ACTION PLAN

Institute for Business Competitiveness of Castilla y Leon

CYBER
Interreg Europe

European Union
European Regional
Development Fund

INTRODUCTION

At a time of an evolving landscape of threats, cybersecurity's place at the top of the EU's political agenda raises no doubts. Since its first ever cybersecurity strategy adopted in 2013, the EU has adopted and initiated a number of policy measures to strengthen its cybersecurity capabilities and resilience against cyberattacks: NIS Directive, Digital Single Market Strategy, the proposal to create the European Cybersecurity Competence Centre and Network, the EU Cybersecurity Act, as well as the Digital Europe and the Horizon Europe programmes.

The current EU policies suggest that in the context of cybersecurity, the core players are Member States' national governments, supported by dedicated EU bodies, such as the European Union Agency for Cybersecurity (ENISA). However, because of its multifaceted and all-encompassing nature, cybersecurity policy requires a diversification of the actors involved in its implementation. On one hand, ensuring a close cooperation with the private sector has been recognized as an important step in strengthening the EU's cybersecurity, resulting in the contractual public-private partnership on cybersecurity signed with the European Cyber Security Organisation (ECSO) in 2016. But on the other hand, European regions have often lacked recognition as important cybersecurity actors.

Uniquely positioned, regions hold a privileged connection to their local ecosystems. They have the biggest potential to connect technology with end users, to assist local small and medium enterprises (SMEs), and to provide them with business support and access to innovative technologies. Regions can significantly contribute to the development and deployment of European cybersecurity products and services, thus reducing the EU's reliance on solutions coming from third countries and non-European providers. In the near future, the EU cybersecurity landscape will be shaped by initiatives having a direct impact on regional ecosystems, such as the European Cybersecurity Competence Centre and Network, the European digital innovation hubs and renewed smart specialization strategy in each region. Interregional cooperation is therefore key to identifying solutions and moving towards a more integrated cybersecurity market.

The **CYBER project** has been initiated under the EU Interreg Europe programme and the European Regional Development Fund (ERDF) financial instrument to strengthen the local cybersecurity SMEs and to boost interactions among the European regional cybersecurity ecosystems. The lack of cooperation among different cybersecurity stakeholders and different ecosystems is identified as one of the challenges preventing local cybersecurity SMEs from scaling up and internationalizing their business. To address this challenge, project partners work together through a series of interregional events to develop and implement regional action plans and concrete policy instruments.

The CYBER involves nine institutional partners, representing different EU countries and regions:

- **Bretagne Development Innovation agency (France),**
- **Institute for Business Competitiveness of Castilla y León (Spain),**
- **Tuscan Region (Italy),**
- **Digital Wallonia agency (Belgium),**
- **Brittany Region (France),**

- **Kosice IT Valley (Slovakia),**
- **Chamber of Commerce and Industry of Slovenia (Slovenia),**
- **Estonian Information System Authority (Estonia),**
- **the European Cyber Security Organisation (Belgium).**

CYBER overall objective is to boost competitiveness of cybersecurity SMEs, thanks to improved public policies. It involves public authorities that can help knock down barriers of market fragmentation, lack of coordination of regional actors and lack of skills. Medium-term aim is to ensure greater coherence between offer and market demand, with a chance to build up skills and merge competences. In the long term, by making the digital world safer, the CYBER initiative contributes to the development of the EU digital market.

During its first phase, CYBER focused on identifying main barriers: lack of coordination between relevant actors, market fragmentation and lack of skills. For each barrier, regional strengths, weaknesses, opportunities and threats were identified, using SWOT analysis. The aim was to identify characteristics and key services that an innovation ecosystem supporting SMEs in the cybersecurity sector should deliver. Based on their level of cyber-development, CYBER partners also identified good practices that represent strengths of their territories and potential solutions to other partners' needs. These good practices fall under two different groups of policy measures: those that support the structure of the cyber innovation ecosystem and those that support advanced services provided within the ecosystem (such as labels, access to public and private funding, capacity building etc.). As a result of this interregional exchange process, good practices and solutions have been selected by partners in a perspective of transfer and adaptation and have been collected into **regional Action Plans**. These Actions Plans represent, for concerned regional authorities, a concrete road map for designing and targeting more and better funding to increase competitiveness of cybersecurity SMEs. Their relevance is also crucial within an EU context, as they provide inputs that can contribute to the European Investment for Growth and Jobs programme and the European Territorial Cooperation programme, as well as to address cybersecurity challenges through the newly proposed NIS2 Directive lenses. Produced by CYBER partners, these Actions Plans are therefore key documents both for regional cooperation across Europe and for policymaking at the EU level.

