TERMS OF REFERENCE

Energy Division – Data Scientist Consultant

Location

The IDB Group is a community of diverse, versatile, and passionate people who come together on a journey to improve lives in Latin America and the Caribbean. Our people find purpose and do what they love in an inclusive, collaborative, agile, and rewarding environment.

About this position

Your responsibilities will include leading the development and enhancement of technological solutions and tools, creating proofs of concept, and testing machine learning, deep learning, and AI models for the electricity sector. You will also support the deployment of these tools—such as Energizad2 and SunScanIDB, two open-source solutions developed by the IDB—for use by our clients.

In addition, you will oversee the organization's data management strategy, ensuring data quality, security, and accessibility, while implementing policies and procedures to strengthen data governance and promote effective data utilization.

We are looking for a talented, experienced, and knowledgeable Data Scientist Consultant. As a Data Scientist Consultant, you will contribute to the innovation agenda of the Division by aiding the software development and deployment of ML/DL/AI proofs of concept to solve sectorial problems.

You will work in the Energy Division of the Infrastructure and Energy Department (INE/ENE). This team is responsible for the planification, preparation and evaluation of projects, investments in new and existing infrastructure, development and recommendation of sector public policy and regulations, institutional strengthening programs, regional dialogue with countries and other multilateral organizations, climate action programs in the sector (mitigation and adaptation practices), among others.

What you'll do:

- Enhance existing models for the analysis of non-technical losses (**Energiza2**) and the estimation of solar generation capacity (**SunScanIDB**), and other relevant solutions.
- Conduct research and develop machine learning, deep learning, and AI models for analyzing electricity consumption patterns, detecting anomalies, and segmenting rooftops suitable for solar panel installation using satellite imagery.
- Design and develop proofs of concept applying ML/DL/AI techniques to support the above-mentioned activities.
- Coordinate the deployment and implementation of solutions such as Energiza2 and

SunScanIDB by client organizations.

Deliverables and Payments Timeline:

The consultant will be required to submit the following deliverables, keeping in consideration the subsequent work required to complete the event:

(a) Deliverable #1. Workplan.

(b) Deliverable #2. Report with the following deliverables:

- Improved models for analysis of non-technical losses
- Research findings and model development advances for segmenting roofs suitable for solar panel installation using satellite imagery.

(b)Deliverable #3. Final report and the following deliverables:

- Delivery of the source code repository and notebooks for research and training processes.
- Delivery of packaged and archived models. This will be done in coordination with the project team.
- If training datasets requiring preparation were used, they will be delivered packaged and archived, also in coordination with the project team.

Deliverable #	**Percentage of payment**	**Planned Date to Submit**
Deliverable # 1	20%	10 days after kick-off
Deliverable # 2	40%	4 months after kick-off
Deliverable # 3	60%	8 months after kick-off

What you'll need

- **Education:** Bachelor’s Degree in areas related to Software Development, Data Science, Computer Science or a related field in an accredited university.
- **Experience:** 5 years and relevant experience in software development projects, including adapting Deep Learning models to cloud infrastructure, Python, DB and AWS services.
- **Languages:** Proficiency in English and one of the other Bank official languages (Spanish, French or Portuguese) is required.

Key skills:

- Learn continuously
- Collaborate and share knowledge
- Focus on clients
- Communicate and influence
- Innovate and try new things

- Strong understanding of Software Development.
- Programming knowledge of Python or R.
- Experience with Cloud Infrastructure, Data Storage and Management infrastructure on which to run analytics tools as well as a place to store and query data.
- Knowledge of how to use cloud services from major providers (AWS or Azure).

Requirements:

- **Citizenship:** You are a citizen of one of our 48-member countries.
- **Consanguinity**: You have no family members (up to the fourth degree of consanguinity and second degree of affinity, including spouse) working at the IDB, IDB Invest, or IDB Lab.
- **COVID-19 considerations:** the health and safety of our employees are our number one priority. As a condition of employment, IDB/IDB Invest requires all new hires to be fully vaccinated against COVID-19.

Type of contract and duration:

- **Type of contract:** Products and External Services Consultant (PEC), Lump Sum
- **Length of contract:** 8 months

Other conditions

Within the framework of this technical cooperation, digital tools will be developed whose licensing will guarantee the Inter-American Development Bank's (IDB) full ownership of the intellectual property rights, in accordance with policy AM-331. To this end, the consultancies shall transfer all necessary rights to modify, adapt, customize, use, maintain, and redistribute the developed system. This transfer includes unrestricted access to the source code and all associated technical artifacts (documentation, libraries, database schemas, among others), enabling the IDB to make continuous improvements, develop new functionalities, and ensure the system's long-term sustainability.

