CONFIDENTIAL
INTERNAL USE
PUBLIC UPON APPROVAL

DOCUMENT OF THE INTER-AMERICAN DEVELOPMENT BANK

ARGENTINA

CYBERSECURITY FOR CRITICAL INFORMATION INFRASTRUCTURE PROGRAM

(AR-L1343)

LOAN PROPOSAL

This document was prepared by the project team consisting of: Mauricio García (ICS/CAR), Project Team Leader; Santiago Paz (IFD/ICS), Alternate Project Team Leader; Krysia Ávila (LEG/SGO); Guillermo Laffaye (CSC/CAR); Pablo Libedinsky, Ariel Nowersztern, Alejandra Aguilar, and Benjamin Roseth (IFD/ICS); Manuel Fernandini (IFD/CMF); Virginia Snyder (INE/ENE); Andrea Bergamaschi (SCL/EDU); Gabriel Casaburi (IFD/CTI); Juliana Almeida (CSD/CCS); Juan Gomez (IFD/FMM); Ana Niubó, Diana de León, Natalia Pérez, and Roberto Laguado (VPC/FMP); Gastón Pierri (SPD/SDV); Florencia Méndez, Roberto Fernández, and Raimundo Arroio (Consultants).

CONTENTS

APPENDICES

ANNEXES	
Annex I	Summary Development Effectiveness Matrix
Annex II	Results Matrix
Annex III	Fiduciary Agreements and Requirements

LINKS

REQUIRED

1. Multiyear execution plan / annual work plan
2. Monitoring and evaluation plan
3. Procurement plan

OPTIONAL

1. Economic analysis of the program
   A. Spreadsheet
2. Vertical logic
3. Program Operating Regulations
4. Gender annex
5. G-SOC technical annex: What is it? And what is it for?
6. G-SOC high-level design
7. Cyber employees impact assessment
8. Legal and governance framework analysis
9. Environmental and social screening filter

ABBREVIATIONS

AFIP	Administración Federal de Ingresos Públicos [Federal Public Revenue Administration]
CERT	Centro de Respuesta a Incidentes de Ciberseguridad [Cybersecurity Incident Response Center]
CII	Critical information infrastructure
DIPROSE	Dirección de Programas y Proyectos Sectoriales y Especiales [Sector and Special Programs and Projects Department]
DPSSYRI	Dirección de Prevención en Seguridad de Sistemas y Redes Informáticas de la SSTI [SSTI Computer Networks and Systems Security Prevention Department]
GDE	Sistema de Gestión Documental Electrónica [Electronic document management system]
G-SOC	Government cybersecurity operations center
ICT	Information and communications technologies
IMF	International Monetary Fund
IRR	Internal rate of return
IT	Information technologies
JGM	Jefatura de Gabinete de Ministros de la Presidencia de la Nación [Office of the Chief of the Cabinet of Ministers of the Office of the President]
NPV	Net present value
OAS	Organization of American States
OI	Output indicator
SIEM	Security Information and Event Management
SIP	Secretaría de Innovación Público [Secretariat for Public Innovation]
SOC	Cybersecurity operations center
SOFR	Secured Overnight Financing Rate
SSTI	Subsecretaría de Tecnologías de la Información de la SIP [SIP Information Technologies Department]
UEPEX	Unidades Ejecutoras de Préstamos Externos [Execution Unit for Projects with External Financing]

PROJECT SUMMARY

ARGENTINA
CYBERSECURITY FOR CRITICAL INFORMATION INFRASTRUCTURE PROGRAM
(AR-L1343)

<table>
<tr><th colspan="5">Financial Terms and Conditions</th></tr>
<tr><td colspan="3">Borrower:</td><td colspan="2">Flexible Financing Facility[a]</td></tr>
<tr><td colspan="3">Argentine Republic</td><td>Amortization period:</td><td>25 years</td></tr>
<tr><td colspan="3">Executing agency:</td><td>Disbursement period:</td><td>5 years</td></tr>
<tr><td colspan="3" rowspan="2">Argentine Republic, through the Office of the Chief of the Cabinet of Ministers of the Office of the President</td><td>Grace period:</td><td>5.5 years[b]</td></tr>
<tr><td>Interest rate:</td><td>SOFR-based</td></tr>
<tr><td>Source</td><td>Amount (US$)</td><td>%</td><td>Credit fee:</td><td>[c]</td></tr>
<tr><td>IDB (Ordinary Capital):</td><td>30 million</td><td>100</td><td>Inspection and supervision fee:</td><td>[c]</td></tr>
<tr><td>Total:</td><td>30 million</td><td>100</td><td>Weighted average life:</td><td>15.25</td></tr>
<tr><td colspan="3"></td><td>Approval currency:</td><td>United States dollar</td></tr>
<tr><th colspan="5">Project at a Glance</th></tr>
<tr><td colspan="5">Project objective/description: The general development objective is to help reduce the cost of cybersecurity incidents for the State and citizens; and the specific development objectives are to: (i) expand coverage of measures for identifying and protecting critical information infrastructure (CII); (ii) improve productivity in the management of cyber incidents; and (iii) improve cybersecurity management efficacy for the prioritized CII.</td></tr>
<tr><td colspan="5">Special contractual conditions precedent to the first disbursement of the loan proceeds: The executing agency will submit to the Bank evidence of the approval and entry into effect of the program Operating Regulations, under terms previously agreed upon with the Bank (paragraph 3.6).</td></tr>
<tr><td colspan="5">Exceptions to Bank policies: None.</td></tr>
<tr><th colspan="5">Strategic Alignment</th></tr>
<tr><td>Challenges:[d]</td><td colspan="2">SI ☐</td><td>PI ☒</td><td>EI ☐</td></tr>
<tr><td>Crosscutting themes:[e]</td><td colspan="2">GE ☒ and DI ☐</td><td>CC ☒ and ES ☐</td><td>IC ☒</td></tr>
</table>

(a) Under the terms of the Flexible Financing Facility (document FN-655-1), the borrower has the option of requesting changes to the amortization schedule, as well as currency, interest rate, commodity, and catastrophe protection conversions. The Bank will take operational and risk management considerations into account when reviewing such requests.

(b) Under the flexible repayment options of the Flexible Financing Facility, changes to the grace period are permitted provided that they do not entail any extension of the original weighted average life of the loan or the last payment date as documented in the loan contract.

(c) The credit fee and the inspection and supervision fee will be established periodically by the Board of Executive Directors as part of its review of the Bank's lending charges, in accordance with the relevant policies.

(d) SI (Social Inclusion and Equality); PI (Productivity and Innovation); and EI (Economic Integration).

(e) GE (Gender Equality) and DI (Diversity); CC (Climate Change) and ES (Environmental Sustainability); and IC (Institutional Capacity and Rule of Law).

I. Project Description and Results Monitoring

A. Background, problem addressed, and rationale

1.1 **Macroeconomic context.** Economic activity in Argentina contracted sharply between 2018 and 2020 (a cumulative 14%), exacerbated by COVID-19. In 2021, the country's gross domestic product (GDP) recovered 10.3%, but remained 5.2% below its 2017 value. Growth of 4.1% is expected for 2022. Annual inflation reached 50.9% in 2021, and the market projects it will accelerate up to 100.3% for 2022. The primary fiscal deficit rose to 6.4% of GDP in 2020, then dropped to 3% in 2021, and the country agreed with the International Monetary Fund (IMF) to bring it down to 2.5% in 2022. In March, the country signed a new agreement with the IMF to refinance its maturing debt from the prior program and receive additional funding, and the two first program reviews were approved. In line with the country's external financing needs and following completion of the second review of the agreement with the IMF, a special development loan from the IDB for US$700 million was approved, supplementing the support from other international lenders for the financing committed under the IMF agreement.

1.2 According to the World Economic Forum, rapid digitalization exposes economies to new, more intense cyber vulnerabilities, since the new technologies and an ever-expanding attack surface enable a more dangerous and diverse range of cybercrimes. This could severely affect the economy and impede the post-pandemic recovery. Notably, cyberattacks are considered the seventh most significant risk facing world economies (ranking below the deterioration in mental health and above the debt crisis). They are also costly: globally, cybercrime cost over US$6 trillion in 2021. Latin America and the Caribbean are not prepared to combat these risks: the Inter-American Development Bank and Organization of American States 2020 report found that the region's cybersecurity capacity is barely "formative," meaning that some aspects have begun to grow in some areas, but may be disorganized and/or have poorly defined processes.[1]

1.3 In Argentina, the national public administration is currently improving its services, making them more efficient, accessible, and transparent. To that end, it has incorporated technological management platforms in its agencies, creating new digital channels for citizens and the private sector. However, in order to take advantage of the opportunities offered by digitalization, the country must also: (i) improve the quality of telecommunications; (ii) develop digital skills; (iii) adopt new technologies in the productive sector; and (iv) properly manage cybersecurity.[2]

---

1 2020 Cybersecurity Report: Risks, progress, and the way forward in Latin America and the Caribbean.

2 Agenda Digital Argentina.

1.4 Along these lines, Argentina has made a number of efforts to protect its cyberspace. In 2011, it created the National Critical Information Infrastructure[3] and Cybersecurity Program; in 2017, it established the Cybersecurity Committee to develop a national cybersecurity strategy;[4] and in 2019, it approved the national cybersecurity strategy,[5] which includes protection of critical information infrastructure (CII), regulations on privacy in the use of personal data in the national public administration, and good practices on the use of information and communications technologies (ICT),[6] among other measures.

