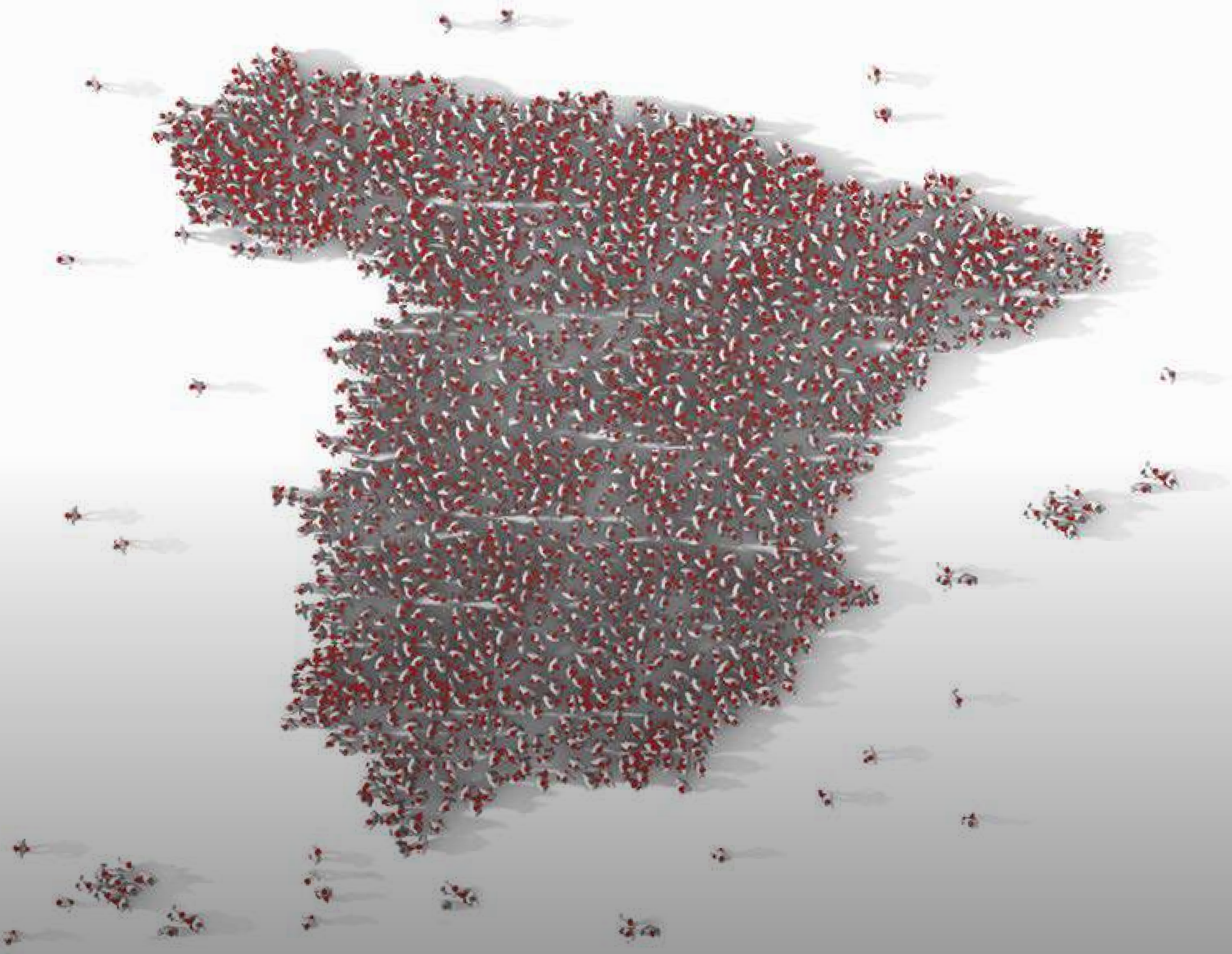
FORO NACIONAL DE CIBERSEGURIDAD



GLOBAL REPORT ON ACTIVITIES CARRIED OUT IN THE FIRST PHASE

NATIONAL CYBERSECURITY FORUM

DRIVER FOR PUBLIC PRIVATE COLLABORATION

Index

+ Global report on the work carriet out

Background

+ 01.

Background

The Spanish cybersecurity model integrates different actors in a common ecosystem, widely regulated and specialized, where collaboration, cooperation and coordination of all of them is encouraged, understanding cybersecurity as a State Policy under the scope of National Security.

The National Cybersecurity Strategy (ENCS) approved by the National Security Council in April 2019, points to **public-private collaboration** as a key element and encourages the materialization of such collaboration through the **National Cybersecurity Forum**, a place to integrate representatives of civil society, independent experts, private sector, academia, associations, non-profit organizations, among others, in order to enhance and create public-private synergies.

The creation of the Forum was approved by the National Security Council on 21 February 2020, as a working group of the National Cybersecurity Council. Its constitution took place on 22 July 2020.

The composition of the Forum was determined with the aim of **bringing together the greatest representation of** public and private bodies and society in the field of cybersecurity. Chaired by the Department of Homeland Security, it has two vice-presidencies, one for the National Cryptologic Centre and the other for the National Institute of Cybersecurity (INCIBE) and is composed, in addition to the public bodies with competence in the field, of **15 organizations representing civil society and the private sector**: the Spanish Chamber of Commerce, the CEOE, CEPYME, the Association of the Self-Employed ATA, CRUE Universities, the Spanish Association of Telecommunications Users AUTELSI, the Spanish network of Cyber Incident Response Teams CSIRT.es, specialized media, such as Ediciones CODA and Editorial Borrmart, ESYS Foundation, International Association of Auditors ISACA, Business Association for the Promotion of Information Security (ISMS Forum), National Network of Excellence in Cybersecurity Research and the think tanks Thiber and the Real Instituto Elcano.

The creation of the Forum was approved by the National Security Council on 21 February 2020, as a working group of the National Cybersecurity Council.

Work carried

+ 02.

Work carried

The first lines of work of the Forum, approved by the National Cybersecurity Council, focused on the study and proposal of initiatives aimed at increasing the culture of cybersecurity; support for industry and R&D&I; and training and support in cybersecurity, all of which are aligned with measures included in the ENCS. Three working groups were created in a public-private co-leadership format for their execution.

1

The cybersecurity culture group, the Department of Homeland Security, the ISMSForum association and the BorredaFoundation have drawn up, as their first project, a **Report on cybersecurity culture**.