The source code of systems developed under this technical cooperation, duly tested and validated in terms of compliance with functional requirements, scalability, and efficient data management, will be stored in the code repository provided by the IDB. The consultancies commit to ensuring that all deliverables are free of third-party rights and that the software does not infringe upon patents, restrictive licenses, or any other applicable legal provisions. Additionally, mechanisms for code verification and quality control, as well as best practices for technical documentation, will be established to facilitate future adoption by the Bank or other authorized stakeholders. These guidelines ensure that the products resulting from this technical cooperation are fully reusable and sustainable, reinforcing their value as regional public goods.

What we offer

The IDB group provides benefits that respond to the different needs and moments of an employee's life. These benefits include:

- A **competitive compensation** package.
- A flexible way of working. You will be evaluated by deliverable.

Our culture

At the IDB Group we work so everyone brings their best and authentic selves to work, willing to try new approaches without fear, and where they are accountable and rewarded for their actions.

Diversity, Equity, Inclusion and Belonging (DEIB) are at the center of our organization. We celebrate all dimensions of diversity and encourage women, LGBTQ+ people, persons with disabilities, Afro-descendants, and Indigenous people to apply.

We will ensure that individuals with disabilities are provided reasonable accommodation to participate in the job interview process. If you are a qualified candidate with a disability, please e-mail us at diversity@iadb.org to request reasonable accommodation to complete this application.

Our Human Resources Team reviews carefully every application.

About the IDB Group

The IDB Group, composed of the Inter-American Development Bank (IDB), IDB Invest, and the IDB Lab offers flexible financing solutions to its member countries to finance economic and social development through lending and grants to public and private entities in Latin America and the Caribbean.

About IDB

We work to improve lives in Latin America and the Caribbean. Through financial and technical support for countries working to reduce poverty and inequality, we help improve health and education and advance infrastructure. Our aim is to achieve development in a sustainable, climate-friendly way. With a history dating back to 1959, today we are the leading source of development financing for Latin America and the Caribbean. We provide loans, grants, and technical assistance; and we conduct extensive research. We maintain a strong commitment to achieving measurable results and the highest standards of integrity, transparency, and accountability.

Follow us:

https://www.linkedin.com/company/inter-american-development-bank/

https://www.facebook.com/IADB.org

https://twitter.com/the_IDB

IDB

HRD Terms of Reference **ANNEX A**

Selección Process XXXXX

TERMS OF REFERENCE

Cybersecurity consultancy for Energy companies and regulator in Latin America and the Caribbean

Regional –

Project number: P001

Technical cooperation number: RG-T4687

Technical cooperation name: Cybersecurity and Digital Transformation in the Energy Sector

1. Background and Justification

1.1 The energy sector is experiencing a deep change due to the need of decarbonization, increased decentralization of electricity generation and digitalization. These ¨three D´s¨ characterize the energy transition that is starting to have some profound effects in electricity systems across the developing world. The first two aspects, the increased use of clean but variable renewable resources and its decentralized characteristic, imply the use of a larger and generally more complex amount of data, as those sources are normally placed far from electricity consumption centers and the typical plant size is much smaller than the traditional thermal plants.

1.2 While the situation varies from one country to another, strengthening governance will be a major and essential task for LAC countries in this time of sector transformation. This includes strengthening institutions, developing long-term policies and plans, building regulatory capacity, and improving sector information and analysis. Latin America's energy challenge over the next two decades is not lack of resources, but rather strengthening institutions.

1.3 As industrial control systems are increasingly essential along the electricity chain (generation, transmission and distribution), and as Information Technology systems are increasingly connected to Operational Technology systems, so do cybersecurity risks increase. According to the World Economic Forum[1], Cyberattacks posed the most significant technological risk in 2018, the third most likely risk, with the 6th biggest potential global impact of all risks. In the United States, determined, well-funded and capable threat actors are known to attack the electric grid, while utilities often lack full perspective of their cyber security posture and desire guidance[2].