1.5 Because of this, Argentina has scored higher than the Latin American and Caribbean average on the International Telecommunication Union's Global Cybersecurity Index (scoring 50.12 and ranking 13th in the region). That said, Latin America and the Caribbean is the second least prepared region in the world to face cybersecurity challenges, after Africa. Furthermore, Argentina's performance is below the Organisation for Economic Co-operation and Development average. This is because the country's efforts to protect the digital space have not advanced at the same pace as the digitalization process.[7] Indeed, the high penetration of ICT[8] magnifies vulnerabilities and increases the potential for incidents and impacts that could occur with expansion of the attack surface.[9] On the private-sector side, 53% of companies do not have cybersecurity strategies in place, and 61% do not have contingency plans for incidents.[10]

1.6 Developing cybersecurity capacities requires properly executing[11] the following five basic steps: (i) identify which assets to protect and their risk level; (ii) protect those assets by implementing defensive actions; (iii) detect potential failures in the defense systems; (iv) respond to the attacks that have evaded the defense measures;[12] and (v) recover from the damage caused by these incidents. To that

---

3 Created through Resolution 580/201. Critical infrastructure is infrastructure that is indispensable for the proper functioning of services essential to society, like healthcare, security, defense, social well-being, the economy, and the effective functioning of the State. The partial or total disruption or destruction of this infrastructure will significantly affect and/or impact these services. Critical information infrastructure, meanwhile, is the information, operation, and communications technology, as well as the associated information, that is vital to the functioning and security of the critical infrastructure. Resolution 1523/19, (former) Government Secretariat of Modernization.

4 Decree 577/2017. See paragraph 3.4.

5 Approved through Resolution 829/2019 of the Government Secretariat of Modernization, and an output of loan 4755/OC-AR (paragraph 1.16).

6 Resolution 40/2018 of the Access to Public Information Agency. Provisions 2/2018 and 3/2018 of the National Office for Information Technologies ("Technological Decalogue").

7 From 2016 to 2022 the number of individuals using online procedures increased 220% (for 20,793,925 digital procedures).

8 Decree 733/2018 establishes the national public administration's obligation to digitalize all citizen transactions.

9 In 2021, 27.1 trillion devices were connected, with per capita traffic of 35 GB/month, increasing the attack surface. https://gblogs.cisco.com/.

10 https://www.pwc.com.ar/.

11 https://www.nist.gov/cyberframework.

12 By implementing actions when a cybersecurity incident is detected, to contain its potential impact.

end, specialized technologies, policies, processes, individuals, and organization are all essential.

1.7 **Cybersecurity governance in Argentina.** Decree 577/2017 and its amendments and Resolution 141/2019 of the Argentine regulatory framework give the Secretariat for Public Innovation[13] (SIP) the power and duty to protect CII. As chair of the Cybersecurity Committee,[14] the SIP develops and implements the national cybersecurity strategy and establishes the guidelines and criteria for defining, identifying, and protecting CII. Specifically, the SIP is responsible for cybersecurity and protecting CII and communications associated with the national public sector and information and communications services. In turn, the SIP Information Technologies Department (SSTI) is responsible for, among other duties, proposing strategies, standards, and regulations for cybersecurity and protecting CII and communications associated with the national public sector and information and communications services.[15] However, these agencies still lack the specialized technological, human, and financial resources needed to fully perform these tasks.

1.8 **Problem and challenges.** The principal problem identified is the high cost of cybersecurity incidents for the government[16] and citizens.[17] Indeed, according to SIP data, 81.7% of the incidents processed in 2021 were high- or critical-severity ones, whose costs are 100 times greater than low-severity ones. In countries in the region like Uruguay, not even 2% of incidents fell into this category.[18] This is because of Argentina's limited capacity for performing the basic CII cybersecurity functions,[19] which results from the following factors:

---

13 Then the Ministry of Modernization. The SIP currently reports to the Office of the Chief of the Cabinet of Ministers (JGM). See Decree 123/2022, as the regulation in force that governs the SIP and the Information Technologies Department (SSTI) in the JGM structure.

14 As of 2019 (Resolution 141), the Cybersecurity Committee reports to the Government Secretary of Modernization, who in turn reports to the JGM.

15 Established in Article 1 of Law 27,078 (objective incorporated by Article 4 of Decree 139/2021, Official Gazette 5 March 2021). See optional link 8.

16 In 2020 the National Migration Office suffered a cyberattack that affected its digital services, preventing people from entering and leaving the country. In 2021, sensitive information on millions of Argentines was stolen from the National Office of Vital Records.

17 Cyber incidents in Argentina in 2021 were estimated to have a total economic impact of US$1.141 billion on the public sector (US$434.4 million) and citizens (US$700.6 million) (optional link 1).

18 https://www.gub.uy/.

19 According to the Cybersecurity Capacity Maturity Model for Nations, in Argentina 5% of the 24 factors that compose the five dimensions of cybersecurity ((i) cybersecurity policy and strategy; (ii) cyberculture and society; (iii) cybersecurity education, training, and skills; (iv) legal and regulatory frameworks; and (v) standards, organizations, and technologies) are in the "start-up" stage; 50% are in the "formative" stage; 40% are "established;" 5% are in the "strategic" stage; and none have reached the "dynamic" stage. www.observatoriociberseguridad.com. Ibid1.

1.9 **Limitations in governance framework.** According to the diagnostic assessment presented in optional link 8, there are various institutional and regulatory limitations, notably:[20]

(i) the SIP's powers and duties are exclusively focused on regulatory and procedural aspects of public cybersecurity, meaning that in practice, the country's operational management is weak;

(ii) the national cybersecurity ecosystem's capacity for analysis is weak,[21] for all stakeholders: public sector, private sector, and citizens;

(iii) the scattered nature of organizations' prevention and response procedures affects their efficacy and speed, ramping up the consequences of the attacks;

(iv) the mechanisms for exchanging information on risks and incidents that would make it possible to coordinate methods, procedures, and tools to ensure that one agency's knowledge can immediately be shared with all potentially affected agencies are limited; and

(v) the public agencies responsible for providing cybersecurity services typically use their own individual proprietary tools, and the lack of standardization in defensive tools, methods, and procedures makes it more difficult for them to establish a shared posture against cyberspace threats.[22]

1.10 These limitations make it more difficult to: (i) prioritize assets for protection by risk level; (ii) coordinate, in a crosscutting way, the design and implementation of CII protection plans; and (iii) rapidly implement the national cybersecurity strategy since although the JGM and the Cybersecurity Committee have established guidelines for identifying CII,[23] to date only the electronic document management system (GDE)[24] has been identified, and no plan has been developed to protect it.

1.11 **Low SIP coverage for identifying and protecting CII.** Of the 11 sectors classified as critical since 2019, namely energy, ICT, transportation, water, health, food, finance, nuclear, chemical, space, and government,[25] only the GDE in the government sector was declared a CII. This makes it difficult to determine cyber risks and set up protection plans for other sectors' information systems. In contrast,

---

20 "From the operational perspective, the current model lacks a central government cybersecurity agency, meaning an agency in charge of proper centralized management of matters related to resources, methods, procedures, tools, outreach, training, and national and international cooperation on cybersecurity, technologies, and legal conditions (always in line with the strategy set by higher-level agencies)." Idem, pp. 91 to 93.

21 The national cybersecurity ecosystem is understood to be the public, private, academic, and civil-society organizations that are involved in jointly establishing the country's cybersecurity.

22 For example, there is no protocol for identifying computer assets that should be protected or their risk level.

23 Approved through Resolution 1523/2019. https://www.argentina.gob.ar/normativa/nacional/.

24 This is a system for managing the State's internal processes, deployed in the federal government, 18 provinces, and 80 municipios.

25 https://www.argentina.gob.ar/.

countries like Israel have already identified 40 CII and 300 connected information systems.[26]

1.12 **Poor productivity in handling cyber incidents (detection, response, and recovery).** When these capacities are limited, incidents are only detected once damage has already been done, and the damage usually keeps escalating until the incident has been resolved. For example, in 2020 Argentina only processed 226 incidents, while Uruguay and Chile processed 2,798 and 15,321, respectively.[27] This is because: (i) Argentina cannot currently monitor attacks and threats to CII in real time; in other countries the government cybersecurity operations center (G-SOC)[28] does this monitoring (paragraph 1.20); (ii) the National Cybersecurity Incident Response Center's (CERT.ar)[29] technological platform can register and track incidents, but does not have the capacity to prevent them or direct the response;[30] and (iii) the mechanisms for exchanging information on cybersecurity incidents and attacks do not provide the confidentiality and security that stakeholders need for prompt collaboration, which impedes the country's prevention and response capacity.

1.13 **The lack of cybersecurity professionals** is considered a challenge around the world[31] and especially in the region.[32] In Argentina, capacity for training cybersecurity specialists has stagnated, despite the high demand for training civil servants. In fact, the universities that do offer official cybersecurity studies have not seen their enrollment increase significantly over the past few years. Currently, they have fewer than 400 students, with a major gender gap as only 15% of them are women (optional link 4).[33] This issue is reflected in the cybersecurity education, training and skills dimension maturity indicators found in the OAS and IDB regional cybersecurity report, which were essentially stalled at the "formative" stage (stage two of five). On the other hand, the rapid growth in demand for these specialists (paragraph 1.5) led to a significant shortage in the education offering, which in turn impacts the country's cyberspace management capacity.[34] While international

---

26 Resolution 36/2020 declared the GDE a government CII. http://www.saij.gob.ar/.

27 In Argentina there are many incidents that generate cybersecurity costs and impacts that the National CERT is thought to fail to detect.