2

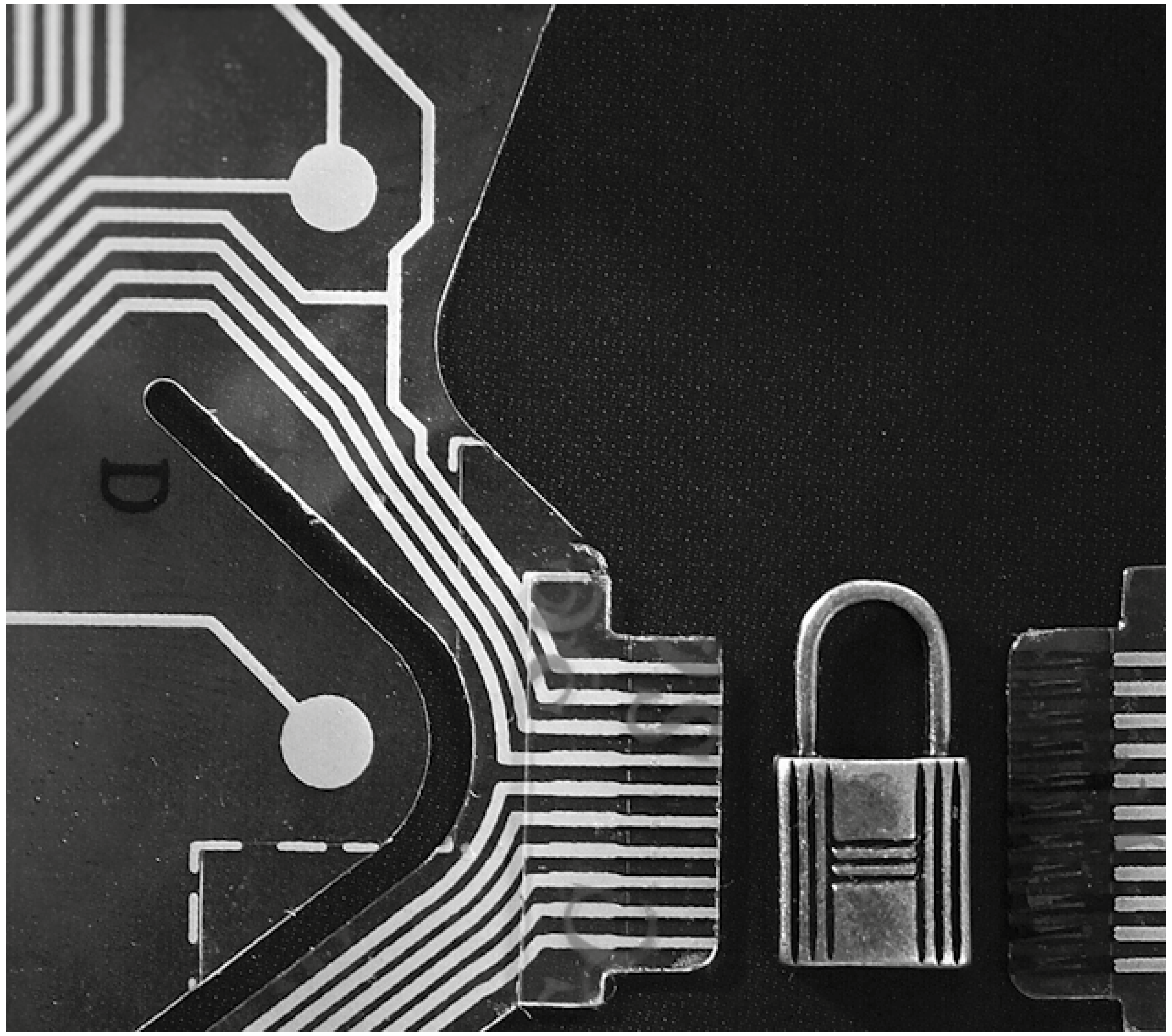
The Industry and R&D&I support group, the National Cybersecurity Institute (INCIBE) and the Spanish Chamber of Commerce, which has developed a **Report on the cybersecurity sector in Spain**.

3

The cybersecurity training, education and support group, the National Cryptologic Centre and the CRUE ICT, which has been responsible for developing a **national certification scheme for those responsible for cybersecurity**.

Finally, at the request of a sectoral association and with the support of the Joint Cyberspace Command, a new group is in the process of being created that is designing the outline of a study to identify the needs and challenges of public-private collaboration in the field of cyber defence. The aim of this work is to have a broader knowledge and to analyse the current capabilities and generic needs of national cyber defence, in order to make progress in proposals or areas of R&D&I development.

The following is an executive summary of each work carried out.



Paper 1: Cybersecurity culture in Spain

+ 2.1

Paper 1: Cybersecurity culture in Spain

Prepared by Working Group 1 on Cybersecurity Culture

2.1.1. Why a Report?

Law 36/2015, of 28 September, on National Security, establishes that the Government will promote a **culture of National Security** that favours the active involvement of society in its preservation and guarantee, as an essential requirement for the enjoyment of freedom, justice, well-being, progress and the rights of citizens. It also points out that one of the **areas of special interest is cybersecurity**, which due to its unique characteristics and cross-cutting nature requires the action of all administrations and society in general to increase knowledge and awareness of the matter.

The 2019 ENCS (ENCS) establishes in its Objective IV the need to improve collective cybersecurity by spreading the culture of cybersecurity through collaboration between public bodies and private entities, enhancing information and assistance mechanisms for citizens and promoting meeting spaces for civil society, administrations and companies. Since cybersecurity is a shared responsibility, Public Administrations must maintain effective coordination with the private sector, citizens and civil society.

The **promotion of a culture of cybersecurity** is therefore one of the central axes for achieving a society that is more aware of the threats and challenges it faces, taking into account the right to enjoy a safe and reliable use of cyberspace and the obligation to contribute to this.

To this end, the National Cybersecurity Forum created the Cybersecurity Culture Working Group, which decided to begin its work by means of a Report in which an indicative analysis of the main existing national and international initiatives was carried out, identifying areas for improvement, lines of action and programmes to facilitate the development of new projects aimed at raising the culture of cybersecurity in Spain, and which should be understood as proposals and recommendations to the National Cybersecurity Council.

2.1.2. What do we mean by cybersecurity culture?

The Report defines the **culture of cybersecurity** as the knowledge and awareness of society in general and of each person in particular, of the risks and threats that could compromise it, of the efforts of the actors and organisations involved in safeguarding it and the co-responsibility of all in the measures of anticipation, prevention, detection, protection, resistance, collaboration and recovery with respect to these risks and threats.

As mentioned above, the 2019 ENCS sets the objective of promoting the culture and commitment to cybersecurity and boosting human and technological capabilities. Its development is embodied in action line seven articulated through eight measures, which constitute the backbone of the Report.

2.1.3 What are the objectives of the Report?

The Report has **4 main objectives**:

Objetive 1

To analyse existing national and international initiatives and trends aimed at promoting a culture of cybersecurity.

