PUBLIC
SIMULTANEOUS DISCLOSURE

DOCUMENT OF THE INTER-AMERICAN DEVELOPMENT BANK

URUGUAY

STRENGTHENING CYBERSECURITY IN URUGUAY

(UR-L1152)

LOAN PROPOSAL

This document was prepared by the project team consisting of Miguel Porrúa (IFD/ICS), Project Team Leader; Roberto Fernández, Alternate Project Team Leader; Alejandro Pareja, Ariel Nowersztern, Benjamin Roseth, Dario Kagelmacher, and Sonia Rojas (IFD/ICS); Harold Villalba (SPD/SDV); Abel Cuba and Emilie Chapuis (FMP/CUR); and Krysia Avila (LEG/SGO).

CONTENTS

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

LINKS

REQUIRED

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

OPTIONAL

1. Project economic analysis
   1.A. Report
   1.B. Spreadsheet
2. Uruguay Digital Agenda 2020
3. Internet Security Threat Report, February 2019
4. Impact of Digital Security Incidents in Colombia 2017
5. Framework for Improving Cybersecurity in Critical Infrastructure, 2018
6. Security report 2016
7. Safeguard Policy Filter and Safeguard Screening Form

ABBREVIATIONS

AGESIC	Agencia para el Desarrollo de Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento [Agency for the Development of e-Government Management and the Information and Knowledge Society]
CGN	Contaduría General de la Nación [General Accounting Office]
CERT.uy	Centro Nacional de Respuesta a Incidentes de Seguridad Informática [Computer Emergency Response Team]
GSOC	Government Security Operation Center
ICTs	Information and communication technologies
NIST	National Institute of Standards and Technology
SIEM	Security Information Event Management
TCR	Tribunal de Cuentas de la República [Office of the Auditor General]

PROJECT SUMMARY

URUGUAY
STRENGTHENING CYBERSECURITY IN URUGUAY
(UR-L1152)

<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">Eastern Republic of Uruguay</td><td>Amortization period:</td><td>25 years</td></tr>
<tr><td colspan="3">Executing agency:</td><td>Disbursement period:</td><td>4 years</td></tr>
<tr><td colspan="3">Eastern Republic of Uruguay, through the Agency for the Development of e-Government Management and the Information and Knowledge Society (AGESIC)</td><td>Grace period:</td><td>5.5 years[b]</td></tr>
<tr><td>Source</td><td>Amount (US$)</td><td>%</td><td>Interest rate:</td><td>LIBOR-based</td></tr>
<tr><td>IDB (Ordinary Capital):</td><td>8,000,000</td><td>80</td><td>Credit fee:</td><td>[c]</td></tr>
<tr><td rowspan="2">Local:</td><td rowspan="2">2,000,000</td><td rowspan="2">20</td><td>Inspection and supervision fee:</td><td>[c]</td></tr>
<tr><td>Weighted average life:</td><td>15.25 years</td></tr>
<tr><td>Total:</td><td>10,000,000</td><td>100</td><td>Approval currency:</td><td>U.S. dollars</td></tr>
<tr><th colspan="5">Project at a Glance</th></tr>
<tr><td colspan="5">Project objective/description: The program will help strengthen Uruguay’s capacity to protect its cyberspace through improved prevention, detection, and response to cyberattacks.</td></tr>
<tr><td colspan="5">Special contractual conditions precedent to the first disbursement: As a condition precedent to the first disbursement, the borrower, acting on its own or through the executing agency, will submit to the Bank evidence that (i) AGESIC’s director of information security has been designated general program coordinator, and (ii) the program’s operations coordinator has been appointed (paragraph 3.5).</td></tr>
<tr><td colspan="5">Exceptions to Bank policies: None.</td></tr>
<tr><th colspan="5">Strategic Alignment</th></tr>
<tr><td colspan="2">Challenges:[d]</td><td colspan="3">SI ☑ PI ☑ EI ☐</td></tr>
<tr><td colspan="2">Crosscutting themes:[e]</td><td colspan="3">GD ☑ CC ☐ 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, and commodity conversions. The Bank will take market conditions as well as 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 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 applicable policies.

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

[e] GD (Gender Equality and Diversity); CC (Climate Change and Environmental Sustainability); and IC (Institutional Capacity and Rule of Law).

I. Description and Results Monitoring

A. Background, problem addressed, and rationale

1.1 **Context.** Uruguay is one of the most developed countries in the region in terms of e-government,[1] e-commerce, and use of information and communication technologies (ICTs). Its progress in development of e-government includes the following: (i) 95% of all transactions with the national government can be started online;[2] (ii) its identity document includes a chip and biometric data; and (iii) digitized medical records are being implemented. The Agency for the Development of e-Government Management and the Information and Knowledge Society (AGESIC) is responsible for the e-government agenda[3] and cybersecurity policy.[4]

1.2 The high rate of ICT penetration in all realms of society increases not only the number of potential vulnerabilities and incidents, but also their potential impact due to an expansion of what experts call the "attack surface."[5] While both e-government and cybersecurity are regulated by AGESIC, cyberspace protection efforts have not kept pace with digitization, thus leaving Uruguay's cyberspace vulnerable to attack.[6] The 2016 Cybersecurity Report found that Uruguay's score on the Cybersecurity Capability Maturity Model was less than half of what would denote sound cybersecurity policy for countries at a comparable level of development.[7]

1.3 Uruguay has carried out numerous initiatives to protect its cyberspace, staking its position as one of the most advanced countries in Latin America and the Caribbean in terms of cybersecurity. Yet, as noted in the 2016 Cybersecurity Report, significant weaknesses remain. AGESIC launched the Computer Emergency Response Team (CERT.uy) in 2008[8] and the Government Security Operation Center (GSOC) in 2017.[9] The technical capacity and technological equipment of CERT.uy have not kept pace with the demands of a rapidly changing digital world, nor does the GSOC have all the resources it needs to fulfill its purpose. The government, though, is committed to achieving a secure digital environment, as reflected in "Uruguay Digital Agenda," one objective of which is

---

1 e-Government Readiness Survey 2018. United Nations.

2 Wait No More: Citizens, Red Tape, and Digital Government. IDB 2017.

3 Law 17.930 of 19 December 2005, Article 72, created AGESIC as the entity in charge of e-government policy.

4 Law 18.719 of 27 December 2010, Article 149, created the Office of the Director of Information Security as part of AGESIC.

5 Cybersecurity Ventures.

6 Cybersecurity: Are We Ready in Latin America and the Caribbean? IDB and the Organization of American States. 2016. This report examines all countries in Latin America and the Caribbean using a methodology of the University of Oxford, which includes 49 indicators grouped into five dimensions.

7 Uruguay scored 149 out of a possible 245.

8 CERT.uy is responsible for cyberspace incident response in Uruguay. It was established by Article 73 of Law 18.362 of 6 October 2008 (see Article 73), and its operations and organizational structure are governed by Decree 451/009 of 28 September 2019.

9 The GSOC is responsible for monitoring, analyzing, and responding to all incidents in the government's ICT infrastructure. According to AGESIC's cybersecurity organizational chart, the GSOC operates as part of CERT.uy.

"trust and security in the use of digital technologies."[10] This objective is complemented by the Information Security Incident Management Policy and related guidelines for implementation.[11]

1.4 This lack of capacity in CERT.uy and the GSOC makes it difficult to detect cyberattacks or can delay detection until after the damage has been done. CERT.uy's own analyses have found that as its technological and human capacity increases, so does its ability to detect cyberspace incidents. After Uruguay established the GSOC in 2017, incident detection increased by 69%.[12]

1.5 According to the International Telecommunications Union, Uruguay is the Latin American country with the most advanced digital agenda,[13] placing 42nd out of 176 countries. In addition, according to the United Nations, Uruguay has the most developed e-government in Latin America and the Caribbean, ranking 34th out of 193 countries worldwide and first in the region. Uruguay is also Latin America's leader in software exports per capita, with more than 300 companies exporting to 52 countries.[14] Cyberattacks are now the risk that companies are most concerned about, more so than terrorist attacks, financial bubbles, or fiscal crises.[15] Cyberattacks take a significant economic toll and are costing an average of 0.5% of worldwide GDP.[16] A study in Colombia by the Colombian government, the Bank, and the Organization of American States found that cybercrime can cost up to 5% of the sales of microenterprises and 1% of those of small and medium-sized enterprises.[17] The same study found that cybersecurity incidents in the public sector cost an average of 0.5% of the investment budget, while 17% of public entities reported more than US$200,000 in costs from damage to assets and infrastructure. A recent study by the International Monetary Fund estimated average losses due to cyberattacks in the financial sector at 9% of net revenues.[18]

1.6 The economic analysis looked at two aspects of the economic impact of Uruguay's current cybersecurity policy. First is the overall economic cost to the country, which could be as much as US$24 million per year. Second is the economic activity that the country could generate by exporting cybersecurity-related training and consulting services to the rest of the region. The economic value of this positive impact of enhanced cybersecurity is difficult to estimate, but given the strength of Uruguay's ICT sector, which grew at an average rate of 11.55% between 2007 and 2017, and the low level of cybersecurity development across Latin America, stronger cybersecurity in Uruguay opens up significant economic opportunities.