28 Technical unit specialized in the detection of and first response to cybersecurity incidents.

29 Operates as an agency of the National Cybersecurity Bureau (CERT.ar), specializing in the response to complex incidents.

30 Because of this, for example, the country was unable to detect the 2021 data breach of the National Office of Vital Records early, and it had a significant adverse impact on the office's role safeguarding citizen data.

31 Globally, the supply of cybersecurity professionals needs to increase 65% to cover demand. https://www.cyberseek.org/heatmap.html.

32 The 2021 Cybersecurity Workforce Study ((ICS)^2, 2021) estimates that the region needs over 500,000 cybersecurity professionals to meet employers' current needs.

33 Data obtained from the following universities: Universidad de Buenos Aires, Universidad de la Plata, Universidad de Defensa, and Universidad Nacional Escalabrini Ortiz.

34 Although cybersecurity professionals earn considerably more than programmers (11% more in the United States, according to figures from the *Bureau of Labor Statistics* (2021), and up to 50% more in Uruguay, according to the Uruguayan Chamber of Information Technologies (2019)), there is such a lack of demand from students that it is rarely profitable to employ specialized professors (Universidad de la República, 2019).

good practices show that at the agencies with the highest cybersecurity capacity maturity levels, approximately 5% to 10% of the information technology (IT) staff are cybersecurity workers,[35] in Argentina's national public administration, only mature organizations like the Federal Public Revenue Administration (AFIP)[36] and the Argentine Satellite Solutions Company (ARSAT)[37] meet this ratio. On top of this lack of specialists, regular employees—the ones who use the different systems and platforms subject to cyberattacks—typically have poor cybersecurity skills. Over two-thirds of cyberattacks on organizations occur due to employee negligence.[38]

1.14 **Diagnostic assessment of gender in the cybersecurity labor market.** Globally, women make up only 25% of the cybersecurity workforce (Microsoft, 2021).[39] An analysis of the gender gap among IT professionals in the Argentine national government shows that at the AFIP Information Security Department, for example, only 28.1% of workers are women. This gap is similar at the state telecommunications company ARSAT, where women account for 27% of the payroll. At the SSTI, there are a total of 34 agents,[40] of which 40% are women. The country is only beginning to address the issue of cybersecurity and gender, and the experience of the Genders in Technology Center is noteworthy.[41] The SSTI and the Ministry of Education's National Institute of Technological Education both participate in this Center. Among the center's various thematic pillars, one focused on cybersecurity seeks to foster initiatives that will boost the training of women in digital security, as well as shrink the gender gaps in science, technology, engineering, and mathematics.

1.15 **Low efficacy cybersecurity management for the prioritized CII.** In 2019, the GDE was used to test 10,538,180 electronic files;[42,43] it is an integrated system for classifying, numbering, tracking, and registering movements for all national public administration actions and files. By January 2022, this figure had gone up to 35,998,117. Despite the importance of this CII, the past two comprehensive

---

35 https://www.nuharborsecurity.com/information-security-staffing-guide.

36 The AFIP has 986 IT employees (27% women), of which 121 (28% women) work in cybersecurity. SIP, 2022.

37 The ARSAT has 761 employees, of which 143 (18% women) work in IT departments, and 27 of those in cybersecurity. ARSAT, 2022.

38 Cybintsolutions, 2020.

39 In a Microsoft study conducted to investigate the reasons behind the gender gap, 56% of the women surveyed responded that they are not adequately represented in the industry. Women are more aware of the industry's gender bias, given that it results in unequal support and salaries.

40 Including administrative staff, technical assistants, and professionals.

41 The center is a consortium of public agencies, ICT companies, and civil society organizations formed to promote inclusion policies to narrow the gender gap in the ICT sector through public-private collaboration. Centro-gt.

42 All the country's ministries and 86% of its public agencies use the GDE.

43 IDB-EVERIS (2019). Agenda Digital de Argentina: Informe diagnóstico.

audits[44] of its ecosystem[45] revealed serious failings such as: (i) an inadequate cybersecurity policy; (ii) improper management of cyber risks; (iii) defective business continuity and disaster recovery plans; and (iv) an improper organizational structure for cybersecurity management; among other findings.

1.16 **Bank experience in the region, country, and the sector.** The Bank has extensive experience designing and implementing digital transformation and cybersecurity projects. In Argentina, the Program for Strengthening the Digital Agenda: Connectivity, Electronic Government, and Digital Productive Transformation (loan 4755/OC-AR), which was approved in 2019 for US$300 million and is currently closed, supported the government's implementation of CII- and data-security-related policies; its outputs included the national cybersecurity strategy and CII protection plan (paragraph 1.4). As recommended in that program's project completion report, this operation will further implementation of the country's digital agenda, especially with regard to data-security policies, strengthening economic actors' digital resilience, and improving people's quality of life and well-being. In the region, the Bank's experience includes projects like Strengthening Cybersecurity in Uruguay (loan 4843/OC-UR), approved in 2019 as the first specific cybersecurity project in the region; digital transformation projects with large cybersecurity components, such as: Panama Online (loan 3683/OC-PN) from 2016, Government Digital Transformation to Strengthen Competitiveness (loan 4549/OC-BH) from 2018, Project to Improve and Expand Support Services for National Service Delivery to Citizens and Enterprises (loan 4399/OC-PE) from 2017, Digital Agenda Support Program (loan 4650/OC-PR) from 2018, Program to Strengthen the Strategic Management of Public Security in Chile (loan 4891/OC-CH) from 2019, Program for Modernization of the Judicial Branch of the State of Ceará (loan 5248/OC-BR) from 2020, and Program for Digital Transformation of the Government of the State of Ceará (loan 5516/OC-BR) from 2022. The Bank has also received technical and financial support from the Governments of Spain and Israel through technical-cooperation funding: (i) for research and dissemination, with "Improving Human Resources Capacity in Cybersecurity" (operation ATN/CF-15598-RG), approved in 2016 for US$3 million, and "Strengthening of Cybersecurity in Latin America and the Caribbean" (operation ATN/FG-16633-RG), from 2018 for US$500,000, both closed, and the continuation of the latter with the same title (operation ATN/CF-19154-RG), from 2022 for US$2 million, still in execution; and (ii) for client support: "Digitalization for Inclusive Socioeconomic Development in times of COVID-19" (operation ATN/FG-18691-RG) from 2021 for US$3 million. These technical-cooperation operations have financed training activities and studies that serve as a fundamental input for the design of this operation.

1.17 **Complementarity with other Bank operations in Argentina.** This project complements the: (i) Program for the Development of the Federal Fiber Optic Network (REFEFO) (loan 5364/OC-AR) from 2021 for US$100 million, with 5.4%

---

44 Audits performed by the Office of the Auditor General in 2019 and the Sadosky Foundation in 2020.

45 The GDE ecosystem has various modules, including official communications, electronic generator of official documents, electronic file, online procedures, single electronic record, works and services contract, multipurpose file registry, assistance and transfer manager, comprehensive registry of recipients, electronic vital records office, digital signature, electronic authentication, etc.

disbursed and in execution, designed to boost internet access and digitalization in Argentina; (ii) Program to Support Integrated Public Expenditure Management (loan 4802/OC-AR) from 2019 for US$40 million, currently 18.2% disbursed and in execution, to finance the development and renovation of CII to make public expenditure more efficient and transparent; and (iii) Digital Transformation (operation ATN/OC-17583-AR), for operational support, approved in 2019 for US$300,000, to support implementation of the digital agenda, including the CII protection plan. It is also complemented by operations currently being prepared, such as: (i) the Conditional Credit Line for Investment Projects for Investments to Promote the Decarbonization of the Energy Sector in Argentina (AR-O0020) for US$1.14 billion and its first individual operation Federal Electric Power Transmission Program (loan 5564/OC-AR), approved in July 2022 for US$200 million, pending signature, to finance the introduction of innovative information systems to modernize electric power transmission systems (energy is a critical sector, paragraph 1.11); the present program will foster cybersecurity for the CII financed with these operations; and (ii) Program to Support the Digital Transformation of MSMEs to Industry 4.0 (loan 5570/OC-AR), approved in August 2022 for US$80 million, pending signature, since by improving the country's cybersecurity environment, it will facilitate MSMEs' digital transformation.

1.18 **Lessons learned.** International best practices in security, knowledge products, and lessons learned from similar Bank operations in the region were considered in the preparation of this program (paragraph 1.16). They include the importance of: (i) strengthening the institutional structure and leadership of the entity responsible for cybersecurity in the country (SIP), by giving it the regulatory frameworks, technological tools, and human talent necessary to lead the project in the country; (ii) interagency coordination and the approach in the ecosystem, including public, private, academic, and civil society institutions; and (iii) building talent to ensure the availability of professionals and services during execution and when the project is completed. These lessons were all incorporated into the various activities planned under the program components (see paragraphs 1.25, 1.26, and 1.27).

