TC Document

I. Basic Information for TC

▪ Country/Region:	REGIONAL
▪ TC Name:	Dissemination of advanced cybersecurity knowledge
▪ TC Number:	RG-T4135
▪ Team Leader/Members:	Nowersztern, Ariel (IFD/ICS) Team Leader; Paz Gonzalez, Santiago (IFD/ICS) Alternate Team Leader; Acevedo Calle, Daniela (LEG/SGO); Florencia Baudino (IFD/ICS); Laura Rodriguez (IFD/ICS); Nicolas Moreno (ORP/GCM); Oglialoro, Claudia (ORP/GCM); Pablo Libedinsky (IFD/ICS); Pedroza Pinzon, Paola Andrea (ORP/REM) Oglialoro, Claudia (ORP/GCM); Pablo Libedinsky (IFD/ICS); Pedroza Pinzon, Paola Andrea (ORP/REM)
▪ Taxonomy:	Research and Dissemination
▪ Operation Supported by the TC:	.
▪ Date of TC Abstract authorization:	05/10/2022
▪ Beneficiary:	Borrowing member countries of the Inter-American Development Bank
▪ Executing Agency and contact name:	Inter-American Development Bank
▪ Donors providing funding:	Cofinancing Special Grants(COF)
▪ IDB Funding Requested:[1]	US$189,191.00
▪ Local counterpart funding, if any:	US$0
▪ Disbursement period (which includes Execution period):	30 months (execution period: 24 months)
▪ Required start date:	June 2023
▪ Types of consultants:	Individual consultants and consulting 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):	N/A
▪ TC included in CPD (y/n):	N/A
▪ Alignment to the Update to the Institutional Strategy 2020-2023:	Institutional capacity and rule of law; Productivity and innovation

II. Objectives and Justification of the TC

2.1 **Background and justification**. Information and Communication Technologies (ICTs) have become the foundation of the efficient functioning of many key areas in Latin American and the Caribbean (LAC) countries, from access to public services to the generation and supply of healthcare, energy, water distribution, and transportation infrastructure, just to mention a few critical areas. The cyberspace, the online world of computer networks and the Internet, became the medium in which people, companies, governments, and machines communicate with each other and carry out transactions. This new ecosystem has also seen the emergence of novel specific harms such as financial theft, service disruption, information theft, cyber terrorist attacks, and cyber espionage. These threats have only grown over recent years. The 2018 report by McAfee and the Center for Strategic and International Studies (CSIS) on the economic impact of cybercrime, estimated that this activity costed the world economy around

[1] Unspent balance of the RG-T2788 ATN/CF-15598-RG from The Government of Israel.

$600 billion annually, or 0.8% of the global GDP, up from the estimated 0.7% in 2014. The most recent December 2020 release of the same report concluded that cybercrime now costs more than US$1 trillion, or over 1% of the global GDP.[2] Ransomware as a threat has evolved as well; such attacks are increasingly targeted, require higher ransom demands, and apply ever more sophisticated mechanisms. Many cyber threats rely on searching the Internet for vulnerable devices and networks, which leaves the increasing number of online users in developing countries with weak online security measures constantly exposed to potential attacks. In particular, the challenges posed by the COVID-19 pandemic, and the widespread move to remote work, set the stage for a spike in some forms of cyber threats, such as phishing and malware campaigns. Moreover, the Check Point Research 2021 Security Report[3] showed that over the first few months of 2020, almost a million attack attempts against Remote Desktop Protocol (RDP) connections, widely used among organizations for employees' remote connections, were observed every day. In fact, RDP attacks were the most popular form of cyberattack, surpassing even phishing emails. According to the ESET Latin America 2021 Security Report, in the LAC region, the number of RDP brute force attacks increased by 704% in 2020.[4] These trends only reaffirm our certainty that the sophistication of attacks and economic motivation driving cybercrime will only continue to intensify.