---

10 Uruguay Digital Agenda: Transforming with Equity 2020. Objective VIII, p. 18.

11 Resolutions 59/010 and 62/010 of the AGESIC Honorary Leadership Council.

12 CERT.uy statistics.

13 ICT Development Index 2017. International Telecommunications Union.

14 Uruguayan Customs Brokers Association.

15 "Cyber attacks are shutting down countries, cities and companies. Here's how to stop them." World Economic Forum. 2018. See table with the Global Risk Report ranking in the article.

16 Net Losses: Estimating the Global Cost of Cybercrime. Center for Strategic and International Studies (CSIS) and McAfee 2014.

17 Impact of Digital Security Incidents in Colombia 2017. Ministry of Information and Communication Technologies, Organization of American States, and IDB. 2017.

18 Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. Antoine Bouveret. International Monetary Fund. 2018. Working Paper 18/143.

1.7 Cybercrime has become a powerful industry that has surpassed drug trafficking in terms of financial resources generated.[19] Such is its level of organization and development that DEF CON—one of the most prominent worldwide gatherings of hackers—draws more than 20,000 people to Las Vegas each year.[20] Perpetrators of criminal cyberattacks have access to a developed market of products and services that support cybercrime, making it an easy, low-cost endeavor.[21] For example, a denial-of-service attack[22] costs only US$5 to US$20 per hour, and a ransomware kit[23] costs less than US$250.

1.8 According to the National Institute of Standards and Technology (NIST)[24]—the most widely used frame of reference for cybersecurity policymaking across the globe—an effective cyber-risk management model should fulfill five functions: identify, protect, detect, respond, and recover. This framework also supports development of a governance model and a common language to facilitate risk management, help distribute it among relevant entities for cyberspace protection, and identify cybersecurity investments based on areas targeted for risk reduction.

1.9 The consequences of digital incidents include (i) economic harm: response and mitigation, impact on service availability, compensation for those harmed, reduced use of services as a result of decreased confidence; for example, a single attack known as NotPeya cost US$10 billion;[25] (ii) reputational harm to organizations and government, as recently happened with multiple governmental websites, including some sites of Presidents; (iii) violations of people's privacy: when the financial company Equifax was hacked, the data of 143 million customers were exposed;[26] (iv) harm to digital and financial inclusion as a result of reduced use of technology; for example, a study by FireEye found that 75% of people would stop purchasing from a company if a data breach were found to be the result of a cybersecurity policy failure;[27] and (v) harm to the democratic system and social unity, as illustrated in some recent presidential elections in the Americas and Europe, when hackers exposed several gigabytes of emails of some parties participating in electoral processes just days before the election.

---

19 "How cyber attacks became more profitable than the drug trade," *Fortune*.

20 DEF CON. See attendance figures here.

21 Information Security Report 2019: Volume 24. February 2019. Symantec.

22 A denial-of-service attack is a simultaneous request for multiple services from a website, exceeding its response capacity and rendering it inoperative.

23 Ransomware is a sophisticated computer virus that blocks users' access to the files on their devices. In many cases, the files can only be rescued by paying the cyberattackers a ransom.

24 The National Institute of Standards and Technology, an agency of the United States Department of Commerce, has developed a cybersecurity policy framework that is widely used across the world.

25 Notpetya.

26 *The Washington Post*. September 2017.

27 *Security Magazine*. May 2016.

1.10 **The main challenge.** The general problem is the low degree of implementation of Uruguay's cybersecurity policy, which leaves the country vulnerable to future cyberattacks.[28] The specific problems related to the general problem are as follows:

1.11 **Lack of operational capacity to monitor, detect, and respond to incidents.**[29] Incidents detected early can be managed more effectively. This limits the damage and reduces the cost of response, since the attack is detected at a less advanced stage. If monitoring systems are nonexistent or unsophisticated, incidents will not be detected until the harm is underway, and this harm increases geometrically with every hour that it goes unresolved. In Uruguay, remediating incidents of a high or very high degree of severity[30] costs about US$48,000.[31] This specific problem is linked to the following causative factors: (i) the GSOC currently uses only perimeter monitoring for government entities, which means that their internal systems are not being monitored; (ii) the GSOC has limited capacity to analyze alerts, and the current monitoring system lacks functionalities related to big data, information sharing, and threat intelligence;[32] and (iii) there is no secure, confidential way to share information on attacks and incidents with the private sector.

1.12 **Lack of trained cybersecurity professionals.** The rapidly growing need for cybersecurity professionals has created a significant gap between supply and demand.[33] Uruguay currently has an estimated 650 cybersecurity professionals and needs to double this figure in the next two years.[34] This gap also has a major gender element. Fewer than 10% of cybersecurity professionals in the country are women, according to AGESIC. In that agency, only three of its 27 team members are women; and at Deloitte Cybersecurity, on a team of 10, there is only one woman. This specific problem is related to the following causative factors: (i) available courses in information security are limited, lack variety, and are only offered in person. Of Uruguay's four universities, only the University of the Republic offers a specialized course in information security. Only 1% of undergraduate and graduate course offerings in ICTs are offered in areas outside the capital, which means that half of Uruguayans must travel to the capital for such training;[35] (ii) there are not enough educators in this field to meet the demand for training for cybersecurity professionals;[36] (iii) there is a lack of standardization in course content, making it difficult to develop professional job descriptions; and

---

28 According to the aforementioned 2016 Cybersecurity Report, Uruguay scored a 149 out of a possible 245. As a point of comparison, Israel scored 200.

29 Study by SecurePro, as input for the design of this project. Uruguay's security operations center is below the average score on the Cyber Security Maturity Model.

30 AGESIC uses an incident rating system based on the standards of the European Union Agency for Network and Information Security. This rating is based on institutional impact, economic impact, and number of hours spent on incident response. Incidents of a high or very high degree of severity require more than 640 hours of response by a senior expert.

31 Figure provided by AGESIC on the basis of its experience over the past 10 years.

32 Ibid. See footnote 30 on SecurePro study.

33 The worldwide gap in cybersecurity professionals was estimated at 1.5 million for 2010. *Harvard Business Review*. May 2017.

34 Cybersecurity Excellence Framework. October 2018. Avnet, p. 37.

35 2017 Report on Academic Training in ICTs. Uruguayan Chamber for Information Technologies.

36 Uruguay has only 22 educators in cybersecurity, who periodically meet as part of a group called Hack and Beers.

(iv) there are few opportunities to participate in international venues for exchanging professional knowledge.[37]

1.13 **The Bank's experience and lessons learned.** The Bank has extensive experience in designing and implementing projects related to the use of ICTs in public administration and, in particular, to the incorporation of components related to cyberspace protection, such as "Panama Online" (loan 3683/OC-PN), "Government Digital Transformation to Strengthen Competitiveness" (loan 4549/OC-BH), "Project to Improve and Expand Support Services for National Service Delivery to Citizens and Enterprises" (loan 4399/OC-PE), and "Digital Agenda Support Program" (loan 4650/OC-PR). The Bank has also received technical and financial support from the Israeli and Spanish governments through two technical cooperation operations "Improving Human Resources Capacity in Cybersecurity" (ATN/CF-15598-RG) and "Strengthening of Cybersecurity in Latin America and the Caribbean" (ATN/FG-16633-RG). These technical cooperation operations have financed training activities and studies that have served as essential input for the design of this operation. The Bank has also been supporting AGESIC, the entity in charge of cybersecurity in Uruguay, for 10 years through the following e-government operations: "e-Government Management Project in the Health Sector" (loan 3007/OC-UR); "Program for Improvement of Public Services and State-Citizen Interaction (loan 3625/OC-UR); "e-Government Management Project in the Health Sector II" (loan 4300/OC-UR); "Program to Support e-Government Management in Uruguay II (loan 2591/OC-UR); and "Public Management Strengthening Program" (loan 3398/OC-UR). A loan operation to support e-government over the next four years is currently being designed. This project is particularly important in order to uphold the work supported by the Bank through loan 2591/OC-UR—which has put all government transactions online and includes creation of the position of "digital ambassador," who will play a key role in the international management of cybersecurity in Uruguay—as well as loan 4300/OC-UR for digitization of medical records in Uruguay. Another loan operation is currently being designed to strengthen the strategic management of public safety in Chile; this operation will include a cybersecurity component with activities similar to this program's. This will facilitate the sharing of lessons learned, both in the design phase and when the programs are ultimately implemented.