1.19 In addition, given the innovative nature of the technologies and services in the program, advancing the strategic procurement of complex technologies and services through requests for information, with terms of reference and technical specifications that follow international standards (to adjust the requirements together with industry leaders), will help the country's ecosystem of this type of companies better prepare to design and deliver services locally. This will be done with the support of expert consultants, who will be financed with nonreimbursable technical-cooperation funds (operation ATN/OC-17583-AR) (paragraph 1.17). Furthermore, with regard to training, the use of simulation platforms has been shown to be a fast and effective way to provide training and education on cybersecurity operations.[46] Accordingly, CyberRange platforms[47] will be used to simulate cybersecurity operations, for learning and evaluation purposes. These virtual platforms simulate complicated ICT scenarios in which complex attacks are

---

[46] The same effect is produced by incorporating skills and/or games, known as "Edutainment;" adding recreational components to trainings yields excellent learning outcomes. Simulating Cyber Operations: A Cyber Security Training Framework, SANS Bryan K. Fite, 2014.

[47] https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf.

executed in controlled environments. Their main benefit is that they help users develop operational cybersecurity skills through simulation techniques.[48]

1.20 **International experience and best practices** also underscore the importance of cybersecurity operations centers (SOCs) (optional link 5) as a fundamental tool. The main role of these centers is to handle computer incidents.[49] SOCs specific to governments are known as government cybersecurity operation centers or G-SOCs. They monitor computer systems in real time, very effectively detecting, responding to, and helping those systems recover from incidents. Examples of these G-SOCs can be found in advanced countries like Spain[50] and Israel.[51] G-SOCs provide a wide variety of cybersecurity services, but their main function is to detect and respond to cybersecurity incidents. To do so, they use "probes"[52] distributed through the various information systems to be monitored. These probes analyze all the events in the system, searching for suspicious activity that could constitute an attack. The analyzed information is sent to a central system called the Security Information and Event Management (SIEM) System, which processes and correlates it and, in real time, indicates when an attack is taking place. At that moment the response process begins, automatically or with human intervention.

1.21 **Strategic alignment.** The program is consistent with the second Update to the Institutional Strategy 2020-2023 (document AB-3190-2) and is aligned with the Productivity and Innovation development challenge, insofar as it promotes the new, high-value-added area of cybersecurity and the development of more efficient methods for the provision of cybersecurity services (paragraph 1.25). It is also aligned with the crosscutting themes of: (i) Gender Equity, through the inclusion of actions designed to increase women's participation in the sector (paragraphs 1.14, 1.22, and 1.26); (ii) Climate Change, since according to the joint methodology of the multilateral development banks, 8.57% of the loan proceeds are invested in climate change mitigation activities, through the procurement of computer equipment that is highly energy efficient (category A), thereby contributing to the IDB climate finance target of 30% of annual approvals; and (iii) Institutional Capacity and Rule of Law, by strengthening the capacity for protecting the digital space and the safe expansion of the digital sector (paragraphs 1.25, 1.26, and 1.27). It will also contribute to the Corporate Results Framework 2020-2023 (document GN-2727-12) level 2 indicator of agencies with strengthened digital technology and managerial capacity, since it will help increase the number of government agencies benefited with technological and management instruments. The program is aligned with the IDB Group Country Strategy with Argentina 2021-2023 (document GN-3051), specifically with the following strategic

---

48 Users can analyze how to detect and resolve these problems and how to develop defensive and offensive tools, and practice doing so. The concept of simulation is well known in the military and aeronautical realms, where there are no real impacts if the user makes a mistake in the simulated scenario, which can be restarted. These platforms do the same thing, but for cybersecurity. SANS Bryan K. Fite, 2014.

49 https://www.mitre.org/sites/default/files/publications/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf.

50 https://www.ccn-cert.cni.es/.

51 https://www.gov.il/en/departments/news/119en.

52 A probe is a technological system able to monitor cybersecurity events, provide warnings, and/or act to prevent a potential attack.

objectives: (i) improve the population's employability, through the investments in cybersecurity training in function of the current and future labor demand (paragraph 1.26); and (ii) digital government, by affording greater security to sector expansion (paragraph 1.27). Lastly, the operation has been included in the Update of the Annex III of the 2022 Operational Program Report (document GN-3087-2).

1.22 **Gender actions.** Pro-gender actions will be incorporated through the: (i) development of cybersecurity certification and technical programs that prioritize the inclusion of women, in coordination with the Genders in Technology Center; and (ii) provision of technical assistance for preparing a gender diagnostic assessment and action plan to outline a course of various actions to bridge the gender gaps in cybersecurity within SSTI.

B. Objectives, components, and cost

1.23 **General development objective:** To help reduce the costs of cybersecurity incidents for the State and citizens.

1.24 **Specific development objectives:** (i) expand coverage of measures for identifying and protecting CII; (ii) improve productivity in the management of cyber incidents; and (iii) improve cybersecurity management efficacy for the prioritized CII. The operation will have the following components:

1.25 **Component 1. Strengthening of the SIP's institutional and technological capacities (US$20 million).** This component will finance: (i) improvements in the design and implementation of the institutional and regulatory framework for identifying and protecting CII;[53] (ii) creation of a G-SOC[54] to monitor and detect attacks, providing it with SIEM tools[55] and sensors;[56] (iii) strengthening of the National CERT's operational capacities;[57] and (iv) development of platforms for threat analysis and the exchange of information within the public sector and with the private sector.[58]

---

53 The component will analyze the national CII protection program (2011) to evaluate its outcomes, and based thereon, propose, develop, and implement a new program that will be executed through the regulatory agencies. Protection plans will be designed for every CII that is identified; by the end of project, half of the sectors should have at least one plan each. At present the GDE is the only CII to have been identified. See paragraphs 1.10 and 1.15.

54 The component will create an organizational unit, supported by the design for it, the development of policies and processes, staff training, hiring of professional services companies (e.g., monitoring, incident response, vulnerability analysis services, etc.) and technology infrastructure.

55 These are tools that combine incident analysis and management, by surfacing user behavior anomalies and using artificial intelligence to automate many of the manual processes associated with threat detection and incident response. What is Security Information and Event Management (SIEM)? | IBM.

56 All procurements of technological tools (hardware and software) will include a maintenance clause.

57 The actions to strengthen the G-SOC and the National CERT will enable detection of more incidents. When detected early and by a centralized agency, ultimately these incidents will not be able to harm the attacked organization, which consequently will not incur any recovery costs. The actions that will be financed include: consulting services for the design, production, maintenance, deployment, and operation of the national probes program and the event aggregator platform, preventive cybersecurity services, advanced cybersecurity services, and the procurement of computer equipment with the energy efficiency seal.

58 The regulatory framework does not currently mandate that they share information with the National CERT.

1.26 **Component 2. Strengthening of human talent in cybersecurity (US$5 million).** This component will finance skill development at the national and subnational levels and will include: (i) a cyberattack simulation platform for specialized training (CyberRange); (ii) cybersecurity certification and technical programs[59] that prioritize women; (iii) e-Learning software to train professionals, to include basic training for the civil servants who will use the institutional systems[60] and accessibility for persons with disabilities; and (iv) cybersecurity change management and curriculum development plans, including a proposal to associate employees' performance as good cybersecurity monitors with tangible career-related incentives.[61]

1.27 **Component 3. Improved protection of the GDE ecosystem (US$3 million).** This component will finance the: (i) formulation and implementation of a cybersecurity policy, to entail: a gap analysis of GDE cybersecurity; business continuity plan; and disaster recovery plan; (ii) implementation of data backup technologies for the GDE; and (iii) development of training on cybersecurity for the GDE ecosystem technical staff and users.[62]

1.28 **Administration, supervision, evaluations, and audits (US$2 million).** These funds will be used to finance administrative expenses, monitoring, evaluations, including the strategic assessment, and program audit. It also provides for the program impact assessment.

1.29 The eligible expenses to be financed by the program include specialized consulting services and goods and nonconsulting services (including the procurement of hardware, software, and training).[63]

C. Key results indicators

1.30 **Expected outcomes.** The general development objective "Savings on cybersecurity incident management costs for the State and society" will derive from an improvement in the national cybersecurity capacity maturity level and reduced annual cyber incident management costs. Achievement of the specific

---

59 Prioritizing institutions with at least one CII, the component will develop at least one technical training program per year with ISO 17024 standards to certify professionals. The component will include pro-gender actions to increase the participation of women through campaigns and outreach events in over 30 cities in the country where potential CII operate, as well as support for new Cyberwoman Challenge programs. See paragraph 1.22.

60 Civil servants' knowledge will be evaluated (through phishing campaigns) and programs on various cybersecurity topics will be developed for public administration users, including a support and content query system.

61 The change management strategy will enable: (i) the generation and dissemination of specific cybersecurity knowledge through high-impact national and international events; (ii) higher retention and encouragement of cybersecurity professionals through incentive plans; and (iii) a greater offering of training programs at academic institutions, which will also increase the availability of trained professionals in these areas.

62 The GDE ecosystem staff's management capacities must be strengthened in order to ensure that the data backup systems to be financed by the component will be successful. The technology, and the training of the team that will operate it, will increase the number of successful recovery tests carried out, and will, therefore, improve the efficacy of the management of the GDE ecosystem, the only CII that has been identified to date.

