegro total o parcial de los importes anticipados indebidamente aplicados o no justificados.

En todas las actuaciones de comunicación, difusión, formación, documentación técnica o publicaciones científicas realizadas en el marco del proyecto, será obligatorio incluir la referencia a la financiación europea y nacional, concretamente:

00323330

• El logotipo de la Unión Europea con la mención «Financiado por la Unión Europea-NextGenerationEU».

• El logo del Plan de Recuperación, Transformación y Resiliencia del Gobierno de España.

• El logotipo del Instituto Nacional de Ciberseguridad (INCIBE).

• El logotipo de la Agencia Digital de Andalucía, en su calidad de órgano convocante.

Estos elementos deberán utilizarse respetando las versiones oficiales de cada entidad, sin alteraciones gráficas, de color o forma, y de acuerdo con los manuales de identidad corporativa facilitados. Cualquier uso indebido o manipulación no autorizada de estas señas supondrá una infracción de los derechos de titularidad de las marcas.

9. PRESENTACIÓN DE SOLICITUDES

Las solicitudes de participación por parte de las entidades destinatarias que cumplan con los requisitos fijados en el apartado tercero de esta convocatoria deberán presentarse exclusivamente en un Registro electrónico. Se remitirá preferentemente a través de la Sede Electrónica General de la Junta de Andalucía, utilizando el Registro Electrónico Único, accesible en el siguiente enlace:
https://www.juntadeandalucia.es/servicios/tramites/presentacion-documentos/registro-electronico.html
http://lajunta.es/laboratoriociber

La presentación se realizará mediante el procedimiento de Presentación Electrónica General (PEG), seleccionando como órgano destinatario la Agencia Digital de Andalucía, e indicando en el asunto: «Invitación Pública-Laboratorio Andaluz de Ciberseguridad-Retech/PRTR» .

No se admitirán solicitudes presentadas por otras vías.

Esta redacción cumple con la normativa aplicable y establece claramente el canal exclusivo para la presentación de solicitudes.

9.1. Documentación a presentar.

Junto con el formulario de solicitud, deberá adjuntarse la siguiente documentación:

• Anexo I. Formulario de Solicitud debidamente cumplimentado y firmado.

• Anexo II. Memoria Técnica detallada de la propuesta.

• Cualquier otra documentación complementaria acreditativa de la experiencia presentada y cumplimiento de los requisitos establecidos.

El Anexo I. Formulario de Solicitud incorpora declaración responsable a firmar por la persona representante legal de la entidad, que incluye expresamente los siguientes extremos:

- Cumple con los requisitos exigidos en la presente invitación pública.

- Ser Entidad adscrita en el Sistema Andaluz del Conocimiento.

- Acredita experiencia en proyectos de ciberseguridad y cuenta con capacidad técnica, operativa y financiera para desarrollar las actuaciones objeto del convenio

- Se compromete a cumplir las obligaciones exigidas, en particular con el compromiso financiero.

- Se encuentra al corriente en el cumplimiento de sus obligaciones tributarias y frente a la Seguridad Social, tanto con la Administración General del Estado como con la Hacienda Autonómica de la Junta de Andalucía.

- Asume el compromiso expreso de la concesión de los derechos y accesos necesarios para garantizar que la Comisión, la OLAF, el Tribunal de Cuentas Europeo, la Fiscalía Europea y las autoridades nacionales competentes ejerzan sus competencias de control, de acuerdo con lo previsto en el artículo 22.2. e) del Reglamento (UE) 2021/241 y en el artículo 129.1 del Reglamento Financiero.

- Declara no estar sujeta a procedimiento concursal ni haber sido sancionada administrativamente por infracciones graves en materia social, laboral, fiscal o medioambiental.

00323330

- No estar incursa en ninguna de las causas de prohibición para contratar previstas en el artículo 71 de la Ley 9/2017, de Contratos del Sector Público.