At the international level, the main initiatives of some countries have been analysed, such as the United Kingdom, the United States, France, Lithuania, Estonia and Singapore, which, together with Spain, and in that order, constitute the TOP of the Global Cybersecurity Index 2018 (CGI) ranking of the International Telecommunication Unit (ITU) of the United Nations.

At national level, the main existing initiatives carried out by both the public and private sectors, at central, autonomous and regional level, are included.

Objetive 2

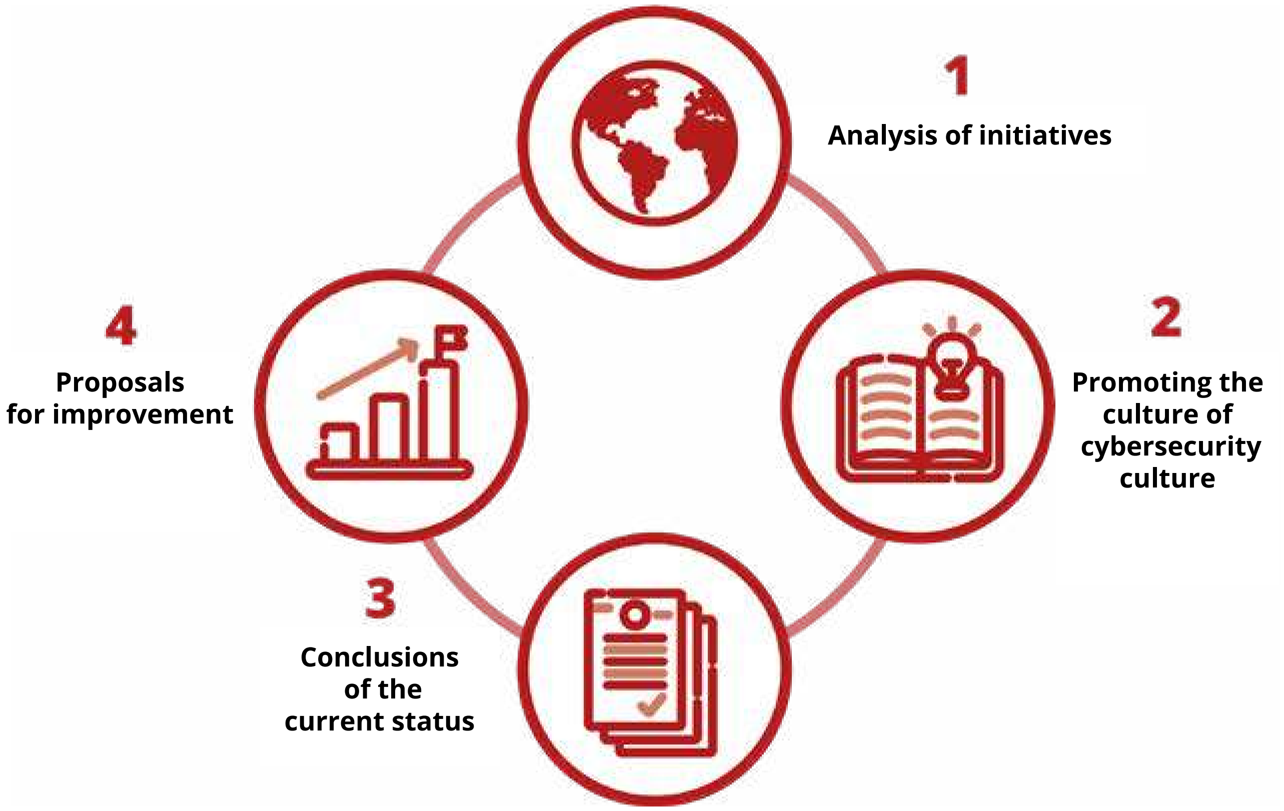
To inform possible actions aimed at fostering national cybersecurity culture and generating a shared social awareness of the importance of cybersecurity.

This objective in turn consists of 8 objectives, which coincide with the measures included in the ENCS:

» Increase awareness campaigns for citizens and companies, and provide them with useful information adapted to each profile, especially in the field of self-employed, small and medium-sized enterprises.

» Promote actions aimed at increasing the co-responsibility and obligations of society in national cybersecurity.

» Promote initiatives and plans for digital literacy in cybersecurity.


1
Analysis of initiatives
2
Promoting the culture of cybersecurity culture
3
Conclusions of the current status
4
Proposals for improvement

- Promote the dissemination of the culture of cybersecurity as a good business practice and recognize the involvement of companies in the improvement of collective cybersecurity as a corporate social responsibility.
- Promote a critical spirit in favour of truthful and quality information and contribute to the identification of fake news and disinformation.
- Raise awareness among managers of organizations, so that they enable the necessary resources and promote cybersecurity projects that their entities may need.
- Promote awareness and training in cybersecurity in educational centres, adapted to all training levels and specialities.
- Seek and recognize the collaboration and participation of the media in order to achieve greater reach in campaigns aimed at citizens and, in particular, minors.

These action plans identify possible areas where improvements can be made that can help achieve the implementation of these measures.

Objetive 3

To draw conclusions on the current state of cybersecurity culture in Spain and assess areas for improvement.

From the analysis of both international and national initiatives, a series of conclusions have been drawn regarding the state of cybersecurity culture in Spain, among which the following stand out:

- There is a disconnection between the many initiatives aimed at awareness-raising and sensitization and the lack of knowledge of their existence.
- There is no comprehensive and accurate picture of the state of cybersecurity culture in society and the impact of the initiatives undertaken.
- Lack of awareness of the cyber risks to which self-employed professionals and small businesses in specific sectoral areas are exposed.
- Cybersecurity in current curriculum designs is insufficient and cybersecurity awareness activities in schools are ad hoc.
- Media collaboration and participation in cybersecurity campaigns is very limited.

Objetive 4

To formulate proposals to improve the state of cybersecurity and generate social awareness of its importance.

In view of the initiatives undertaken, both nationally and internationally, there is a clear need to adopt a series of measures aimed at increasing the culture of cybersecurity and promoting a shared social awareness. These include training and awareness-raising actions in various areas, the reinforcement of culture in the educational sphere and the promotion of digital literacy.

Undoubtedly, the most important measure is the need to have a global and accurate view of the state of cybersecurity culture in society, as well as the impact of the initiatives collected and future campaigns. This measurement framework would be part of an **Observatory for the development and monitoring of the Comprehensive Cybersecurity Barometer** involving the industry and research ecosystem, the public and private sectors and citizens in general, with special dedication to a system for measuring the culture of cybersecurity in Spain.

2.1.4. Conclusions

The process of digitalization and digital transformation of our society has been accelerated by the COVID-19 pandemic, which has driven the adaptation of the private and public sector and society in general to a new reality on which the economic growth, recovery and social transformation at all levels must be based.

