Annex 3: Short description of the measures contributing to the general objectives

Index

Section 4: Short description of the measures contributing to the general objectives

4.1 Introduction

This section provides an in-depth description of some of the measures implemented to contribute to the general objectives. It includes a list of specific activities, both completed and planned, along with a comprehensive implementation timeline in the national roadmaps. Budget details, distinguishing between national and EU funds, or human resources deployed are also provided, as well as the expected impact and its timing.

4.2 Description of the measures

4.2.1 Digital Citizenship

<table>
<tr><td colspan="2">Name of the measure: Agreements to promote the implementation of the Digital Bill of Rights with stakeholders</td></tr>
<tr><td>Responsible unit: RED.es</td><td>New measure: Yes</td></tr>
<tr><td colspan="2">Short description: According to the Spanish Digital Rights Charter (July 2021) and the Joint Declaration on Digital Rights and Principles for the Digital Decade by the European Parliament, Council, and Commission, Spain incorporated the implementation of these documents into its 2026 digital strategy (July 2022) to ensure the protection of fundamental rights in the digital world. To achieve this goal, in May 2023, an invitation was issued, calling upon non-profit entities and other stakeholders to submit proposals for the development of digital rights in the following areas:
Rights of freedom, protection and security in the digital world
Digital world equality rights
Participation rights
Digital rights in the workplace and business environment
Rights in specific environments
Rights in new digital environments.
The agreements aim to understand the demands and perspectives of stakeholders, mobilize and raise awareness among the population regarding digital rights, as well as assess the factual situation of digital rights at the national, European, and international levels, in order to continue developing actions and public policies to guarantee and promote them. These entities will contribute with their expertise, mobilization capabilities, and awareness efforts to advance digital rights.

This measure will benefit the general public, governmental and non-governmental entities, researchers, and other stakeholders by establishing an ecosystem of stakeholders capable of proposing legislative and non-legislative measures to ensure fundamental rights in the digital environment.</td></tr>
<tr><td colspan="2">List of concrete actions implemented/planned:
(May 2023) Launch of collaboration proposals from non-profit entities.
(July 2023) Selection of collaboration proposals from non-profit entities.
(December 2023) Implementation of a stakeholder system for the development of legislative and non-legislative proposals.</td></tr>
</table>

- (2024-2026) Analysis and exploration of digital rights status in specific domains.
- (2024-2026) Gathering demands and proposals from experts for the development of legislative and non-legislative proposals.
- (2024-2026) Dissemination and visibility of digital rights in specific domains.

General objective: Digital citizenship (digital rights).

Link to the objective: The measure is linked to the objective: Digital citizenship (digital rights).

Reference to RRP or other relevant documents/strategies: Component 19: National Digital Skills Plan (digital skills) C19.I1 Transversal Digital Skills.

Tentative timeline: Starting in May 2023 and expected to finish in June 2026.

Budget allocated or planned and, if relevant, other resources – including human resources – allocated:

Public investment: EUR 4.890 million / Already allocated: EUR 4.890 million.

- - Thereof from EU sources: EUR 4.890 million / Already allocated: EUR 4.890 million

Private investment: EUR 1.2225 million

Expected impact and related timing: The implementation of this measure will impact at least 181 organizations operating in the field of digital rights. Additionally, it will benefit the general public, governmental and non-governmental entities by:

- The development of legislative and non-legislative measures.
- The raise of awareness among stakeholders.
- Dissemination of digital rights.
- The promotion of digital rights in Latin America

Name of the measure: Agreements to establish a Digital Rights Observatory space

Responsible unit: RED.es	**New measure:** Yes

Short description: In the context of the Spain Digital 2025 Strategy, the Government of Spain presented the Digital Rights Charter (July 2021). Subsequently, the European Parliament, Council, and Commission jointly issued the Joint Declaration on Digital Rights and Principles for the Digital Decade, aiming to interpret and adapt existing law to the digital environment without normative character.

The Spain Digital 2026 Strategy (July 2022) included the implementation of both documents to safeguard fundamental rights in the digital world. To achieve this objective, an Invitation was issued to sign Agreements with non-profit organizations and other stakeholders to collaborate with red.es in the establishment of a Digital Rights Observatory (May 2023)."

The Digital Rights Observation Space aims to establish an open, inclusive, and participatory observatory for promoting knowledge, discussion, and the dissemination of Digital Rights among the general public and public and private entities, both at the national and international levels. As a result, the agreement between the parties will reflect their mutual interest in promoting the culture of Digital Rights and its impact on society, as well as its full integration into digital transformation processes. This work will be carried out through the development of reports, studies, and outreach programs.

This measure will benefit the general public, businesses, public administrations, and researchers by raising awareness in the field of digital rights. Additionally, stakeholders will have the opportunity to benefit from their involvement in an open space for knowledge and discussion.

List of concrete actions implemented/planned:

- (May 2023) Launch of collaboration proposals from non-profit entities
- (July 2023) Selection of collaboration proposals with non-profit entities.
- (December 2023) Launch of the Digital Rights Observatory.
- (2024-2026) Preparation of reports and studies on the status of digital rights.
- (2024-2026) Dissemination and discussion of the progress of digital rights.
- (2026-2030) Maintenance of the Digital Rights Observatory.

General objective: Digital citizenship (digital rights).

Reference to RRP or other relevant documents/strategies: Component 19. National Digital Capacities Plan. C19.I1 Transversal Digital Skills.

Tentative timeline: Starting in May 2023 and expected to finish in June 2026. Thereafter, the Observatory will be maintained until 2030.

Budget allocated or planned and, if relevant, other resources – including human resources – allocated:
Public investment (2023- 2026): EUR 3.825 million / Already allocated: EUR 3.825 million

- Thereof from EU sources: EUR 3.825 million / Already allocated: EUR 3.825 million

Private investment (if known): EUR 0.956250 million.

Expected budget (2026- 2030): EUR 6 million.

Expected impact and related timing: This measure will have an impact on the general public, governmental and non-governmental entities, and stakeholders, with the formal support of at least 22 organizations in the following areas:

- Raising awareness and promoting the understanding of digital rights culture among citizens.
- Creating sources of information for governmental and non-governmental decision-making.
- Integration of stakeholders' need in the development of public policies.
- Rasising awareness and promoting understanding of digital rights culture among citizens.
- Making national and European efforts in promoting Digital Rights visible.

- Establishing mechanisms to increase participation and formal adherence to the promotion of the Digital
- Rights Charter.

Name of the measure: AI Regulatory Sandbox

Responsible unit: SGIATHD	**New measure:** Yes

Short description: The AI Regulatory Sandbox, co-developed with the European Commission, is a digital platform that fosters collaboration between authorities and AI developers to define best practices for future European AI regulation. It aims to create guidelines, particularly for SMEs and startups, by studying the operability of future regulations, documenting obligations of AI providers, and facilitating proper monitoring methods. The initiative also encourages cooperation among European actors, inviting member states to participate, while also initiating consultations with the Spanish AI Supervision Agency.

This pilot proposed by the Spanish government will study the operability of the requirements of the future regulation, as well as the conformity assessments or post-marketing activities.

List of concrete actions implemented/planned:

- 2022: Sandbox Launch within the UE
- December 2022: public licitation process related to consultancy support for the development of the sandbox published.

  https://contrataciondelestado.es/wps/poc?uri=deeplink%3Adetalle_licitacion&idEvl=B50kunPByvoSugstABGr5A%3D%3D
- July 2023: call for participants to be published.
- 2024-2025: IA Pilot execution, proof development, guidelines and best practices; quality brand and public event. Website launch.
- 2026: applicable regulation.

Digital target or general objective: Digital citizenship

Link to the objective: The AI Regulatory Sandbox supports Digital Citizenship by fostering a human-centered, inclusive, and transparent approach to AI development and regulation. It safeguards fundamental rights by shaping best practices for AI technologies, ensures inclusivity by focusing on SMEs and startups, and promotes transparency through European cooperation. By examining the operability of future regulations, it contributes to security and interoperability within the digital environment. Lastly, by involving various member states and agencies, it reinforces accessibility, ensuring secure, rights-respecting AI technologies are accessible throughout the Union.

Reference to RRP or other relevant documents/strategies: Component 16: National Artificial Intelligence Strategy C16.R1 National AI Strategy
Tentative timeline: The programme started in June 2022 with the official launch in Brussels, and it will be completed during the Spanish presidency of the UE Council. In July 2023 the signing of the contract of the consultancy services is expected to be signed. The programme is expected to be available until Q1of 2026.
Budget allocated or planned and, if relevant, other resources – including human resources – allocated: Call for tender: 43.000.000 €
Expected impact and related timing: It is expected to have 15-20 participants in the Regulatory Sandbox, covering different kind of companies in terms of size, AI technology used, business sector, maturity of their high-level risk systems (systems already in the market or soon to be launched). It is also expected to generate a lot of collaboration with other Member States, regulatory agencies, industry and human rights associations and research entities. In this sense, a governance framework has been defined to orchestrate collaboration in the sandbox.