GENERAL INFORMATION

Name of the project: CYBER (Regional Policies for Competitive Cybersecurity SMEs)
Partner organization: Institute for Business Competitiveness of Castilla y Leon
Country: Spain
NUTS2 region: ES41

Contact person:

Beatriz Asensio Núñez	Montse Fernández Martínez	Ricardo Ramos Valdivieco
beatriz.asensio@jcyl.es	montserrat.fernandezmartinez@jcyl.es	ricardo.ramos@jcyl.es
+34 983 983 324 240	+34 983 324 158	+34 983 504 605

POLICY CONTEXT

The Action Plan aims to impact:

- *Investment for Growth and Jobs programme*
- European Territorial Cooperation programme
- Other regional development policy instrument

Name of the policy instrument addressed:

"2014-2020 ERDF Operational Programme of Castilla y León"

- Thematic objective 3: Improving the competitiveness of SMEs.
- Specifics Objectives:
    - • OE.3.1.2. Creation of new enterprises and business incubators with improved access to funding and advanced support services.
    - • OE.3.4.2. Promoting SME innovation and cooperation for innovation in all sectors.
    - • OE.3.4.3. Foster the internationalisation of SMEs.

DETAILS OF THE ACTIONS ENVISAGED

ACTION 1: Promotion, Monitoring, Follow-Up and Evaluation of the Improved Call for Grants 'Promotion of Innovation in SMEs' by Inclusion of New Topics Concerning Innovative Development Actions in Cybersecurity

The background

As part of the cyber project, a Regional Working Group on Cybersecurity (LOCKS) has been set up, including the Universities of Castilla y León, the Supercomputing Centre, AETICAL (Federation of Associations of Information, Communication and Electronic Technology Companies of Castilla y León), Large companies such as Telefónica, IBM, CSA or DELOITTE, as well as SMEs and specialized companies, Clusters, and other DIH such as IoT DIH (Internet of Things) and DIHBU (Advanced Manufacturing DIH), Technology Centers, the City of León, and the Castilla y León Regional Government itself.

In previous studies of the CYBER project at European level, three main **barriers to the competitiveness of SMEs** in cybersecurity were identified:

- Coordination between relevant actors.
- Market fragmentation / market access.
- Cybersecurity skills gap.

Taking these three barriers as a reference, the working group made an analysis and developed a **SWOT analysis** (Strengths, Weaknesses, Opportunities and Threats) for each of them, with the aim of detecting the territorial needs in terms of cybersecurity. The main cybersecurity needs detected were, among others:

- Regional public financing funds do not cover all the stages needed for a product development, its introduction in the market and its implementation by a company.
- Make companies aware of cybersecurity importance (it would lead to an increase in demand).
- Castilla y León is a big territory therefore the needed resources for support actions are high.
- Regional cybersecurity ecosystem is not well known.
- Actions for the attraction, recovery and retention of talent.

Of these needs, the first was considered the most important, therefore, as a result of the territorial analysis carried out, we identified the **improvement of innovation in cybersecurity** as the main **territorial need** that we would like to satisfy. As such, we decided to **modify the call for grants "Promotion of Innovation in SMEs"**, whose objective is granting of subsidies to facilitate the financing of business projects aimed at promoting innovation in the technological field of SMEs in Castilla y León. The modification consists in including new topics related to **cybersecurity**, as follows:

In the section on ***Eligible projects and requirements.***

- Projects for the **testing and validation of innovative products/services in cybersecurity** and enabling technologies of Industry 4.0 (among others Internet of things, Artificial Intelligence, Big Data, Robotics, additive manufacturing, 3D...) through the implementation of prototypes close to the market or vertically applicable in demonstrators, first customers or first use cases, provided that they are SMEs.
- **Cybersecurity audits** with customized implementations, **Projects** for the preparation of a certification in cybersecurity and/or digital trust, as well as any **Innovation action** in cybersecurity within the scope of this call.
- **Technological diagnosis** and advice to access and implement secure teleworking.

In the section on ***Eligible costs or expenses*****.**

- Costs of **certification** of systems implemented for process and/or product improvements.
- **Consultancy costs in cybersecurity** and related technologies (among others, Internet of Things, Artificial Intelligence, Big Data, Robotics...) oriented to the validation and testing of innovative products/services through the implementation of near-market prototypes or vertical applicable in demonstrators, first customers or first use cases, provided that they are SMEs (the direct beneficiaries of the subsidy will be the SMEs to which the solutions are implemented).
- Consultancy costs required for any innovation activity, cybersecurity audit with customized implementation of cybersecurity measures or for the preparation of the corresponding **certification and/or seal in cybersecurity and/or digital trust**.
- Consultancy costs for **technological diagnosis** and advice on accessing and implementing secure telework.

In the section on ***Justification of the conditions of the subsidy*****.**

- Presentation of the certification obtained as a result of the subsidized innovation actions, as well as the report of improvements on product/service derived from the implementation of prototypes or verticals in SME demonstrators. If applicable, technological diagnosis and results of the advice to access and implement safe teleworking.