1.14 This is the first Bank-supported operation devoted fully to cybersecurity. Given the need of countries in Latin America and the Caribbean to strengthen their cybersecurity policies, this operation is a valuable opportunity for learning, method generation, and replicability in other countries in the region. According to the 2019 Cybersecurity Report, Uruguay is the most advanced country in Latin America and the Caribbean despite scoring at only the halfway point of the cyber security maturity model. Uruguay has a security operation center, a computer emergency response team, a team of cybersecurity professionals, and an operational framework for cybersecurity as a result of its own translation and adaptation of NIST standards. Operations previously executed with AGESIC have yielded lessons on leadership, institutional coordination, participation, teamwork, and the role of the private sector, and these lessons have been incorporated into the design of this operation. AGESIC has engaged the technology-related private sector in designing this operation in order to help open up a new area of export-oriented technological activity. Only 13 other countries in Latin America and the

[37] Conversation with educators at a gathering of Hack and Beers.

Caribbean have cybersecurity strategies, with most of them scoring at less than 40% on the maturity model, as noted in the 2016 Cybersecurity Report. This signals significant potential for the Bank's work and for Uruguay to export knowledge on the basis of the work to be carried out in this program.

1.15 **Strategic alignment.** The program is aligned with the Update to the Institutional Strategy 2010-2020 (document AB-3008) and is strategically aligned with the development challenges of (i) Social Inclusion and Equality, as it promotes the availability of in-person training in cybersecurity in areas outside the capital through the Technological University (UTEC), making this training more accessible to low-income people; and (ii) Productivity and Innovation, as it contributes to the challenge of "low productivity and innovation" by promoting a new area of high-value economic activity in the form of cybersecurity. The program is also aligned with the crosscutting issues of (i) Gender Equality and Diversity, as it promotes the training of women in cybersecurity (paragraph 1.19 – Activity ii); and (ii) Institutional Capacity and Rule of Law, as it strengthens AGESIC's capacity to protect Uruguay's cyberspace. The program will also contribute to the Corporate Results Framework 2016-2019 (document GN-2727-6) in the following indicators: (i) government agencies benefited by projects that strengthen technological and managerial tools to improve public service delivery; (ii) teachers trained; (iii) countries using country fiduciary systems; (iv) crime information systems strengthened; and (v) projects supporting innovation systems. It is also aligned with the Sector Strategy on Institutions for Growth and Social Welfare (document GN-2587-2) because it contributes to the topic of institutions for innovation and technological development, especially in relation to the objectives of (i) improving policies and governmental action in the ICT sector; (ii) developing advanced human capital; and (iii) strengthening institutions and networks. The program is consistent with the Citizen Security and Justice Sector Framework Document (document GN-2771-7), as it contributes to the goal of efficiency and effectiveness of public policies on citizen security and justice in the region, in order to contribute to the reduction of crime and violence.[38] The program is also aligned with the Bank's country strategy with Uruguay 2016-2020 (document GN-2836) in its priority area of greater efficiency in public institutions, as part of its strategic objective of strengthening public management systems. The program is also aligned with the 2019 Operational Program Report (document GN-2948). Lastly, the program will collaborate with implementation of the "Transactions 100% Online" initiative, which is part of Uruguay's 2015-2019 Government Program, as well as with fulfillment of objective viii of "Trust and security in the use of digital technologies" from the Uruguay Digital Agenda 2020.

B. Objectives, components, and cost

1.16 **Program objective.** The program will help strengthen Uruguay's capacity to protect its cyberspace through improved prevention, detection, and response to cyberattacks. To this end, the program will be divided into the following components:

[38] In particular, it contributes to dimension of success 2: "Police work is results-based and involves close collaboration with the community with the aim of preventing, addressing, and solving crime."

1.17 **Component 1. Improving operational capacity and tools for CERT.uy (US$5,415,000).** The following activities will be carried out: (i) update of technological tools for analyzing and managing cybersecurity events (Security Information Event Management—SIEM);[39] (ii) expansion of the Next Generation Intrusion Prevention System,[40] increasing the number of monitored institutions and the functionalities of the tool; (iii) incorporation of a big data platform to help exchange information with the private sector[41] and intelligent threat analysis;[42] (iv) CERT.uy laboratory tools (forensic, proof of concept, sensor development, incident management, etc.); (v) specialized services related to SIEM installation and operation, including parameterization and configuration of the SIEM as well as deployment and operation of all nodes; and (vi) incorporation of research on emerging and innovative technologies, such as artificial intelligence, cryptography, and threat intelligence, in order to identify threats and optimize responses, as well as incorporation of human resources qualified to operate the new tools, especially project managers specializing in cybersecurity and level 1, 2, and 3 technical specialists.

1.18 **Component 2. Use of advanced technology for human resource development (US$1.9 million).** The following activities will be carried out: (i) implementation of a cyberattack simulation platform with multiple scenarios[43] that can be used by institutions providing cybersecurity training in order to provide advanced specialized training using sector-specific scenarios, including training for the CERT.uy team, educators in academia, and software developers in how to use the platform; and (ii) implementation of an e-learning platform to train cybersecurity professionals in order to provide access to hands-on specialized training and disseminate knowledge on cybersecurity policies, methodologies, and standards promoted by AGESIC.

1.19 **Component 3. Strengthening of the cybersecurity knowledge ecosystem in Uruguay (US$1.85 million).** The following activities will be carried out: (i) support for development of a cybersecurity training curriculum, at both the technical, undergraduate, and graduate levels, which may be used by educational institutions in Uruguay; to this end, an international academic institution renowned in the field of cybersecurity will be commissioned, and cybersecurity educators will be trained

---

39 SIEM is a technological tool that helps integrate functions related to analysis of information on cybersecurity incidents with the management of such incidents, thereby enhancing detection capacity and making response management more efficient. SIEM currently has a capacity of 4,500 events per second and two remote nodes. After project implementation, its capacity will be 20,000 events per second and 17 remote nodes.

40 This is a strategically placed sensor system that enhances the capacity to detect system intrusions.

41 The current regulatory framework does not require the private sector to share information on cyberspace incidents with CERT.uy. A number of companies, however, are already doing so in order to garner support for greater security. Having a mechanism to help share this information in a secure and simple manner will make it easier for more companies to adopt the practice of sharing with CERT.uy. AGESIC plans to bolster its technical support for the private sector and create venues for ongoing dialogue where it can show private-sector experts the forensic analytical work carried out with shared data, which can be used to prevent future incidents. For the purposes of this activity, the private sector consists primarily of companies, with special emphasis on those operating in areas related to critical infrastructure such as energy or health care, as well as in key economic sectors such as finance, agriculture, or tourism.

42 Prevention capacity will be strengthened by updating the SIEM systems (AGESIC is currently using the QRadar tool), installing probes at the most prominent ministries, and incorporating a big data platform.

43 Simulation platforms are commonly used in the most cybersecurity-advanced countries in order to allow professionals to manage cyberattacks and their effects as they actually occur in real life.

to teach the curriculum; (ii) creation of a national network of experts with active international connections, which will be used to promote the inclusion of women in cybersecurity professions;[44] (iii) dissemination activities at the national and international level, including exchange initiatives and promotion and communication events; and (iv) design of a change management strategy.[45]

1.20 **Main beneficiaries.** The main beneficiaries will be the general public and, in particular, the companies whose cyberspace will be more secure. Also, as noted in the results matrix, public entities will directly benefit because their technological infrastructure will be more secure. The five public and private universities that offer training in information systems in Uruguay will benefit because they will add cybersecurity to their course offerings and their instructors will bring their knowledge on cybersecurity up to date. The private sector will benefit from the increased availability of cybersecurity professionals, and Uruguay's ICT business sector will benefit from repositioning Uruguay as an advanced country in terms of cybersecurity, with professionals and services available to meet regional needs. Women, who as a group are underrepresented among cybersecurity professionals and will be targeted in specific actions to encourage them to pursue this profession, will be a collective beneficiary of this operation.