63 The estimated breakdown is 40% for consulting services and 60% for goods and services.

development objectives will be measured through: (i) an increase in the coverage of measures for identifying and protecting CII and for the ministries monitored through the G-SOC, to be assessed based on the coverage of sectors with identified CII and the number of ministries monitored; (ii) improvements in the productivity of cybersecurity management derived from the increase in managed incidents and the reduction in the proportion of incidents classified as high or critical severity; (iii) women at the SIP certified in cybersecurity and agencies with strengthened digital technology and managerial capacity; and (iv) improvements in cybersecurity management efficacy for the prioritized CII, derived from the increase in the number of findings resolved and the performance of successful tests to address IT problems.

1.31 **Beneficiaries.** The direct beneficiaries will be the citizens, companies, and organizations that operate CII, including the GDE, with approximately 3.3 million users, who with improved SIP cybersecurity services will see their savings increase vis-à-vis cybersecurity incidents and will enjoy better data protection. The indirect beneficiaries will be the public servants, especially women (approximately 80 SIP employees will be certified in cybersecurity), since their professional cybersecurity capacities will improve. Public institutions in general will also benefit, since their technology infrastructure will be better protected as a result of the project.

1.32 **Economic analysis.** The economic evaluation, based on a cost-benefit analysis (optional link 1), considers two types of benefits:[64] (i) lower operating costs for remedying the damages caused by cyberattacks on public institutions, due to fewer high-severity incidents (which have a higher unit operating cost); and (ii) less of an adverse economic impact on public institutions from cyberattacks, thanks to the enhanced prevention and response capacity. Each section of the analysis and estimation of benefits was based on its own assumptions and methodology. To calculate the operation's return, the evaluation used a discount rate of 12% (standard for the Bank) and a period of eight years for calculating the benefits (five years for project implementation and three years post-implementation). The analysis yields a suitable expected return: in the base case, an estimated internal rate of return (IRR) of 36%, a net present value (NPV) of US$14.6 million, and cost-benefit ratio of 1.71. Starting in the final year of program implementation, annual savings on the incident management operating costs are projected to reach US$4.8 million, together with US$8.5 million per year as a result of the adverse impacts prevented for organizations and citizens.

1.33 The sensitivity analysis shows the project's economic return to be acceptable even under adverse assumptions and scenarios. If the project is less effective in reducing the percentage of high- and critical-severity incidents among the total number of incidents handled annually by the National CERT, and it only reduces this percentage from the starting value of 81.7% to 10% (instead of the target value of 5% established in the results matrix), the resulting NPV would be US$11.2 million and the IRR, 34%. If the project is unsuccessful in increasing the total number of incidents managed annually by the National CERT to 10,000, and only reaches 6,000/year, the NPV would be US$12.5 million and the IRR, 33%.

---

64 https://www.incibe.es/las-7-fases-ciberataque; https://www.ibm.com/topics/security-operations-center.

Lastly, if the project does not achieve the effectiveness established in the base case with regard to preventing damages to institutions and persons thanks to earlier detection and defense of data and the systems, and only reduces the annual negative economic impact by 1% starting in the fifth year, the NPV would be US$3 million and the IRR, 17%. The project's economic return is therefore quite robust.

II. Financing Structure and Main Risks

A. Financing instruments

2.1 This program is designed as a specific investment loan for a total of US$30 million, to be financed with the Bank's Ordinary Capital resources, with a disbursement period of five years. This modality is justified by the comprehensive logic of the planned intervention, given the technical and economic assessment and the type of investments to be financed.[65]

Table 1. Estimated program costs (US$)[66]

Item of expenditure	Total	%
Component 1. Strengthening of the SIP's institutional and technological capacities	**20,000,000**	**66.7**
Output indicator (OI) 1. Institutional and regulatory framework for identifying and protecting CII, approved	920,000	3.1
OI 2 Actions to strengthen the monitoring and detection of attacks (G-SOC) with SIEM tools and sensors	12,955,000	43.2
OI 3 Actions to strengthen the CERT's operational capacities	4,375,000	14.6
OI 4 Platforms for threat analysis and information exchange with the private sector, implemented	1,750,000	5.8
Component 2. Strengthening of human talent in cybersecurity	**5,000,000**	**16.7**
OI 5 Cyberattack simulation platform installed	2,000,000	6.7
OI 6 Cybersecurity certification and technical programs (prioritizing women) developed	1,025,000	3.4
OI 7 E-learning software installed and operating	875,000	2.9
OI 8 Cybersecurity change management and curriculum development plan implemented	1,100,000	3.7
Component 3. Improved protection of the GDE ecosystem	**3,000,000**	**10.0**
OI 9 Cybersecurity policy developed (including business continuity and disaster recovery plans)	500,000	1.7
OI 10 Backup technologies implemented (hardware and software)	2,000,000	6.6
OI 11 SIP staff with strengthened GDE cybersecurity capacities	500,000	1.7
Administration, supervision, evaluations, and audits	**2,000,000**	**6.6**
Management	1,300,000	4.3
Monitoring	300,000	1.0
Evaluations: midterm, final, strategic, before and after, and impact	300,000	1.0
Audits	100,000	0.3
Total	**30,000,000**	**100.0**

[65] See multiyear execution plan.

[66] The output-level amounts are indicative.

2.2 **Disbursement timetable.** The disbursement period was set at five years (see Table 2), mainly due to: (i) the average time required to design and implement the proposed program activities; (ii) alignment with the national cybersecurity strategy; and (iii) the counterpart's request to execute as many activities as possible during the period, to leverage synergies with other government interventions on digitalizing transactions.

Table 2. Disbursement schedule (US$ millions)

Components	Year 1	Year 2	Year 3	Year 4	Year 5	Total
IDB	3.295	5.505	5.650	7.660	7.890	**30**
%	11.0	18.4	18.8	25.5	26.3	**100.0**

B. Environmental and social safeguard risks

2.3 Pursuant to the new Environmental and Social Policy Framework (document GN-2965-23), this was classified as a Category "C" operation. The executing agency's environmental and social management system was reviewed during the institutional capacity analysis, and the predicted negative environmental and social impacts are minimal to nonexistent. Through the Sector and Special Programs and Projects Department (DIPROSE), the JGM has implemented a mechanism for managing complaints, including on socioenvironmental and labor issues.[67] The labor management procedures established by the country's national legislation will be in force during the life cycle of the operation. Notably, the national legislation incorporates the multilateral treaties that Argentina has signed in the context of the International Labour Organization and United Nations.

C. Fiduciary risks

2.4 One fiduciary risk related to the internal procurement processes was preliminarily identified as medium-high, namely, that delays between identification of a need and the time it takes for the various goods and services to be incorporated could slow project progress. To mitigate this risk, qualified staff with experience in multilateral organizations' procurement management procedures will be trained and hired as necessary and in agreement with the Bank, and the Bank will provide support and training on fiduciary issues.

D. Other risks and key issues

2.5 Two medium-high level risks were noted. The first involves the institutional climate: if the public organizations and CII operators are resistant to accepting the project implementation activities, they may not sufficiently take on the protection measures, and the exposure to cyber incidents would continue unabated. To mitigate this risk, the operation will establish change management strategies and implement training, communication, and awareness-raising activities (paragraph 1.26). The other risk involves human resources: if it is difficult to retain trained technical professionals, the project deliverables may not be completed on

[67] A complete description of the mechanism is available at: https://www.argentina.gob.ar/quejas_y_reclamos.pdf.

time or with the proper quality. To mitigate this risk, the operation will provide the technicians with advanced courses and more modern tools and engage them in the decision-making processes on CII-protection measures and policies (paragraph 1.26).

2.6 **Program sustainability.** Financially, the program should lead to significant savings derived from reduced cyberattack response costs and the improved capacity for recovering from the damages they cause. The technological investments will be made with a service maintenance plan to improve their sustainability. In terms of capacities, the SIP and the national public administration will be strengthened through the professionalization of cybersecurity employees and an increase in their numbers. Lastly, at the institutional level, the program is aligned with the digital agenda, the national cybersecurity strategy, and the CII protection plan, which are political commitments taken on by the government, in force since the prior administration was in power, thereby boosting sustainability.

III. Implementation and Management Plan

A. Summary of implementation arrangements

3.1 **Borrower and executing agency.** The borrower will be the Argentine Republic. The program executing agency will be the borrower through the JGM, operating through DIPROSE, which will be responsible for administrative and financial coordination; and the SSTI Computer Networks and Systems Security Prevention Department (DPSSYRI), which will be the substantive program area. [68,69] In addition, the strategic evaluation (paragraph 3.15) has the executing agency responsible for fiduciary execution, and the Ministry of the Economy's Undersecretariat of International Financial Relations for Development (SSRFID), as the party responsible for technical-methodological execution.[70]

3.2 **Program Operating Regulations.** The program Operating Regulations will be the instrument that steers program execution and will establish, among other items: (i) the program's organizational structure; (ii) the technical and operational arrangements for execution; (iii) the plans for programming, monitoring, and evaluating results; (iv) guidelines for the financial, auditing, and procurement processes; (v) details of the executing agency's duties as well as other relevant ministerial agencies' responsibilities in the planned program processes; and (vi) the activities included in the program's various components and subcomponents.

3.3 **Institutional capacity analysis.** In 2022, the Bank analyzed the JGM's institutional capacity. The analysis found that the JGM does have experience in projects with the Bank and other multilateral institutions, but that its institutional capacity needs to be strengthened in order for it to take on the responsibility of managing program resources, to include financial administration and accounting,

---

68 See the executing agency's composition and responsibilities in the program Operating Regulations.

69 "Substantive area" is understood to be the area with leadership in technical, non-fiduciary aspects of the program.

