# TC Document

## I. Basic Information for TC

| | |
|---|---|
| ▪ Country/Region: | REGIONAL |
| ▪ TC Name: | Strengthening Cybersecurity Capacity in LAC |
| ▪ TC Number: | RG-T4010 |
| ▪ Team Leader/Members: | Nowersztern, Ariel (IFD/ICS) Team Leader; Paz Gonzalez, Santiago (IFD/ICS) Alternate Team Leader; Acevedo Calle, Daniela (LEG/SGO); Isabel Williamson, David Alejandro (ORP/GCM); Katia Rivera (IFD/ICS); Libedinsky, Pablo (IFD/ICS); Michelle Manzur Madariaga (IFD/ICS); Pedroza Pinzon, Paola Andrea (ORP/REM); Rojas Gonzalez, Sonia Amalia (IFD/ICS) |
| ▪ Taxonomy: | Research and Dissemination |
| ▪ Operation Supported by the TC: | . |
| ▪ Date of TC Abstract authorization: | October 13, 2021. |
| ▪ 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$2,000,000.00 |
| ▪ Local counterpart funding, if any: | US$0 |
| ▪ Disbursement period (which includes Execution period): | 48 months (execution period: 42 months) |
| ▪ Required start date: | December 2021 |
| ▪ 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 2010-2020: | Productivity and innovation; Institutional capacity and rule of law |

## 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 the 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] These funds will be administered by the IDB through a Project-Specific Grant (PSG). The Government of Israel will contribute US$2,000,000 in the form of PSG and will be subject to the corresponding Administration Agreement to be entered into between the Bank and the Donor.

$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 The Hidden Cost of Cybercrime, McAfee & CSIS.
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 Specific Grant 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.

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, as a result of countries' increased awareness of the importance of protecting their cyberspace, on the national, sectoral and organization-specific levels.

2.7 This project is carried out in partnership with the Government of Israel, which is donating 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 500 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.

2.9 **Objective.** The objective of this project is to assist beneficiary countries to strengthen the capacity of their institutions to cope with cybersecurity challenges, by supporting their cybersecurity capacity at the national, sectorial and organizational levels, and by providing government officials and policymakers access to the most advanced training, knowledge, expertise and best practices worldwide.

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

---

6 Why Israel Dominates in Cyber Security. Fortune.

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

Growth and Improve Lives" (AB-3190-2), in particular 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 supporting the modernization of legal and regulatory frameworks to attend cybersecurity challenges and by strengthening cybersecurity capacities and governance at national, sectorial and organizational levels. Moreover, it is aligned with the Bank's "Vision 2025. Reinvest in the Americas: A Decade of Opportunity" (AB-3266), in particular with the opportunities presented by the Digital Economy. In this sense, this project will contribute to the Bank's efforts to leverage the benefits of technology while mitigating its risks, via: (i) supporting the adoption of global innovations and digital technologies in the public and private sectors, while dealing effectively and efficiently with the underlying cybersecurity risks involved; (ii) investing in the necessary pre-conditions of digital technology adoption, such as institutional development and regulatory reforms; (iii) strengthening the Bank's position as a trusted broker and advisor in the face of the growing complexity of such developments, while fostering opportunities for regional cooperation in addressing them; and (iv) supporting the region in attracting, training and retaining public sector employees in the context of the increasing digitalization of governments.

## III. Description of activities/components and budget

3.1 **Component 1. Develop national cybersecurity capacity (US$635,000).** This component will support beneficiary countries[8] in strengthening their national cybersecurity capacity, by planning the improvement of operational capabilities such as SOCs and CERT/CSIRTs;[9] assessing and recommending governance, strategy, and public policy aspects; designing national initiatives for issues such as workforce skill building and threat information sharing. These efforts will benefit from advanced experiences and accumulated knowledge such as Israel's CyberNet information sharing platform. The planned activities include: (i) 6 pilot study projects to provide policy and technical advice to different countries' national authorities; (ii) 4 regional and thematic studies to gather information and provide guidance in dealing with cybersecurity issues at the national level; (iii) executive trainings to be offered to 35 public officials with cybersecurity responsibilities from beneficiary countries[10]. These trainings will be provided on site, in Israel, through the most important academic institutions[11] and experts in the country; the National Cybersecurity Directorate (Office of the Prime Minister of Israel) will support the organization of these courses that will last between 10 and 15 days; (iv) the production of 2 LAC workshops, events and policymaker dialogues that will bring together government officials, and may include