Therefore, **guaranteeing the cybersecurity** of this process must be one of the priorities and for this it is essential to know the risks to which one is exposed. For this reason, the **promotion of cybersecurity culture** is one of the central axes to achieve a society that is more aware of the threats and challenges it faces, taking into account the right to enjoy a safe and reliable use of cyberspace and the obligation to contribute to this.

In order to achieve this objective, **everyone's commitment** is essential. For this reason, this Report, in line with the National Cybersecurity Strategy, proposes a series of measures and actions to increase the degree of cybersecurity culture in all sectors and society in general and to increase the coordination, effectiveness and efficiency of current initiatives, in the conviction that a greater cybersecurity culture will make us stronger and more resilient to face the challenges that are yet to come.

Paper 2: Spanish cybersecurity industry and research

+ 2.2

Paper 2: Spanish cybersecurity industry and research

Prepared by Working Group 2 on support for industry and R&D&I.

The Spanish cybersecurity ecosystem has been developing over the last twenty years on the basis of solid legislative foundations and with the leadership of government agencies, technology centres, universities and user and supplier companies in the private sector. This background has positioned Spain as the fourth European country in terms of maturity level on some cybersecurity fronts at a global level.

However, if specific industry and research indicators were analysed, the position would drop in the ranking: the results of the research network are not being transferred to industry, the use of Spanish and European technology is scarce, and the penetration in the national market of specialised SMEs with excellent products and services is insufficient.

Until now, the actors work in silos in a poorly coordinated manner.

The public-private collaboration that has been established in the National Cybersecurity Forum (FNCS) can help to eliminate these silos and encourage all actors to work together.

The problem of R&D&I and industrial development is not exclusive to cybersecurity, although the sector has particular aspects due to its implications for national security. The boost to this innovative ecosystem should be based on both specific actions and more cross-cutting reforms.

2.2.1. How to improve applied knowledge of cybersecurity?

The basis of the improvement lies in an adequate measurement, aimed at specifying the following points:

Who?
Global cybersecurity value chain

What?
Taxonomy of cybersecurity competences

How and how much?
Cybersecurity barometer in industry and research

Where?
Integral observatory of cybersecurity

The study of the complete value chain, with the inclusion and categorization of new actors and roles, will allow a better understanding of the ecosystem, of the available capacities and will contribute to the elimination of barriers between them.

The value chain proposal includes a typification of actors by roles (decision makers, facilitators, knowledge providers, developers, supporters and customers), by size and by function in the value chain.

The disconnection between industry and research is the weakest link between the two major areas of the global value chain. The construction of a global cybersecurity value chain detailing the roles, activities and interactions between the different actors needs to be further developed.

Having a common taxonomy aligned with European criteria allows the categorization of market products and services, application domains, research and knowledge. It also facilitates the balanced mapping of the different entities that research, provide and demand cybersecurity services.

The current reality is that there is no single taxonomy of cybersecurity. The research considers it appropriate to work with the JRC taxonomy created by the European Commission, against which the international R&D&I community is mapped. For its part, the industry is usually mapped against the cybersecurity products and services of the ECSO taxonomy, which has become a reference at European level.

To increase the maturity of the ecosystem and avoid the existing gap at national and European level, it is critical to reach a consensus on a common taxonomy applicable to R&D&I and industry, which could be based on an evolution of the one proposed in the Report. It is proposed to continue with this work and to carry out a pilot to verify its validity.

The measurement of the maturity level of industry and research should take the form of a barometer that compiles key indicators, either for specific analysis (Industry and Research Barometer) or as a component of a broader barometer (Comprehensive Cybersecurity Barometer).

The barometer must identify the necessary indicators to measure the maturity of the components identified in the previous taxonomy and in each of the actors of the value chain, and it is essential to measure and know the current situation in Spain, to compare ourselves with Europe and to observe its evolution.

For the elaboration and monitoring of the Comprehensive Cybersecurity Barometer, the creation of a Cybersecurity Observatory is proposed, based on public-private collaboration and with the participation of all actors in the global value chain, especially research and industry.

2.2.2. What are the cybersecurity challenges for SMEs?

The group of SMEs is no stranger to the increase in frequency and severity of security incidents.

It is urgent that SMEs address digitization, and therefore all the necessary measures regarding cybersecurity. For this, the Next EU funds represent an extraordinary opportunity, so it is necessary that they are incorporated into the projects associated with its implementation through the Recovery, Transformation and Resilience Plan.

The small average size of Spanish companies can be a challenge when it comes to addressing the digital needs of the company and, particularly, those related to cybersecurity. Adaptation and customization to the specific circumstances of the SME must be the basis of all actions.

The proposals identified to respond to the cybersecurity challenges of Spanish SMEs and which, in turn, can be a boost for Spanish industry and research in cybersecurity are as follows:

Six proposals to address the cybersecurity challenges facing Spanish SMEs

+ **Raise the level of awareness of SMEs** about the existence of cybersecurity risks.

+ **Strengthen digital competencies in cybersecurity of SMEs**, through training and tools.

+ **To make a prospective of international programs to support cybersecurity in SMEs.**

+ **Define common, standardized and centralized metrics for measuring the aggregate level of cyber risk on SMEs in Spain.**

+ **Build a matrix that allows categorizing SMEs according to characteristics such as size, sector, level of digital maturity and human capital literacy, criticality of information and economic situation of the SME.** The ultimate goal is to adapt and customize cybersecurity content and tools to the specific circumstances of the company.

+ **Promote the development and encourage the dissemination in the market of cybersecurity products and services with the appropriate capillarity to reach SMEs and freelancers.**

In order to implement and execute the proposals and to do so as efficiently as possible, it is advisable to use existing institutions. To this goal, it is necessary to count on the coordinated participation of the entities and bodies that have an outstanding proximity to Spanish SMEs.

2.2.3
How to improve public-private collaboration in this area?

Public-private collaboration, which has been institutionalized in some areas of Spanish cybersecurity, has not yet been articulated in the field of research and industry.

It is proposed the creation of an ecosystem of industry and research in cybersecurity (EI2C) in connection with the rest of ecosystems. The EI2C's specific objective is to promote the application of research (knowledge) to public policies (services) and to the digital economy (industry) on a national scale. Its implementation must coincide with the operability of the Network and Community of National Coordination Centres of the EU.

Competently, the EI2C should specialise in applied research for the cybersecurity industry to facilitate scale and the sharing and transfer of knowledge, infrastructure and funding across the research and industry community.

To ensure its functioning and attractiveness, it is necessary to provide the EI2C with a set of instruments, a research agenda and a good governance system.