C. Key results indicators

1.21 **Expected outcomes.** The impact of this program will be a more mature capacity for cybersecurity in Uruguay and an increased average cybersecurity maturity level in public entities. The expected outcomes are (i) increased operational capacity to monitor, detect, and respond to cybersecurity incidents; and (ii) increased human capital with training in cybersecurity, including a pro-gender indicator to measure the percentage of women receiving cybersecurity training.

1.22 **Economic evaluation.** The economic evaluation, using a cost-benefit analysis, identified three ways in which the program is expected to generate monetary returns: (i) reduced operational costs in remediating damage caused by cyberattacks on public institutions, through a reduced proportion of highly severe attacks; (ii) reduced economic impact of cyberattacks on public institutions, as a result of greater capacity for prevention and response; and (iii) generation of economic activity through the training of professionals in cybersecurity and subsequent entry into the workforce. The related costs are program expenses, including the Bank's contribution and the local counterpart. Each part of the benefits analysis uses its own assumptions and methodology, as described in the annex. The only shared assumptions are a 12% discount rate, which is the Bank standard, and a 10-year period for calculating benefits. The program is expected to have a high return; even in a conservative scenario, the internal rate of return is projected at 45%, net present value at over US$40 million, and the cost-benefit ratio at 7.07.

---

[44] Women in the network will carry out volunteer activities to promote cybersecurity in secondary schools and universities in order to spark the interest of women and girls in the profession. Initiatives were also carried out to promote cybersecurity as a profession among women, testing the impact of different strategies for attracting them and documenting the effectiveness of each of these. The strategies include the use of economic arguments, job flexibility, and motivation through prestigious women professionals in the field who can serve as a point of reference (see monitoring and evaluation plan, paragraphs 3.17, 3.20, and 3.22 and Table 7).

[45] The strategy will include information, communication, and participation activities to engage public officials and secure their support for the program's cybersecurity activities.

II. FINANCING STRUCTURE AND MAIN RISKS

A. Financing instruments

2.1 This program, with a total cost of US$10 million, is structured as a specific investment loan from the Bank's Ordinary Capital in the amount of US$8 million. The local counterpart will be US$2 million. Table 1 shows the consolidated budget for each component, which is detailed in the itemized budget. The executing agency plans to execute all project activities in four years (see Table 2) on the basis of the following criteria: (i) AGESIC's proven execution capacity in the five loan operations it has previously executed;[46] and (ii) progress on prior consulting work and information gathering efforts for the two most complex procurement processes related to the monitoring system and training simulator.

Table 1. Project Budget (US$)

Components	IDB	Local	Total	%
Component 1. Improving operational capacity and tools for CERT.uy	4,438,525	976,475	5,415,000	54
Component 2. Use of advanced technology for human resource development	1,557,377	342,623	1,900,000	19
Component 3. Strengthening of the cybersecurity knowledge ecosystem in Uruguay	1,516,393	333,607	1,850,000	19
Administration and other contingencies	487,705	347,295	835,000	8
Total	**8,000,000**	**2,000,000**	**10,000,000**	**100**

Table 2. Tentative disbursement schedule (US$)

Source	Year 1	Year 2	Year 3	Year 4	TOTAL
IDB	1,606,595	2,102,496	2,328,589	1,962,319	8,000,000
Local	368,451	477,549	527,290	626,711	2,000,000
%	20	26	28	26	100

B. Environmental and social risks

2.2 In accordance with the Bank's Environment and Safeguards Compliance Policy (document GN-2208-20, Operational Policy OP-703), this has been classified as a category "C" operation. As the program will not finance any components for physical infrastructure, no associated environmental or social risks are foreseen.

C. Fiduciary risks

2.3 AGESIC has an extensive and positive track record as an executing agency for Bank operations. No fiduciary risks were identified in the risks workshop. In accordance with the fiduciary agreements and requirements (Annex III), fiduciary risk is deemed to be low in view of AGESIC's track record as an executing agency and the successive external audit reports in which the Office of the Auditor General has issued favorable opinions on the projects it has administered.

D. Other risks and key considerations

2.4 The following risks have been identified:

[46] AGESIC has been executing the following operations as planned: e-Government Management Project in the Health Sector (loan 3007/OC-UR); Program for Improvement of Public Services and State-Citizen Interaction (loan 3625/OC-UR); e-Government Management Project in the Health Sector II (loan 4300/OC-UR); and Program to Support e-Government Management in Uruguay I and II (loans 1970/OC-UR and 2591/OC-UR).

a. **Governance.** Two medium-level risks were identified: (i) delays in institutional agreements, which could have an adverse effect on implementation of Components 1 and 3 since they largely call for active participation by entities external to AGESIC. To mitigate this risk, an advisory committee consisting of all participating academic institutions will be created and consulted on the most important decisions related to project execution, and work plans will be developed; and (ii) resistance to change: although AGESIC has 10 years of experience carrying out technological projects for the central government, this is its first time implementing an activity of this nature that will cede a significant amount of control over ministries' technological infrastructure to a central entity. This might generate resistance among sector and technology managers in these ministries. To mitigate this resistance, the project includes change management activities emphasizing communication and participation, as well as significant training efforts.

b. **Public management and governance.** A change in administration was identified as a medium risk that might adversely affect the status of cybersecurity as a priority of the public-sector agenda. Despite the upcoming elections in October 2019, the digital agenda is a State policy and multiple political parties have spoken favorably of the work of AGESIC. To mitigate this risk, dialogue will be maintained with various political forces on the importance of protecting Uruguay's cyberspace, and the private sector will be engaged in project design and execution.

c. **Fiscal sustainability**. Fiscal constraints have been identified as a medium risk that could limit the availability of counterpart resources and fiscal room for execution. Uruguay is experiencing fiscal constraints that are forcing the government to contain spending and public investment, which may have a doubly adverse effect on project execution, both for counterpart resources and the fiscal room for execution of Bank-financed components. To mitigate this risk, AGESIC will submit to the Ministry of Finance, which is responsible for budgetary allocations, a detailed description of the economic importance of this operation in order to ensure that it understands the extent of the potential economic impact of an insecure cyberspace.

2.5 **Intellectual property and sustainability.** About half of the investment included in this project is targeted to the purchase of technological goods and services. AGESIC has extensive experience in purchasing and managing technology. It is currently managing more than 60 applications of both open-source and proprietary software, and it has technology and operations units with ample experience in operating technological solutions. Some of these applications require contractual relationships with renowned vendors in the sector.[47] It provides related services in its cloud-based architecture with more than 20 applications to numerous government agencies. AGESIC also has a policy on public software[48] and its reuse in public administration, providing more than 25 applications for use both by the Uruguayan government and the governments of other countries in Latin America and the Caribbean through the GNU GPL 3 license.[49] AGESIC's 12 years of

[47] AGESIC currently has contractual relationships with Microsoft, IBM, Oracle, and other renowned ICT companies.

[48] Uruguayan public software.

[49] Uruguay has been a leader and active participant in the public software initiative of Latin America and the Caribbean, which has been financed as a Bank regional public good. See here.

experience at the helm of Uruguay's digital agenda have helped it develop a technology management policy that includes open-source and proprietary software, provides budgetary resources for regular renewal of applications and equipment, and includes a qualified team[50] to manage it in a way consistent with its position as the most digitized country in the region. The digital agenda has also been established as a policy of the country, as evidenced by the fact that Uruguay is currently implementing the third version of its digital agenda in the past 10 years.[51] Technical and financial sustainability of technological solutions is based on the stability of the digital agenda that AGESIC has been managing for 12 years, the quality of services provided by AGESIC to other government institutions, AGESIC's effectiveness in reporting outcomes, and private-sector participation.

III. Implementation and Management Plan

A. Summary of implementation arrangements

3.1 **Execution mechanism.** The borrower will be the Eastern Republic of Uruguay. The executing agency will be the Eastern Republic of Uruguay through AGESIC, which will be responsible to the Bank for execution and will maintain the direct relationship with the Bank. The program is aligned with AGESIC's legal mandate and current administrative and operational structure.[52] Applicable laws and regulations make AGESIC responsible for all matters related to implementation of specific plans and projects for e-government and information security.

3.2 **Internal coordination mechanism.** The program will be led by AGESIC's Office of the Director of Information Security. The director will serve as general program coordinator, will be responsible for directing the program, and will hold strategic and planning meetings with the Bank. In fulfilling these duties, the general coordinator will have the following support: (i) an operations coordinator, who will implement the annual work plan, request disbursements, propose procurement items, report on the use of resources, and submit the annual work plans, procurement plans, and progress reports to the Bank; (ii) a senior consultant for administration and finance; and (iii) a senior procurement consultant.