Name of the measure: "UNICO – Demanda Rural"	
Responsible unit: SETID	**New measure:** No
Short description: The program's objective is to provide access to 100 Mbps broadband in areas without coverage (mainly remote rural areas) on affordable terms. In particular, the program will focus on providing to the end user an affordable broadband connection service at a minimum transmission speed of 100 Mbps downstream from a fixed location, mainly in remote, dispersed and sparsely populated rural areas, as well as covering the costs directly related to the registration of end users to access this service, which includes the acquisition of user equipment, its installation and commissioning regardless of the technology used.	
List of concrete actions implemented/planned: The budget of this program is intended for the implementation of the following actions: - €44.8 million for the configuration of a network resources platform that allows the provision of 100 Mbps, divided into two annuities: €23.7 million in 2022 and €21.1 million in 2023 (cost of the action for 2023, 2024 and 2025). - €40M to cover 100% of the cost of installation and end-user registration, with the following distribution: €15M in 2022 and €25M in 2023 (cost of action for 2023, 2024 and 2025).	

Digital target or general objective: Digital citizenship
Link to the target or objective: There are still certain remote, dispersed and sparsely populated rural areas, which do not yet enjoy adequate coverage of terrestrial high-speed broadband services. For example, there are specific areas where operators have not deployed their networks and do not have broadband service offerings comparable to those contracted by the majority of the population. In these areas, citizens and companies can only access high-speed broadband access services with an extra cost on the prices paid by most users. This program aims to achieve the target set in the Digital Spain 2026 Agenda of 100% of the population with 100 Mpbs coverage by 2025.
Reference to RRP or other relevant documents/strategies: This program is aligned with the implementation of the Digital Spain 2026 Agenda, whose first strategic axis is Digital Connectivity, which seeks to guarantee adequate digital connectivity for the entire population, promoting the disappearance of the digital divide between rural and urban areas. The objective is that 100% of the population has 100 Mbps coverage in 2025. The national Digital Infrastructures and Connectivity Plan for society develops the mentioned first axis of the Digital Spain 2026 Agenda. The objective is the use of connectivity and digitalization as tools to contribute to closing the existing digital gaps for socioeconomic, gender, generational, territorial or environmental reasons. It will contribute to Component 15 of the Recovery, Transformation and Resilience Plan, specifically to investment 1 - Promote territorial vertebration through the deployment of networks: Extension of ultra-fast broadband. The program will contribute to milestones: - #236: Award of the project of extending ultra-fast broadband - #237: Completion of the aforementioned projects.
Tentative timeline: Aids awarded in May 2023. Projects have to be finished by December 31, 2025.
Budget allocated or planned and, if relevant, other resources – including human resources – allocated: Public investment: EUR 76,32 million / Already allocated: EUR 76,32 million - Thereof from EU sources: EUR 76,32 million / Already allocated: EUR 76,32 million
Expected impact and related timing: The rule will have a positive economic impact derived from the promotion of connectivity in eligible areas, having calculated that the number of 12,000 current end customers who access in these areas at speeds of at least 100 Mbps would increase by the end of the program (2025) up to 56,250 final

customers, who would benefit from costs similar to those assumed by citizens for this service in other areas of the Spanish territory.

The impact on SMEs is also considered positive, as the difficulties inherent in unbundling in increasingly rural and dispersed areas increase the opportunity for SMEs in the sector to be subcontracted by the beneficiaries or even to become retail operators.

Name of the measure: "UNICO – Bono social"	
Responsible unit: SETID	**New measure:** No
Short description: The UNICO program stands for Universalización de Infraestructuras Digitales para la Cohesión (i.e., Digital Infrastructure Universalization for Cohesion, in English). The objective of the measure "Bono social" is to provide connectivity vouchers for people or families classified as vulnerable, for the acquisition of a broadband connection package. It has a budget of €30M.	
List of concrete actions implemented/planned: "Bono social" program is led by the Autonomous Communities. Currently 3,033 resolutions have been executed, with 10,344 requests. The resolution of all requests is expected by the end of 2024.	
Digital target or general objective: Digital citizenship	
Link to the target or objective: The aid to vulnerable people aims to foster social cohesion and ensure and effective digital citizenship for everybody in Spain.	
Reference to RRP or other relevant documents/strategies: It will contribute to Component 15 of the Recovery, Transformation and Resilience Plan, specifically to investment 3 - Connectivity vouchers for SMEs and vulnerable groups. The program will contribute to milestone #239 - Connectivity vouchers for SMEs and vulnerable groups.	
Tentative timeline: 2022-2024	
Budget allocated or planned and, if relevant, other resources – including human resources – allocated: Public investment: EUR 30 million / Already allocated: EUR 30 million - Planned: EUR 0 million - Thereof from EU sources: EUR 30 million / Already allocated: EUR 30 million - Planned: EUR 0 million	
Expected impact and related timing: Granting of at least 125 000 connectivity vouchers for individuals or families classified as 'vulnerable' (to purchase a broadband connection package with the most appropriate technology) by the end of 2024.	

Name of the measure: "UNICO – Bono pyme"	
Responsible unit: SETID	**New measure:** No
Short description: The UNICO program stands for Unversalización de Infraestructuras Digitales para la Cohesión (i.e., Digital Infrastructure Universalization for Cohesion, in English). The objective of the measure "Bono pyme" is to provide connectivity vouchers to small and medium-sized enterprises and the self-employed (the vouchers will consist of two elements, 100 Mbps connectivity and a set of value-added services, VPN and cybersecurity). It has a budget of €50M.	
List of concrete actions implemented/planned: "Bono pyme" program will be led by Red.es, entity attached to the Secretary of State for Digitalization and Artificial Intelligence (SEDIA), while SETID grants a monetary contribution to Red.es. The regulatory bases and call for aid have already been published, the full amount of vouchers will be granted by the end of 2024.	
Digital target or general objective: Digital citizenship	
Link to the target or objective: The aid to small and medium-sized enterprises and self-employed workers to improve their digital connectivity and the services linked to it. The program aims to minimize the barrier that the cost of such connectivity and services represents for their digital transformation.	
Reference to RRP or other relevant documents/strategies: It will contribute to Component 15 of the Recovery, Transformation and Resilience Plan, specifically to investment 3 - Connectivity vouchers for SMEs and vulnerable groups. The program will contribute to milestone #239 - Connectivity vouchers for SMEs and vulnerable groups.	
Tentative timeline: 2023-2024	
Budget allocated or planned and, if relevant, other resources – including human resources – allocated: Public investment: EUR 50 million / Already allocated: EUR 50 million - Planned: EUR 0 million - Thereof from EU sources: EUR 50 million / Already allocated: EUR 50 million - Planned: EUR 0 million	
Expected impact and related timing: Granting of at least 11 000 connectivity vouchers for SMEs (the vouchers will consist of two distinct elements, 100 Mbps connectivity and a set of value-added services, VPN and cybersecurity) by the end of 2024.	

Name of the measure: "FEDER BA 100 Mbps"	
Responsible unit: SETID	**New measure:** Yes
Short description: Aid scheme for end users to contract broadband connections at more than 100 Mbps, provided by any registered operator. Update and extension of the "Royal Decree 898/2017, of October 6, which regulates the direct granting of subsidies for the contracting of high-speed fixed broadband access services at 30 megabits per second", to update the objective to speeds of more than 100 Mbps and expand its scope. This program is financially supported by ERDF (FEDER in Spanish) funding.	
List of concrete actions implemented/planned: No actions are planned so far since the program is expected to start in 2026.	
Digital target or general objective: Digital citizenship	
Link to the target or objective: The program aims to achieve the target set in the Digital Spain 2026 Agenda of very high-speed coverage for 100% of the population by 2025	
Reference to RRP or other relevant documents/strategies: The program is part of the ERDF funds program. This measure is aligned with the implementation of the Digital Spain 2026 Agenda, whose first strategic axis is Digital Connectivity, which seeks to guarantee adequate digital connectivity for the entire population, promoting the disappearance of the digital divide between rural and urban areas and advancing in the universalization of ultra-fast (gigabit) coverage throughout the national territory, as well as contributing to the transformation of productive sectors.	
Tentative timeline: The program is expected to start in 2026, and it is expected to be finished by 2029.	