70 If the executing agency's organizational structure is changed, it can act through the areas of offices with similar authority and competencies that replace them in the future, with the prior agreement of the Bank for the purposes of this program.

procurement, and contracting, and the planning and monitoring of activities. To that end, the program will finance the hiring of technical support staff and a team of administrative-financial consultants to complement the JGM's capacities and, in turn, support SIP management.

3.4 **Executing agency functions and responsibilities.** As outlined in the program Operating Regulations, the executing agency will: (i) coordinate the program-related financial and administrative procedures; (ii) coordinate, consolidate, prepare, and submit to the Bank all the information on and documentation of the program's integrated management; and (iii) ensure the coordination, coherence, and fulfillment of the plans set forth in the program management tools, to foster achievement of the expected results. The following stand out among its duties: (i) collaborate in the preparation and approval of the terms of reference for contracting; (ii) prepare the technical and administrative documentation relevant to bidding and contracting processes as applicable; and (iii) coordinate the contracting processes called for by the director general.

3.5 **Interagency coordination mechanisms.** To be effective, cybersecurity must involve all the institutions responsible for CII, and therefore, it is necessarily multisectoral. Since 2017, the country has had a Cybersecurity Committee[71] (paragraphs 1.4 and 1.6) whose primary duties, in addition to developing the national cybersecurity strategy, include preparing the necessary action plan for implementing the national cybersecurity strategy, convening other agencies to participate in implementing measures in connection with the action plan that has been drawn up, and establishing the guidelines and criteria for defining, identifying, and protecting the country's critical infrastructure.[72] Accordingly, the Cybersecurity Committee has all of the legal support it needs to be responsible for interagency coordination on the national cybersecurity strategy. Specifically for CII, the SIP is directly responsible for interagency coordination (paragraph 1.7) and will be strengthened with funds from this operation to do so fully (paragraph 1.26).

3.6 **Special contractual condition precedent to the first disbursement of the loan. The executing agency will submit to the Bank evidence of the approval and entry into effect of the program Operating Regulations, under the terms previously agreed upon with the Bank.** This measure is necessary since approval of the Operating Regulations prior to the first disbursement will facilitate organization of operational aspects for successful implementation.

3.7 **Retroactive financing.** Under the Bank policy on recognition of expenditures, retroactive financing, and advance procurement (document GN-2259-1/OP-507), the Bank may finance, retroactively from the loan proceeds up to US$3 million (10% of the loan amount) in eligible expenditures incurred by the borrower before the loan approval date for payments corresponding to the advance procurement of consulting services and goods and services for the design and rapid implementation of critical program activities, provided that they comply with requirements substantially similar to those established in the loan contract. Such

---

71 The Cybersecurity Committee is made up of the government secretaries of modernization and strategic affairs at the JGM, as well as the ministries of defense, security, foreign affairs and worship, and justice and human rights.

72 Article 2, Decree 480/2019.

expenditures must have been incurred on or after 7 April 2022 (project profile approval date), but in no case will expenditures incurred more than 18 months before the date the Bank's Board of Executive Directors approved the loan be included. The retroactive financing amount will be subject to the disbursement limitations.

3.8 **Procurement of goods and services.** Procurement processes partially or fully financed with loan proceeds will be conducted in line with the Policies for the Procurement of Works and Goods Financed by the Inter-American Development Bank (document GN-2349-15) and the Policies for the Selection and Contracting of Consultants Financed by the Inter-American Development Bank (document GN-2350-15).

3.9 **Financial management.** The loan proceeds will be disbursed through the advance payments, reimbursement, and/or direct payments modalities, established in the OP-273-12 guidelines. Advances of funds will be disbursed based on a financial plan to cover program needs for the next six months or other reasonable period. After the first advance payment, subsequent payments may be processed upon justification of 80% of the total cumulative balance pending justification. The executing agency will use the Execution Unit for Projects with External Financing (UEPEX) system as the financial management system.

3.10 **Auditing.** During execution, the execution agency will submit, on an annual basis, the audited financial statements for the program, in the terms required by the Bank in its policies (document OP-273-12). These audited financial statements will be submitted to the Bank within the 120 days following the close of each fiscal year, duly audited by an independent audit firm eligible for the Bank or by the Office of the Auditor General. The final audited financial statements will be submitted within the 120 days after the date of the final program disbursement.

B. Summary of arrangements for monitoring results

3.11 **Monitoring.** The executing agency will monitor and control all project management processes, which at a minimum will include the following: (i) tracking and reporting the progress made on program execution; (ii) tracking and reporting of program performance towards making the annual physical and financial targets; (iii) tracking of procurement plan execution; (iv) tracking of risk management documents; (v) monitoring of the traceability of outputs and outcomes; (vi) preparation of the semiannual progress reports; (vii) updating of the program's multiyear execution plan, which will be sent to the Bank as part of every semiannual progress report; (viii) preparation of the project completion report; and (ix) systematization of good practices and lessons learned with a view to program closing. The Bank will hold an annual follow-up meeting with the executing agency, at which they will discuss, among other items: (i) the progress made on the activities identified in the annual work plan; (ii) the degree of fulfillment of the indicators established for each component; (iii) the annual work plan for the following year; (iv) the procurement plan for the following 18 months; and (v) the potential modifications of the budget allocations by component (monitoring and evaluation plan).

3.12 **Evaluation.** The results matrix and monitoring and evaluation plan, among other tools, will be used for program evaluation. A midterm and final evaluation and

impact assessment are planned under the program and will include the technical, administrative, and financial aspects. The midterm evaluation will be conducted 90 days from the date on which 50% of the loan proceeds have been disbursed, or two and a half years of execution have elapsed, whichever occurs first. The main objectives of this evaluation will be to review the progress on all the activities planned for that time as well as potential departures from the plan that have occurred and the causes thereof; to propose corrective measures to be applied; and to verify the intermediate outputs generated, the occurrence of risks foreseen in the corresponding matrix, and implementation of the mitigation measures.

3.13 The final evaluation will be submitted to the Bank 90 days from the end of the original disbursement period or any extensions thereto. It will include: (i) results of the physical-financial execution; (ii) degree of fulfillment of the results matrix targets, including a summary of outcomes comparing them to the baseline prepared in the first year of execution; (iii) a summary of the results of the audits performed and of implementation of the improvement plans; (iv) an analysis of the sustainability of program investments, especially with regard to costs and human capital management; and (v) a summary of the main lessons learned. It will also include the “before and after” evaluation and the economic evaluation, which will be performed through an ex post cost-benefit analysis that will replicate the ex ante economic analysis performed before the program, using data gathered during execution and updating the comparator-related data (monitoring and evaluation plan). These analyses will also be reflected in the project completion report prepared by the Bank.

3.14 Lastly, the impact assessment’s objective is to generate knowledge on how to best promote good practices in cybersecurity behavior among public servants. Examples of such good practices include: not opening suspicious links, not sharing sensitive information with unknown people, and periodically changing passwords. The operation will seek to achieve this objective through a field experiment that will test several strategies, including: (i) “learn by doing” or repeated exposure to attack attempts, followed by feedback on the employee’s performance; and (ii) training, with various types of incentives. The theory of change underlying the assessment is that a significant and growing number of cyberattacks on institutions occur through employees (paragraph 1.13). This is because it is more cost-effective for cybercriminals to try to exploit gaps in employees’ knowledge or attention than to overcome the protective barriers installed in software or hardware. The main outcome indicator for the assessment, which also appears in the program results matrix, is the percentage of civil servants who fall into a phishing trap sent in a controlled fashion by the government, after they have completed the various trainings (optional link 7).

3.15 In addition, the borrower, through the executing agency, will perform a strategic evaluation of the program, to generate information on the loan’s contributions to achieving the strategic management priorities. The strategic evaluation design and implementation methodology and arrangements will have to receive the Bank’s no objection.

Development Effectiveness Matrix		
Summary	AR-L1343	
I. Corporate and Country Priorities		
Section 1. IDB Group Strategic Priorities and CRF Indicators		
Development Challenges & Cross-cutting Issues	-Productivity and Innovation -Gender Equality and Diversity -Climate Change -Institutional Capacity and the Rule of Law	
CRF Level 2 Indicators: IDB Group Contributions to Development Results	-Agencies with strengthened digital technology and managerial capacity (#)	
2. Country Development Objectives		
Country Strategy Results Matrix	GN-3051	(i) Improve the population's employability; and (ii) Digital government
Country Program Results Matrix	GN-3087-2	The intervention is included in the 2022 Operational Program.
Relevance of this project to country development challenges (If not aligned to country strategy or country program)		
II. Development Outcomes - Evaluability		Evaluable
3. Evidence-based Assessment & Solution		8.4
3.1 Program Diagnosis		1.9
3.2 Proposed Interventions or Solutions		3.5
3.3 Results Matrix Quality		3.0
4. Ex ante Economic Analysis		7.5
4.1 Program has an ERR/NPV, or key outcomes identified for CEA		1.5
4.2 Identified and Quantified Benefits and Costs		3.0
4.3 Reasonable Assumptions		0.0
4.4 Sensitivity Analysis		2.0
4.5 Consistency with results matrix		1.0
5. Monitoring and Evaluation		10.0
5.1 Monitoring Mechanisms		4.0
5.2 Evaluation Plan		6.0
III. Risks & Mitigation Monitoring Matrix		
Overall risks rate = magnitude of risks*likelihood		Medium High
Environmental & social risk classification		C
IV. IDB´s Role - Additionality		
The project relies on the use of country systems		
Fiduciary (VPC/FMP Criteria)	Yes	Financial Management: Budget, Accounting and Reporting, External Control. Procurement: Information System.
Non-Fiduciary		
The IDB's involvement promotes additional improvements of the intended beneficiaries and/or public sector entity in the following dimensions:		
Additional (to project preparation) technical assistance was provided to the public sector entity prior to approval to increase the likelihood of success of the project	Yes	ATN/OC-17583-AR

Evaluability Assessment Note: The general objective of developing the program is to contribute to the reduction of costs for the state and citizens attributed to cybersecurity incidents. To achieve this end, the loan defines a focus on three specific areas in which the project intervenes.