We analyzed good practices from other regions and found two that fit our regional SME needs, and used them to improve our policy instrument:

1.“**Regional calls for testing innovative digital products and services**”, from the Regional Council of Brittany (Brittany, France).

Call to create a regional dynamic by accelerating and placing on the market innovative digital products and services applied to one of the priority sectors. This call for projects aims to:

- Promote these new interconnections vectors of innovation and new promising markets for Brittany.
- Foster the adaptation of an existing innovative digital solution on a new market or on its first targeted market.

2.**"Cybersecurity voucher"**, from the Slovene Enterprise Fund (Slovenia).

The purpose of the voucher is to encourage SMEs to increase their cybersecurity, thereby increasing their competitiveness, added value, and revenues from sale, through two types of bonuses:

- System security review, focused on SMEs of all sectors, for the realization of a system security review.
- Penetration test, focused on companies that develop some kind of product, (Web shop, Custom web application, Custom Mobile application, etc.), with the objective of testing it before launching it to the market.

At the 4th interregional meet-up in León (21-22 October 2019), the LP summarized the steps that will lead to the preparation of action plans. Starting with the SWOT analysis and thanks to the GP exchange, the partners have had access to the content needed to get inspiration from other regions and change our policy instruments. Working with regional stakeholders and interregional exchange have been key to identify significant improvement at policy level that responds to real territorial needs thanks to innovative solutions discovered in other partner regions.

The **learning process** was according to the following list:

- Presentation of the GP "Regional calls for testing innovative digital products and services" by the region of Brittany, at the meeting in Wallonia (4th-5th June 2019). We considered that one of the calls included (*Expérimentation d'innovations numériques*) has the potential to be incorporated into our political instrument.
- After initial consultations, the Region of Brittany provides us the call for its line of subsidies (*Expérimentation d'innovations numériques*). This call was then analyzed.
- Explore GP in a view of transfer to our region (in accordance with the policy instrument and the real needs of the regional SMEs), considering the incorporation of projects for:
    - For a SME, adapting an existing innovative digital solution to a new market.
    - For a start-up, getting a first customer reference on its first targeted market.

We decided to establish as an **action to improve our Policy Instrument**, the **modification of our call for grants "Promotion of Innovation in SMEs"**, incorporating the lessons learned in the exchange of experiences from the GP of Brittany, adapting them to the context of the region of Castilla y León. At the 4th consortium meeting, in León, this action was presented to the CYBER project team.

- CYBER/Conference Call 12th February: Audio conference of the CYBER project partners focused on the policy improvement process and exchange of actions and challenges. At this moment, each partner had linked learning with the policy improvement process and had started identifying actions. The purpose was to share the actions and contact with other regions that can help us. The exchange continued with bilateral contacts.
- On 3rd March 2020, a virtual **bilateral meeting** was held between the project teams of Brittany and Castilla y León to ask for details. Previously, a questionnaire was sent by e-mail to Brittany advancing the requested information. In this meeting, information was obtained about:
    - Structure of a project.
    - Role of the Technopoles.
    - Funding and financing.
    - Evaluation process.
    - Measure of success.
    - Issues in program implementation and development.
- From this *Bilateral Meeting*, the process of adapting the lessons learned to the call for aid "Promotion of Innovation" began.
- The virtual interregional meet-up (April 1st and 2nd, 2020) was essential in our learning process. The webinar presented on the GP "**Cybersecurity vouchers**" inspired the incorporation of its content into the policy instrument under modification. As we had very limited time to publish the modifications in the call, unfortunately no bilateral contacts were made with Slovenia, limiting the learning process to the detailed analysis of the Webinar and the GP published on the Interreg Europe website. Given the high quality of the content of both information sources, the aspects to be incorporated and the necessary adaptations to the context of Castilla y León were defined:
    - Review of the Cybersecurity system for companies in different sectors.
    - Testing Cybersecurity products and services before launching it to the market.

We are supported in the learning by **Brittany and Slovenia.**

The consequent **needs of adaptation** the GPs exchanged to the regional context of Castilla y León:

1.**"Regional calls for testing innovative digital products and services",** from the Regional Council of Brittany (Brittany, France):

In all projects, there must be a partnership, made up of at least a leader (SME located in Brittany) with a tester (any kind of structure, any location) to implement the solution developed. The tester must be legally independent of the project owner.

The call of grants is based on support for science and technological centers in Brittany as part of a regional strategy. All projects must be accompanied by a Breton Technological Center, for the development and supervision of the project.

The eligible costs in the call for *"Expérimentation d'innovations numériques"* are:

- Staff costs.
- Consumables.
- Amortization of R&D&I equipment
- Subcontracting expenses.
- Travel expenses.
- Indirect costs attributable to the project: 20% of staff costs.