Budget allocated or planned and, if relevant, other resources – including human resources – allocated:
Total investment: EUR 136 million
- Public investment: EUR 118 million / Already allocated: EUR 0 million - Planned: EUR 118 million
  o Thereof from EU sources: EUR 100 million / Already allocated: EUR 0 million - Planned: EUR 100 million
  o Thereof from national sources: EUR 18 million / Already allocated: EUR 0 million - Planned: EUR 18 million
- Private investment: EUR 18 million	

Expected impact and related timing: By 2029, the program is expected to achieve approximately 95k installations of broadband. Within those, 95% are expected to subscribe broadband services, which would account for approx. 90k subscriptions.	

4.2.2 Fostering leadership and sovereignity

Name of the measure: "UNICO – 6G I+D"	
Responsible unit: SETID	**New measure:** No
Short description: The UNICO program stands for Universalización de Infraestructuras Digitales para la Cohesión (i.e., Digital Infrastructure Universalization for Cohesion, in English). In particular, this program aims to create a R+D and innovation ecosystem around 5G Advanced and 6G. To this end, three subprograms of aid are included to promote the development of these technologies: - Direct aid to public universities and public R+D centers, aimed at Spanish groups that had participated in projects of the 5G PPP initiative of Horizon 2020, in order to reinforce their leadership in cellular research, so that they are positioned at the forefront of 6G development. The aid granted involves intense public-private collaboration, since the beneficiaries must allocate at least 70% of the funds received to subcontracting, with a minimum of 15% directed to the subcontracting of Spanish SMEs. - One subprogram aimed at financing research infrastructures and acquisition of scientific-technical equipment in the field of 5G Advanced and 6G, whose recipients are public universities and public R+D centers. - A second subprogram aimed at financing industrial research and experimental development projects in 5G Advanced, with an intermediate level of technological maturity, led by Spanish private companies.	
List of concrete actions implemented/planned: - December 2021: award of aid to 12 public universities and public R+D centers for EUR 94,5 million to carry out 113 R+D projects in 5G Advanced and 6G and to develop a Plan for promoting Telecommunication studies. - August 2022: Regulatory Bases and First Call published with a budget of EUR 116 million for financing 2 subprograms: (1) research infrastructures and acquisition of scientific-technical equipment in the field of 5G Advanced and 6G, aimed at public universities and public R+D centers; (2) industrial research and experimental development projects in 5G Advanced, with an intermediate level of technological maturity, led by Spanish private companies. - December 2022: Publication of the Second Call with a budget of EUR 62 million. - June 2023: Final Resolution of the 1st call, awarding EUR 48,82 million to 48 projects. - October 2023: Provisional Resolution of 2nd call published	
Digital target or general objective: Promote leadership and sovereignty	
Link to the target or objective: Investing in 6G technology will foster Spain's and EU's leadership and sovereignty from various angles including reducing dependency	

on foreign technology, strengthening EU/national security, and bolstering economic resilience and influence.

Reference to RRP or other relevant documents/strategies: This measure is aligned with the implementation of the Digital Spain 2026 Agenda, whose second strategic axis points to boost 5G technology as a key task for the economic development and digital transformation of the country.

As part of the Digital Spain 2026 Agenda, the national Strategy for the promotion of 5G Technology includes actions related to foster innovation on 5G technology, publishing grant calls for companies, research entities and universities to boost innovation on 5G and the future 6G.

These grants are also aligned with the State Plan for Scientific, Technical and Innovation Research 2021-2023 (PEICTI), integrated into the Spanish Strategy for Science, Technology and Innovation 2021-2027.

The program also contributes to Component 15 of the Recovery, Transformation and Resilience Plan, specifically to investment 6: 5G deployment: networks, technological change and innovation. The program will contribute to milestones:

- #243: Award of grants to support 5G and 6G related R&D projects for innovation ecosystems (200 projects) and 5G cyber security ecosystems.
- #244: Completion of the aforementioned projects.

Tentative timeline: 2021-2026

Budget allocated or planned and, if relevant, other resources – including human resources – allocated:

Public investment: EUR 205 million / Already allocated: EUR 143.32 million - Planned: EUR 62 million

- Thereof from EU sources: EUR 205 million / Already allocated: EUR 143.32 million - Planned: EUR 62 million

Private investment: EUR 10 million (expected)

Expected impact and related timing: It will favour the creation of an ecosystem based in Spain that attracts investment, that encourages the emergence of startups and innovative companies for the development of equipment and services in 5G Advanced, that generates employment and stable and high-quality jobs. Intense public-private collaboration is also expected.

Name of the measure: "UNICO – I+D Cuántica"	
Responsible unit: SETID	**New measure:** No
Short description: The UNICO program stands for Universalización de Infraestructuras Digitales para la Cohesión (i.e., Digital Infrastructure Universalization for Cohesion, in English). This subprogram aims to develop space capabilities needed to design, develop and build the first quantum key distribution (QKD) mission on board a geostationary satellite.	
List of concrete actions implemented/planned: Evolution of expenditure on aid granted: • Actual expenditure 2022: 25.000.000€ • Allocated expenditure 2023: 100.000.000€	
Digital target or general objective: Promote leadership and sovereignty	
Link to the target or objective: This program is linked with achieving the objective to be at the cutting edge of quantum capabilities by 2030 and also fosters EU's leadership and sovereignty in that area.	
Reference to RRP or other relevant documents/strategies: It is part of the Aerospace PERTE – Satellite and Terrestrial systems for quantum communications. They contribute to Component 15 of the Recovery, Transformation and Resilience Plan, specifically to investment 5 - Deployment of cross-border digital infrastructures. The program will contribute to milestones: - #241: Award of projects regarding R&D&I for strengthening capabilities on quantum communications and secure satellite communications - #242: Completion of the aforementioned projects.	
Tentative timeline: 2022-2026	
Budget allocated or planned and, if relevant, other resources – including human resources – allocated: Public investment: EUR 125 million / Already allocated: EUR 125 million - Planned: EUR 0 million - Thereof from EU sources: EUR 125 million / Already allocated: EUR 125 million - Planned: EUR 0 million	
Expected impact and related timing: By 2026, the objective is to have achieved the development of the space technological capabilities necessary for the development of the first geostationary satellite with quantum keys.	

Name of the measure: "UNICO - 5G Ciberseguridad"	
Responsible unit: SETID	**New measure:** No
Short description: The UNICO program stands for Universalización de Infraestructuras Digitales para la Cohesión (i.e., Digital Infrastructure Universalization for Cohesion, in English). This subprogram provides for the creation of a public center to ensure compliance with the requirements, among others certification, derived from the 5G Cybersecurity Law, which in turn implements the "European Union Toolbox for the security of 5G networks", covering the needs left by the situation previously contemplated. Furthermore, this program will support the creation of ecosystems for cybersecurity in the field of 5G and avoid the risks derived from it.	
List of concrete actions implemented/planned: Execution in 2022: €33.8M Planned execution in 2023: €15M	
Digital target or general objective: Promote leadership and sovereignty	
Link to the target or objective: Cybersecurity is essential for EU's leadership and sovereignty. It helps protect critical infrastructure, prevents financial disruptions, and preserves data privacy and sovereignty. It also fosters technological innovation and ensures EU's resilience in the face of evolving digital challenges.	
Reference to RRP or other relevant documents/strategies: They contribute to Component 15 of the Recovery, Transformation and Resilience Plan, specifically to investment 6. The program will contribute to milestones: - #243: Award of projects to support 5G cybersecurity ecosystems. - #244: Completion of the aforementioned projects.	
Tentative timeline: These projects are meant to be finish by 30 June 2026.	
Budget allocated or planned and, if relevant, other resources – including human resources – allocated: Public investment: EUR 48.8 million / Already allocated: EUR 33.8 million - Planned: EUR 15 million - Thereof from EU sources: EUR 48.8 million / Already allocated: EUR 33.8 million - Planned: EUR 15 million	
Expected impact and related timing: Enhanced cybersecurity in 5G public networks.	