Instruments are needed to stimulate the participation of the different actors of the industry and research community (decision-makers, facilitators, insiders and developers) and to avoid their displacement to other European or technological ecosystems where better incentives are offered.

In particular, it is considered necessary to create a national cybersecurity budget to develop the measures envisaged in the NACS. Its creation, amount and purpose should be included in the National Cybersecurity Plan under development.

The definition of a strategic research and innovation agenda is essential to increase national technological and industrial autonomy and coordinate public and private priorities and programmes. Within it, the technological and industrial cybersecurity capabilities critical to national security and the instruments to develop them must be defined. Their development should be included in the National Cybersecurity Plan.

Finally, it is proposed to provide the EI2C with a governance system (hub) to lead the development of national industry and research, ensuring the participation of the public and private sectors in all phases of the collaboration process.

The adoption of the proposals is essential if the national strategic autonomy claimed in the ENCS is to be enhanced, the current dependence reduced and the national market share increased in line with the European Union's objectives for cybersecurity technologies.

These proposals will contribute to the development of Action Line 5 of the NSDS, and -in particular- to measures 1, 2 (invigorate the industrial sector), 3 (strengthen autonomy, intellectual property and national security) and 9 (promote R&D&I programmes).

2.2.4
What are the opportunities for R&D&I?

In order to position our technology on the international scene, a series of proposals must be addressed that will contribute in a structural way to promote the development of Spanish cybersecurity technology and stimulate its consumption.

It is necessary to define a strategic research and innovation agenda (SRIA) for Spain in the field of cybersecurity, aligned with EU priorities, our ENCS, and based on internationally accepted cybersecurity taxonomies.

Five lines of research aligned with the ENCS have been initially identified:

- **Develop the protection of digital identity** to improve the protection of citizens, the business fabric and the reliability of electronic services offered by public administrations.
- **Promote the creation of a network of 5G laboratories** that focus on cybersecurity within the design, deployment and operation processes.
- **To open a strategic line of research in security and artificial intelligence** that will serve as a framework for action to place us at the scientific-technological forefront in this field and facilitate the transfer to industry.
- **To open a strategic line of research in quantum technologies applied to cybersecurity challenges**. This line is reflected in the European Cybersecurity Strategy for the Digital Decade when mentioning the creation of the European cyber-shield based on quantum communications.
- **Open a strategic line of research in security by design, cybersecurity management and supply chain** that responds to current challenges of the national industry. Its development is foreseen in Action Line 5 (Measure 3) of the ENCS and in the Cybersecurity Act.

New funding models need to be designed to make these lines of research sustainable.

The ambition of reaching a position of international leadership will be more viable if the work is oriented with a perspective of specialization, selecting niches with high growth potential, low maturity of the competition and that responds to challenges of the most internationalized national industry.

It is necessary to design new funding models that make these lines of research sustainable and turn our ecosystem into an international benchmark.

Therefore, it is essential to carry out a comparative study of R&D&I capacities and funding models, taking as a reference public and private funding models that are different from the Spanish one and that can be considered successful benchmarks. The conclusions of the study will be oriented to select and prioritize the most appropriate instruments to finance the research lines that are part of the SRIA.

The sectoral cohesion of R&D&I activities in cybersecurity takes on a stellar role as a catalyst for efficiency.

The first step involves the creation of a cybersecurity competence network at Spanish level along the lines of the four European pilots: SPARTA, CyberSec4Europe, ECHO and CONCORDIA. In order to speed up its start-up, it is recommended to rely on the places with the highest concentration of R&D&I capabilities in cybersecurity.

The second step will be to create a comprehensive and detailed map of cybersecurity R&D&I capabilities, including business R&D&I and the specialization disciplines that may be present in each node.

In order to value all the work and project its quality and competitiveness, a campaign is proposed to promote the quality of national cybersecurity technology that instills confidence in the consumer business network.

The initial priority should be oriented towards the Spanish market: cybersecurity consumer organizations and cybersecurity solutions and services companies that are responsible for bringing technology to consumers.

Secondly, the campaign will be directed towards international geographies that have Spain as a reference (LATAM) or geopolitically related economies (such as the European Economic Area).

2.2.5 How can we generate, transform, retain and attract talent?

Cybersecurity talent is a scarce production factor, with an inelastic supply, and for which there is competition on a global scale. The time required to train this human capital varies depending on the profile, experience and knowledge, although they are, in general, long.

It is essential to raise awareness of early vocations as soon as possible, in schools and secondary schools. This action should be supported by scholarships and direct aid to outstanding students, as well as funding for the provision of laboratory infrastructures, in addition to giving visibility to professional development opportunities for young people in the media.

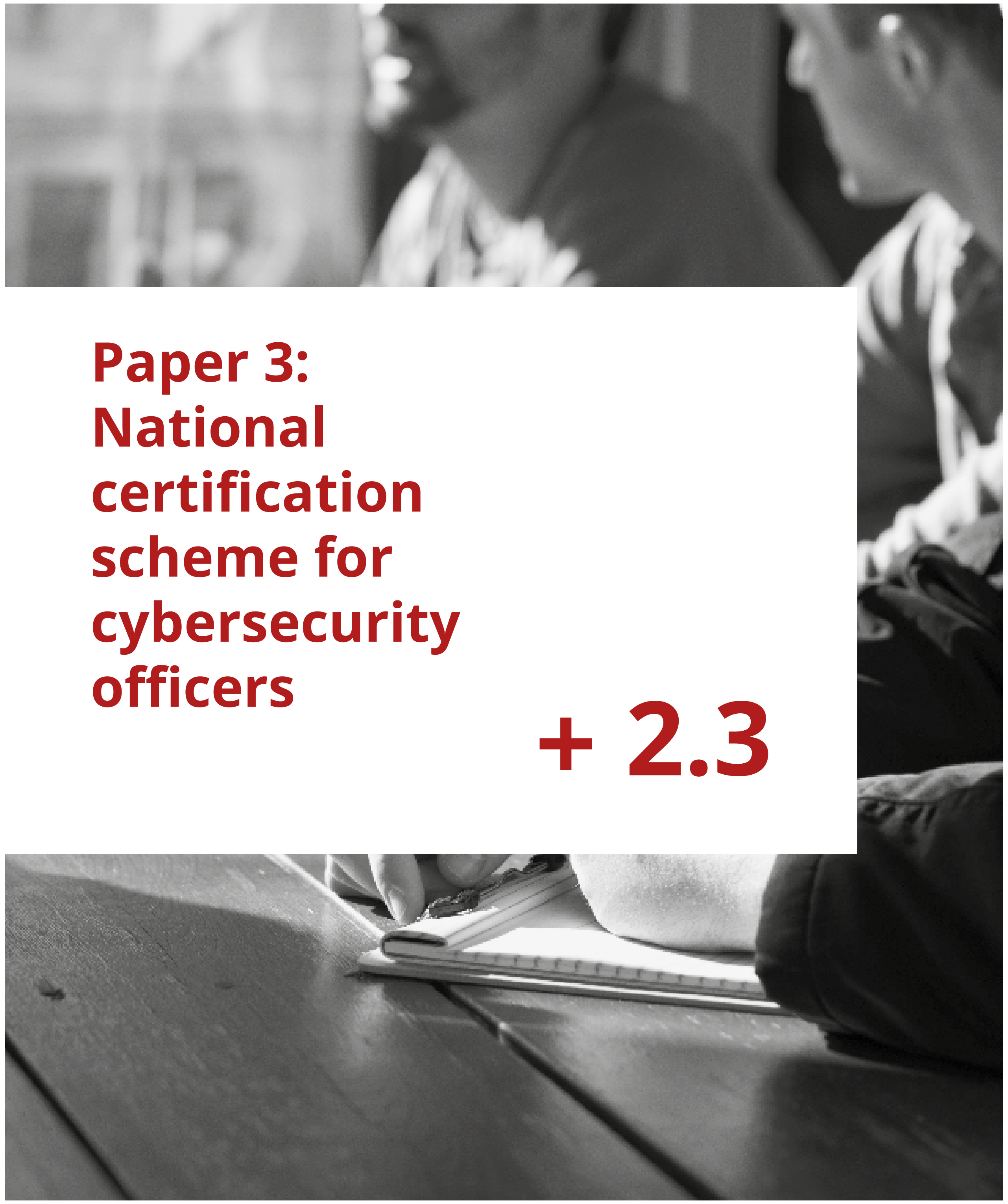
For today's workforce we need a framework that defines and harmonizes roles at European level, cataloguing professional competences and skills, guiding companies and workers on career design, wage and non-wage incentives, etc. The SPARTA CSF project is the ideal candidate that Spain can start implementing without delay and should support at European level.