In accordance with the process of the call for grants in which these lessons learned are incorporated, the new projects have been adapted. They retain the eligible concept, but the structure of the project and the eligible costs is simplified, so that the applicant for the subsidy is equivalent to the leading company, and the tester would not be involved. The Technological Centers are not involved either, with instead an SME in the sector providing the service and acting as an expert, and the subsidy covers only consultancy costs.

2.**"Cybersecurity voucher"**, from the Slovene Enterprise Fund (Slovenia)**:**

The applicant selects a contractor from the catalogue of experts in which contractors themselves are pre-registered, but the entry requires Digital Innovation Hub (DIH) Slovenia's approval.

The application is sent to the DIH, which evaluates and approves the project.

Once the project is completed and the service is paid to the provider, DIH validates documentation and pays the grant.

In the case of Slovenia, the criteria for adapting GP learning are the same. There is no catalogue of experts validated by DIH; the company can contract the service to companies in the sector. The role of DIH is substituted by the Institute for Business Competitiveness of Castilla y León (ICE), to which the application is sent, and after justifying the project, ICE pays the grant

.

The action

As described above, the policy instrument was modified during phase 1. The date of the modification of the call was 22/06/2020. The **actions** to be carried out during phase 2 focus on monitoring and promoting activities:

- Initiative 1: Promoting the call for grants "Promotion of Innovation in SMEs":
    - General information on the call.
    - Focus on new cybersecurity topics.

A communication plan has been designed to make companies in the region aware of the new funding opportunities for cybersecurity projects. Regular communications have been planned, using appropriate and available media: social networks, email communications to potential beneficiaries, sending information in ICE newsletters, planned online meetings, and others at the request of applicants to receive support and resolve doubts. These meetings and communications can be specific to this call (Promotion of innovation in SMEs) or in conjunction with other related grants, in the hope of reaching a wider audience and increasing the number of applications.

The design of the communication plan has considered the requirement to reach all SMEs in the Region, with a frequency enough to be known and remembered by all potential applicants for grants, but without too many messages that could cause them to lose attention.

The promotion plan for the call for grants to be carried out during phase 2 of the project is as follows:

Communication Channel	**Information**	**Frequency**
TWITTER	Message reminding of the availability of grants for funding cybersecurity projects, with a link to the website for more information and applications.	Published monthly
ICE Newsletter	A message with information on the different possibilities for funding support for cybersecurity projects, with a link to access more information or apply for each of them.	Published quarterly
E-mail	E-mail communication to potential beneficiaries. Informative communication on cybersecurity opportunities in the different calls for aid from ICE, with special mention of the "Promotion of innovation in SMEs".	Once per semester

Stakeholders meeting	One of the agenda items will be the progress of the action plan and the need to keep reminding potential grant recipients of the opportunities for funding support for cyber security projects.	Semester 7
ICE Website	Regular updates.	At least twice yearly

A record will be kept of the promotion actions carried out, which will make it possible to relate the progress made to the project's objectives and, if necessary, to modify the frequencies or include new actions.

- Initiative 2: Monitoring and follow-up of the defined indicators:
  - Definition of indicators.
  - Definition of monitoring calendar.
  - Monitoring of indicators.

In the sixth semester of phase 1, monitoring indicators have been determined to allow a proper analysis of the territorial impact of the action. The indicators under consideration are described in paragraph 7 of this part. At the same time as the indicators are defined, targets have been set.

Work has also done on some kind of impact indicator, which would make it possible to assess the increasing of maturity of companies in cyber-security aspects.

Monitoring data will be collected from the start of Phase 2, with a periodicity allowing sufficient time to assess the evolution, but not too high to be able to act if necessary. The frequency of data collection is described in section 7.

- Initiative 3: Data analysis:
  - Analysis of monitoring results
  - Verification of project success.

A monitoring report will be drawn up at the end of semester 7 with the first results obtained from the indicators, which will be updated at the end of each semester, based on the analysis of the data obtained in each period. Each data collection will allow to analyze the progress of the action, and to know the need to intensify the dissemination and diffusion actions.

This report, when updated at the end of phase 2 of the project, will result as the Final Report on the impact of the modification of the policy instrument on the evolution of the different indicators monitored, the increase in the maturity of our SMEs in the implementation of cybersecurity and the improvement of the competitiveness of Cybersecurity SMEs in the Region.

The report will include the results of the indicators obtained to date, data and graphical presentation of progress, as well as a review on the actions of promotion of the modification of the policy instrument carried out in the period. A final section of conclusions will include an analysis of the results.

Identified risks.