- Conoce y acepta todas las obligaciones impuestas por el Mecanismo de Recuperación y Resiliencia (MRR) y el Plan de Recuperación, Transformación y Resiliencia (PRTR), en especial las relativas al principio de 'no causar un perjuicio significativo al medio ambiente' (DNSH), la ausencia de conflic-to de intereses (DACI), la trazabilidad de los fondos, el cumplimiento del etiquetado digital, la ce-sión y tratamiento de datos entre Administraciones Públicas, la adecuada publicidad y visibilidad institucional, la prevención de la doble financiación y la conservación de la documentación justifi-cativa durante el plazo establecido por la normativa aplicable, conforme al Reglamento (UE) 2021/241, el Reglamento (UE, Euratom) 2018/1046 y demás normativa de aplicación.

La presentación de solicitudes podrá realizarse durante el plazo de vigencia de la presente invitación, y se considerará como fecha válida la del registro electrónico de entrada.

Las entidades participantes se comprometen a conservar los justificantes de presentación, así como a atender cualquier requerimiento de subsanación o aclaración que pudiera ser solicitado por la Agencia Digital de Andalucía.

La presente invitación permanecerá abierta durante diez días hábiles, a contar desde el día siguiente a la publicación oficial de la misma, salvo que se modifiquen los plazos por resolución publicada al efecto.

9.2. Documentación acreditativa de cumplimiento de requisitos a presentar previa a la firma del convenio.

La documentación acreditativa se requerirá únicamente a la entidad seleccionada, y deberá presentarse con carácter previo a la formalización del convenio. Dicha documentación incluirá:

• Documentación acreditativa de la representación legal de la persona firmante, mediante poder notarial o acuerdo del órgano competente, excepto la solicitud sea firmada mediante certificado digital de representante de persona jurídica.

• Acreditación de constitución de la entidad solicitante: escritura de constitución, estatutos.

• Certificado emitido por el Registro Electrónico de Agentes del Sistema Andaluz del Conocimiento (REAC) de inscripción en el Sistema Andaluz del Conocimiento, expedido por la Consejería competente en materia de Universidad, Investigación e Innovación.

• Acreditación de encontrarse al corriente en el cumplimiento de sus obligaciones tributarias y frente a la Seguridad Social, tanto con la Administración General del Estado como con la Hacienda Autonómica de la Junta de Andalucía.

• Certificado de situación en el censo de actividades económicas expedido por la Agencia Estatal de Administración Tributaria, que acredite:

- El domicilio fiscal en Andalucía.

- El desarrollo de actividad vinculada al ámbito de la ciberseguridad, tecnología o I+D+i.

• Currículum institucional o memoria de actividades reciente que permita acreditar experiencia en proyectos de ciberseguridad, tecnología e innovación.

• Memoria económico-financiera o informe de situación patrimonial y de ingresos, que permita valorar la capacidad financiera para el desarrollo del proyecto y su sostenibilidad más allá del periodo financiado.

En caso de que la entidad seleccionada no aporte la documentación requerida en el plazo establecido, se le tendrá por desistida de su solicitud, previa resolución expresa que deberá dictarse en los términos previstos en el artículo 21 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, conforme a lo dispuesto en su artículo 68.1. En tal caso, se continuará el procedimiento con la siguiente entidad según el orden de prelación resultante de la evaluación.

00323330

9.3. Proceso de evaluación y selección.

Con el fin de garantizar el cumplimiento de los principios de transparencia y objetividad establecidos en el artículo 3.1 de la Ley 40/2015, de 1 de octubre, y en coherencia con el principio de igualdad de trato derivado del artículo 14 de la Constitución Española y de su proyección en la normativa europea y estatal en materia de fondos públicos, los criterios de valoración definidos en esta Invitación Pública han sido diseñados en atención a la finalidad específica del proyecto, permitiendo a las entidades participantes conocer de forma clara y anticipada los aspectos evaluables y la documentación requerida, conforme a estándares técnicos objetivos y verificables.

9.3.1. Fases del proceso.

El proceso de selección seguirá las siguientes fases:

a) Recepción de solicitudes

ADA verificará la validez formal y documental de las solicitudes presentadas. En caso de que se requiera subsanación o documentación adicional, se concederá un plazo máximo de 10 días hábiles.

b) Evaluación técnica.