Name of the measure: "UNICO 5G Sectorial"	
Responsible unit: SETID	**New measure:** No
Short description: The UNICO program stands for Universalización de Infraestructuras Digitales para la Cohesión (i.e., Digital Infrastructure Universalization for Cohesion, in English). The "5G Sectorial" subprogram aims to promote the development of an ecosystem between companies, operators and other agents to facilitate the application of 5G technology in an agile and fast way in key economic sectors in our country. It is intended to promote a productive fabric that thinks, creates and designs applications and services that take advantage of this technology, exercising a driving and demonstrative role for the specific application sector, and thus reinforce the role of Spain as one of the driving poles of digitalization through the application of 5G technology throughout the EU.	
List of concrete actions implemented/planned: Expenditure executed 2021: €26.2M for ADIF (Rail Infrastructure Administrator) on logistic terminals. Expenditure executed 2022: €35.7M, including €20.7M on Ministry of Defense sectorial projects and €15M on emergencies. Expenditure allocated 2023: €15M on intelligence; and €19.9M (call of 2022) and €9.5M (1st call 2023) on various industry use cases. Additional expenditure planned 2023: €6.2M (2nd call 2023) on various industry use cases.	
Digital target or general objective: Promote leadership and sovereignty	
Link to the target or objective: This call aims to promote the development of ecosystems between operators, technology and solution providers and other agents involved, all to facilitate the application of this technology in a fast and agile way in key economic sectors in our country – which will foster its resilience and an overall EU leadership and sovereignty.	
Reference to RRP or other relevant documents/strategies: These efforts are aligned with the implementation of the Digital Spain 2026 Agenda, whose second strategic axis points to the promotion of 5G technology as a key task for the economic development and digital transformation of the country. Specifically, measure 9: 5G in sectoral digitalization tractor projects, with the objective, among others, of identifying and financing 5G use cases in tractor projects of companies that occupy strategic positions within the productive fabric of each sector. These grants are also aligned with the State Plan for Scientific, Technical and Innovation Research 2021-2023 (PEICTI), integrated into the Spanish Strategy for Science, Technology and Innovation 2021-2027.	

Finally, they also contribute to Component 15 of the Recovery, Transformation and Resilience Plan, specifically to investment 6. The program will contribute to milestones:

- #243: Award of 5G deployment projects in in key economic activities essential services (43 connectivity projects)
- #244: Completion of the aforementioned projects.

Tentative timeline: The program started in 2021, and it is expected to be finished by June 2026.

Budget allocated or planned and, if relevant, other resources – including human resources – allocated:

Public investment: EUR 112.5 million / Already allocated: EUR 106.3 million - Planned: EUR 6.2 million

- Thereof from EU sources: EUR 112.5 million / Already allocated: EUR 106.3 million - Planned: EUR 6.2 million

Expected impact and related timing: By 2026, 5G deployed in main transportation corridors, essential services and in relevant economic activity sectors.

Name of the measure: "FEDER Pilotos 6G"	
Responsible unit: SETID	**New measure:** Yes

Short description: Public aid for the realization of pilot experiences aimed at testing the new generation of 6G mobile network technology from 2026 – when it is estimated that the previous technological developments will be completed.

This action is intended to give continuity to the measure to support the development of this technology through aid to R + D + i provided in the PRTR.

This program is financially supported by ERDF (FEDER in Spanish) funding.

List of concrete actions implemented/planned: No actions are planned so far since the program is expected to start in 2026.

Digital target or general objective: Promote digital leadership and sovereignty in the EU

Link to the target or objective: Investing in 6G technology will foster Spain's and EU's leadership and sovereignty from various angles including reducing dependency on foreign technology, strengthening EU/national security, and bolstering economic resilience and influence.

Reference to RRP or other relevant documents/strategies: These efforts are aligned with the implementation of the Digital Spain 2026 Agenda, whose second strategic axis

points to the promotion of 5G technology as a key task for the economic development and digital transformation of the country. The challenge for 2026 is to continue leading the deployment of 5G/6G technology, promoting R+D+i and encouraging the contribution of this technology to the increase in economic productivity, social progress and territorial structuring.

Tentative timeline: The program is intended to start in January 2026 and finish by 2029.

Budget allocated or planned and, if relevant, other resources – including human resources – allocated:

Total investment: EUR 50 million

- Public investment: EUR 20 million / Already allocated: EUR 0 million - Planned: EUR 20 million
    - Thereof from EU sources: EUR 20 million / Already allocated: EUR 0 million - Planned: EUR 20 million
- Private investment: EUR 30 million

Expected impact and related timing: The program is estimated to generate 10 projects. Assuming an average of 2 beneficiaries per project and 0.7 companies per beneficiary, the program is estimated to deliver aid to 14 companies by 2029.

Name of the measure: National Coordination Centre for Spain (NCC-ES)	
Responsible unit: Centro de Coordinación Nacional (NCC-ES)	**New measure:** Yes

Short description: The National Coordination Centre for Spain (NCC-ES) is part of a new European management framework consisting of the European Cybersecurity Competence Centre (ECCC) in Bucharest and a Network of 27 National Coordination Centres established by European Regulation (EU) 2021/887 of May 2021. The ECCC, together with its NCC network, have been created by the Commission in 2021 in order to increase Europe's cybersecurity capacities and competitiveness and to build a strong Cybersecurity Community.

The NCC-ES bases its activity in four main pillars:

- Support the strategic tasks of the ECCC
- Foster cross-border cooperation and preparation of joint actions
- Act as national Point at National and European level
- Improve Cooperation at National Level by promoting and intensifying dialogue in the field of research and innovation in cybersecurity

List of concrete actions implemented/planned: The NCC-ES is designed to foster a European and Spanish Cybersecurity Ecosystem, but also to ensure coordination within

the NCC network. The focus of activities is on open, agile and adaptive cooperation between different stakeholders, to promote synergies and mutual understanding. The ongoing and planned activity of the NCC-ES includes: • Act as contact point at national level • Provide knowledge, expertise and actively contribute to strategic functions considering relevant national and regional challenges for cybersecurity in different sectors • Facilitate the participation of civil society, industry, in particular start-ups and SMEs, the academic and research community and other stakeholders at national level in cybersecurity projects and actions on cross-border cybersecurity funded through any of the European Union's programmes • Provide support and guide for the stakeholders at the project's application stage, according to the rules of financial management, especially with regard to conflicts of interest • Seek synergies with relevant activities at national, regional and local level, such as, for example, national policies on research, development and innovation in the field of cybersecurity, in particular the policies set out in the national cybersecurity strategies • Promote and disseminate relevant results of the work of the Network, the Community and the Competence Centre at national, regional or local level and also managing everything related with the community members from Spain
Digital target or general objective: Improving resilience to cyberattacks, contributing to increasing risk-awareness and the knowledge of cybersecurity processes, and increasing the efforts of public and private organisations to achieve at least basic levels of cybersecurity.
Link to the target or objective: Promote digital leadership and sovereignty in the EU
Reference to RRP or other relevant documents/strategies: Component 15. Digital connectivity, promotion of cybersecurity and deployment of 5G C15.I7 Cybersecurity: Strengthening the capacities of citizens, SMEs and professionals; and Promotion of the sector ecosystem. Digital European Programme.
Tentative timeline: NCC-ES is in the cusp of the signature of a grant agreement on a European Commission Digital Europe Programme call to enhance National Coordination Centres capacity building. Said proposed project has the 1st of November, 2023, as starting date, and will last for 24 months. Nonetheless, the NCC-ES measure will carry out its activities as long as the European Cybersecurity Competence Centre and the Cybersecurity Competence Community are in place.
Budget allocated or planned and, if relevant, other resources – including human resources – allocated: Regarding the NCC-ES Digital Europe Programme Call project, its planned investment is distributed as follow:

- Thereof from national sources: Planned 596,337.75€
- Thereof from EU sources (Digital European Programme): Planned 596,337.75€

The budget projected for the next 4 years (estimation): 2,5M€

The NCC-ES will also have INCIBE personnel at its disposure in order to ensure the successful development of the listed actions related to the measure.

Expected impact and related timing: Offering support and promoting nationally to encourage participation in projects promoted by the ECCC and the European Union is something that the NCC-ES will be concerned with, in order to favour the creation of consortia that present projects aligned with the needs indicated by the Commission. European

Entities (including from civil society, SMEs, academia and research) being supported to participate in relevant, national and international/ EU, cybersecurity projects and collaboration activities.

Name of the measure: RETECH	
Responsible unit: INCIBE	**New measure:** Yes

Short description: Territorial Networks of Technological Specialization (RETECH) are a tool to make digital transformation a reality throughout the territory, making the most of the potential of each region. Its objective is to launch **territorial digital transformation projects** jointly driven by several regions that will allow supporting tractor projects, fostering regional leadership and cooperation in the promotion of tractor projects of high territorial and economic impact, promoting 9 lines of action (Artificial Intelligence and other enabling digital technologies applied to industries, Digital Twins, Digital Health, FashionTech, GreenTech, Cybersecurity, Digital Entrepreneurship Networks, Technology with social impact and RuralTech).

RETECH Ciberseguridad is a strategic initiative of the country for the development of the cybersecurity ecosystem (capabilities, industry, R+D+i, talent, etc.), which, with the coordination of INCIBE, will bring together 15 autonomous communities in its first phase.

The main objectives of the RETECH initiative are:

1. Contribute to closing the existing territorial gap.
2. To articulate regional projects aimed at digital transformation and specialization.
3. Promote leadership and interregional cooperation in the promotion of driving projects of high territorial and economic impact.
4. Generate or promote disruptive initiatives based on the different visions, experiences and knowledge acquired by regional administrations.
5. Promote tractor effects in the territory as a whole to move towards new models of more sustainable and inclusive development.