For a good analysis and evaluation of results it is necessary to have enough data to allow the conclusions to be representative of the sector in the Region. Therefore, the risks that have been identified, which could hinder the analysis of project results, are:

- A low number of responses to the surveys, and
- The call for grants for the *Promotion of Innovation in SMEs* will receive few applications in the analysis period.

In both cases, an analysis would be carried out on the diffusion and dissemination actions carried out so far, how they have reached SMEs, intensifying them and launching a new information campaign with new actions defined according to the results obtained, with the collaboration of the *Regional Cybersecurity Working Group* (Stakeholders).

The crisis situation generated by the COVID-19 pandemic in the business sector, and particularly in companies in the cybersecurity sector, may have as a direct consequence a lack of liquidity. This would penalize expenditure on the implementation and development of cybersecurity projects, which indirectly affects the response to both surveys and

requests for grants within the established monitoring period.

Players involved

ICE

Partner of the Interreg Europe CYBER project. It is the agency of regional economic development, with the competence of management of grants in Castilla y León, and responsible for the Calls for Grants. It has been directly responsible for the modifications introduced in the call for subsidies " Promotion of innovation in SMEs ", and its role in the implementation of the action plan is:

- Coordination of the participants in the action plan.
- Diffusion of the modifications made in the call for subsidies "Promotion of innovation in SMEs".
- Definition of indicators.
- Monitoring of the indicators.
- Analysis of monitoring data.

General Directorate for Budget and Statistic Regional Government of Castilla y León.

Policy: Managing Authority.

- Responsible for the efficient management and implementation of an operational program
- Responsible for the validation of the modifications made in the call for grants and ensure the fulfillment of its objectives.

Group of stakeholders (LOCKS).

They collaborate in the promotion and information about the new possibilities of financing in Cybersecurity of the call for grants "Promotion of innovation in SMEs and provide data on the state of maturity in cybersecurity. The LOCKs are involved in the definition of strategies and analysis of the results of the action since the sector requested the modification and will collaborate in the evaluation of the success of it.

Timeframe

SPECIFIC ACTIVITIES AND TIMEFRAME:

22/06/2020	Date of the modification of the call **"Promotion of Innovation in SMEs"**.
September – December 2020	First promoting actions: - Tweets - Stakeholders communications - ICE Technology Newsletter - Presentation at cybersecurity meetings or events …..
June 2021- May 2023	Indicator monitoring Promoting actions Analysis of the monitoring results
April – May 2023	Project Results
May 2023	End of the Project

Cost

Development of Action Plan: No extra costs, staff costs covered by the Institute for Business Competitiveness from Castilla y León (ERDF, policy instrument addressed).

Costs of funded projects: depending on project; typical project volume 10.000 – 50.000 €, min. 35% contribution of companies, up to 75% public funding

Funding sources

Action Plan, no relevant costs, only staff costs covered by own expenses.

Monitoring and indicators

Monitoring.

ICE will collect and report indicators. Beneficiary companies will be asked to cooperate in providing data for the evaluation of the impact of the grants.

The definition of indicators seeks not only a quantitative but also a qualitative approach to the analysis, allowing an assessment to be made of the competitive improvement of the sector.

The monitoring process starts in phase 2 (1 June 2021), with a defined frequency for each type of indicator.

7 **quantitative indicators** have been defined **(Group 1)**, obtained from the data ICE has on the subsidy files submitted and granted in the call for grants for the Promotion of Innovation in SMEs, with which the impact of the policy modification will be evaluated. The follow-up and monitoring of this group of indicators is quarterly, starting the analysis on 01 June 2021 from the data existing prior to the start of the monitoring, which will serve as a basis for comparison.

A **second group**, consisting of 2 **qualitative indicators**, will be calculated on the basis of a survey of the companies benefiting from grants. These indicators reflect the increase in the cybersecurity maturity of companies in the Region. This is an indirect monitoring factor of the success of the dissemination measures and of the modification of the policy instrument itself. For the calculation of this indicator, for each participating company (beneficiaries of grants under the call for grants in reference), the image in two moments or situations will be considered. (A. / B.):