Una Comisión Técnica evaluará las propuestas recibidas conforme a los criterios establecidos. La puntuación máxima será de 30 punto s, distribuidos de la siguiente manera:

9.3.2. Criterios de evaluación:

a) Experiencia y capacidades de la entidad en proyectos de ciberseguridad y tecnología (hasta 12 puntos):

- Hasta 3 puntos: Experiencia previa en implantación de laboratorios de ciberseguridad o entornos de evaluación de la ciberseguridad de tecnologías específicas.
- Hasta 3 puntos: Participación en proyectos financiados por fondos europeos o programas nacionales de I+D+i directamente relacionados con la ciberseguridad.
- Hasta 2 puntos: Historial de colaboraciones con administraciones públicas, universidades o centros tecnológicos en ámbitos relacionados.
- Hasta 4 puntos: Certificaciones o reconocimientos en el ámbito de la ciberseguridad.

b) Calidad técnica y adecuación de la propuesta de actividades (hasta 10 puntos):

- Hasta 5 puntos: Nivel de adecuación de las actividades propuestas a los objetivos del laboratorio.
- Hasta 5 puntos: Metodología prevista para la implantación, gestión y prestación de los servicios del laboratorio.

c) Capacidad de impacto y sostenibilidad del proyecto (hasta 8 puntos):

- Hasta 4 puntos: Estrategia de sostenibilidad económica a partir de 2026 (fase 2).
- Hasta 2 puntos: Acciones previstas de transferencia de conocimiento y colaboración con el ecosistema.
- Hasta 2 puntos: Plan de comunicación y visibilidad del laboratorio.

9.3.3. Descripción detallada de los subcriterios.

En el presente apartado se describe de forma más detallada cada uno de los subcriterios.

En ningún caso se podrá asignar por un subcriterio una puntuación superior a su valoración máxima asignable.

Subcriterio a.1.

Nombre: Experiencia previa en implantación de laboratorios de ciberseguridad o entornos de evaluación de la ciberseguridad de tecnologías específicas.

Valoración máxima asignable a este subcriterio: 3 puntos.

Descripción:

Se valorará la experiencia previa en proyectos que cumplan los siguientes requisitos:

1. El proyecto debe consistir en, o tener entre sus objetivos la implantación de, al menos, un labora-torio de ciberseguridad o un entorno de evaluación de la ciberseguridad.

00323330

2. El laboratorio o el entorno de evaluación citado debe tener o haber tenido como área principal o relevante de aplicación los ámbitos de las tecnologías de IoT (Internet de las Cosas), IA (Inteligencia Artificial), OT (Tecnologías de Operación), 5G y 6G.

Para que un laboratorio o entorno de validación pueda ser objeto de valoración, la entidad solicitante deberá indicar en la Memoria Técnica:

• El nombre del laboratorio o entorno de evaluación.

• La dirección completa, localidad y provincia de la sede física del laboratorio o entorno de pruebas.

• El área o las áreas de aplicación cubiertas por el laboratorio o entorno de evaluación, de entre las anteriormente citadas.

Subcriterio a.2.

Nombre: Participación en proyectos financiados por fondos europeos o programas nacionales de I+D+i directamente relacionados con la ciberseguridad.

Valoración máxima asignable a este subcriterio: 3 puntos.

Descripción:

Se valorará la participación en proyectos que cumplan las siguientes características:

1. El objetivo del proyecto debe tener relación directa con la ciberseguridad.

2. Durante el periodo de participación de la entidad solicitante mencionado en el punto anterior, el proyecto debe haber contado con financiación procedente de fondos europeos o de pro-gramas nacionales de I+D+i o de ambos conceptos.

Para que un proyecto pueda ser objeto de valoración, la entidad solicitante deberá indicar en la Memoria Técnica los siguientes datos:

• El nombre del proyecto.

• Una justificación de la relación directa del proyecto con la ciberseguridad.

• El importe total en euros de la financiación recibida por el proyecto con cargo a fondos europeos o programas nacionales de I+D+i.

• La forma de participación en el proyecto.