List of concrete actions implemented/planned:

The launch of the project took place on March 24, 2023 at an event in which the memorandums of understanding were signed with the participating autonomous communities and which make up 3 participating NODES:

- **NODE 1 - Cybersecurity Nodes Network ("ARGOS Network"):** whose objective is to boost and strengthen the national cybersecurity ecosystem and increase the global adoption of cybersecurity, mainly by companies, based on the generation of specialized capabilities and the networking of different regional cybersecurity nodes. This project is made up of the Autonomous Communities of Castilla y León (as coordinator of the node and with actions in the aerospace and mobility fields), the Basque Country (smart industry and energy), Andalusia (health and smart cities) and Madrid (health).

- **NODE2 - Deployment of the Innovation and Competence Centre in health sciences, Smart Transportation, connected industry and operational excellence**, with the aim of expanding, developing and promoting the technological and industrial cyber capabilities necessary to ensure digital security in the strategic areas determined by each of the Autonomous Communities that make up this node, consisting of Catalonia (as node coordinator), the Valencian Community and Galicia.

- **NODE3 - CIBERREG - Impulso a la Ciberseguridad desde los territorios**: which aims to be a unique and collaborative work environment with a high degree of participation of Autonomous Communities so that, based on the actions and experiences of each region, the working groups and forums created to share progress collaboratively allow a qualitative advance in the adoption of the principles of cybersecurity in the economic fabric of each territory. This project is made up of the Autonomous Communities of Navarra (as coordinator of the node and with actions for SMEs and citizens, green energy, food and electric and connected mobility), Asturias (Industry 4. 0, defence and agri-food companies), Canary Islands (tourism, SMEs and self-employed and construction), Cantabria (industry, blue economy, agri-food, health and culture and tourism), Castilla-La Mancha (ICT companies), Extremadura (rural environment, SMEs and self-employed and citizenship), Balearic Islands (tourism) and Murcia (agri-food).

Digital target or general objective: Digital Transformation of business. More than 90% of European SMEs reach at least a basic level of digital intensity.

Link to the target or objective: Promote digital leadership and sovereignty in the EU

Reference to RRP or other relevant documents/strategies: Component 15. Digital connectivity, promotion of cybersecurity and deployment of 5G C15.I7
Cybersecurity: Strengthening the capacities of citizens, SMEs and professionals; and Promotion of the sector ecosystem.

Component 19 National Plan of Digital Competences (digital skills). C19.I4. Digital professionals. Scholarship programs for digital talent.

Tentative timeline: The relevant intermediate milestones will be established in the Annual Operating Plans derived from the signing of the agreements and intermediate measurements and indicators will be established for the validation and verification of the fulfilment of such milestones.

Once the Agreements that make up the RETECH initiative have been signed, the Annual Operating Plan for the first year will be planned annually and must be approved within two months of the signing of the respective Agreement. For the 2024, 2025 and 2026 annuities, the Plan will be prepared by the Bilateral Commissions before December 1 of the previous annuity and must be approved by the Agreement Monitoring Committee before December 15. The execution term of the RETECH Cybersecurity program will be assimilated to the completion terms of C15.I7 (June 30, 2026) and C19.I4 (December 31, 2025), in each case.
Budget allocated or planned and, if relevant, other resources – including human resources – allocated: Thereof from EU sources: EUR 110,719,008/ Planned: EUR 110,719,008 Thereof from Comunidades Autónomas sources: EUR 38.235.796,51 / Planned: EUR 38.235.796,51 The budget is already planned and will be allocated according to the budget items transcribed in the respective Agreements.
Expected impact and related timing: The estimated impact and the temporality of the same, will be determined in the Annual Operational Plans and depending on the projects that are finally carried out within each node and each Autonomous Community. - The RETECH Cybersecurity programs will develop initiatives focused on attracting and generating talent to the cybersecurity sector, through training in cybersecurity at both the supply and demand levels. Likewise, initiatives will be launched with the aim of training and raising the awareness of citizens in basic cybersecurity skills for an appropriate and safe use of new technologies. - In the axis of digital transformation of companies, RETECH Cybersecurity programs will launch initiatives to promote entrepreneurship and acceleration of cybersecurity companies, increase the global adoption of cybersecurity measures, from the design and the other stages in the development of new solutions and awareness at the level of companies, SMEs and self-employed in the use of digitization with a secure and sustainable approach. - In the axis of secure and sustainable digital infrastructures, actions will be implemented to help improve capabilities (infrastructure, equipment and resources) at regional and local level, improving the deployment of new technologies with the cybersecurity factor by default. Likewise, innovation and research actions will be promoted in the field of ICT cybersecurity.

Name of the measure: Cybersecurity strengthening for citizens and minors	
Responsible unit: INCIBE	**New measure:** Yes
Short description: This measure focus on strengthening cybersecurity capabilities and digital trust of citizens and children, highlighting the need to implement a cybersecurity	

culture: investing in awareness of the risks associated with digitization, as well as training in cybersecurity digital skills. This measure is part of Confía Program, which provides a comprehensive cybersecurity framework composed of four integral aspects: raising awareness and communication through campaigns for citizens, children and businesses; providing cybersecurity training for citizens, minors, and companies with specific resources; fostering cooperation and coordination through bilateral and multilateral agreements for cybersecurity culture and incident management; and developing and promoting specific technological solutions for minors, citizens and businesses. It aims to create a holistic cybersecurity culture that encompasses all societal sectors.

List of concrete actions implemented/planned:

These actions will be carried out within the framework of the CONFÍA Program through INCIBE channels for different audiences, such as the Internet User Safety Office (OSI), for citizens and seniors, and Internet Segura For Kids (IS4K), for children, their families, educators and other professionals working with minors, around 4 axes:

- **Awareness and communication actions**, such as massive dissemination campaigns, events and proximity actions, which incorporate interactive and gamified dynamics and resources.
- **Training in cybersecurity** through the development of training programs and specific resources for the acquisition of digital skills in cybersecurity. Cooperation and coordination with bilateral and multilateral agreements for the consolidation of a culture of cybersecurity or management of incidents and the development of a network of relevant actors.
- **Cybersecurity tools and solutions**, with the development and promotion of specific technological solutions for minors and citizenship.
- As a complement to the previous ones, it is proposed to establish an increase in the services and coordinated response actions of the **Cybersecurity Help Line 017**.

Digital target or general objective: Promote digital leadership and sovereignty in the EU

Link to the objective: The focus is to continue the information, awareness and training mechanisms in this field, expanding the services available to citizens, including minors and their references groups (families, educators). There will be bonds with public and private actors, both nationally and internationally. The appropriate ecosystems and channels for cooperation and joint defence against common threats will be taken in, with the aim of improving digital capabilities.

Reference to RRP or other relevant documents/strategies: Component 15: Digital connectivity, promotion of cybersecurity and deployment of 5G C15.I7 Cybersecurity: Strengthening the capacities of citizens, SMEs and professionals; and Promotion of the sector ecosystem.

Tentative timeline: The actions listed are focused on the 2021-2026 period:

- **Awareness and communication actions.**
- **Cybersecurity training** with training programmes and specific resources for

the acquisition of digital skills in cybersecurity.

- **Cooperation and coordination** with bilateral and multilateral agreements for the consolidation of a culture of cybersecurity as well as incident management and the development of a relevant actor's network.
- **Cybersecurity tools and solutions**, with the development and promotion of specific technological solutions for companies.

Budget allocated or planned and, if relevant, other resources – including human resources – allocated:

Public investment: EUR 13,3 million / Already allocated: EUR 13,3 million

Thereof from EU sources: EUR 13,3 million / Already allocated: EUR 13,3 million

Expected impact and related timing: Citizens and children, including their reference groups, are expected to improve their overall cybersecurity awareness and to identify threats and also to know how to react in the event of a cybersecurity incident.

Name of the measure: Cybersecurity strengthening for citizens, small and medium-sized enterprises (SMEs) and professionals

Responsible unit: INCIBE	**New measure:** Yes

Short description: This measure focus on strengthening cybersecurity capabilities and digital trust of citizens and companies, highlighting the need to implement a cybersecurity culture: investing in awareness of the risks associated with digitization, as well as training in cybersecurity digital skills. This measure is part of Confía Program, which provides a comprehensive cybersecurity framework composed of four integral aspects: raising awareness and communication through campaigns for citizens, children and businesses; providing cybersecurity training for citizens, minors, and companies with specific resources; fostering cooperation and coordination through bilateral and multilateral agreements for cybersecurity culture and incident management; and developing and promoting specific technological solutions for minors, citizens and businesses. It aims to create a holistic cybersecurity culture that encompasses all societal sectors.