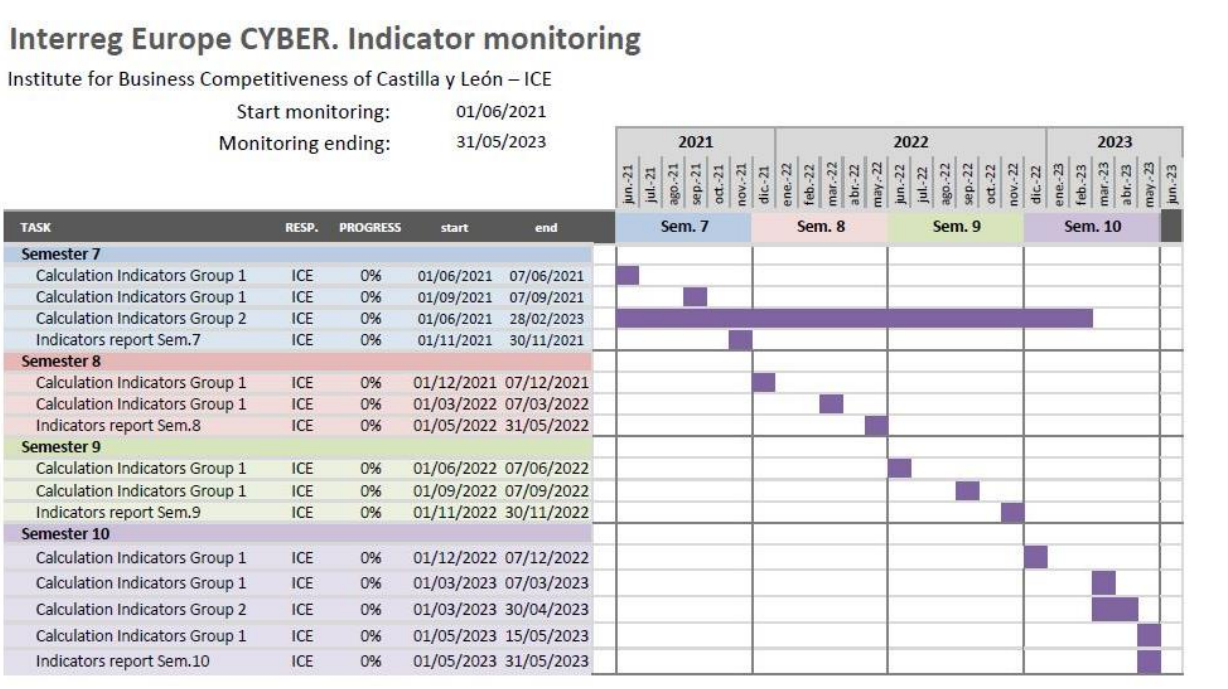
A. Situation preceding the implementation of the project. At the time of submission of the grant application. The beneficiary will be asked to fill in the survey at the time of making the application, making a quarterly compilation of the results. Start of monitoring coinciding with the beginning of phase 2 (June-July 2021), requesting the completion of the survey.

B. Advanced status of the project. At the beginning of the last quarter of phase 2 (March-April 2023).

During phase 2, the data corresponding to situation A., will be collected quarterly from the companies applying for aid corresponding to the "Promotion of Innovation in SMEs" call, and at the end of phase 2, the survey will be sent again to the beneficiary companies, obtaining the result of situation B.

The score in each situation is the percentage of companies in each of the four levels defined for each indicator (see definition of indicators).

The timeline of the different stages in the monitoring of the indicators is shown in the following image:



Indicators.

The way indicators are defined take into account two objectives: they must make it possible to assess the impact of Policy Change on the region's cybersecurity companies, and the evolution of the maturity in cybersecurity aspects of the regional business sector.

The initially defined indicator, which appears in the Application Form, is:

No. of entities benefiting from improved instruments to develop innovative activities in Cybersecurity (unit of measure: n° of entities).

We consider it suitable to keep this indicator as part of the Group 1 indicators, complementing them with additional indicators that allow us to quantitatively monitor the modification made to the policy instrument.

As indicated above, the indicators for monitoring the modification made to the policy instrument fall into two groups:

Group 1. Quantitative indicators. These indicators reflect the impact of the modification of the policy instrument on Cybersecurity Innovation Projects in SMEs in the Region.

The data used for the calculation of the following indicators concern the call for grants ***Promotion of Innovation in SMEs*** since the modification made to include new projects related to Cybersecurity (22/06/2020).

Indicator:	**APPLICATION FILES**		
I_1	Number of approved dossiers dealing with issues related to the modification of the policy instrument (Cybersecurity)		
	Unit of measure: **nº of dossiers**		
	Quarterly and cumulative monitoring	Quarterly Target: **3**	Cumulative Target: **25** *(31/05/2023)*
	Quantitative indicator measuring the success of the modification of the call for grants and the SMEs' appreciation of the modifications made.		

Indicator:	**% CYBER**	
I_2	Ratio of cumulative approved cybersecurity-related dossiers to total approved dossiers.	
	Unit of measure: **ratio**	
	Quarterly monitoring	Quarterly Target: **>0,15**
	Quantitative indicator that measures the boost in the success of the call due to the new cybersecurity actions incorporated.	

Indicator:	**ENTITIES**		
I_3	No. of entities benefiting from improved instruments to develop innovative activities in Cybersecurity (unit of measure: n° of entities).		
	Unit of measure*:* **n° of entities**		
	Quarterly and cumulative monitoring	Quarterly Target: **3**	Cumulative Target: **20** *(31/05/2023)*
	Quantitative indicator that measures the success of ICE's cybersecurity awareness and dissemination actions.		