Subcriterio a.3.

Nombre: Historial de colaboraciones con administraciones públicas, universidades o centros tecnológicos en ámbitos relacionados.

Valoración máxima asignable a este subcriterio: 2 puntos.

Descripción:

Se valorará las colaboraciones que haya establecido la entidad solicitante que cumplan con los siguientes requisitos:

1. La colaboración debe haberse regulado mediante un convenio u otro instrumento jurídicamente vinculante para las partes intervinientes que establezca obligaciones concretas para estas y que no posea carácter contractual.

2. Los objetivos de la colaboración o las actividades realizadas en el marco de esta deberán tener relación directa con, al menos, una de las siguientes materias:

a) Ciberseguridad.

b) Inteligencia Artificial.

c) IoT (Internet de las cosas).

d. OT (tecnologías de la operación).

e) 5G.

f) 6G.

Para que una colaboración pueda ser objeto de valoración, la entidad solicitante deberá indicar en la Memoria Técnica todos los siguientes datos:

• La forma jurídica usada para formalizar la colaboración (por ejemplo: convenio).

• El nombre de la colaboración.

• Entidad o entidades con las que se firmó la colaboración.

Subcriterio a.4.

Nombre: Certificaciones o reconocimientos en el ámbito de la ciberseguridad.

Valoración máxima asignable a este subcriterio: 4 puntos.

00323330

Descripción:

Se valorará la posesión por la entidad solicitante de certificaciones o acreditaciones relacionadas de forma directa con la ciberseguridad.

Para poder ser valoradas, las certificaciones o acreditaciones deberán estar otorgadas por entidades independientes y estar vigentes en el momento de finalización del plazo de presentación de solicitudes establecido para la siguiente convocatoria.

Las entidades podrán alegar para su valoración un máximo de cuatro (4) acreditaciones o certificaciones, indicando:

• El nombre completo de la misma

• La justificación de su relación con la ciberseguridad.

Las acreditaciones o certificaciones alegadas serán objeto de estudio por la Comisión Técnica de Evaluación con objeto de determinar si procede o no su valoración.

Las certificaciones o acreditaciones deberán estar expedidas a nombre de la entidad solicitante.

Subcriterio b.1

Nombre: Nivel de adecuación de las actividades propuestas a los objetivos del laboratorio.

Valoración máxima asignable a este subcriterio: 5 puntos.

Descripción:

Se valorará la adecuación de las actividades propuestas en el apartado 4.1 «Propuesta de las actividades a realizar en el Marco del Convenio por la Entidad» de la Memoria Técnica aportada por la entidad solicitante conforme al Anexo II de la convocatoria, teniendo en cuenta:

1. La adecuación de todas las actividades propuestas a los objetivos del laboratorio.

2. La justificación que aporte la entidad solicitante del carácter original, innovador o diferenciador de su propuesta y su contribución a los objetivos del laboratorio.

Subcriterio b.2.

Nombre: Metodología prevista para la implantación, gestión y prestación de los servicios del laboratorio.

Valoración máxima asignable a este subcriterio: 5 puntos.

Descripción:

Se valorará la adecuación de la metodología propuestas en el apartado 4.2 «Descripción de la metodología propuesta para la implantacion, Gestión y Prestación de los Servicios» de la Memoria Técnica aportada por la entidad solicitante conforme al Anexo II de la convocatoria, teniendo en cuenta:

1. La adecuación de la metodología a los objetivos del laboratorio.

2. La medida en que la metodología propuesta puede conseguir de forma plena los objetivos del laboratorio.

3. El nivel de detalle en las descripciones de los elementos y procesos de la metodología propuesta que sean adecuados a los objetivos del laboratorio.

Lo indicado en la Memoria Técnica sobre la metodología propuesta no será vinculante para la Agencia Digital de Andalucía, debiendo establecerse de forma expresa la metodología a emplear a través de lo indicado en el convenio que esta firme con la entidad adjudicataria y los acuerdos que entre ambas se establezcan a tal efecto con posterioridad.

Subcriterio c.1.