1.4 For these reasons the World Energy Council recommends that energy companies view cyber risks as core business risks[3]. Companies should cooperate to asses, understand and

[1] The Global Risks Report 2018, 13th Edition. World Economic Forum

[2] Cyber Threat and Vulnerability Analysis in the U.S. Electric Sector. 2016, Idaho National Laboratory

[3] The Road to Resilience – Managing Cyber Risks. 2016, World Energy Council

build strong resilience towards these risks, which threaten service continuity, reputation, data, and systems[4]. Technical and human factors should be improved, and standards and best practices developed by all stakeholders to tackle these ongoing threats.

1.5 The IDB, together with the support of the Regional Energy Integration Commission (CIER), have carried out the first regional evaluation on the state of cybersecurity preparedness of companies in the electricity sector in Latin America[5]. The study will be presented in this webinar, including expert recommendations on best practices in the sector and mitigation factors.

1.6 In 2016, the technical study "Cybersecurity Report- Are we ready in Latin America and the Caribbean?" was developed and published by the IDB, in collaboration with the OAS. This report analyzed the state of preparedness of 32 countries in the region, based on 49 indicators of cybersecurity capability. In 2020 IDB and OAS develop a new study of the region using the same methodology "Cybersecurity: Risks, Progress and the Way Forward in Latin America and the Caribbean[6]". By 2020 only 7 countries of the region have a cybersecurity strategy in place to identify and protect Critical Infrastructures, including energy facilities.

1.7 In order to take advantage of its experience, the Bank has been working in collaboration with Spain, considered one of the leading countries in global cybersecurity, through the operations RG-T2408 "Cybersecurity: Laying the foundations for a secure cyberspace", and currently RG-T3024 "Strengthening of Cybersecurity in Latin America and the Caribbean". This project is framed in Component 3 of the operation RG-T3024: "Technical assistance in cyber security". The objective of this Component is to strengthen the national capacities of the countries of the region in their actions and policies against cybercrime.

2. Objectives

2.1. The objective of this contract is to support governments in Latin America and the Caribbean to strengthen their capacity to manage cybersecurity threats in the energy sector. To this end, the consulting firm will advise clients in the development of preventive measures by providing assessment, recommendations and ethical hacking services.

3. Key Activities

3.1. Service Requests: This contract is for up to 250 hours of assessment, recommendations and ethical hacking services to be performed by the Consulting Firm.

3.1.1.The IDB may contact the Consulting Firm requesting to perform some or all of the above

[4] Marsh-Microsoft Global Cyber Risk Perception Survey. 2017, Marsh

[5] https://publications.iadb.org/es/estado-de-preparacion-en-ciberseguridad-del-sector-electrico-en-america-latina

[6] https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-seguir-en-america-latina-y-el-caribe

services for a public sector organization in Latin America or the Caribbean (the Client).

3.1.2.. For each Request, the Consulting Firm will quote the number of professional service hours required to perform the required services for a specific Client. Upon completion of the Request deliverables (as defined below), the Consulting Firm will be eligible for payment for the number of hours estimated above.

3.1.3.IDB is not obligated to request performance of any amount of the contracted professional services; therefore, this contract may expire if all, some or none of the hours of service have been requested or performed.

3.2. Cybersecurity consulting and advisory services: The consulting firm will provide consulting services based on the organization's needs as identified through preliminary assessments. These could include elements of assessment, recommendations, and development of master plans.

3.3. Ethical Hacking Services.

3.3.1.Planning: The consulting firm will develop a plan to achieve the objectives of a Request using any possible attack technique (internal or external) in order to locate logical and social vulnerabilities and document evidence of each finding.

3.3.1.1. Goals: The Customer and IDB will select and define the applicable target systems and techniques to be tested in the context of any specific Request. These may include Client infrastructure, applications, or both.

3.3.1.2. Tools: Penetration testing shall be performed using both automated and manual tools.

3.3.1.3. Methods: Penetration testing shall normally be performed using “gray box” methods; in some cases, “white box” or “black box” methods may be selected by mutual agreement.

3.3.1.4. Techniques: May include social engineering, phishing, or other techniques.

3.3.1.4.1. Social engineering: Call from the IT department or another organization asking for passwords, posting jobs, making deliveries, etc.

3.3.1.4.2. Phishing: E-mail campaigns with malicious links, requesting credentials, password resets, updates, etc.

3.4. Technical support: The consulting firm will provide the client with technical support to strengthen its capacity to respond to cybersecurity incidents, according to the findings of the assessments and penetration tests performed.

3.5. Execution: The Consulting Firm will perform the services according to the submitted plan.

3.6. Reporting. The Consulting Firm shall report findings and recommendations to correct any deficiencies in the form of a written report and presentation to be delivered remotely. The report shall include: an executive summary, the methodology used, findings grouped by risk level, screen shots documenting the findings, specific and general recommendations.