The first area of focus seeks to increase management coverage for the identification and protection of ICIs; the second focuses on improving productivity in the management of cyber incidents, while the third seeks to make improvements in the efficacy of cybersecurity management of the prioritized ICIs.

The loan proposal presents a diagnosis of the problem based on the economic effects related to cyberattacks and the high cost of processing cybersecurity incidents for the state and citizens. Gender gaps in the cybersecurity workforce are also considered. The proposed solutions focus on improving technological and institutional capacity, human resources, inter-institutional coordination, and the interaction on the ecosystem of actors.

These solutions are appropriate to respond to the identified problems and their contributing factors. The results matrix (RM) is consistent with the vertical logic of the project. The result indicators are properly defined to monitor the achievements of the program and the fulfillment of its specific objectives. The impact indicators are aligned with the general development objective.

The ex-ante economic analysis of the operation is appropriate under the assumptions applicable to this type of project, as well as according to reasonable sensitivity analyses. It is based on the potential benefits of generating an improved capacity to prevent and respond to cyber-attacks. The analysis shows a positive net present value in the central scenario, as well as under various conditions included in the sensitivity analysis.

The monitoring and evaluation plan includes an experimental methodology with a view to generating evidence on the effectiveness of promoting good cybersecurity behavioral practices. Administrative data will be used for all baseline variables. The monitoring and evaluation activities will be carried out by the Argentinian Chief of the Cabinet of Presidency Ministers (JGM) in coordination with the Bank.

RESULTS MATRIX

Project objective:	The specific development objectives are to: (i) expand coverage of measures for identifying and protecting critical information infrastructure (CII); (ii) improve productivity in the management of cyber incidents; and (iii) improve cybersecurity management efficacy for the prioritized CII. Achievement of these objectives will contribute to the general development objective of helping to reduce the costs of cybersecurity incidents for the State and citizens.

GENERAL DEVELOPMENT OBJECTIVE

Indicators	Unit of measure	Baseline value	Baseline year	Expected year achieved	Target	Means of verification	Comments
General development objective: Savings on cybersecurity incident management costs for the State and society							
1. National cybersecurity capacity maturity level	Score	125	2020	2027	165	OAS IDB report	See the monitoring and evaluation plan.
2. Annual cyber incident management costs	US$ millions	8.2	2021	2027	3.4	Ex post cost-benefit evaluation	See the monitoring and evaluation plan.

SPECIFIC DEVELOPMENT OBJECTIVES

Indicators	Unit of measure	Baseline value	Baseline year	Final target	Means of verification	Comments
Specific development objective 1: Expanded coverage of measures for identifying and protecting CII						
1.1 Coverage of sectors with identified CII	%	9	2021	50	SIP semiannual progress report	See the monitoring and evaluation plan.
1.2 Coverage of ministries monitored through the G-SOC	%	0	2021	60	SIP semiannual progress report	See the monitoring and evaluation plan.
1.3 Hardware procured with the energy efficiency seal	%	0	2021	90	SIP semiannual progress report, to include the National Public Procurement Office annual report	Pro-climate indicator. See the monitoring and evaluation plan.

Indicators	Unit of measure	Baseline value	Baseline year	Final target	Means of verification	Comments
Specific development objective 2: Improved productivity in cybersecurity incident management						
2.1 Cyber incidents managed per year	Number	591	2021	10,000	SIP semiannual progress report	See the monitoring and evaluation plan.
2.2 Managed cyber incidents classified as high or critical severity (high impact)	%	81.7	2021	5	SIP semiannual progress report	See the monitoring and evaluation plan.
2.3 Women SIP employees certified in cybersecurity	%	28	2021	34	SIP semiannual progress report	Pro-gender indicator. See the monitoring and evaluation plan.
2.4 Agencies with strengthened digital technology and managerial capacity	Number	0	2021	2	SIP semiannual progress report	See the monitoring and evaluation plan.
Specific development objective 3: Improved cybersecurity management efficacy for the prioritized CII						
3.1 GDE cybersecurity findings resolved	%	0	2021	50	SIP semiannual progress report and 2021 audit report	See the monitoring and evaluation plan.
3.2 Successful recovery tests after IT problems	Number	0	2021	4	SIP semiannual progress report including restoration exercises performance report	See the monitoring and evaluation plan.

OUTPUTS

Indicators	Unit of measure	Baseline value	Baseline year	Year 1	Year 2	Year 3	Year 4	Year 5	End of project	Means of verification	Comments
Component 1. Strengthening of the SIP's institutional and technological capacities											
1.1 Institutional and regulatory framework for identifying and protecting the CII, approved	Institutional framework	0	2021	0	1	0	0	0	1	SIP semiannual progress report and JGM administrative decision approving the institutional framework	See the monitoring and evaluation plan.
1.2 Actions to strengthen the monitoring and detection of attacks (G-SOC) with SIEM tools and sensors	Actions	0	2021	1	1	1	1	1	5	SIP semiannual progress report	See the monitoring and evaluation plan.
1.3 Actions to strengthen the National CERT's operational capacities	Actions	0	2021	1	1	1	1	1	5		
1.4 Platforms for threat analysis and information exchange with the private sector, implemented	Platform	0	2021	0	1	0	0	0	1	SIP semiannual progress report and platform use report	See the monitoring and evaluation plan.
Component 2. Strengthening of human talent in cybersecurity											
2.1 Cyberattack simulation platform installed	Platform	0	2021	0	1	0	0	0	1	SIP semiannual progress report and simulation platform use report	

Indicators	Unit of measure	Baseline value	Baseline year	Year 1	Year 2	Year 3	Year 4	Year 5	End of project	Means of verification	Comments
2.2 Cybersecurity certification and technical programs (prioritizing women) developed	Programs	0	2021	1	1	1	1	1	5	SIP semiannual progress report to include enrollment report	Pro-gender indicator. See the monitoring and evaluation plan.
2.3 E-learning software installed and operating	Software	0	2021	0	1	0	0	0	1	SIP semiannual progress report including software use report	See the monitoring and evaluation plan.
2.4 Cybersecurity change management and curriculum development plan implemented	Document	0	2021	0	1	0	0	0	1	SIP semiannual progress report to include approved document	
Component 3. Improved protection of the GDE ecosystem											
3.1 Cybersecurity policy developed	Document	0	2021	0	1	0	0	0	1	SIP semiannual progress report including document approved by the competent authority	See the monitoring and evaluation plan.
3.2 Backup technologies implemented (hardware and software)	Systems	0	2021	0	0	1	0	0	1	SIP semiannual progress report including system reports	See the monitoring and evaluation plan.
3.3 GDE cybersecurity trainings implemented	# of workshops	0	2021	2	2	2	2	2	10	SIP semiannual progress report including system reports	

Country: Argentina **Division:** IFD/ICS **Operation No.:** AR-L1343 **Year:** 2023

FIDUCIARY AGREEMENTS AND REQUIREMENTS

Executing agency: Argentine Republic, through the Office of the Chief of the Cabinet of Ministers (JGM) of the Office of the President

Operation name: Cybersecurity for Critical Information Infrastructure Program

I. FIDUCIARY CONTEXT OF THE EXECUTING AGENCY

1. **Use of country system in the operation**

☒ Budget	☒ Reports	☒ Information system	☐ National Competitive Bidding (NCB)
☐ Treasury	☐ Internal audit	☐ Shopping	☐ Other
☒ Accounting	☒ External control	☐ Individual consultants	

2. **Fiduciary execution mechanism**

☒	Special features of fiduciary execution	The borrower will be the Argentine Republic. The executing agency will be the borrower through the JGM, acting through the DIPROSE, which will be responsible for administrative and financial coordination, and the SSTI Computer Networks and Systems Security Prevention Department (DPSSYRI), which will be the substantive program area. To that end, it will be supported by an expert integrated team with diverse roles.

3. **Fiduciary capacity**

Fiduciary capacity of the executing agency	The institutional analysis found that the executing agency's institutional capacity for taking on the responsibility of managing program resources, to include financial administration and accounting, procurement, contracting, and the planning and monitoring of activities, needs to be strengthened. To that end, the program will finance the hiring of technical support staff and a team of administrative-financial consultants to complement the JGM's capacities and, in turn, support the SIP management.

4. **Fiduciary risks and risk response**

Area (financial management / procurement)	Risk	Risk level	Risk response
Internal processes	Delays between identification of a need and the time it takes to incorporate the various goods and services could slow project progress.	Medium-high	Train and hire, as necessary and in agreement with the Bank, qualified employees with experience in multilateral organizations' procurement management procedures; the Bank will provide support and training on fiduciary issues.