3.3 **External coordination mechanism.** To facilitate dialogue and coordination with the leading actors related to this operation, AGESIC will form an advisory committee consisting of representatives of the six universities that offer training in information systems in Uruguay.[53] Public and private institutions will gradually be added to this advisory committee on the basis of needs identified by the committee in the course of project activities.

---

50 AGESIC has more than 300 staff members, approximately one third of whom have training in information systems.

51 Digital Uruguay: 10 years of digital policy.

52 As noted in footnote 3, AGESIC was created by Law 17.930 (Article 72) of 19 December 2005 as the entity in charge of e-government. As noted in footnote 4, Law 18.719 of 27 December 2010 created the Office of the Director of Information Security as part of AGESIC, for the purpose of protecting the public sector's cyberspace. The laws and regulations associated with AGESIC may be found here.

53 University of the Republic, Technological University (UTEC), ORT University Uruguay, Catholic University, and University of Montevideo.

3.4 For working relationships with the public entities that will benefit from this operation, AGESIC has signed framework agreements[54] with all public entities as part of the e-government work agenda. Under these framework agreements, AGESIC and each public entity will sign specific agreements to incorporate cybersecurity activities into the work plan. For relations with the academic institutions participating in the program, AGESIC will establish a standard participation agreement stating the benefits that the institutions will receive and the obligations they must assume in order to participate.

3.5 **Special contractual conditions precedent to the first disbursement. As a special contractual condition precedent to the first disbursement, the borrower, acting on its own or through the executing agency, will submit to the Bank evidence that (i) AGESIC's information security director has been designated general program coordinator, and (ii) the program's operations coordinator has been appointed.** These two roles are critical in order to review operational planning and begin implementation.

3.6 The fiduciary agreements and requirements set forth the financial management and planning framework, as well as the program's framework for procurement supervision and execution.

3.7 Program activities will be scheduled in accordance with the multiyear execution plan (which details program execution as a whole). The annual review of this plan will be set forth in the annual work plan. The multiyear execution plan will be revised each year in view of actual progress. The annual reviews of the multiyear execution plan and annual work plan will be submitted to the Bank for approval.

3.8 **Procurement of works, goods, and nonconsulting and consulting services.** Procurement activities financed in full or in part by the Bank will be carried out in accordance with Policies for the Procurement of Goods and Works Financed by the Inter-American Development Bank (document GN-2349-9) and the Policies for the Selection and Contracting of Consultants Financed by the Inter-American Development Bank (document GN-2350-9).

3.9 **Single-source selection.** The program will commission the individual consultants identified in the procurement plan. Due to the need to maintain technical continuity during the project, the procurement plan calls for using the same individual consultants who were hired with the proceeds from loans 3007/OC-UR and 3625/OC-UR. These consultants will continue to provide services for this operation, in accordance with Section V, paragraph 5.4(a), of document GN-2350-9, with the understanding that the contractual conditions for the identified consultants remain the same and the performance for each consultant will be evaluated on an annual basis. These consultants will perform technical duties related to CERT.uy and the security operation center, as well as technical coordination for the project, budgetary and financial analysis, monitoring, financial and accounting management, and procurement management. The contracts will

[54] AGESIC has signed agreements and work plans with the various State entities since 2009 to develop and implement 90 e-government solutions and applications, with financing from loans 1970/OC-UR and 2591/OC-UR using funds awarded by competition. The framework agreements identify as a general objective the interest of both institutions in working together to carry out activities related to the digital agenda. The specific agreements detail specific activities to be carried out under the framework agreement, identify the duties of each party, and regulate the transfer of knowledge and training. Examples of both agreements may be found here.

be for up to US$1,361,000 for the four years of the program.[55] The procurement plan details procurement activities to be carried out and the Bank's procedures for reviewing them. Consulting and nonconsulting services will be procured using the United Nations Office for Project Services, the United Nations Development Programme, or the Julio Ricaldoni Foundation, and, in accordance with the agreements signed by AGESIC, will be subject to Bank policies.

3.10 **Disbursements.** The main disbursement modality will be "advances" based on actual liquidity needs. Preferrably, the advances will be made every six months, once at least 70% of the previous advance has been justified.[56] The required documentation to be submitted will be the expense forms and the financial planning spreadsheet. The documentation will be reviewed ex post.

3.11 **Audits.** The executing agency will submit the program's audited financial statements to the Bank on an annual basis during the project, in accordance with the financial management guidelines (document OP-273-6), within 120 days after the end of the fiscal year. The program's final audited financial statements will be submitted within 120 days after the original disbursement period, or any extensions thereto, elapses. These financial statements may be audited by the Office of the Auditor General or an auditing firm.

B. Summary of arrangements for monitoring results

3.12 **Monitoring by the executing agency.** The following documents, *inter alia*, will be used: (i) results matrix, (ii) multiyear execution plan; (iii) annual work plan; (iv) monitoring and evaluation plan; (v) procurement plan; (vi) risk matrices; (vii) disbursement plan; and (viii) program monitoring reports. The executing agency will submit semiannual progress reports to the Bank for review.

3.13 **Monitoring by the Bank.** Oversight missions or inspection visits will be carried out depending on the importance and complexity of execution, in accordance with the timetable set forth in the multiyear execution plan. For monitoring purposes, the Bank will use the program monitoring report system, which is based on estimates of disbursements and fulfillment of physical targets and outcomes.

3.14 A joint meeting with the executing agency and the Bank will be held at least once per year, to discuss, *inter alia*: (i) progress on activities identified in the annual work plan; (ii) the fulfillment of indicators set forth in the results matrix; (iii) the annual work plan for the following year; and (iv) the procurement plan for the next 18 months and possible changes to budgetary allocations for each component.

3.15 **Evaluation.** The results matrix and the monitoring and evaluation plan will be used to evaluate the program. Given the innovative nature of this operation, it is expected to yield a number of evaluations and knowledge products for the purpose of generating evidence and lessons learned on the cost-effectiveness of investing in cybersecurity. A midterm evaluation, a final evaluation, an impact evaluation, and a methodology for measuring the economic impact of cyberattacks in Uruguay are expected. The midterm evaluation will be conducted after 24 months have

---

[55] These consultants were initially selected on the basis of a comparison of qualifications, with the Bank's prior no objection in each instance.

[56] Pursuant to the financial management guidelines (document OP-273-6), this percentage is justified because central government entities (of which AGESIC is one) must have the financing in Central Bank accounts to undertake new obligations. Moreover, the processing of payments requires the preventive intervention of the Office of the Auditor General (TCR) and the General Accounting Office (CGN).

elapsed since the loan contract took effect or when 50% of the total loan amount has been committed, whichever occurs first. The main objectives of this evaluation are to review progress on all activities programmed by that time, any possible deviations, the causes of such deviations, and proposed corrective measures, in addition to verifying the intermediate outputs, the emergence of risks identified in the corresponding matrix, and measures to mitigate these risks. The final evaluation will be conducted when the original disbursement period, or any extensions thereto, has elapsed, or when 90% of the loan amount has been committed, whichever occurs first; and its objectives are to verify progress in fulfilling the targets for each expected outcome and producing the outputs for each component.

3.16 **Impact evaluation.** An impact evaluation will be carried out using a controlled, randomized study to answer the following questions: (i) Is there an effective, cost-efficient way to increase demand for cybersecurity courses? (ii) What is the most effective and cost-efficient way to close the gender gap in cybersecurity? To this end, the evaluation will be based on the activities of Component 3, which are aligned with the generation of human capital and closure of the gender gap among cybersecurity professionals, and the operation is expected to yield causal evidence for public policy recommendations on programs to promote demand for ICT courses and professional career programs.

3.17 **Estimation of economic impact of cyberattacks.** The objective of this evaluation document will be to generate knowledge on the economic impact of cyberattacks and the economic benefits of investing in cyberspace protection. To this end, a methodology that includes a cyberattack rating system and an incident response protocol will be developed in agreement with AGESIC. This methodology will be implemented on a pilot basis in a number of public entities in Uruguay, which is expected to yield a better understanding of the magnitude and likelihood of risks that are avoided by implementing public policy on cybersecurity.