Nombre: Estrategia de sostenibilidad económica en la fase 2 del convenio.

Valoración máxima asignable a este subcriterio: 4 puntos.

00323330

Descripción:

Documento que describa la estrategia de sostenibilidad durante la 2.ª fase del convenio, en la que la aportación de los fondos del PRTR realizada por la ADA ha finalizado.

Subcriterio c.2.

Nombre: Acciones previstas de transferencia de conocimiento y colaboración con el ecosistema.

Valoración máxima asignable a este subcriterio: 2 puntos.

Descripción:

Se valorará el compromiso de realización de actividades de transferencia del conocimiento y de colaboración con el ecosistema andaluz de la ciberseguridad, del tipo:

1. Realización de actividades de formación

2. Elaboración y publicación documentos sobre las materias objeto del laboratorio a que se refiere la presente convocatoria. La publicación podrá realizarse:

- Por la propia entidad solicitante o a través de otras entidades.

- En revistas especializadas, u otros tipos de medios especializados, en materia de tecnología o ciberseguridad.

3. Elaboración y publicación para su acceso universal y gratuito de uno o varios vídeos con contenidos especializados sobre las materias objeto del laboratorio a que se refiere la presente convocatoria.

4. Participación en asociaciones y fundaciones de ámbito andaluz o cuyo ámbito incluya varias localidades de la Comunidad Autónoma de Andalucía cuya área de actividad sea la ciberseguridad durante todo el periodo de vigencia del convenio.

5. Participación en grupos de trabajo permanentes sobre ciberseguridad de asociaciones y fundaciones de ámbito andaluz o cuyo ámbito incluya varias localidades de la Comunidad Autónoma de Andalucía cuya área de actividad sea la ciberseguridad durante todo el periodo de vigencia del convenio.

6. Otros compromisos que asuma la entidad solicitante en materia de transferencia de conocimiento y colaboración con el ecosistema, que habrán de ser descritos en la Memoria Técnica, elaborada conforme al Anexo II de la presente convocatoria.

Subcriterio c.3.

Nombre: Plan de comunicación y visibilidad del laboratorio.

Valoración máxima asignable a este subcriterio: 2 puntos.

Descripción:

Se valorará la inclusión de un plan de comunicación y visibilidad del laboratorio durante el tiempo de vigencia del convenio objeto de la presente convocatoria. En dicho plan se valorará que se incluyan:

• Organización y realización por la entidad solicitante de jornadas y seminarios de difusión del laboratorio y su actividad y resultados.

• Participación de la entidad solicitante en congresos y jornadas en las que intervenga en mesas redondas y ponencias para dar visibilidad y promocionar el laboratorio o exponer su actividad y resultados.

La entidad solicitante no podrá requerir de las personas o entidades a las que vayan dirigidas dichas actividades ningún tipo de contraprestación económica por asistencia, participación o acceso a las mismas.

9.3.4. Documentación a aportar para la valoración.

Para la valoración de los criterios establecidos en la presente convocatoria, las empresas solicitantes deberán aportar la información requerida a tal efecto en el formato establecido en el Anexo II, «Memoria Técnica» , de la presente convocatoria.

La información que se consigne en dicha Memoria Técnica tendrá consideración de declaración responsable y establecerá obligaciones para la entidad solicitante en caso de resultar adjudicataria de la presente convocatoria.

00323330

La inclusión de datos falsos o incorrectos en dicha Memoria Técnica o el incumplimiento de los compromisos adquiridos en ella en caso de resultar adjudicataria podrán dar lugar a la resolución del convenio objeto de la presente convocatoria por causas imputables a la entidad solicitante, con las consecuencias económicas, administrativas y de cualquier otro tipo que ello pudiera conllevar, sin perjuicio de cualesquiera otras responsabilidades que pudieran ser exigibles y cualesquiera otras actuaciones a las que pudieran dar lugar, conforme a la normativa aplicable.

En todo caso, la Comisión Técnica de Evaluación podrá requerir a las entidades solicitantes la documentación justificativa o las aclaraciones que precises para la realización de sus funciones, debiéndose proporcionar dicha documentación en un plazo de tres días a partir de la realización de la correspondiente comunicación.