Indicator:	**FINANCING call**		
I_4	Financial amount of the grants awarded.		
	Unit of measure: **€**		
	Quarterly and cumulative monitoring	Quarterly Target: **20 K€**	Cumulative Target: **150 K€** *(31/05/2023)*
	Quantitative indicator that measures the economic incentive of the call for grants to the cybersecurity sector.		

Indicator:	**INDUCED BUDGET**		
I_5	Overall budget of approved projects.		
	Unit of measure: **€**		
	Quarterly and cumulative monitoring	Quarterly Target: **40 K€**	Cumulative Target: **200 K€** *(31/05/2023)*
	Quantitative indicator that measures the impact of the new Cybersecurity actions incorporated in the economic dynamization of the sector in the Region.		

Indicator:	**SME contracting**	
I_6	Percentage of contracting with companies in the Region in approved files relating to cybersecurity actions.	
	Unit of measure: **%**	
	Cumulative monitoring	Cumulative Target: **50%** *(31/05/2023)*
	Quantitative indicator that indirectly measures the competitiveness of cybersecurity SMEs in the Region.	

Indicator:	**INNOVATION IN CYBERSECURITY**.		
I_7	Number of approved files related to innovation actions in cybersecurity *(Projects for the validation and testing of innovative products/services in cybersecurity through the implementation of near-market or vertical prototypes applicable in demonstrators, first customers or first use cases, and other innovation actions in cybersecurity).*		
	Unit of measure: ***Nº of files***		
	Quarterly and cumulative monitoring	Quarterly Target: **1**	Cumulative Target: **10** *(31/05/2023)*
	Quantitative indicator measuring the success of the inclusion of cybersecurity innovation actions in the call for grants		

Group 2. Qualitative indicators. These indicators reflect the increasing cybersecurity maturity of companies in the Region. This is an indirect monitoring factor of the success of the dissemination measures and of the modification of the policy instrument itself.

The data used for the calculation of the following indicators correspond to surveys carried out on companies applying for call for grants "Promotion of Innovation in SMEs" managed by ICE in two stages of phase 2 of the Interreg CYBER project: Application for a grant (June 2021-February 2023) / End Phase 2 (March-April 2023).

Calculation of the indicators: Based on the responses in the surveys, each entity is assigned a rating as a result of adding the numerical value of each response. Depending on the rating, the entities can be classified into four levels: Very low, Low, High, Very high, which reflect the degree of maturity in each section. The result calculated in each of the two situations (A./B.) is the percentage of companies with a high or very high rate. The cumulative value of the indicator (final result) is the percentage increase of enterprises with a high or very high rate between situations A. and B.

For the definition of these indicators, we have been inspired by those used in the report "EDPR 2017 - Integration of Digital Technology" (Europe's Digital Progress Report 2017), published by the European Commission

The indicators defined are:

Indicator:	**CYBER-SECURITY INTENSITY INDEX**
iIC	Based on the value obtained from the index, calculated from the survey responses, the company is categorized into one of the following four groups: - The company has a very low cybersecurity intensity index. - The company has a low cyber security intensity index. - The company has a high cyber-security intensity index - The company has a very high cyber security intensity index. The result is the percentage of companies included in each group.
	Unit of measure: ***% Level (Very low, Low, High, Very high)***
	Monitoring at Application for a grant and end of Phase 2 of the project
	Cumulative Target: **10%** percentage increase of entities with a high or very high rate between situation A. and B**.** *(31/05/2023)*
	Qualitative indicator. Measures the level of cybersecurity of the participating entities in terms of knowledge, planning and implementation of cybersecurity technology.

Indicator:	**EFFECTIVENESS RATIO in CYBERSECURITY**
iEC	Based on the value obtained from the index, calculated from the survey responses, the company is categorized into one of the following four groups: - The company has a very low effectiveness ratio in cybersecurity index. - The company has a low effectiveness ratio in cybersecurity index. - The company has a high effectiveness ratio in cybersecurity index - The company has a very high effectiveness ratio in cybersecurity index. The result is the percentage of companies included in each group.
	Unit of measure: ***% Level (Very low, Low, High, Very high)***
	Monitoring at Application for a grant and end of Phase 2 of the project
	Cumulative Target: **20%** percentage increase of entities with a high or very high rate between situation A. and B**.** *(31/05/2023)*
	Qualitative indicator. Measures the level of cybersecurity of participating entities in terms of awareness and effective implementation of cybersecurity technologies and procedures.