Development Effectiveness Matrix		
Summary		
I. Corporate and Country Priorities		
1. IDB Development Objectives	Yes	
Development Challenges & Cross-cutting Themes	-Social Inclusion and Equality -Productivity and Innovation -Gender Equality and Diversity -Institutional Capacity and the Rule of Law	
Country Development Results Indicators	-Government agencies benefited by projects that strengthen technological and managerial tools to improve public service delivery (#)* -Teachers trained (#)* -Countries that use fiduciary country systems (#)* -Crime information systems strengthened (#)* -Projects supporting innovation ecosystems (#)*	
2. Country Development Objectives	Yes	
Country Strategy Results Matrix	GN-2836	To strengthen public management systems
Country Program Results Matrix	GN-2948	The intervention is included in the 2019 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	8.2	
3.1 Program Diagnosis	1.8	
3.2 Proposed Interventions or Solutions	4.0	
3.3 Results Matrix Quality	2.4	
4. Ex ante Economic Analysis	9.0	
4.1 Program has an ERR/NPV, or key outcomes identified for CEA	3.0	
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	8.5	
5.1 Monitoring Mechanisms	2.2	
5.2 Evaluation Plan	6.4	
III. Risks & Mitigation Monitoring Matrix		
Overall risks rate = magnitude of risks*likelihood	Medium	
Identified risks have been rated for magnitude and likelihood	Yes	
Mitigation measures have been identified for major risks	Yes	
Mitigation measures have indicators for tracking their implementation	Yes	
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, Treasury, Accounting and Reporting. 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		

Note: (*) Indicates contribution to the corresponding CRF's Country Development Results Indicator.

The main goal of the operation is to strengthen the capacity of the country to protect its digital environment by improving the prevention, detection, and response to cyber-attacks. To achieve this, the proposal defines two specific areas of intervention. The first area proposes a technological investment for improving the capacity of monitoring incidents through a Security Information Event Management. The second area is focused on a human capital formation through the creation of courses, curricula design, and teachers training in cybersecurity and the implementation of an E-learning platform for students and public servants.

The project proposal diagnosis describes that Uruguay has a high digital government development. However, the country has not the same strength in the protection of the digital environment; for this reason, digital risks management is an important challenge for Uruguay and the region. In the same way, diagnosis identifies a critical skills gap. Currently, labor market demands at least 200 cybersecurity professionals and the universities only offer a graduate course. The solutions are aligned to the problems. There is no evidence on effectiveness for some proposed solutions in the country. Some outputs indicators are not SMART.

The economic analysis provides a quantification of some economic benefits. It quantifies benefits associated with: (i) the reduction of costs in remediation of the damages caused by cyber-attacks; (ii) the decrease in the economic impact caused by cyber-attacks to public institutions; and (iii) the generation of economic activity through the training of professionals in cybersecurity and its subsequent insertion into the labor market. The assumptions on the magnitude of the expected benefits are based on international experiences such as the United States and Estonia. The costs include maintenance and investments associated with the loan. The analysis concludes the Project has a net present value of US$40 million.

The Project presents a robust monitoring and evaluation plan, it considers two different evaluations, the first one, is an ex-post economic analysis it will include a proposal of methodology for measuring the economic impacts of cyber-attacks in Uruguay and the second one, is an impact evaluation for measuring the effects of the component three on the creation of human capital, employment and the inclusion of women in this ICT area.

RESULTS MATRIX

Project objective:	The program will help strengthen Uruguay's capacity to protect its cyberspace through improved prevention, detection, and response to cyberattacks.

EXPECTED IMPACT

Indicators	Unit of measure	Baseline	Base year	Year 1	Year 2	Year 3	Year 4	Final target	Means of verification	Comments
IMPACT #1: Increased cybersecurity capacity maturity										
National cybersecurity capacity maturity	Score	149	2016				165	165	OAS/IDB report	This indicator reflects national capacities; maximum score is 245. A document titled "Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States" examines these four countries using the maturity model selected to measure the impact of this operation. The document shows that investments by these countries in strengthening their technological capacity and developing their human resources have helped position them as advanced countries in terms of cyberspace security.

Indicators	Unit of measure	Baseline	Base year	Year 1	Year 2	Year 3	Year 4	Final target	Means of verification	Comments
										In fact, 5 of the 49 indicators in this maturity model are related to education, and 9 are related to strengthening technological capacities addressed in this program. The educational efforts in each country are described on the following pages: Estonia, pp. 15-16; Israel, pp. 27-28; South Korea, pp. 38-39; United States; pp. 48-49.
Average cybersecurity maturity level in public entities	Score	1.5	2018				2.5	2.5	External audit of cybersecurity framework	This indicator reflects the capacities of the 10 most digitized public entities in Uruguay; maximum score is 4.

EXPECTED OUTCOMES

Indicators	Unit of measure	Baseline	Base year	Year 1	Year 2	Year 3	Year 4	Final target	Means of verification	Comments
OUTCOME #1: Enhanced operational capacity to monitor, detect, and respond to cybersecurity incidents										
Number of public entities monitored through the SOC	Number of ministries	2	2018	2	5	11	17	17	Annual report from the cybersecurity agency	This indicator is not per year, but rather the cumulative number of entities.

Indicators	Unit of measure	Baseline	Base year	Year 1	Year 2	Year 3	Year 4	Final target	Means of verification	Comments
Number of cyberspace incidents detected each year	Number of incidents	2,043	2018	2,250	3,267	6,889	10,000	10,000	Annual report from cybersecurity agency	An incident is defined as “a violation or imminent threat of a violation of an implied or express policy on information security, and an event that compromises the security of a system (confidentiality, integrity, or availability) (Decree 4541/009 of 28 September 2009, Article 3). An incident report by the Spanish government’s National Cryptological Center found that the more the government invested in its monitoring capacity, the more incidents of all levels of dangerousness were detected; see p. 41.
Percentage of high-impact cyberspace incidents	Percentage	2.1	2018	2.25	1.84	1.51	1.24	1	Annual report from cybersecurity agency	According to AGESIC’s incident rating procedure document, high-impact incidents are those that require more than 640 hours of work by a senior expert to be resolved.

Indicators	Unit of measure	Baseline	Base year	Year 1	Year 2	Year 3	Year 4	Final target	Means of verification	Comments
OUTCOME #2: Increased human capital trained in cybersecurity										
Number of people who have received at least 40 hours of cybersecurity training per year	Number of people	50	2018	0	0	150	150	350	Student records from institutions of tertiary education	This indicator measures the number of persons receiving cybersecurity training each year.
Women receiving at least 40 hours of cybersecurity training per year	Percentage	0	2018	0	0	15	20	25	Student records from institutions of tertiary education	Pro-gender This indicator measures the number of persons receiving cybersecurity training each year.

OUTPUTS

Indicators	Unit of measure	Baseline	Base year	Year 1	Year 2	Year 3	Year 4	Final target	Means of verification	Comments
Component 1: Improving operational capacity and tools for CERT.uy										
1.1 Up-to-date QRadar license	License	0	2018	1	0	0	0	1	QRadar licensing agreement	
1.2 NIGPS intrusion detection system up and running	System	0	2018	0	0	1	0	1	AGESIC program reports	
1.3 Big data platform up and running	Platform	0	2018	0	0	1	0	1	AGESIC program reports	
1.4 CERT laboratory installed	Laboratory	0	2018	0	0	1	0	1	AGESIC program reports	This output includes forensics, proof of concept, sensor development, and incident management.

Indicators	Unit of measure	Baseline	Base year	Year 1	Year 2	Year 3	Year 4	Final target	Means of verification	Comments
1.5 SIEM system implemented	System	0	2018	0	1	0	0	1	SIEM report prepared by AGESIC	
1.6 CERT equipped and up and running	System	0	2018	0	0	1	0	1	AGESIC program reports	A system is a set of technologies, methods, and people qualified to manage the cyberspace incidents that are fielded by CERT.
Component 2: Use of advanced technology for human resource development										
2.1 Cyberattack simulation platform up and running	Platform	0	2018	1	0	0	0	1	AGESIC program reports	For the platform to be up and running, the software must be installed and the CERT team trained.
2.2 E-learning platform installed	Platform	0	2018	0	0	1	0	1	AGESIC program reports	
Component 3: Strengthening of the cybersecurity knowledge ecosystem in Uruguay										
3.1.a Cybersecurity training curricula designed	Curriculum	0	2018	0	0	1	0	1	AGESIC program reports	Curriculum includes training programs for different educational levels and job descriptions, as well as content.
3.1.b Instructors trained in the new cybersecurity training curriculum.	Instructors	0	2018	0	0	110	110	220	AGESIC program reports	Each year: 10 instructors from each of the 5 higher education institutions, plus 3 instructors from each of the country's 19 departments, plus 3 people from AGESIC.