4. Expected Outcome and Deliverables

4.1. Hours of cybersecurity consulting services, as described in Activities 3.2, 3.3, and 3.4.

4.1.1.A brief written plan.

4.1.2. A detailed report and presentation of findings, delivered and presented as detailed in Activity 3.6;

5. Project Schedule and Milestones

5.1. The work shall be carried out in the span of one (1) year from the time of contract signature.

5.2. The Planning (Activity 3.3.1), Execution (Activity 3.5) and Reporting (Activity 3.6) activities related to each Service Request shall be carried out within one month from the time of the Service Request.

5.3. In order to comply with the project schedule, the full and timely availability of the Client's and IDB's points of contact is confirmed.

6. Acceptance Criteria

6.1. The consulting firm shall maintain regular communication with the point of contact at the IDB in carrying out the activities and developing all deliverables described in this contract. The consulting firm shall obtain the IDB's approval of each deliverable before associated payments will be processed.

7. Supervision and Reporting

7.1. The IDB shall supervise execution of the activities and completion of the deliverables indicated in these terms of reference and approve all payments. The point of contact at the IDB for all matters related to this contract will be Jose Luis Irigoyen, Operation Lead Specialist (JOSELUISI@iadb.org).

8. **Other conditions**

8.1. Within the framework of this technical cooperation, digital tools will be developed whose licensing will guarantee the Inter-American Development Bank's (IDB) full ownership of the intellectual property rights, in accordance with policy AM-331. To this end, the consultancies shall transfer all necessary rights to modify, adapt, customize, use, maintain, and redistribute the developed system. This transfer includes unrestricted access to the source code and all associated technical artifacts (documentation, libraries, database schemas, among others), enabling the IDB to make continuous improvements, develop new functionalities, and ensure the system's long-term sustainability.

8.2. The source code of systems developed under this technical cooperation, duly tested and validated in terms of compliance with functional requirements, scalability, and efficient data management, will be stored in the code repository provided by the IDB. The consultancies commit to ensuring that all deliverables are free of third-party rights and that the software does not infringe upon patents, restrictive licenses, or any other applicable legal provisions. Additionally, mechanisms for code verification and quality control, as well as best practices for technical documentation, will be established to facilitate future adoption by the Bank or other authorized stakeholders. These guidelines ensure that the products resulting from this technical cooperation are fully reusable and sustainable, reinforcing their value as regional public goods.

9. Schedule of payments

Deliverable	Percentage
According to the agreed number of service hours for each service request, against approval of the deliverables stipulated in Section 4.	Up to 100%
TOTAL	100%

Selección Process XXXXX

TERMS OF REFERENCE

Cybersecurity Training for Energy companies and regulator in Latin America and the Caribbean

Regional –

Project number: P002

Technical cooperation number: RG-T4687

Technical cooperation name: Cybersecurity and Digital Transformation in the Energy Sector

HRD Terms of Reference **ANNEX A**

1. Background and Justification

1.1 The energy sector is experiencing a deep change due to the need of decarbonization, increased decentralization of electricity generation and digitalization. These ¨three D´s¨ characterize the energy transition that is starting to have some profound effects in electricity systems across the developing world. The first two aspects, the increased use of clean but variable renewable resources and its decentralized characteristic, imply the use of a larger and generally more complex amount of data, as those sources are normally placed far from electricity consumption centers and the typical plant size is much smaller than the traditional thermal plants.

1.2 While the situation varies from one country to another, strengthening governance will be a major and essential task for LAC countries in this time of sector transformation. This includes strengthening institutions, developing long-term policies and plans, building regulatory capacity, and improving sector information and analysis. Latin America's energy challenge over the next two decades is not lack of resources, but rather strengthening institutions.

1.3 As industrial control systems are increasingly essential along the electricity chain (generation, transmission and distribution), and as Information Technology systems are increasingly connected to Operational Technology systems, so do cybersecurity risks increase. According to the World Economic Forum[7], Cyberattacks posed the most significant technological risk in 2018, the third most likely risk, with the 6th biggest potential global impact of all risks. In the United States, determined, well-funded and capable threat actors are known to attack the electric grid, while utilities often lack full perspective of their cyber security posture and desire guidance[8].