---

8 The specific beneficiaries of Component 1 will be government organizations and their officials responsible for aspects of cybersecurity on the national level, often within Ministries of Presidency, Interior, National Security, Telecommunications, e-Government agencies and similar.

9 Computer Emergency Response Team / Computer Security Incident Response Team.

10 One instance including 35 trainees is planned. Trainees will be selected from an applicant pool, which is populated through an open call for candidacies, outreach through country offices and through beneficiary cybersecurity contacts. The selection considerations from the pool will be as outlined in article 3.6, aiming to include at least one qualified applicant per beneficiary country per instance of the training.

11 The Hebrew University of Jerusalem is world-renowned for its research and teaching, with a strong cybersecurity practice. After evaluating alternatives, it has been selected to provide several trainings carried out in 2018 and 2019, which had very high participant satisfaction rates and reasonable costs. The Hebrew University is expected to be contracted as a Single Source supplier for similar trainings.

partners, international experts, and Israeli experiences; and (v) supporting LAC cybersecurity networks focusing on constituents like academic institutions, government officials or professionals.

3.2 **Component 2. Develop sectorial cybersecurity capacity (US$405,000).** This component will strengthen the capacity of the different sectors[12] that the Bank supports in LAC, such as the financial, transportation, healthcare, utilities, law enforcement and others, to build capacity and respond to cybersecurity challenges, such as by assessing sectorial posture, supporting sectorial ISACs,[13] sectorial SOCs, critical infrastructure regulation and forensics capabilities, using best practices, methodologies and experiences such as those of Israel. The planned activities include: (i) 6 pilot study projects to provide policy and technical advice to different sectorial authorities; (ii) 4 regional and thematic studies to gather information and provide guidance in dealing with sectorial cybersecurity issues; (iii) sectorial-themed workshops and study tours -a total of one study tour is planned to be held in Israel as a leading country in the field of cybersecurity, but could be held in a different country if the dialogue with LAC countries indicate so, in which case it will have an Israeli presence; (iv) the participation of 6 experts in events related to cybersecurity in specific sectors; and (v) creating 3 evaluation tools and methodologies to incorporate cybersecurity in development projects.

3.3 **Component 3. Develop organizational cybersecurity capacity (US$780,000).** This component will provide in-depth consulting project support to strengthen public-sector organizational cybersecurity capacity in beneficiary countries.[14] The planned activities include: (i) providing technical advisory and supporting 24 beneficiary organizations to apply stronger cybersecurity processes and technologies using internal consultancies; (ii) providing 12 instances of focused services to promote cyber-readiness in client government units, using external consultancies; (iii) 14 instances of utilizing technological platforms for information sharing, cyber-readiness assessment, visibility and preparedness; (iv) producing 3 cybersecurity best practices guides, evaluation tools and learning materials for organizations; (v) producing 3 online learning materials, and knowledge sharing and dissemination activities; and (vi) organizing 14 presential and virtual events, workshops, study tours, policy dialogues, and trainings for client personnel with cybersecurity responsibilities.

3.4 The realization of pilot project and advisory services, as well as the production of knowledge material, will be carried out by individuals or firms, and may also involve supporting activities such as data collection, language editing, translating, graphics design, production in different formats, printing, online dissemination, administration, promotion and related events. The production of events requires, inter alia, travel and logistics costs, related materials, coordination by individuals or firms, and interpretation.