The **questions** included in the surveys for the calculation of these two indicators are as follows *(The answers and their assessment are included):*

***iIC*: CYBER-SECURITY INTENSITY INDEX**

a. Who performs the maintenance and installation of software on the computer systems:
   - *In-house IT staff/their own employees/an external contracted company.* (3/0/3)

b. Do you have contracted anti-virus software?
   - *Yes/No/Free online software* (3/0/0,5)

c. Do all computers use firewall software?
   - *Yes/No/Only those of employees with free access to information* (3/0/0,5)

d. Do employees with access to ICT devices (PC, smartphone, tablet, etc.) receive regular training/information on ICT security?
   - *Yes/No/Personally updated* (3/0/0)

e. Does the company have insurance to cover damages due to cyber-attacks?
   - *Yes/No/I think it is covered by general insurance* (3/0/0)

f. Do you have systems for the protection of your customers' and suppliers' information?
   - *Yes/No/I am not sure* (3/0/0)

g. Do we have a tested cybercrime response plan?
   - *Yes/No/No need* (3/0/0)

h. Is there access control/registration of visitors to the premises?
   - *Yes/No/Only control without logging* (3/0/0,5)

i. Do you have a system or procedure for updating passwords?
   - *Yes, mandatory/No/ Yes, recommended* (3/0/1)

j. Do you have a planned system of regular backups?
   - *Yes/No/Sometimes backups are made* (3/0/0,5)

k. In case of system downtime due to cyber-attacks, do you have an alternative plan to continue the activity?
   - *Yes/No/Not necessary* (3/0/0)

l. Physical access to servers and routers:
   - *Location with restricted access/In offices/No restricted access to provide access in case of problems* (3/0/0.5)

***iEC*: EFFECTIVENESS RATIO in CYBERSECURITY**

a. When faced with an IT problem, who acts in the first instance?
   - *Staff IT specialist/ The users themselves/ An employee with computer skills.* (3/0/1,5)

b. How often do you update your anti-virus software?
   - *It is done automatically/semi-annually/ I don't have anti-virus software* (3/0/0)

c. Are employees updated on new cyber risks with a certain frequency?
   - *Yes/No/When new risks appear* (3/0/1)

d. Have you had any problems or system downtime due to cyber-attacks in the last 12 months?
   - *Yes/No/I don't think so* (1/3/0)

e. How often do you use Windows Update?
   - *Automatic update option/I don't update Windows to avoid risks/annually/I don't know that application* (3/0/1/0)

f. Version of Windows installed on your computer:
   - *10/The one that came with the computer but is always up to date/I don't know* (3/1,5/0)

g. Does your organisation have an IT administrator who monitors all systems on a continuous basis?
   - *Yes, on a continuous basis/Regular monitoring/No* (3/1/0)

h. Is the backup plan complied with?
   - *Yes/No/I think so* (3/0/0)

i. Who has access to modify content on the website?
   - *All employees/Authorised users/IT Manager/external company* (0/1/2/3)

j. Is the company aware of and compliant with Cybersecurity and Data Protection legislation?
   - *Yes/Aware, but not 100% compliant/Don't know* (3/1/0)

k. Who has access to internal applications and digital information?
   - *All employees/ Authorised users/Users with password* (0/1/3)

l. Has a cybersecurity audit or diagnosis been carried out in the last year?
   - *Yes, by a specialised company/Yes, by a partner or employee/No* (3/0/0)

Based on the value obtained from the index, calculated from the survey responses, the company is categorized into one of the following four groups:

- *VLO*: The company has a very low effectiveness ratio in cybersecurity index. *Score between 0 and 10*
- *LO*: The company has a low effectiveness ratio in cybersecurity index. *Score between 11 and 20*
- *HI*: The company has a high effectiveness ratio in cybersecurity index. *Score between 21 and 30*
- *VHI*: The company has a very high effectiveness ratio in cybersecurity index. *Score between 31 and 36*

The result is the percentage of companies included in each group.

The concepts included in the survey reflect the analysis that the CYBER project working group.

Date

Signature: Beatriz Casado Sáenz

Head of Innovation and Entrepreneurship Department

CASADO SAENZ BEATRIZ ASUNCION - 00416096A

Firmado digitalmente por CASADO SAENZ BEATRIZ ASUNCION - 00416096A
Fecha: 2021.09.23 15:27:06 +02'00'

Stamp of the organization:

CYBER
Interreg Europe

Action plan Castilla y León (Institute for Business Competitiveness of Castilla y Leon – Endorsement letter

Valladolid, 24th September 2021

As Intermediate Body of the ERDF Regional Operational Plan of Castilla y León 2014-2020, I agree with the contents of the action plan for the Interreg-Europe project **CYBER** (*Regional Policies for Competitive Cybersecurity SMEs*), elaborated and to be carried out by the *Institute for Business Competitiveness of Castilla y Leon*) during the project's second phase.

Yours faithfully,

General Director for Budgets and Statistics