Indicators	Unit of measure	Baseline	Base year	Year 1	Year 2	Year 3	Year 4	Final target	Means of verification	Comments
3.2 Network of experts up and running	Network of experts	0	2018	1	0	0	0	1	AGESIC program reports	
3.3 National and international dissemination plan implemented	Plan	0	2018	0	1	0	0	1	AGESIC program reports	
3.4 Change management strategy designed	Document	0	2018	1	0	0	0	1	Change management strategy document	

FIDUCIARY AGREEMENTS AND REQUIREMENTS

Country:	Eastern Republic of Uruguay
Project number:	UR-L1152
Name:	Strengthening Cybersecurity in Uruguay
Executing agency:	Eastern Republic of Uruguay, through the Agency for the Development of e-Government Management and the Information and Knowledge Society (AGESIC)
Prepared by:	Abel Cuba and Emilie Chapuis (FMP/CUR)

I. EXECUTIVE SUMMARY

1.1 This operation is in the amount of US$10 million, of which US$8 million will be financed by the Bank and US$2 million by the local counterpart. The borrower is the Eastern Republic of Uruguay, and the executing agency is AGESIC. AGESIC's organizational and administrative structure will be in charge of executing the operation's resources and managing the timely financing of local counterpart contributions. The objective of the loan operation is to help strengthen Uruguay's capacity to protect its cyberspace through improved prevention, detection, and response to cyberattacks. The operation has three components: (i) Component 1, improving operational capacity and tools for CERT.uy (US$5,415,000); (ii) Component 2, use of advanced technology for human resource development (US$1.9 million, IDB); and (iii) Component 3, strengthening of the cybersecurity knowledge ecosystem in Uruguay (US$1.85 million).

1.2 The fiduciary agreements and requirements for this program are based on AGESIC's track record as executing agency of loans 1970/OC-UR, 2591/OC-UR, 3007/OC-UR, 3625/OC-UR, and 4300/OC-UR.

II. THE EXECUTING AGENCY'S FIDUCIARY CONTEXT

2.1 AGESIC is a model entity in the public administration. Its effective execution capacity in all areas has been demonstrated in the four previous projects for which it has served as executing agency. AGESIC has solid prior experience in procurement under Bank policies. Its processes and general internal control environment are deemed suitable overall.

2.2 The following country systems or their equivalents will be used on this operation:

a. **Budget.** The country budgeting system will be used. Proceeds from this operation will be recorded in the new Five-year Budget Act 2020-2025. AGESIC is expected to have the same budgetary base as in 2019, which is sufficient for the overall program and includes proceeds from the loan and the local counterpart.

b. **Treasury.** To administer the program's resources, a special account will be opened in the program's name at the Central Bank of Uruguay as part of AGESIC's single national account.

c. **Accounting and financial reports.** The executing agency will use the International Projects System in coordination with the General Accounting Office (CGN), which administers the SIIF.

d. **Internal control.** AGESIC maintains a system of internal controls to manage its operations. The effectiveness of this system is evaluated when the Office of the Auditor General (TCR) audits the expenses and payments and when the designated accountants perform the appropriate checks of legal compliance.

e. **External control.** The Office of the Auditor General has been responsible in recent years for the annual audits of Bank-financed programs; its work is framed by international auditing standards issued by the International Organization of Supreme Audit Institutions.

III. Fiduciary Risk Evaluation and Mitigation Actions

3.1 As noted at the risk workshop for this program, and in view of the executing agency's track record in execution, fiduciary risk has been evaluated as low, based on the following:

a. The fact that AGESIC, as an entity of the central government, is governed by clear procedures set forth in laws and regulations enforced under strict internal and external controls as provided by law, which reduces the risks related to financial management.

b. The track record of the executing agency, which has extensive experience in fiduciary and procurement management under Bank policies, as well financial management, combined with the fact that this program will be administered by the same team that is in charge of the loan operations now in execution.

c. The specific experience of AGESIC in purchasing technology in general and cybersecurity-related applications in particular, considering that AGESIC already has a computer emergency response team (CERT) and a security operation center (SOC) up and running.

3.2 In view of the foregoing, the program should only require significant mitigating measures to be identified over the course of the loan operation through the Bank's own oversight activities or the audits required as part of this operation.

IV. Considerations for the Special Provisions of Contracts

4.1 The following considerations will be taken into account in special provisions:

a. **Exchange rate.** For accounting in U.S. dollars, the exchange rate as of the effective date of payment by AGESIC to contractors will be used, and the conversion method will be as specific in Article 4.10(b)(ii) of the General Conditions of the loan contract.

b. **Audited financial statements.** These statements will be submitted within 120 days of the end of each fiscal year. The audit may be conducted by the

Office of the Auditor General or an auditing firm. If an auditing firm is used, the terms of reference will be agreed upon with the Bank, and the auditing firm must be acceptable to the Bank. The submittal deadline will be as specified in Article 7.03 of the General Conditions of the loan contract. The last set of audited financial statements will be submitted to the Bank within 120 days after the original disbursement period, or any extensions thereto, elapses.

V. AGREEMENTS AND REQUIREMENTS FOR PROCUREMENT EXECUTION

A. Procurement execution

5.1 The Bank's procurement policies set forth in documents GN-2349-9 (Policies for procurement of works and goods) and GN-2350-9 (Policies for selection and procurement of consulting services) will apply to all procurement activities for this operation. All procurement activities will be included in the procurement plan, which will cover an initial period of at least 18 months and will subsequently be updated on an annual basis. The procurement plan will be registered, approved, and posted on the procurement plan e-system: www.iniciativasepa.org before commencing any procurement. Once registered, the procurement plan will be updated annually or as necessary whenever substantial changes are made to the original plan.

5.2 The project's sector specialist is responsible for the relevance of expenditures—i.e. terms of reference, technical specifications, and budget—and prior no objection is required before commencing procurement, in accordance with the project team leader's operational criteria.

5.3 Procurement items for small amounts will be carried out in accordance with Bank policies and the ex post oversight guide for small purchases, developed for AGESIC's operations on the basis of its experience in managing procurement processes under Bank policies.

5.4 No exceptions to Bank policies and no retroactive financing are expected. In accordance with paragraph 1.9 of document GN-2349-9 and paragraph 1.12 of document GN-2350-9, the executing agency may carry out the procurement process before the loan is approved. According to the Bank's procurement policies, the borrower "undertakes such advance contracting at its own risk, and any concurrence by the Bank with the procedures, documentation, or proposal for award does not commit the Bank to make a loan for the project in question." An advance procurement process may be deemed eligible if it is duly registered and documented in the executing agency's systems and if it has been carried out in accordance with Bank policies or using similar procedures consistent with the applicable provisions of Bank policies. As AGESIC has noted, no retroactive financing is expected.

5.5 **Procurement of works, goods, and nonconsulting services.** Contracts for works, goods, and nonconsulting services[1] under the project and subject to international competitive bidding will be carried out using the standard bidding documents issued by the Bank. Procurement processes subject to national

[1] Policies for the Procurement of Goods and Works Financed by the Inter-American Development Bank (document GN-2349-9), paragraph 1.1: Nonconsulting services are treated as goods.

competitive bidding will be carried out using national bidding documents that are satisfactory to the Bank. The project's sector specialist will review the technical specifications for procurement processes while these processes are being prepared.

5.6 According to the procurement plan for this operation, no works are expected. Goods estimated at US$3,315,000 and nonconsulting services estimated at US$440,000 will be procured. These procurement processes will be subject to the provisions of document GN-2349-9 (Policies for the procurement of works and goods).

5.7 **Selection and contracting of consultants.** Consulting services under the project will be procured using the standard request for proposals issued by the Bank for all international bidding processes or a request form satisfactory to the Bank for all national bidding processes. The project's sector specialist will review the terms of reference for the procurement of consulting services.

a. **Processes for procurement of the services of consulting firms** will be competitive processes carried out in accordance with the applicable provisions of document GN-2350-9 (policies for the procurement of consulting services).

b. **Selection of individual consultants.** The program will commission the individual consultants identified in the procurement plan. Due to the need to maintain technical continuity during the project, the procurement plan calls for single-source selection of individual consultants who were commissioned with the proceeds from loans 3625/OC-UR and 2792/OC-UR. These consultants will continue to provide services for this operation, in accordance with Section V, paragraph 5.4(a), of document GN-2350-9, with the understanding that the contractual conditions for the identified consultants remain the same and the performance for each consultant will be evaluated on an annual basis. These consultants will perform technical duties related to CERT.uy and the security operation center, as well as technical coordination for the project, budgetary and financial analysis, monitoring, financial and accounting management, and procurement management. The contracts will be for up to approximately US$1,361,000 for the four years of the program.[2] The procurement plan details procurement activities to be carried out and the Bank's procedures for reviewing them. Consulting and nonconsulting services will be procured using the United Nations Office for Project Services, the United Nations Development Programme, or the Julio Ricaldoni Foundation, and, in accordance with the agreements signed by AGESIC, will be subject to Bank policies.