List of concrete actions implemented/planned:

- **Awareness and communication actions:**
  - Protege Tu Empresa blog and INCIBE-CERT blog are information services with educational components. These blogs help companies and professionals to stay up-to-date on cybersecurity with a close language to businessmen. Real cases, informative videos and infographics are also posted on the blog. A help section for companies where they can learn how to face cybersecurity problems, and also how to receive support about a cybersecurity incident they might have suffered. Interactive and gamified resources that promote awareness in a distended way.
- **Cybersecurity training** with training programmes and specific resources for

the acquisition of digital skills in cybersecurity. • **Cooperation and coordination** with bilateral and multilateral agreements for the consolidation of a culture of cybersecurity as well as incident management and the development of a relevant actor's network. • **Cybersecurity tools and solutions**, with the development and promotion of specific technological solutions for companies. • As a complement to the previous ones, it is proposed to establish an increase in the services and coordinated response actions of the **Cybersecurity Help Line 017**.
Digital target or general objective: Promote digital leadership and sovereignty in the EU
Link to the objective: The focus is to continue the information, awareness and training mechanisms in cybersecurity, expanding the services available to citizens, SMEs and professionals. There will be bonds with public and private actors, both nationally and internationally. The appropriate ecosystems and channels for cooperation and joint defence against common threats will be taken in, with the aim of improving digital capabilities.
Reference to RRP or other relevant documents/strategies: Component 15: Digital connectivity, promotion of cybersecurity and deployment of 5G C15.I7 Cybersecurity: Strengthening the capacities of citizens, SMEs and professionals; and Promotion of the sector ecosystem.
Tentative timeline: The actions listed are focused on the 2021-2026 period: • **Awareness and communication actions.** • **Cybersecurity training** with training programmes and specific resources. • **Cooperation and coordination** with bilateral and multilateral agreements. • **Cybersecurity tools and solutions**.
Budget allocated or planned and, if relevant, other resources – including human resources – allocated: Public investment already allocated: 2.098.450 EUR Thereof from EU sources already allocated: 2.098.450 EUR
Expected impact and related timing: Small and medium-sized enterprises (SMEs) and professionals are expected to improve their overall cybersecurity awareness and to identify threats and also to know how to react in the event of a cybersecurity incident.

Name of the measure: CyberEx	
Responsible unit: INCIBE	**New measure:** Yes
Short description: The INCIBE-CERT cyber exercise service, CyberEx, allows to train and assess the organisation's capacity to respond to a cybersecurity incident. This	

capability is put to the test, both from technical aspects and from the organisational point of view and coordination between agencies and entities.

The service consists of different activities:

- Role play: a simulation or role play in an entire organisation with the profiles and departments that are most important for the business, making them face a crisis or threat situation.
- Simulation of cyberattacks or incidents: a technical exercise that begins with notification of an incident by INCIBE-CERT. The purpose of the test is to train the ability to carry out the investigation quickly and reliably, combining decision-making, collaboration and internal and external collaboration. Upon finishing this test, the incident must be fully controlled and the foundations for recovery from the impact caused to the participating organisation must be laid.
- Targeted attacks: a practical exercise that is presented as a test in which you have to achieve an intrusion into the technological infrastructure of the participating organisation. The ultimate purpose of the attack is to obtain some kind of evidence that makes it possible to verify that the attacker has managed to penetrate this infrastructure.

After the execution of the three activities, a formal evaluation report of the performance of the participants is produced, providing also a comparative vision with other participants, and recommendations to improve the organizations cybersecurity.

List of concrete actions implemented/planned:

- 2020 – Design and Execution of CyberEx- Edition 2020: 27 organizations participating (OES, DSPs and other strategical entities)
- 2021 - February: Final reports of Cyberex delivered to participants
- 2021 - Design of CyberEx- Edition 2022
- 2022 - Execution of CyberEx 2022 edition: 30 organizations participating (OES, DSPs and other strategical entities).
- 2023 – Follow-up after execution, to receive feedback and tracking of improvement plan and initiatives identified after the cyberexercise

Digital target or general objective: Promote digital leadership and sovereignty in the EU

Link to the objective: This service contributes to improve the cybersecurity capabilities and maturity by training, assessing and testing the organization incident response and crisis management capability, to reinforce internal and inter-agency coordination, to deepen awareness-raising around risks at all levels, and to improve the organisation's image and reputation.

Reference to RRP or other relevant documents/strategies: Component 15: Digital connectivity, promotion of cybersecurity and deployment of 5G C15.I7 Cybersecurity: Strengthening the capacities of citizens, SMEs and professionals; and Promotion of the sector ecosystem

Tentative timeline: New editions of CyberEx are planned to be launched in late 2023,

and expected to continue until 2028. It is expected also to increase the frequency and participants to a maximum of 6 editions and 180 organizations participating.
Budget allocated or planned and, if relevant, other resources – including human resources – allocated: - Public investment: 2.360.729,32 EUR / Already allocated: 0 EUR - Planned: 2.360.729,32 EUR - Thereof from EU sources: 2.360.729,32 EUR / Already allocated: 0 EUR - Planned: 2.360.729,32 EUR
Expected impact and related timing: Participating entities are expected to improve their overall organization incident response and crisis management capabilities and also cybersecurity awareness. It is also expected to increase the number of participating entities and so the number of entities trained and assessed.

Name of the measure: Helpline **"**Your Help in Cybersecurity"	
Responsible unit: INCIBE	**New measure:** Yes
Short description: "Your Help in Cybersecurity" helpline is a national, free and confidential service offered by INCIBE for internet and technology users, aiming to assist them with any cybersecurity issues that might happen in their daily life. This helpline is intended for citizens (general internet users), businesses, and professionals who use the internet and new technologies in their work and need to protect their assets and business; also, for minors and their environment (parents, educators, and professionals working in the minor's sphere or online protection linked to this audience). A multidisciplinary team of experts provides this service, offering technical, psychosocial and legal advice through different contact options such as: calling 017, instant messaging (WhatsApp and Telegram), email or filling out a web form and since 2023 face to face onsite attendance.	
List of concrete actions implemented/planned: • Reinforcement of helpline capacities to respond to possible increases in citizens demand, extending service hours from 8:00 a.m. to 11:00 p.m. • Improvements in the technical capacities for receiving calls, queries and manage them. • Greater attention to preventive advice as opposed to reactive advice. • Assistance and operation in cybersecurity operations in particular: e.g. elections, special cyberincidents. • On-site service: requesting an appointment to go to the INCIBE facilities to address the issues and possible queries. • Improvements in technological and/or coordination capabilities for reporting and resolving cyberincidents. • Improvements to increase the accessibility of the service for the citizens. • Dissemination actions and improvements in service management and	

coordination.
Digital target or general objective: Promote digital leadership and sovereignty in the EU
Link to the objective: This program contributes to improving resilience to cyberattacks by offering a multidisciplinary team of experts to assist internet and technology users with cybersecurity issues by providing technical, psychosocial and legal advice. The program enhances risk-awareness and knowledge of cybersecurity processes among citizens, businesses, and professionals. Moreover, by serving as a supportive resource, it encourages both public and private organizations to increase their efforts in achieving basic levels of cybersecurity.
Reference to RRP or other relevant documents/strategies: Component 15: Digital connectivity, promotion of cybersecurity and deployment of 5G C15.I7 Cybersecurity: Strengthening the capacities of citizens, SMEs and professionals; and Promotion of the sector ecosystem
Tentative timeline: Helpline was launched on February 11, 2020. In 2022, the capacity and opening hours for the public were increased. On-site helpline service begins in 2023. In 2023, capacity improvements will begin to integrate information flows of possible cyber incidents with other INCIBE services and resolve them holistically. Completion date: sine die.
Budget allocated or planned and, if relevant, other resources – including human resources – allocated: Public investment: EUR 11,3 million / Already allocated: EUR 5,8 million - Planned: EUR 5,5 million - Thereof from EU sources: EUR 11,3 million / Already allocated: EUR 5,8 million - Planned: EUR 5,5 million
Expected impact and related timing: On the service third anniversary the service had already handled more than 184,199 queries, with an average of more than 1,295 queries per week. 67,322 inquiries were answered through the number 017 and its different contact channels, during 2022. Specifically, 44,331 by telephone, 5,977 through the web form and 17,014 through chats. And 35,563 queries attended until June 2023. The service hour opening hours increase has allowed to increase service levels up to 94% and user satisfaction above 9.1. Almost all the inquiries from citizens who used 017 belong to adults between 25 and 65 years of age (69%). The remaining 31% was distributed among those over 65 years of age, young people between 18 and 24 years of age, and other groups Helpline will increase capacity to resolve/assess more queries per month during 2023.