2.2 The increasing use of ICT in LAC is a catalyst for economic and social progress; however, it introduces inherent cybersecurity risks which must be managed on a continued basis, else citizen safety and the public trust in ICT, including consumer faith in online transactions and access to digital public services, may be negatively affected. Thus, strengthening cybersecurity is essential to safeguard citizens' rights in the digital sphere, such as privacy and property, to promote citizens' trust in digital technologies, and to support economic growth through safe digital transformation. Citizens must be assured that the digital systems they use for their personal or professional activities, as well as those that involve their personal data, possess adequate security measures to guarantee the integrity, confidentiality, and availability of their information and the services they depend on.

2.3 In this context, being prepared, and knowing where we stand, is key. The Inter-American Development Bank (IDB) carries out assessments to capture the evolving capacities of its 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", developed in partnership with the Organization of American States (OAS), showed that countries were in varying stages of development in their preparedness to face cybersecurity challenges, but generally still had ample room for improvement. While in 2016, the year of the report's first edition, 80% of the countries in the region did not have a national cybersecurity strategy in place, this number was only down to 60% in 2020. 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.[5] This is one of the most worrying findings of

---

2 Zhanna Malekos Smith and Eugenia Lostri. The Hidden Cost of Cybercrime.
3 Check Point Research 2021 Security Report.
4 ESET Latin America 2021 Security Report.
5 Argentina, Brazil, Dominican Republic, Jamaica, Panama, Paraguay, and Uruguay.

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.

2.4 In terms of countries' capacity to manage and respond to cybersecurity incidents, the same study found that 63% of countries had security incident response teams in place, such as Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Team (CSIRTs). However, of the 20 countries that did, only 3 had reached advanced maturity in their ability to coordinate such responses. In fact, 23 out of the 32 countries were still in an initial stage of maturity in this respect. This finding called attention to the general need for countries to strengthen the capacity of their teams to effectively coordinate their responses to cyber incidents.

2.5 This project builds on and intends to advance the work carried out through execution of Project ATN/CF-15598-RG, "Improving Human Resources Capacity in Cybersecurity", which has been in execution since 2016 with support from the Government of Israel. That work has contributed to LAC countries' efforts in strengthening their cybersecurity by documenting its status in the region and advising on the way forward through focused support in areas such as Security Operation Center (SOC) design, national cybersecurity work plan development, sectorial and workforce studies, and best practices documents; provided public sector cybersecurity professionals with access to advanced expertise through comprehensive on-site trainings held in Israel; and fostered regional knowledge exchanges at policymaking and sectorial workshops. This project is complementary to additional non reimbursable technical cooperations in the same subject matter, including ATN/CF-19154-RG, ATN/KR-19795-RG and ATN/OC-18936-RG.

2.6 As a result of these efforts, the Bank has seen a significant increase in demand by IDB member countries for technical and operational support in cybersecurity. This demand is expected to continue growing in the coming years, because of countries' increased awareness of the importance of protecting their cyberspace, on the national, sectoral, and organization-specific levels. For example, a great deal of public attention was drawn to the publication of "Israeli Cybersecurity Methodologies", a series of publications with 9 volumes to date, which have been translated into Spanish based on knowledge generated by the Israeli National Cybersecurity Directorate (INCD). These documents have had over 1,000 downloads in less than a month of their release.

2.7 This project will be carried out in partnership with the Government of Israel, which will donate not only resources via a project-specific grant, but also its advanced cybersecurity expertise for the benefit of LAC. Israel's cooperation with the IDB provides valuable knowledge and experience for many LAC countries which are taking preliminary steps to set up national cybersecurity initiatives.

2.8 Israel continues to be one of the most advanced countries worldwide in cybersecurity.[6] It has more than 400 firms specialized in cybersecurity and most of the big cybersecurity companies have research and development centers in Israel.[7] The National Cyber Directorate of Israel operates within the Prime Minister's Office and has the responsibility for implementing Israel's cybersecurity strategy.

---

6 Number of active cyber security companies in Israel from 2011 to 2021.

7 Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea and the United States. Inter-American Development Bank. 2016.

2.9 **Objective.** The objective of this project is to support beneficiary countries in strengthening the knowledge and capacity of their institutions responsible for addressing cybersecurity challenges by providing government officials and policy makers with access to knowledge, experience, best practices, and additionally, realizing select pilots' implementations with advanced technologies.