1.4 For these reasons the World Energy Council recommends that energy companies view cyber risks as core business risks[9]. Companies should cooperate to asses, understand and build strong resilience towards these risks, which threaten service continuity, reputation, data, and systems[10]. Technical and human factors should be improved, and standards and best practices developed by all stakeholders to tackle these ongoing threats.

1.5 The IDB, together with the support of the Regional Energy Integration Commission (CIER), have carried out the first regional evaluation on the state of cybersecurity preparedness of companies in the electricity sector in Latin America[11]. The study will be presented in this webinar, including expert recommendations on best practices in the sector and mitigation factors.

1.6 In 2016, the technical study "Cybersecurity Report- Are we ready in Latin America and the

[7] The Global Risks Report 2018, 13th Edition. World Economic Forum

[8] Cyber Threat and Vulnerability Analysis in the U.S. Electric Sector. 2016, Idaho National Laboratory

[9] The Road to Resilience – Managing Cyber Risks. 2016, World Energy Council

[10] Marsh-Microsoft Global Cyber Risk Perception Survey. 2017, Marsh

[11] https://publications.iadb.org/es/estado-de-preparacion-en-ciberseguridad-del-sector-electrico-en-america-latina

Caribbean?" was developed and published by the IDB, in collaboration with the OAS. This report analyzed the state of preparedness of 32 countries in the region, based on 49 indicators of cybersecurity capability. In 2020 IDB and OAS develop a new study of the region using the same methodology "Cybersecurity: Risks, Progress and the Way Forward in Latin America and the Caribbean[12]". By 2020 only 7 countries of the region have a cybersecurity strategy in place to identify and protect Critical Infrastructures, including energy facilities.

1.7 In order to take advantage of its experience, the Bank has been working in collaboration with Spain, considered one of the leading countries in global cybersecurity, through the operations RG-T2408 "Cybersecurity: Laying the foundations for a secure cyberspace", and currently RG-T3024 "Strengthening of Cybersecurity in Latin America and the Caribbean". This project is framed in Component 3 of the operation RG-T3024: "Technical assistance in cyber security". The objective of this Component is to strengthen the national capacities of the countries of the region in their actions and policies against cybercrime.

2. Objectives

2.1. The objective of this consultancy is to design and develop cybersecurity training materials and courses for the Energy Sector (with special emphasis in electricity). The consulting firm should also deliver the training. The consulting firm should develop two sets of training, one for electric utility managers and electricity regulators, and a second one for technicians and utility operators.

3. Key Activities

3.1. Development of tree different cybersecurity training programs for the electric sector. The first will aim to provide general theoretical knowledge on cybersecurity related to the energy sector. The second will be aimed at technical audiences and will focus on practical topics which will be accompanied by laboratories and/or simulators. The third program will be oriented to decision makers and will aim to theoretically simulate cybersecurity incidents in the context of the energy sector.

3.2. For three programs, the developed materials will include detailed session by session contents, slides, previous knowledge requirements and recommended bibliography of reading material, practical exercises and case studies.

3.3. The general theoretical program should cover the following requirements:

3.3.1. Should be unattended where the student can follow the course at his own speed. The provider shall make available the platform on which the students will take the course.

3.3.2. Each course should take the student an average of 6 hours to complete.

[12] https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-seguir-en-america-latina-y-el-caribe

- 3.3.3. It should have complementary materials that help learning, such as videos or simple exercises.
- 3.3.4. Each course in this program must include a test at the end of the course to validate the knowledge acquired.
- 3.3.5. Each course should include one of the following topics:
  - 3.3.5.1. Cybersecurity awareness
  - 3.3.5.2. Cybersecurity basics in the energy context
  - 3.3.5.3. Industrial cybersecurity concepts

3.4. For the technical program, courses are expected to meet the following requirements:

- 3.4.1. They must be online classes with at least one teacher.
- 3.4.2. The duration of each shall be limited to 4 hours
- 3.4.3. They should address specific technical topics along with the use of laboratories or simulators.
- 3.4.4. The number of participants in each exercise will be between 20 and 30.
- 3.4.5. Each course should include one of the following topics:
  - 3.4.5.1. Smart Grid Security
  - 3.4.5.2. Smart Meter Security
  - 3.4.5.3. Secure Communication Protocols in the Energy Sector
  - 3.4.5.4. Incident Detection and Response in Industrial Environments

3.5. The program for decision makers shall meet the following requirements

- 3.5.1. Must be carried out in person
- 3.5.2. It will simulate a cybersecurity incident where the decision makers will have to answer a series of questions which will condition the outcome of the simulation.
- 3.5.3. The objective will not be to evaluate technical aspects but rather issues related to communications, decision making and crisis management.
- 3.5.4. The number of participants in each exercise will be between 10 and 20.