The public authorities should support other organizational positions and professional profiles in cybersecurity, in addition to the Information Security Manager, and not only in the private sector, but also in the Public Administration itself, through the creation of a Senior Corps of Cybersecurity Risk Management Technicians of the AGE.

Singularly, the Armed Forces (FAS) and the State Security Forces and Corps (FF.CC.SS.EE), are organizations where the peculiar techniques of talent management can offer their best results and therefore, where their use can be more interesting for the best adaptation to the new challenges in the national defense.

In order to maximize the return on investment in R&D&I, both in the public and private sectors, which allows us to compete on a global scale, Spain must avoid the fragmentation and isolation of talent, as well as reduce the rigidity and cost of current administrative processes.

We must promote collaboration between technology and research centres, universities, public bodies and companies, with staff rotation, secondments, etc., in addition to reviewing the regulatory framework for entrepreneurship to encourage ideas and talented people, whether or not they arise within the public or private organisations that manage them.



Paper 3: National certification scheme for cybersecurity officers

+ 2.3

Paper 3: National certification scheme for cybersecurity officers

Prepared by Working Group 3 on training, education and mentoring

2.3.1. What is the National Cybersecurity Officers Certification Scheme?

The **National Cybersecurity Officers Certification Scheme (RCSEG)** sets the conditions and requirements for the certification of cybersecurity professionals. It encompasses four figures contained in two regulations: responsible for the Security of the National Security Scheme[1], responsible for Security and Liaison of critical infrastructures[2], responsible for information security and responsible for Security[3] of ICT services or products of companies that provide critical infrastructures or essential services[4].

2.3.2. Who are the agents of the Scheme?

The National Intelligence Centre, through the CCN; the Secretary of State for Digitalisation and Artificial Intelligence, through the SGAD; and the Secretary of State for Security, through the OCC, are co-owners of the Scheme and responsible for its promotion and development. They may authorize other agents to be part of it: ENAC and Certification Bodies.

[1] RD 3/2010, of 8 January

[2] Law 8/2011, of 28 April,

[3] Royal Decree 43/2021, of 26 January

[4] Law 40/2015 of 1 October

2.3.3. Who can be Certification Entities, CBs?

In order to operate within the Scheme, RCSEG CBs must be accredited by ENAC, in accordance with the requirements established in the UNE-EN ISO/IEC 17024:2012 standard for this Scheme.

To use the certification mark they must have the approval of the Scheme Management Committee and demonstrate a minimum of ten assessed persons.

A Register of already accredited Certification Entities and a Register of Certified Persons shall be generated.

2.3.4. What is the certification mark?

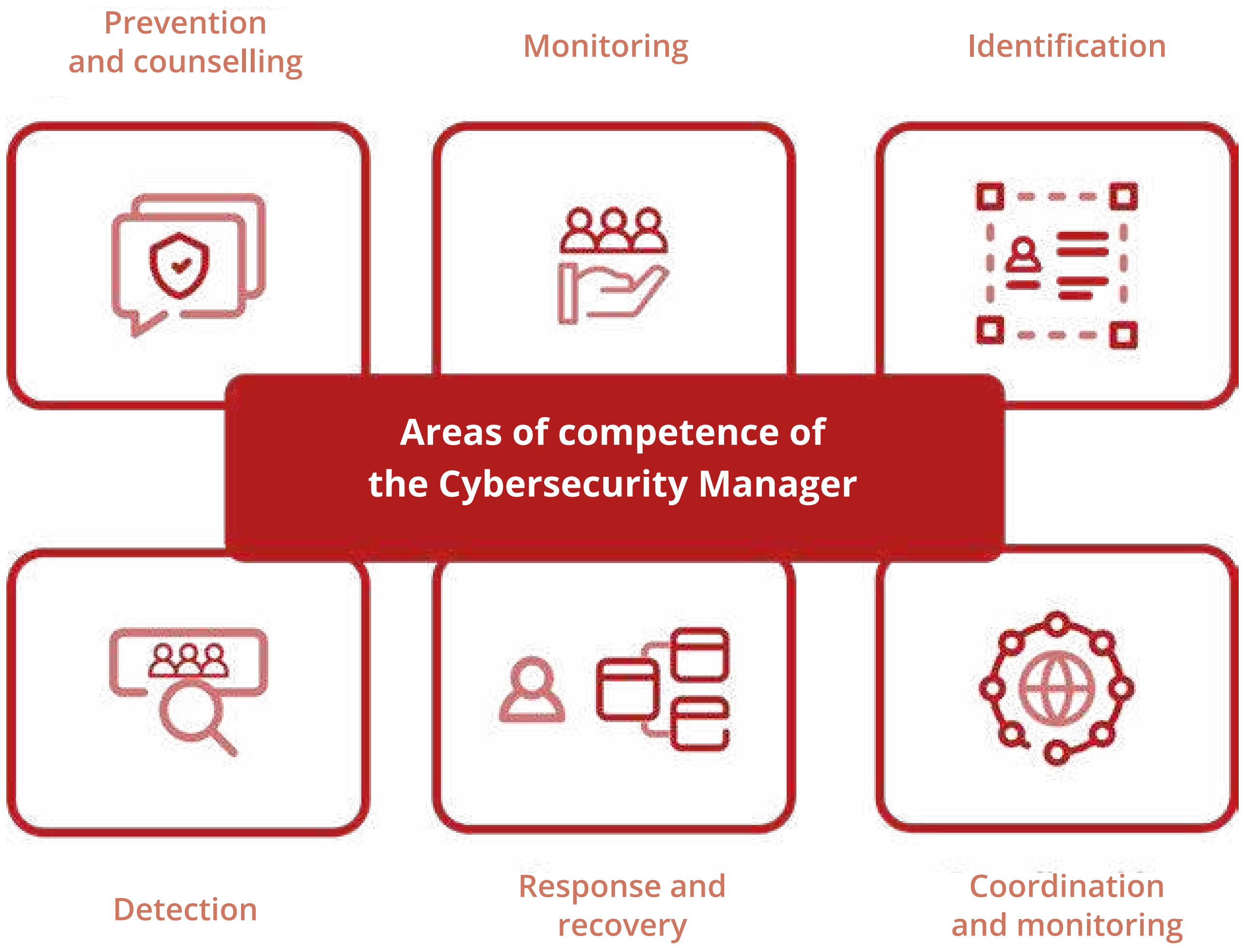
In order for the market to be able to identify the status of Certification Body and certified professional, the Scheme Mark is created. This symbol may be used on its own or associated to an own mark.