2.10 **Strategic alignment.** This Technical Cooperation (TC) is aligned with the Bank's "Update to the Institutional Strategy 2020-2023: Development Solutions that Reignite Growth and Improve Lives" (AB-3190-2), with the development challenge of Productivity and Innovation, by reducing risks introduced by the prevalence of ICT and digital innovations, thus increasing their adoption, and maximizing their benefits. It is also aligned with the Strategy's cross-cutting issue of Institutional Capacity and the Rule of Law, by strengthening capabilities to attend cybersecurity challenges. Finally this TC is aligned with SDG 9.A Facilitate sustainable and resilient infrastructure development in developing countries through enhanced financial, technological and technical support to African countries, least developed countries, landlocked developing countries and small island developing States 18, and 9.B Support domestic technology development, research and innovation in developing countries, including by ensuring a conducive policy environment for, inter alia, industrial diversification and value addition to commodities.

III. Description of activities/components and budget

3.1 **Component 1. Generation and documentation of best practices in cybersecurity (US$69,191).** This component supports the generation, design, publication and launch of knowledge products including documenting and training in best practices, policies, strategies, and methodologies, based on advanced experiences such as Israel's and the INCD's, data collection, diagnostic, research, and reporting products. This work will be carried out as needed by individual consultants, consulting firms and external service providers such as translators, designers, editors and similar.

3.2 **Component 2. Dissemination of knowledge and experiences in Cybersecurity (US$120,000).** The objective of this component is to provide a space for dialogue and the exchange of experiences and best practices through workshops, on-site visits, and dissemination events, benefitting participants from LAC governments, public sector, and critical organizations, by showcasing advanced experiences such as Israel's. The events' agenda will focus on key elements of cybersecurity practice, including public policy, identification, protection, detection, response, recovery, and resilience capabilities. One or two workshops are planned to be held in Israel as a leading country in the field of cybersecurity but could be held in another country if dialogue with LAC countries so indicates, in which case it will have an Israeli presence.

This component will finance said workshops, on-site visits and dissemination events including travel, logistical, venue, organization and coordination by individuals or consulting firms, interpretation, related materials, and production expenses as needed.

3.3 In addition, travel expenses for staff members of the Bank may be funded by this project when necessary for the execution of project activities, such as events, knowledge generation, disseminating methodologies for development, and regional networks. Such expenses are contemplated in the project budget table and may be required according to the amount of international in person activities.

3.4 The beneficiaries of this project's components and activities will be selected to include at least 10 countries (in total) from all different Country Departments. Participant selection considerations include the potential for significant, effective, efficient, and inclusive development impact including synergies with Bank operations and with other technical assistance; the availability of co-financing for project activities for additional leverage; an incipient cybersecurity maturity level; equitability; and on a first come-first-serve basis.

3.5 The Government of Israel expects to commit US$189,191 to this project, which are unexecuted funds from the Technical Cooperation ATN/CF-15598-RG. This TC will be subject to the corresponding Management Agreement to be formalized between the Bank and the Donor.

Indicative Budget (US$)

Component	Total Funding (IDB)
Component 1: Generation and documentation of best practices in cybersecurity	$69,191
Component 2: Dissemination of knowledge and experiences in Cybersecurity	$120,000
Total	**US$189.191**

3.6 Resources of this project to be received from the Government of Israel will be provided to the Bank through a Project Specific Grant (PSG). A PSG is administered by the Bank according to the "Report on COFABS, Ad-Hocs and CLFGS and a Proposal to Unify Them as Project Specific Grants (PSGs)" (Document SC-114). As contemplated in these procedures, the commitment from the Government of Israel will be established through a separate administration arrangement ("Administration Agreement").[8]

IV. Executing agency and execution structure

4.1 This TC will be executed by the Bank through the Innovation in Citizen Services Division (IFD/ICS). Over the past years, the Bank has undertaken significant efforts to support cybersecurity in the region, thereby accumulating valuable experience in this area. Specifically, experience has been gained executing project ATN/CF-15598-RG, "Improving Human Resources Capacity in Cybersecurity", which has been in execution between 2016 and 2022 with support from the Government of Israel. 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, and thus numerous LAC countries could benefit from the activities of this TC.