Name of the measure: Cyber-resilience Improvement Indicators (CII)	
Responsible unit: INCIBE	**New measure:** Yes

Short description: The Indicators for Improving Cyber Resilience model is a tool for self-diagnosis and measurement of the ability of organizations to withstand and overcome disasters and disruptions from the digital environment.

The objective is to assist all stakeholders in the enhancement of their cyberresilience capabilities, and to provide a procedure to understand the maturity level of their controls to anticipate, resist, recover and evolve after suffering adverse conditions, stress or attacks against the organizational cyberresources.

The CII (Cyber-resilience Improvement Indicators) model enables organizations to assess their ability to anticipate, withstand, recover and evolve following incidents that may affect the delivery of their services. The model defines four objectives, which correspond to the aforementioned resilience capabilities, and nine functional domains: cybersecurity policy, risk management, training, vulnerability management, continuous monitoring, incident management, continuity management, configuration and change management, and communication.

List of concrete actions implemented/planned:

- 2022 - Measurement of cyber resilience to operators of essential services, inviting 200 entities.
- 2023 - Measurement of cyber resilience to operators of essential services and digital service providers, inviting 270 entities.
- 2024 - Measurement of cyber resilience to operators of essential services and digital service providers, inviting 300 entities.

Digital target or general objective: Promote digital leadership and sovereignty in the EU

Link to the objective: This project contributes to improving resilience to cyber-attacks by providing participating organizations with an insight into their capabilities to anticipate, resist, recover and evolve, as well as a comparison with other participants in their sector and in general. Participants also have insight into their areas for improvement, as well as recommendations regarding their weaknesses and how far they are from the maturity of other participants, allowing them to become more aware and work harder on those areas to improve their cyber resilience.

Reference to RRP or other relevant documents/strategies: Component 15: Digital connectivity, promotion of cybersecurity and deployment of 5G C15.I7 Cybersecurity: Strengthening the capacities of citizens, SMEs and professionals; and Promotion of the sector ecosystem.

Tentative timeline: The Indicators for Improving Cyber Resilience project started in 2022 and will continue until 2025. During this period, three measurements will be conducted (one each year) to determine the level of maturity and cyber resilience of the institutions.

Budget allocated or planned and, if relevant, other resources – including human resources – allocated: Public investment already allocated: 354.474,00 EUR - Thereof from EU sources already allocated: 354.474,00 EUR
Expected impact and related timing: Participating entities are expected to improve their overall cybersecurity awareness, become more cyber-resilient and improve their capabilities to anticipate, withstand, recover and evolve from incidents that may affect the delivery of their services. It is expected that the number of participating entities and their level of maturity will increase throughout the project and that this analysis can be carried out periodically to assess the effectiveness of the measures and thus try to improve and increase the cyber resilience of the entities.

Name of the measure: Computer security incident response team	
Responsible unit: INCIBE	**New measure:** Yes
Short description: Royal Decree-Law 12/2018, of 7 September, recognises INCIBE-CERT as a leading cyber security response and early warning centre for citizens and organisations subject to private law in Spain The cybersecurity incident response is offered to both citizens and organisations governed by private law. Within organisations governed by private law, critical and strategic infrastructure, essential services or digital service providers stand out. INCIBE-CERT provides a 24/7/365 cybersecurity incident response service which, by using or being aimed at technological elements, may affect the proper operation of critical and strategic infrastructure, essential services or digital service providers. Throughout the process the team responsible for the service coordinates with the organisation's security team, as well as with other organisations that can make it easier to mitigate the impact: International ISPs, CERT/CSIRT and Law Enforcement Agencies (LEAs), with the cooperation of the Office of Cyber Coordination (OCC) of the Ministry of the Interior. The incident management process follows the guidelines and processes agreed by all the national agencies listed in the "National Guide for incident notification and management". An analysis of cyber threats is carried out from the cyber threats associated with the management of Cybersecurity incidents, information on high-impact or novel cyber threats. Apart from the incidents that are received by those affected, it is also important to proactively detect some types of incidents about which the affected party is not aware. Likewise, several high-impact incidents in relevant organizations or in a large volume of organizations could trigger a cybersecurity crisis. For this reason, we must have the necessary resources, processes and training to be prepared for this scenario.	
List of concrete actions implemented/planned: • 2022-Reinforcement of the incident management level 2 team • 2023-Reinforcement of the incident management level 1 team. Integration of	

tools for greater effectiveness and efficiency in incident handling.

- 2024-DNS service for the protection of citizens and companies from the information obtained from incident management cyberthreats. Cybercrisis training.

Digital target or general objective: Promote digital leadership and sovereignty in the EU

Link to the objective: This project contributes to improve the collective resilience of member States and resilience against cyberattacks by providing support to the incidents that suffer organizations and citizens to hold and recover to the normal situation as soon as possible. It is also reinforced with the proactive detection of incidents that allow the detection of exposed vulnerable systems that could be used to carry out other types of actions, detection of infected computers, etc.

Reference to RRP or other relevant documents/strategies: Component 15: Digital connectivity, promotion of cybersecurity and deployment of 5G C15.I7 Cybersecurity: Strengthening the capacities of citizens, SMEs and professionals; and Promotion of the sector ecosystem.

Tentative timeline: There is no defined timeline. The incident management service, and the auxiliary services on which it is supported, have been provided continuously. Within the auxiliary services, other services and tools are being added, but they provide support for incident management.

Budget allocated or planned and, if relevant, other resources – including human resources – allocated:

Public investment: EUR 25,5 million / Already allocated: EUR 9,4 million - Planned: EUR 16 million

-Thereof from EU sources: EUR 25,5 million / Already allocated: EUR 9,4 million - Planned: EUR 16 million

Expected impact and related timing: The expected impact is, on the one hand, a large increase in the number of incidents, mainly detected proactively, which in the long term should decrease as they are resolved. On the other hand, other important impact is to provide support in the resolution of incidents of enterprises and citizens.

Name of the measure: Programme to foster ISMS (Information Security Management Systems) certifications

Responsible unit: INCIBE	**New measure:** Yes

Short description: The Initiative to promote ISMS certifications is a grant programme offered by INCIBE to promote ISMS certifications of SMEs in accordance with international (ISO 27001) and national (ENS) standards, with the aim of making them became key players as secure supply chain for private and public entities in the essential and important sectors within the scope of the NIS2 Directive.

The grants are aimed directly at consultancy companies that implement and certify the aforementioned standards as pivotal agents of change, which are instrumental in ensuring certification is effectively delivered to the SMEs that are the indirect beneficiaries of the programme. In order to achieve a wide impact of the initiative and to support us in its management, we count on the assistance of collaborating entities with a great capacity to reach both SMEs and consultancies in cybersecurity standards. This Programme pursues the dual objective of boosting SMEs as a secure supply chain for the ICT services of important and essential entities, while at the same time promoting the cybersecurity consultancy sector.
List of concrete actions implemented/planned: • Publication of the regulatory bases of the grants for the Initiative to foster ISMS certifications. Signing of agreements with collaborating entities. Open call for ISMS standards consulting firms to participate in the Initiative. • Publication of the beneficiaries of the Initiative. Start of implementation and certification projects in SMB. • End of implementation and certification projects with award verification and payment of the grants.
Digital target or general objective: Promote digital leadership and sovereignty in the EU
Link to the target or objective: This programme contributes to improving resilience to cyberattacks, contributing to increasing risk-awareness and the knowledge of cybersecurity processes, and increasing the efforts of public and private organizations to achieve at least basic levels of cybersecurity. It also contributes to promoting a Union digital regulatory environment to support the ability of Union undertakings, especially that of SMEs, to compete fairly along global value chains.
Reference to RRP or other relevant documents/strategies: Component 15: Digital connectivity, promotion of cybersecurity and deployment of 5G C15.I7 Cybersecurity: Strengthening the capacities of citizens, SMEs and professionals; and Promotion of the sector ecosystem.
Tentative timeline: The programme is due to start in July 2023, with the publication of the bases, the signing of the agreements with the collaborating entities and the opening of the call for applications. The beneficiaries, consultancy firms, will be identified before the end of the year. During the following two and a half years, until June 2026, the implementation and certification project will be carried out by the beneficiaries in the SMEs that apply.
Budget allocated or planned and, if relevant, other resources – including human resources – allocated: Public investment: EUR 20 million / Planned: EUR 20 million - Thereof from EU sources: EUR 20 million Planned: EUR 20 million
Expected impact and related timing: Around 70 ISMS consultancies and 25 certification companies should apply, and at least 75% will be awarded the grants. Thus, 1,000 SMEs will be able to apply for ISMS implementation and certification

for a key service they offer to third parties, and 70% of these projects are expected to be successful.