5. **Policies and guidelines applicable to the operation**: Goods and works will be procured in accordance with the Policies for the Procurement of Goods and Works Financed by the Inter-American Development Bank (document GN-2349-15) and consultants will be selected and contracted pursuant to the Policies for the Selection and Contracting of Consultants Financed by the Inter-American Development Bank (document GN-2350-15). The Financial Management Guidelines for IDB-financed Projects (document OP-273-12) or its applicable updates will apply for financial management.

6. **Exceptions to Policies and Guidelines**: None.

II. CONSIDERATIONS FOR THE SPECIAL PROVISIONS OF THE LOAN CONTRACT

Exchange rate: For the purposes of the provisions of Article 4.10 of the General Conditions, the parties agree that the exchange rate to be used will be the rate stipulated in Article 4.10(b)(i). For the purpose of determining the equivalency of expenditures incurred in local currency chargeable against the local contribution, or of reimbursements for expenditures chargeable against the loan proceeds, the agreed-upon exchange rate will be the rate in effect on the first working day of the month in which the borrower, the executing agency, or any other person or corporation with delegated authority to incur expenditures makes the respective payments to the contractor, vendor, or beneficiary.
Audited annual financial reports: The executing agency will submit audited annual financial reports on the use of the funds, as per the terms of reference agreed upon with the Bank, within the 120 days following the close of the fiscal year. The project's final financial reports will be submitted within the 120 days following the date of the final disbursement. The external audit of the program will be carried out by an independent audit firm eligible to audit Bank-financed operations, selected and contracted pursuant to the terms of reference and model contract previously agreed upon with the Bank or by the Office of the Auditor General.

III. AGREEMENTS AND REQUIREMENTS FOR PROCUREMENT EXECUTION

<table>
<tr><td>☒</td><td>Bidding documents</td><td>The Bank's standard bidding documents or other documents agreed upon between the executing agency and the Bank for a specific procurement item will be used for works, goods, and nonconsulting services procured in accordance with the Policies for the Procurement of Goods and Works Financed by the Inter-American Development Bank (document GN-2349-15) and subject to international competitive bidding (ICB). Likewise, consulting services will be selected and contracted in accordance with the Policies for the Selection and Contracting of Consultants Financed by the Inter-American Development Bank (document GN-2350-15) using the Standard Request for Proposals issued by the Bank or a request for proposals agreed upon by the executing agency and the Bank for a specific selection. For the procurement of goods and services, the Compr.AR system will be used preferentially, with bidding documents adapted and accepted by the Bank. The project's sector specialist will be responsible for reviewing the technical specifications and terms of reference for procurement during the preparation of selection processes. This technical review may be conducted ex ante and is independent of the procurement review method used.</td></tr>
<tr><td>☒</td><td>Advance procurement / Retroactive financing</td><td>Pursuant to the Bank's policy on recognition of expenditures, retroactive financing, and advance procurement (document GN-2259-1/OP-507), the Bank may finance, retroactively from the loan proceeds, eligible expenditures incurred by the borrower before the loan approval date, up to US$3 million (10% of the loan) for payments corresponding to the advance procurement of consulting services and goods and services for the design and rapid implementation of critical program activities, provided requirements substantially similar to those established in the loan contract have been met. Such expenditures must have been incurred on or after 7 April 2022 (the project profile approval date), but in no case will expenditures incurred more than 18 months before the date on which the Bank Board of Executive Directors approved the loan be included. The retroactive financing amount will be subject to the limitations applicable to the disbursements.</td></tr>
<tr><td>☒</td><td>Procurement supervision</td><td>Supervision will be ex post, except where ex ante supervision is justified. The supervision method (ex ante or ex post) will be determined for each selection process. Ex post reviews will be conducted every 18 months as per the project supervision plan, which is subject to change during execution. Ex post review reports will include at least one visit. The thresholds for ex post review are:
<table>
<tr><th>Works</th><th>Goods/services</th><th>Consulting services</th></tr>
<tr><td>5 million</td><td>500,000</td><td>200,000</td></tr>
</table></td></tr>
<tr><td>☒</td><td>Records and files</td><td>For procurement processes executed with Compr.AR, the system will serve as a repository for Bank supervision.</td></tr>
</table>

Main procurement items

Procurement description	Selection method	Estimated date	Estimated amount (US$ thousands)
Goods			
Basic equipment	National competitive bidding (NCB)	June 2023	400
Software and hardware for SIEM, aggregation, backup, etc. (Various)	ICB	September 2023	10,600
Nonconsulting services			
Preventive cybersecurity services	NCB	June 2023	2,300
Training and event organization	Shopping by open invitation	June 2024	880
Firms			
GDE cybersecurity gap analysis	Quality- and cost-based selection (QCBS)	January 2024	500
Academic programs and specialized courses (various processes)	Selection Based on the Consultant's Qualifications (CQS)	March 2024	740
Pro-gender actions in the sector	CQS	February 2023	150
Consulting services for various certifications	CQS	February 2024	400
Strengthening the National CERT's operational capacities	CQS	February 2023	200
E-learning consulting platform	QCBS	June 2023	625
Consulting services—Platforms, Notification, and Coordination of Incidents and Threat Information Exchange	QCBS	February 2024	320
Risk analysis consulting services	QCBS	March 2023	250
Consulting services for CERT.ar / G-SOC L1-L2 operation	QCBS	March 2023	2,900
Advanced cybersecurity services	QCBS	June 2023	980

Procurement description	Selection method	Estimated date	Estimated amount (US$ thousands)
Event aggregator platform	QCBS	June 2023	675
National probes program	QCBS	April 2023	1,400
Consulting services on the detection and identification of technological and human assets	QCBS	April 2023	450
Consulting services for the design and launch of the G-SOC	QCBS	January 2023	600
Consulting services for identification of CII and design of protection plans	QCBS	January 2023	320
Consulting services for the design of the institutional and regulatory framework	QCBS	February 2023	600
Individuals			
Monitoring of academic courses and certifications	Selection of individual consultant (3CV)	January 2023	275
Communications management	3CV	January 2023	250
CERT.ar G-SOC team	3CV	January 2023	375
Specialized consulting services for fiduciary strengthening and administration	3CV	January 2023	1,300

To access the procurement plan, see this link.

Procedures	Rationale for use
E-procurement of goods and services	The Bank approved the use of Compr.AR in 2018 following established procedures.

IV. FINANCIAL MANAGEMENT AGREEMENTS AND REQUIREMENTS

☒	Programming and budget	The executing agency will be responsible for formulating and programming the annual budget and will take all the necessary steps to consolidate it for approval. When entries must be expanded or reassigned, the execution unit will request the modifications and take responsibility for procuring approval. Budget appropriations are made through quarterly commitment fees and monthly accruals, allocated by the National Budget Office (Ministry of the Economy).
☒	Treasury and disbursement management	**Bank accounts:** The executing agency will keep one special account in dollars and one in pesos at the Banco Nación for the exclusive management of program funds. They will be separated and identified for accounting and operations. **Financial plan:** Disbursements will be made according to a detailed financial plan based on the program's actual liquidity needs. **Disbursement method:** The Bank will disburse funds according to the advance of funds modality or another modality established in the OP-273-12 guidelines. After the first advance of funds, subsequent disbursements may be processed upon justification of 80% of the prior advances, since the operation is a decentralized program that is complex to execute. The "online disbursement" electronic platform will be used to manage disbursements.
☒	Accounting, information systems, and reporting	The executing agency will use the Execution Unit for Projects with External Financing (UEPEX) system as the financial management system. Under this system, program funds and financing sources can be identified. UEPEX earmarks, as per the Bank-approved chart of accounts, the program investments by cost table component. Accounting transactions are recorded on a cash basis, and the International Financial Reporting Standards will be followed as applicable in accordance with established national criteria.
☒	External control and financial reports	External control is handled by the Office of the Auditor General, the governing external control agency, which reports to and assists the national congress in controlling the public sector's accounts. The establishment and operation of this office are regulated in Title VII, Chapter I of Law 24,156 on Financial Administration and External Control Systems. The program's annual financial statements, based on the terms of reference previously agreed upon with the Bank, will be audited by an independent auditor acceptable to the Bank, which could be the Office of the Auditor General or an independent audit firm.
☒	Financial supervision of the operation	The financial supervision plan will arise from the evaluations of the executing agency's fiduciary capacity and risk and will include on-site supervision visits and desk reviews, as well as the analysis and tracking of outcomes and the auditors' recommendations for the program's annual financial reports.

DOCUMENT OF THE INTER-AMERICAN DEVELOPMENT BANK

PROPOSED RESOLUTION DE-__/23

Argentina. Loan ____/OC-AR to the Argentine Republic. Cybersecurity for Critical Information Infrastructure Program

The Board of Executive Directors

RESOLVES:

That the President of the Bank, or such representative as he shall designate, is authorized, in the name and on behalf of the Bank, to enter into such contract or contracts as may be necessary with the Argentine Republic, as borrower, for the purpose of granting it a financing aimed at cooperating in the execution of the Cybersecurity for Critical Information Infrastructure Program. Such financing will be for the amount of up to US$30,000,000, from the resources of the Bank's Ordinary Capital, and will be subject to the Financial Terms and Conditions and the Special Contractual Conditions of the Project Summary of the Loan Proposal.

(Adopted on _____ 2023)

LEG/SGO/CSC/EZSHARE-1044359933-20319
AR-L1343