4.2 The Cybersecurity Specialist of IFD/ICS will be responsible for the management of the day-to-day activities of this project, including budget planning, design, and implementation, contract supervision, project communications and periodic reporting.

4.3 The project team will coordinate the execution of this TC with IDB Country Offices as relevant, including when events, delegations or missions are held in beneficiary

[8] The fee is not included in the Budget table because the 5% of the total contribution was already charged in the operation RG-T2788 - ATN/CF-15598-RG.

countries, and when pilot projects or interventions focus on organizations in specific countries. Realizing missions, delegations, events, pilot projects and interventions in LAC counties will require non-objection letters, requests, and authorizations in writing by said countries, as relevant.

4.4 The Bank and the Donor will review the project execution by means of periodic meetings, semiannually or as needed to analyze progress, discuss strategic planning and implementation issues, and point out emerging opportunities for increased impact.

4.5 The Israeli National Cyber Directorate will make its and other Israeli methodologies, procedures, experience, tools, findings, and know-how available to improve cybersecurity in LAC countries, sectors, and organizations. Such in-kind donations of expertise may be utilized where applicable. This project supports said knowledge transfer to LAC by aptly incorporating it into some of the abovementioned project activities, by providing administrative and logistical support, and by financing expenses required to realize the in-kind donations.

4.6 **Procurement**. All TC activities will be contracted in accordance with Bank's current procurement policies and procedures, including AM-650 for individuals, GN-2765-4 and its operational guides (OP-1155-4) for firms, and GN-2303-28 for non-consulting services. Non consulting services include logistical or incidental costs incurred to carry out project activities, such as those mentioned in section 3.4.

4.7 **Reporting**. The Project Team will be responsible for the preparation and submission of project reporting to the Donor, as stipulated in the Administration Agreement. If, at the end of project execution, the project is closed with a positive uncommitted and unspent balance, the project team will be responsible for requesting ORP/GCM to transfer the unspent balance as agreed to by the Donor and the Bank pursuant to the terms of the Administration Agreement.

4.8 **Monitoring and evaluation**. The Project Team will conduct project monitoring and evaluation in according to the Bank's Technical Cooperation Monitoring and Reporting (TCM) framework.

4.9 **Data privacy**. TC activities will be conducted in accordance with Bank's current personal data privacy and protection policies and procedures, including AM-305 for Information Resources Security.

V. Major issues

5.1 Varying travel and gathering restrictions due to the global Covid-19 pandemic may affect the ability to hold in-person international events, delegations, and activities. This risk will be mitigated by monitoring ongoing conditions and scheduling activities, accordingly, only starting in 2023. In case in-person events could not be held as planned, event plans would be adapted to accommodate prevailing restrictions, changed to virtual modalities, or reduced.

5.2 Furthermore, given the limited availability of human resources in the institutions responsible for cybersecurity in LAC, government might be reluctant to let their cybersecurity experts to be away from office for a certain period even if for training purposes. This risk will be mitigated by limiting the length of the training activities and by assuring the availability of daily time to maintain contact with their offices of origin.

5.3 Finally, there exists the challenge of promoting cybersecurity efforts that are sustained over time evolve continuously. To mitigate this risk, this project's aspect of providing support to Bank specialists in integrating cybersecurity in sectoral operations is key, as it is expected to lead to cybersecurity components and activities in investment operations, which may be larger in scale and will execute over the long term.

VI. Exceptions to Bank policy

6.1 No exceptions to Bank policy are foreseen.

VII. Environmental and Social Strategy

This TC will not finance feasibility or pre-feasibility studies of investment projects or associated environmental and social studies; therefore, it does not have applicable.

Annexes:

Request from the Client - RG-T4135

Results Matrix - RG-T4135

Terms of Reference - RG-T4135

Procurement Plan - RG-T4135