[2] These consultants were initially selected on the basis of a comparison of qualifications, with the Bank's prior no objection in each instance.

Table 1. Thresholds for international bidding and international short list (thousands of US$)

Works			Goods and services			Consulting services	
International competitive bidding	National competitive bidding	Price comparison	International competitive bidding	National competitive bidding	Price comparison	International advertising for consulting services	Shortlist 100% national
≥ 3,000,000	≤ 3,000,000 ≥ 250,000	≤ 100,000	≥ 250,000	≤ 250,000 ≥ 50,000	≤ 50,000	≥ 200,000	≤ 200,000

B. Main procurement items

5.8 The main procurement items for this operation will be divided up as set forth in the following table. All other planned activities are set forth in the procurement plan, which is one of the links to the main document.

Table 2. Goods

Process number	Associated activity	Executing unit	Activity	Additional description	Procurement method (select one)	Estimated amount (US$)
B1	1.1.1	AGESIC	ICB_1 – Procurement of QRadar licenses	IBM licenses	ICB	915,000
B2	1.2.1	AGESIC	ICB_2 – Procurement of NGIPS (virtual and physical), HW servers, and VMWare		ICB	500,000
B4	2.1.1	AGESIC	ICB_3 – Procurement of simulation platform	Cyberattack simulation platform with multiple scenarios up and running	ICB	1,800,000

Table 3. Consulting firms

Process number	Associated activity	Executing unit	Activity	Procurement method (select one)	Estimated amount (US$)
CF4	1.5.1	AGESIC	QCBS_4: Contracting of consulting firm to provide operation and maintenance services	QCBS	400,000
CF5	1.5.2	AGESIC	QCBS _5: Contracting of consulting firm to provide advisory and deployment services	QCBS	1,600,000
CF7	3.1.1	AGESIC	QCBS _7: Contracting of consulting firm to develop curricula in cybersecurity and train-the-trainers	QCBS	1,350,000

C. Procurement supervision

5.9 In view of the executing agency's experience and track record, procurement activities will be subject to ex post review, except in processes using ICB or an international shortlist and whenever ex ante review is justified in accordance with the procurement plan. Ex post reviews will be carried out every 12 months in accordance with the project's supervision plan. The following table lists the relevant thresholds.[3]

Table 4. Thresholds for ex post review (US$)

Works	Goods	Consulting services
<3,000,000	<250,000	<200,000

D. Records and files

5.10 Project reports will be prepared and filed using the forms or procedures that have been agreed upon with the Bank for prior operations and which are consistent with the Bank's applicable policy requirements. Each file will be self-contained and will include all documentation related to procurement processes, including the procurement plan, bidding documents and all related information (specific procurement notices, evaluation and award recommendation reports, etc.), and contract management documents.

VI. Financial Management Agreements and Requirements

6.1 **Programming and budget.** AGESIC, which is part of the Office of the President, submits its proposed budget to the Ministry of Finance, which considers it as part of the proposed consolidated national budget and then submits it for consideration to the Office of the President, which in turn sends it to the legislative branch for consideration and approval.

6.2 AGESIC will program and prepare the budget on the basis of the agreed-upon annual work plan, which is based on the program execution plan. The project's budget will be managed using the country system (financial information system, SIIF). The executing agency will manage local counterpart resources in a timely manner for the purposes of pari passu compliance.

6.3 **Accounting and information systems.** The project will maintain the program's accounting records in the country system (SIIF), which will be used to manage the budgetary allocations approved in the five-year budget law for the project. The relevant procedures established by the General Accounting Office (CGN) will be followed in processing project-related commitments and payments.

6.4 The project's financial statements will be issued on a regular basis in accordance with generally accepted accounting standards, and these statements will be audited on an annual basis. The following statements will be issued: (i) statement of cash received and disbursements made; and (ii) statement of cumulative

[3] The threshold amounts for ex post review are based on the executing agency's fiduciary capacity and may be modified by the Bank in the event of any changes to such capacity.

investments. These statements will be accompanied by the corresponding explanatory notes.

6.5 **Disbursements and cash flow.** Project resources will be managed using the Single National Account. To this end, the Office of the Treasury, at the request of the project execution unit, will open a special account at the Central Bank of Uruguay. Funds disbursed by the Bank will be deposited into this account, but because it is only a nominal account (unable to make payments), a project-specific bank account will be opened at the State commercial bank (Banco de la República Oriental del Uruguay-BROU) for the purpose of making payments.

6.6 Disbursements will be made in the form of advance payments based on actual liquidity needs supported by appropriate financial and disbursement projections. These advance payments will be made preferably on a semiannual basis once at least 70% of the amount advanced has been accounted for.[4] Financial planning and fund reconciliation documents will be attached to each disbursement request. The e-disbursement system will be used to process disbursement requests. The exchange rate in effect on the payment date will be used to convert payments in local currency to the loan currency.

6.7 **Internal control and internal auditing.** The internal control system is based on the country system in accordance with current laws and regulations. According to the accounting and financial management provisions known as TOCAF, the Office of the Auditor General will preemptively audit all project-related expenditures. Under Uruguayan law, AGESIC is under the control of the National Internal Audit Office (AIN). Efforts will be coordinated with the AIN if the program is subject to review.

6.8 As for institutional controls, the executing agency will uphold the conditions set forth for Bank-financed projects currently in execution, while ensuring the continued presence and participation of fiduciaries on such projects.

6.9 **External control and reports.** To fulfill the Bank's contractual requirements, the program's annual audits may be performed by the Office of the Auditor General or a Bank-eligible independent auditing firm. If the audits are performed by the Office of the Auditor General, the relationship with AGESIC will be set forth in a service agreement that will include the terms of reference agreed upon with the Bank.

6.10 The financial audit reports will be submitted on an annual basis during the disbursement phase, up until 30 April and 120 days after the date of the last disbursement, in accordance with international auditing standards. The hiring of the auditing firm, as well as the related terms of reference, will be in accordance with the financial management guidelines set forth in document OP-273-6. The costs of the audit may be financed with proceeds from the loan.

6.11 **Financial supervision plan.** The financial supervision plan addresses the following topics:

---

[4] Pursuant to the financial management guidelines (document OP-273-6), this percentage is justified because central government entities (of which AGESIC is one) must have the financing in Central Bank accounts to undertake new obligations. Moreover, the processing of payments requires the preventive intervention of the Office of the Auditor General (TCR) and the General Accounting Office (CGN).

a. Participation in the startup workshop held by the project team, including a presentation of the most relevant fiduciary considerations.

b. Review of the annual work plan and initial financial plan prepared by the project execution unit as a backup to the first advance payment to be requested once the program becomes eligible.

c. Financial site visits may be carried out during the project on the basis of an evaluation of portfolio risks. These visits will evaluate the main financial and control aspects of the project, as well as file management. Disbursements will be reviewed on an ex post basis.

6.12 **Execution mechanism.** The borrower will be the Eastern Republic of Uruguay. The executing agency will be the Eastern Republic of Uruguay acting through AGESIC, which will be responsible to the Bank for execution and will maintain the direct relationship with the Bank. The program is aligned with AGESIC's legal mandate and current administrative and operational structure.[5] Applicable laws and regulations make AGESIC responsible for all matters related to implementation of specific plans and projects for e-government and information security.

[5] As noted in footnote 2, AGESIC was created by Law 17.930 (Article 72) of 19 December 2005 as the entity in charge of e-government. As noted in footnote 3, Law 18.719 of 27 December 2010 created the Office of the Director of Information Security as part of AGESIC, for the purpose of protecting the public sector's cyberspace. The laws and regulations associated with AGESIC may be found here.

DOCUMENT OF THE INTER-AMERICAN DEVELOPMENT BANK

PROPOSED RESOLUTION DE-___/19

Uruguay. Loan ____/OC-UR to the Eastern Republic of Uruguay
Strengthening Cybersecurity in Uruguay

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 Eastern Republic of Uruguay, as borrower, for the purpose of granting it a financing aimed at cooperating in the execution of the program Strengthening Cybersecurity in Uruguay. Such financing will be in the amount of up to US$8,000,000 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 ___ _____ 2019)

LEG/SGO/CSC/EZSHARE-1028536987-10988
UR-L1152