3.5 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, creating and disseminating methodologies for development,

---

12 The specific beneficiaries of Component 2 will be sectorial ministries, regulators, agencies and public-sector companies, including their officials, responsible for aspects of cybersecurity for a specific sector, critical infrastructure or emergency preparedness in a country.

13 Information Sharing and Analysis Centers.

14 The specific beneficiaries of Component 3 will be public-sector organizations, often ministries, agencies, authorities or companies, including their officials responsible for the organizations' cybersecurity.

consulting projects, 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.

3.6 The beneficiaries of this project's components and activities will be selected to include at least 18 countries from all different Country Departments, 8 or more different sectors the Bank is supporting in the region, and various public sector organizations. Support selection considerations include the potential for significant, effective, efficient and inclusive development impact including synergies with Bank operations and with other technical assistance; alliances with other parties and the availability of co-financing for additional leverage; an incipient maturity level; equitability; and on a first-come-first-serve basis.

3.7 The Government of Israel expects to commit US$2,000,000 to this project with the possibility of an additional contribution of US$1,000,000. Local contribution is not expected for this project.

**Indicative Budget (US$)**

| Activity/Component | Donor Funding | Total Funding |
|---|---|---|
| **Component 1:** Develop national cybersecurity capacity | 635,000 | 635,000 |
| **Component 2:** Develop sectorial cybersecurity capacity | 405,000 | 405,000 |
| **Component 3:** Develop organizational cybersecurity capacity | 780,000 | 780,000 |
| Monitoring and evaluation | 40,000 | 40,000 |
| Unforeseen and travel[15] | 40,000 | 40,000 |
| Administrative fee (5%) | 100,000 | 100,000 |
| **Total** | **2,000,000** | **2,000,000** |

3.8 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"). Under this agreement, the resources for this project will be administered by the Bank and the Bank will charge a non-refundable administration fee of 5% of the total contribution, which is included in the budget of this project. The 5% administration fee will be charged upon the Bank's receipt of the contribution.

## 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 since 2016 with support from the Government of Israel. In addition, it has particular 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.

[15] Given the amount and variety of activities supported by this project, and the duration of its execution, a budget line item is included for expenses necessary to attain the project's goals, but unforeseen at the planning stage.

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 of targeted support to countries, contract supervision, project communications and periodic reporting. Given the complexity, workload and magnitude of this project, the necessary cybersecurity project coordination capabilities will be added to the IFD/ICS team with the support of this TC.

4.3 The project team will coordinate the execution of this TC with IDB Country Offices as relevant, including when events or missions are held in beneficiary countries, and when pilot projects or interventions focus on organizations in specific countries. Realizing missions, 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 A selection Committee with one representative from the IDB, one from the Government of Israel and one from an academic institution will be established and will be responsible for the definition of the list of participants, and the pilot projects, eligible under Component 1, activities (i) and (iii); and Component 2, activities (i) and (iii).

4.7 **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.

4.8 **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.

4.9 **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.

4.10 **Data privacy**. TC activities will be conducted in accordance with Bank's current personal data privacy and protection policies and procedures, including GN-3031-1.

## V. Major issues

5.1 In some countries, institutional weakness and fragmentation poses a challenge for the stability of cybersecurity initiatives, including the retention of human resources. This risk will be mitigated by promoting the set-up of CERTs, as well as by placing an

emphasis on providing advice on defining the appropriate institutional architecture to manage a stable cybersecurity program.

5.2 Varying travel and gathering restrictions due to the global Covid-19 pandemic may affect the ability to hold in-person international events and activities. This risk will be mitigated by not planning such events for 2022, 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.

5.3 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 of time 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.

5.4 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

7.1 According to the Environment and Safeguards Compliance Policy (OP-703), the TC has been classified as category C. No potential negative environmental and/or social impacts of the TC were identified and therefore no mitigation strategy is required to address any impact (See Safeguard Policy Filter Report and Safeguard Screening Form).

**Required Annexes:**

Results Matrix - RG-T4010

Terms of Reference - RG-T4010

Procurement Plan - RG-T4010