The Regulation of the National Certification Scheme specifically specifies the rules for the use of the mark and its model contract.

2.3.5. Who can be certified as Responsible for Cybersecurity, RCSEG?

The RCSEG must have specialized knowledge of cybersecurity, as well as practical experience in information security and, where appropriate, data protection. They must also be familiar with the ENS, the NIS Directive and its transposition to the Spanish legal system, the LPIC, including the regulations derived from or developing these regulations, as well as any other applicable regulations.

The generic competences of the RCSEG can be specified in the following capabilities, classified by areas:


Prevention and counselling
Monitoring
Identification
Areas of competence of the Cybersecurity Manager
Detection
Response and recovery
Coordination and monitoring

2.3.6. How can I access the RCSEG Certification?

There are two modes of access to certification:

Mode 1: certification aimed at professionals with **more than 15 years** of continuous **experience** in the competency areas covered by the Scheme. Access to the assessment will require a level 1 or higher qualification within the Spanish Framework of Qualifications for Higher Education (MECES).

Mode 2: certification aimed at **other professionals**. A university degree equivalent to or higher than a university degree (in ICT areas) will be required. Additionally, a requirement combining years of professional experience (two to five years) with minimum training (150 to 600 hours) will be required.

The Regulation of the RCSEG National Certification Scheme develops how the professional experience referred to in the aforementioned regulations shall be specified.

2.3.7. What is the evaluation procedure?

The evaluation process may be based on an assessment of competencies including:

Knowledge
Theoretical test type questions.

Skills
Practical questions with advanced simulations and exercises on laboratories or cyber-ranges platforms.

Attitude
Quantitative and qualitative analysis of the different possibilities of correctly performing the questions and skill exercises.

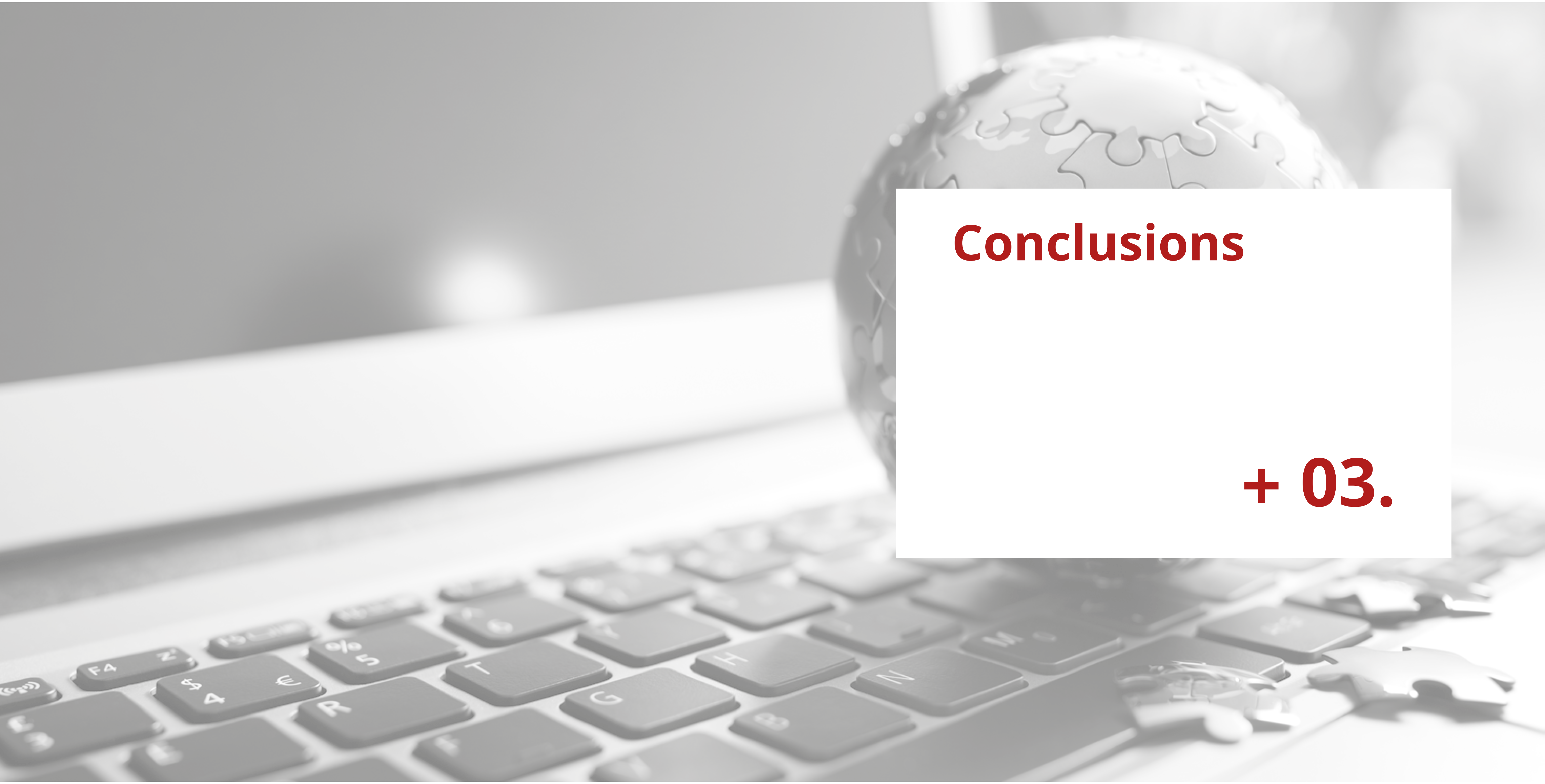
2.3.8. Is there a regulation governing the operation of this Scheme?

