TC ABSTRACT

I. Basic Project Data

▪ Country/Region:	REGIONAL/IDB
▪ TC Name:	Strengthen Cybersecurity Public Policies and Human Capital in LAC countries
▪ TC Number:	RG-T4172
▪ Team Leader/Members:	Paz Gonzalez, Santiago (IFD/ICS) Team Leader; Nowersztern, Ariel (IFD/ICS) Alternate Team Leader; Pablo Libedinsky (IFD/ICS); Koo, Hyo-Sun (IFD/ICS); Florencia Baudino (IFD/ICS); Aguilar Blandon, Maria Alejandra (IFD/ICS); Vila Saint-Etienne, Sara (LEG/SGO); Lafuente, Mariano (IFD/ICS); Veyrat-Pontet, Alexandre (IFD/ICS)
▪ Taxonomy:	Client Support
▪ Number and name of operation supported by the TC:	N/A
▪ Date of TC Abstract:	26 Jul 2022
▪ Beneficiary:	Latin America and Caribbean member countries, in particular Brazil, Dominican Republic and Perú
▪ Executing Agency:	INTER-AMERICAN DEVELOPMENT BANK
▪ IDB funding requested:	US$500,000.00
▪ Local counterpart funding:	US$0.00
▪ Disbursement period:	36 months
▪ Types of consultants:	Individuals; Firms
▪ Prepared by Unit:	IFD/ICS - Innovation in Citizen Services Division
▪ Unit of Disbursement Responsibility:	IFD/ICS - Innovation in Citizen Services Division
▪ TC included in Country Strategy (y/n):	Yes
▪ TC included in CPD (y/n):	No
▪ Alignment to the Update to the Institutional Strategy 2020-2023:	Institutional capacity and rule of law

II. Objective and Justification

2.1 The objective is to assist beneficiary countries to strengthen cybersecurity public policies at the national and sectorial levels by: (i) assessing the cybersecurity GAP; (ii) designing action plans for the countries; (iii) providing support for cybersecurity education and training; and (iv) implementing cybersecurity pilot projects.

2.2 COVID-19 has accelerated the digitization of our societies, so cybersecurity has become central to the world's concerns. Cybersecurity is one of the fundamental enablers of digital transformation. Technological advances that improve our quality of life, such as telemedicine, e-health, online education, digital government, or e-commerce, would not be possible without cybersecurity measures that bring the system to an acceptable level of risk.

2.3 According to the World Economic Forum's Global Risk Report, cybersecurity is among the five most important risks faced by companies and citizens who mention the risk of their information being stolen as one of the factors that inhibits them from mass adoption of digital technologies.

2.4 The Inter-American Development Bank (IDB) and OAS assessed the evolving capacity of their member states to defend against the growing threats in the cyberspace. The 2020 Regional Cybersecurity Maturity Report: “Risks, Progress and the Way Forward in Latin America and the Caribbean” showed that only 13 of the 32 of the countries in the region have a national cybersecurity strategy in place. Furthermore, only

a few countries manage the exposure of their critical infrastructure –such as their energy, healthcare, telecommunications, transportation, water supply, and financial sectors– to cyberattacks. As revealed by the 2020 Report, only 7 countries of the 32 assessed had a critical infrastructure protection plan in place. This is one of the most worrying findings of all, considering the catastrophic impact that attacks on these sectors could have not only on national economies, but on the lives of all their citizens. Additionally of 32 countries, only 22 have a National Computer Emergency Response Team (CERT) in place, and just 7 of them have implemented a Governmental Cybersecurity Operations Center (GSOC). This reflects the region's a vulnerability, because the lack of CERTs and GSOC implies the absence of capability to detect and respond to cybersecurity incidents.

2.5 Governments, companies and other institutions around the world face a shortage of cybersecurity professionals estimated at more than 3 million, almost as many of occupied working positions. In the United States, unsatisfied demand is estimated over the 50%. More mature countries, such as the United States, the United Kingdom or Korea have faced this problem by developing action plans collaboratively with the entire cybersecurity ecosystem. However, this is not the case in the region, where the educational offer in cybersecurity is very limited. To change this situation, it is necessary to have teachers, laboratories, technologies, appropriate curricula and partnerships between government, private sector, and academia.

2.6 The Republic of Korea is considered one of the world leaders in cybersecurity, as can be seen in the Global Cybersecurity Index (GCI) prepared by the International Telecommunication Union (ITU) in 2021, where it is ranked 4th out of 194 countries analyzed.

III. Description of Activities and Outputs

3.1 **Component I: Cybersecurity policies roadmaps.** This component will finance: (i) Policy Makers Dialogues; (ii) Workshops on Cybersecurity Public Policy to design a Public Policy Development Roadmap for the region (iii) Sectorial Case of Studies of Recognized Cybersecurity Public Policies with special focus on the experience of Korea. The activities of this component will support the design of cybersecurity policy roadmaps in three countries.

3.2 **Component II: Strengthening capacity on education and human capital development.** This component will finance: (i) Support of recognized Universities and government organizations for the development of cybersecurity educational frameworks in the region; (ii) Advance cybersecurity training from lead institutions, using advance education platforms such as CyberRange; (ii) Cybersecurity knowledge material development.

3.3 **Component III: Cybersecurity pilot projects.** This component will finance three consultancy pilot projects based on the Korean experience of cybersecurity. Advanced conversations with the beneficiary countries led us to propose: a pilot project focused on strengthening the Brazilian CSIRT.gov.br with the development of an action plan; a cyber forensic pilot in Peru and its roadmap for next years; a critical infrastructure protection pilot in the Dominican Republic including the analysis of the current situation with a recommended roadmap.

IV. Budget

Indicative Budget

Activity/Component	Total Funding (IDB)
Cybersecurity policies roadmaps	US$200,000.00
Strengthening capacity on education and human capital development	US$120,000.00

Activity/Component	Total Funding (IDB)
Cybersecurity pilot projects	US$180,000.00
Total	**US$500,000.00**

V. Executing Agency and Execution Structure

5.1 This Regional TC will be executed by the Bank (HQ) through the Innovation in Citizens Services Division (IFD/ICS). The project team has demonstrated in previous editions its capacity for leading a project of this type.

5.2 Procurement: All activities to be executed under this TC will be contracted in accordance with the Bank policies as follows: (i) individual consultants, as established in the document AM-650 - Complementary Workforce; (ii) consulting firms for services of an intellectual nature according to the Policy for the Selection and Contracting of Consulting Firms in Bank executed Operational Work (GN-2765-4) and its associated operational guides (OP-1155-4); and (iii) logistic services and other services other than consulting, according to the Corporate Procurement Policy (GN-2303-28).

5.3 Over the past years, the Bank has undertaken significant efforts to support cybersecurity in the region, thereby accumulating valuable experience in this area. In addition, it has technical and administrative expertise in the execution of Research and Dissemination projects; thus, it can ensure that administrative burdens be reduced in the participating countries, particularly in the contracting of international experts, and that numerous LAC countries benefit from the activities of this TC.

VI. Project Risks and Issues

6.1 The main risks are: (i) the possible lack of coordination between in-country cybersecurity authorities and the agencies responsible for critical systems; and (ii) a high demand for training activities, which exceeds the scope of the project. These problems will be mitigated by: (i) defining a coordination and follow-up mechanism prior to the start of each initiative between the in-country cybersecurity authority and the agencies responsible for critical systems; and (ii) prioritizing the demand for training, with the guidance of the cybersecurity authorities as the governing body.

VII. Environmental and Social Classification

7.1 The ESG classification for this operation is "undefined".