9.3.5. Formalización del convenio.

Una vez acordados los términos de colaboración, se procederá a la remisión del borrador de convenio a la entidad seleccionada para su firma. El convenio será suscrito por el representante legal de la entidad y la persona titular de la Dirección Gerencia de la Agencia Digital de Andalucía.

9.3.6. Comisión Técnica de Evaluación:

La Comisión Técnica responsable de la evaluación de las solicitudes estará compuesta por:

- Subdirector/a de Planificación, Estrategia y Ciberseguridad de la Agencia Digital de Andalucía.
- Consejero/a técnico del Centro de Ciberseguridad de Andalucía.
- Un/a técnico/a del Servicio de Ciberseguridad de la ADA o de la Oficina Técnica de seguimiento del programa Retech.
- Una persona representante de la Secretaría General de la ADA.

Esta comisión podrá contar con el apoyo técnico de personal experto externo en caso de ser necesario, y podrá solicitar cuanta información o aclaraciones considere oportunas para la correcta valoración de las solicitudes.

9.3.7. Proceso de selección.

La Comisión Técnica de Evaluación podrá no realizar el análisis de aquellos requisitos alegados o de aquellas solicitudes presentadas cuyo estudio no afecte al resultado final del proceso de selección.

10. RÉGIMEN JURÍDICO

El Convenio resultante de la presente invitación se regirá por la siguiente normativa:

a) Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia.

b) Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia.

c) Orden HFP/1031/2021, de 29 de septiembre, por la que se establece el procedimiento y formato de la información a proporcionar por las entidades del sector público estatal, autonómico y local para el seguimiento del cumplimiento de hitos y objetivos del Plan de Recuperación, Transformación y Resiliencia.

d) Orden HFP/55/2023, de 24 de enero, relativa al análisis sistemático del riesgo de conflicto de interés en los procedimientos que ejecutan el Plan de Recuperación, Transformación y Resiliencia.

e) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

f) Decreto-ley 3/2021, de 16 de febrero, por el que se adoptan medidas de agilización administrativa y racionalización de los recursos para el impulso a la recuperación y resiliencia en el ámbito de la Comunidad Autónoma de Andalucía.

g) Real Decreto-ley 36/2020, de 30 de diciembre, por el que se aprueban medidas urgentes para la modernización de la Administración Pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia.

00323330

Toda la normativa nacional y europea vinculada a fondos NextGenerationEU y las demás que resulten de aplicación.

11. PUBLICIDAD Y DIFUSIÓN

Las partes deberán dar visibilidad a la financiación europea recibida y a la participación institucional de la Agencia Digital de Andalucía, en cumplimiento de lo dispuesto en el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia, así como en las disposiciones recogidas en la Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia, y en las Directrices de comunicación del PRTR aprobadas por la Administración General del Estado.

En todas las actuaciones de difusión, documentación, materiales formativos, presentaciones públicas, publicaciones y soportes digitales o físicos vinculados al proyecto, deberá incluirse de forma visible:

- El logotipo oficial del Plan de Recuperación, Transformación y Resiliencia (PRTR).
- El emblema de la Unión Europea, junto con la mención: «Financiado por la Unión Europea – NextGenera-tionEU».
- El logotipo institucional de la Agencia Digital de Andalucía como entidad promotora.

Estos elementos deberán respetar las versiones gráficas oficiales y los manuales de identidad visual establecidos por las autoridades competentes, no pudiendo ser alterados ni modificados. La inadecuada visibilidad o la misión de estos requisitos podrá dar lugar a requerimientos de subsanación o, en su caso, a la pérdida de financiación, conforme a lo previsto en la normativa aplicable.

12. MÁS INFORMACIÓN

Para cualquier consulta, las entidades interesadas podrán dirigirse a:
Agencia Digital de Andalucía /Centro de Ciberseguridad
Correo electrónico: retech.cian@juntadeandalucia.es

Sevilla, 1 de julio de 2025.- El Director Gerente, Raúl Jiménez Jiménez.

00323330