Yes, the **RCSEG National Certification Scheme Regulation** has been developed, which regulates the conditions and requirements that make up the operation of this Scheme, whose evaluation referential is based on the ISO/IEC 17024:2012 standard.

It contains the requirements to be accredited by the professional candidates to the certification processes (training and professional experience), the detailed syllabus for the Domains of the RCSEG Certification Scheme and the rules for the use of the Scheme Mark.

Likewise, the procedure for the selection and appointment of assessors of the candidates to receive the certificate; the model report of the results of the theoretical tests of the applicants and a model document justifying the certification are indicated.

Finally, the Regulation includes three annexes with the Code of Ethics for Certification Bodies and another for those responsible for Cybersecurity, as well as the main competencies and skills required of the RCSEG in monitoring technological trends, development of information security strategy, risk management and information security management and governance of information systems and services.



Conclusions

+ 03.

Conclusions

One year after its constitution, the National Cybersecurity Forum has become a success story, recognized both nationally and internationally, and is considered a good practice that can be extrapolated to other areas of national security and other countries.

The often mentioned, but rarely achieved public-private collaboration, has seen in the National Cybersecurity Forum a clear example of materialization with the completion of the first works commissioned by the National Cybersecurity Council, demonstrating how it is possible to take advantage of the existing synergies between the private and the public organisations in a field as cross-cutting as cybersecurity. All its components, professionals of recognised prestige in their respective areas, with the knowledge and experience pooled, have drawn up the first 3 works of the Forum.

The strength of the National Cybersecurity Forum lies in its composition and its degree of representativeness, in such a way that, through its members, it has managed to identify the best experts to participate in the different Working Groups and Subgroups.

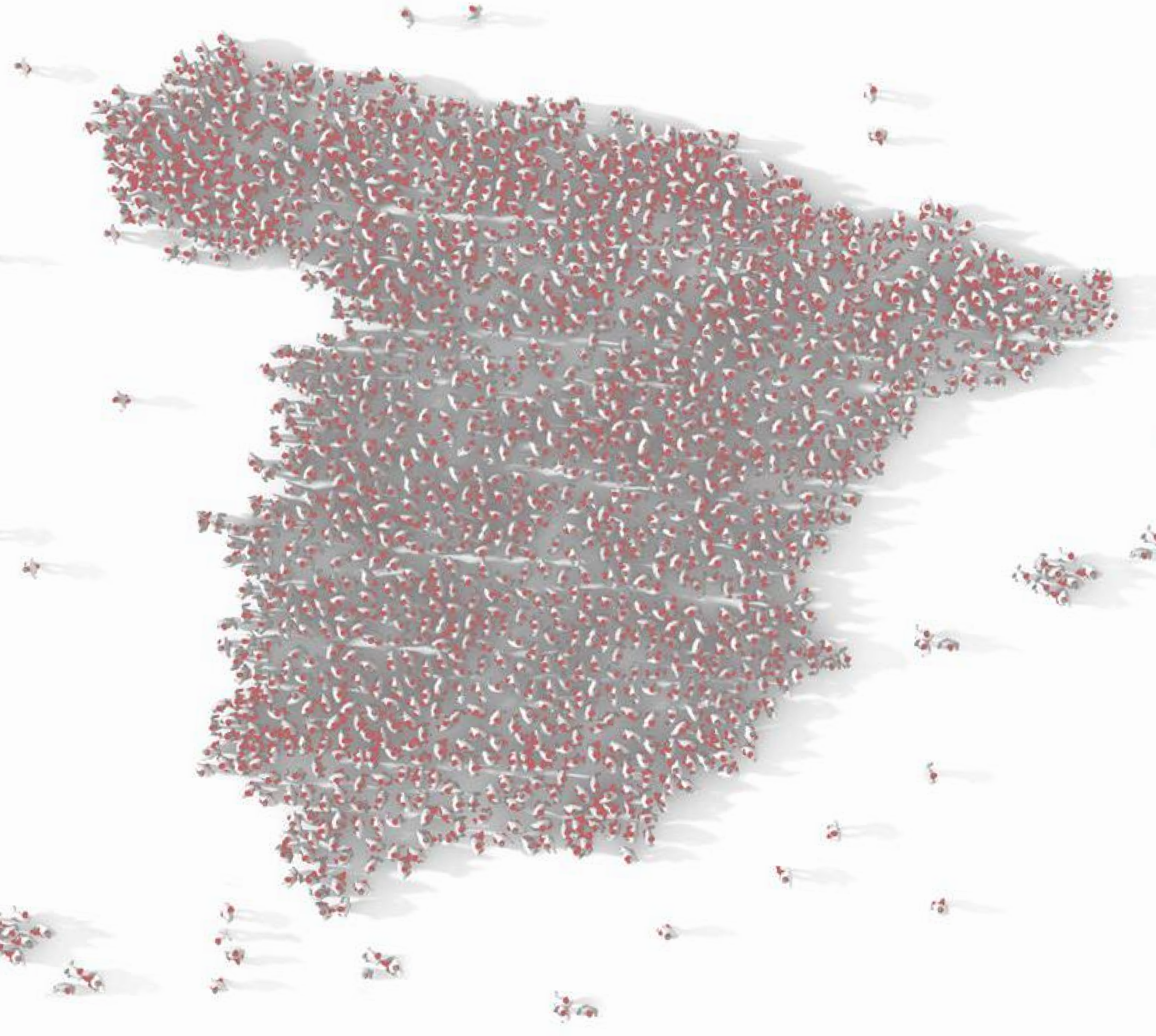
Finally, it should be noted that this work is a first step towards further progress in increasing public-private collaboration and new projects and actions to be undertaken in the future have been identified.

It will be the National Cybersecurity Forum itself and, ultimately, the National Cybersecurity Council, who will approve the projects carried out and establish and prioritize the new activities to be undertaken in the near future, always in line with the ENCS.

This work is a first step towards further progress in increasing public-private collaboration.

+++

NATIONAL CYBERSECURITY FORUM



FORO
NACIONAL DE
CIBERSEGURIDAD