4. Expected Outcome and Deliverables

4.1. Workplan indicating timeline and methodology for the completion of contract activities;

4.2. Draft training material for the general theorical program:

- 4.2.1. Detailed training program
- 4.2.2. Training support material for each course
- 4.2.3. Learning platform available
- 4.2.4. Informative and awareness presentation about the course for potential participants

4.3. Draft training material for the technical program:

- 4.3.1. Detailed training program
- 4.3.2. Training support material for each course
- 4.3.3. Cyber-Range or Labs practices activities (guides and demos)
- 4.3.4.
- 4.3.5. Informative and awareness presentation about the course for potential participants

4.4. Draft training material for the decision makers program:

- 4.4.1. Detailed training program

4.4.2.Training support material

4.5. Final training material for the drafts delivered in 4.2;

4.6. Final training material for the drafts delivered in 4.3;

4.7. Final training material for the drafts delivered in 4.4;

4.8. General theorical course available (at least three of the topics for one year)

4.9. Technical course (at least three topics, to be delivered in several sessions)

4.10. Decision makers exercise (at least two instances)

5. Project Schedule and Milestones

5.1. The work shall be carried out in the span of two (2) years from the time of contract signature. The selected firm must present a proposed timeline for completion of the activities within two weeks of contract signature.

5.2. The deliverables 4.2, 4.3 and 4.4 must be delivered in the span of three (3) months from the time of contract signature

6. Training Requirements

6.1. All deliverables will be presented in Spanish by the Firm unless otherwise noted;

6.2. For the live trainings, whether on-line or in person. If the training is in person, the bank will pay for the cost flights, accommodation and per-diem.

6.3. The trainings must include specific topics of electric sector cybersecurity (i.e. IEC62443, NIST Cybersecurity Framework, NERC, M2C2, SCADA, RTUs, etc.) as detailed in the Firm's proposal;

6.4. For the technical program all the courses shall include practical exercises and examples relevant for the electricity sector;

6.5. The technical training must include practical exercises using Cyber-range platforms;

7. Acceptance Criteria

7.1. The consulting firm shall maintain regular communication with the point of contact at the IDB in carrying out the activities and developing all deliverables described in this contract. The consulting firm shall obtain the IDB's approval of each deliverable before associated payments will be processed.

8. Supervision and Reporting

8.1. The IDB shall supervise execution of the activities and completion of the deliverables indicated in these terms of reference and approve all payments. The point of contact at the IDB for all matters related to this contract will be Jose Luis Irigoyen, Operation Lead Specialist (JOSELUISI@iadb.org).

9. Other conditions

9.1. Within the framework of this technical cooperation, digital tools will be developed whose licensing will guarantee the Inter-American Development Bank's (IDB) full ownership of the intellectual property rights, in accordance with policy AM-331. To this end, the consultancies shall transfer all necessary rights to modify, adapt, customize, use, maintain, and redistribute the developed system. This transfer includes unrestricted access to the source code and all associated technical artifacts (documentation, libraries, database schemas, among others), enabling the IDB to make continuous improvements, develop new functionalities, and ensure the system's long-term sustainability.

9.2. The source code of systems developed under this technical cooperation, duly tested and validated in terms of compliance with functional requirements, scalability, and efficient data management, will be stored in the code repository provided by the IDB. The consultancies commit to ensuring that all deliverables are free of third-party rights and that the software does not infringe upon patents, restrictive licenses, or any other applicable legal provisions. Additionally, mechanisms for code verification and quality control, as well as best practices for technical documentation, will be established to facilitate future adoption by the Bank or other authorized stakeholders. These guidelines ensure that the products resulting from this technical cooperation are fully reusable and sustainable, reinforcing their value as regional public goods.

10. Schedule of payments

Deliverable	Percentage
Approval of deliverable 4.1	5%
Approval of deliverable 4.2	5%
Approval of deliverable 4.3	5%
Approval of deliverable 4.4	5%
Approval of deliverable 4.5, 4.6 and 4.7	10%
Approval of deliverable 4.8	20%
Approval of deliverable 4.9 (Maximum of 10 dictations)	Up to 35 (3,5% for each delivery)

Approval of deliverable 4.10 (Maximum of 3 dictations)	Up to 15 (5% for each delivery)
TOTAL	100%