Name of the measure: Sectorize INCIBE-CERT services based on new challenges	
Responsible unit: INCIBE	**New measure:** Yes
Short description: The objective of this measure is to prepare Spain to assume the new challenges and commitments described in the new NIS 2 directive and other regulations. INCIBE, as the reference CERT for citizens and private companies, is working to adapt its services to the specific needs of each of strategic business sectors in the country.	

List of concrete actions implemented/planned:
• **In-depth study of the sector:**
  ○ Each of the strategic sectors framed within the NIS 2 directive has its particular needs and as such they must be understood and addressed from the perspective of their protection. Therefore, it is essential to know in depth each of the cases.
• **Approach to each strategic sector:**
  ○ In order to offer adequate protection services adapted to the real needs of companies, a direct approach to them is necessary. To this end, INCIBE is establishing collaboration ties with the most important business associations in the country.
• **Reinforcement and improvement of current services**
  ○ Once the approach to each of the strategic sectors has been carried out, the next objective is to listen to the opinion and needs of the companies involved in order to readapt and improve INCIBE-CERT services.	

Digital target or general objective: Promote digital leadership and sovereignty in the EU	
Link to the target or objective: As INCIBE's services adapt to the particularities and needs of each of the country's strategic sectors, the nation's security will increase and strengthen, since its strategic companies will be better protected.	
Reference to RRP or other relevant documents/strategies: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).	
Tentative timeline: The actions listed are focused on the 2023-2026 period: • In-depth study of the sector: 2023-2024 • Approach to each strategic sector: 2023 • Reinforcement and improvement of current CERT services: 2024-2026	

Budget allocated or planned and, if relevant, other resources – including human resources – allocated:

- Public investment already allocated: 2.500.000 EUR. Thereof from EU sources already allocated: 0 EUR
- Specific Area in INCIBE, Strategic Sectors. 16 people full time.

Expected impact and related timing: A significant response is expected from the companies involved in each of the strategic sectors, as well as a high workload and an increase in the level of demand for the quality of the services provided by INCIBE. The expected result of the effort is the improvement of the security of Spain and, therefore, of the EU.

Name of the measure: Chairs and R&D&I Missions Programs

Responsible unit: INCIBE	**New measure:** Yes

Short description: The financing programs are aimed at public Spanish universities or consortia made up of public and private universities, in which the public university exercises the function of coordinator.

Both programs, Chairs Program (Public invitation for collaboration in the promotion of Cybersecurity Chairs in Spain) and R&D&I Missions Program (Public invitation for collaboration in the promotion of Strategic Cybersecurity Projects in Spain), are intended to develop a culture of Cybersecurity and promote the consolidation of digital trust for citizens and companies.

The specific objective of each program is:

- Chairs Program: support the organization of events, the development of academic programs and capacity building in cybersecurity.
- R&D&I Missions Program: support the development of research, development and innovation programs and capacity building in cybersecurity.

For the Chairs program, currently, the program has a total amount of 16.800.000€, with the next characteristics:

- INCIBE will finance a maximum of 75% of the projects presented, with a maximum of 900.000€ by project
- If the Chair is international, the maximum amount will be 1.200.000€. The foreign university always be beneficiary through the public university.

For the R&D&I Missions Program, the program has a total of 18.000.000€. In this case, the maximum amount to finance by INCIBE will be 900.000€ by project (NCIBE will contribute a maximum of 75% of the eligible costs).

The investment will serve to strengthen the capacities of citizens, SMEs and professionals in the field of cybersecurity.

Please see the detailed funding conditions here (only available in Spanish): https://www.incibe.es/ed2026/ciberinnova/catedras

https://www.incibe.es/ed2026/ciberinnova/misionesidi.

List of concrete actions implemented/planned: INCIBE receives proposals from different publics universities that will be evaluated every three months.

- With the proposals approved, a collaboration agreement is signed.
- With the sign of the collaboration agreement, INCIBE will pay 50% of the contribution to finance.
- The payment of the balance will be with the justification of the activities. An activity monitoring commission is established every three months, to carry out technical and economic monitoring.
- Once a year, the universities have to present the progress of their Projects: technical and economic.

Digital target or general objective: Promote digital leadership and sovereignty in the EU

Link to the target or objective: The measure is focused on SMEs, professionals and citizens promoting actions aimed at developing capacities of the Spanish cybersecurity ecosystem within the framework of the European digital sovereignty. Therefore, this measure is expected to contribute directly to the achievement of the digital transformation target.

Reference to RRP or other relevant documents/strategies:

Component 15. Digital connectivity, promotion of cybersecurity and deployment of 5G C15.I7 Cybersecurity: Strengthening the capacities of citizens, SMEs and professionals; and Promotion of the sector ecosystem.

Tentative timeline:

December, 1 2022 - The Public invitation for collaboration in the promotion of Cybersecurity Chairs in Spain related with the Chairs program was published.

December, 5 2022 - The Public invitation for collaboration in the promotion of Strategic Cybersecurity Projects in Spain related with the R&D&I Missions program was published.

December ,2023 - The two public invitations are expected to be available until at least the end of 2023 or until the budget will be exhausted.

December, 2025 - The execution period of the financed activities is until

From January, 2026 - The universities could continue with the activities with their own funds.

Budget allocated or planned and, if relevant, other resources – including human resources – allocated

Chairs program budget:

Thereof from EU sources: EUR 16,800,000 / Already allocated: EUR 6,451,417 - Planned: EUR 6,451,417

Thereof from Universities sources: EUR 5,600,000 / Already allocated: EUR 2,203,306.00 - Planned: EUR 2,203,306.00

R&D&I Missions program budget: Thereof from EU sources: EUR 18,000,000 / Already allocated: EUR 7,147,441.10 - Planned: EUR 7,147,441.10 Thereof from Universities sources: EUR 6,000,000 / Already allocated: EUR 2,790,618.62 - Planned: EUR 2,790,618.62
Expected impact and related timing: More than 15 Chairs (7 of which international) will receive funding for the organization of events and the development of academic programs and capacity building in cybersecurity to citizens, SMEs, professionals and other target audiences. More than 27 strategic projects will receive funding for development of investigation projects that allow increase the digital transformation in Spain. More than 26 public Spanish universities are expected to participate in these programs.

4.2.3 Contributing to the green transition

Name of the measure: National Green Algorithms Program (PNAV)	
Responsible unit: SGIATHD	**New measure:** Yes
Short description: The National Green Algorithms Program is designed to drive sustainable Artificial Intelligence (AI), incorporating eco-friendly aspects from the algorithm's inception. The initiative addresses the need for environmentally responsible AI through encouraging research in Green Tech, promoting energy-efficient infrastructure, integrating Green AI and blockchain into the economy, and stimulating the Spanish market through green tech solutions. The following actions will be included: • Preparation of a good practice guide. • Preparation of a catalog of efficient algorithms and another of algorithms to address environmental problems. • Generation of standards for the elaboration of impact calculators for self-assessment. • Measures to support the awareness and training of AI developers.	
List of concrete actions implemented/planned: November 2021: publication of an expression of interest, where 88 expressions were gathered, contributing to the definition of the National Green Algorithms Programme (PNAV). December 2022: Publication of the PNAV action plan that comprises actions related to sustainable AI developed in the context of the National Strategy on Artificial Intelligence:	

https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2022/20221213_plan_algoritmos_verdes.pdf December 2022: published the call for tenders to execute the actions. https://contrataciondelestado.es/wps/poc?uri=deeplink%3Adetalle_licitacion&idEvl=jpyCNjJ8BMWmq21uxhbaVQ%3D%3D
General objective: Contributing to the green transition
Link to the objective: The National Green Algorithms Program contributes to sustainability by fostering energy-efficient AI and Green Tech, promoting eco-friendly infrastructures, and integrating Green AI and blockchain into the economy. These actions align with the goals of the European Green Deal, improving resilience, and fostering a climate-neutral economy.
Reference to RRP or other relevant documents/strategies: Component 16: National Artificial Intelligence Strategy C16.R1 National AI Strategy
Tentative timeline: The programme started in December 2022, with the contract expected to be signed in July 2023, activities starting September 2023 and it is expected to finish by the end of 2025.
Budget allocated or planned and, if relevant, other resources – including human resources – allocated: 3.700.000 €
Expected impact and related timing: The current call for tenders intends to develop the measures of the Programme, such as the creation of a good practices handbook in the development of sustainable artificial intelligence and the development of a of a certification scheme that will provide an added value to local technology suppliers. In addition, the PNAV places special emphasis on disseminating and raising social awareness of the importance of promoting sustainable technological development, to promote sustainable technological development, seeking to differentiate local technological solutions through sustainability.