

DOCUMENTO DEL BANCO INTERAMERICANO DE DESARROLLO

**ARGENTINA**

**PROGRAMA DE CIBERSEGURIDAD PARA INFRAESTRUCTURAS CRÍTICAS DE  
INFORMACIÓN (ICI)**

**(AR-L1343)**

**PERFIL DE PROYECTO**

Este documento fue preparado por el equipo compuesto por: Mauricio García (IFD/ICS), Jefe de Equipo; Santiago Paz (IFD/ICS), Jefe Alternativo de Equipo; Krysia Avila (LEG/SGO); Guillermo Laffaye (CSC/CAR); Pablo Libedinsky, Ariel Nowersztern, y Alejandra Aguilar (IFD/ICS); Ana Niubó, Natalia Perez y Roberto Laguado (VPC/FMP); Florencia Méndez (SCL/GDI); Gastón Pierri (SPD/SDV) y Raimundo Arroio (Consultor).

De conformidad con la Política de Acceso a Información, el presente documento está sujeto a divulgación pública.

## PERFIL DE PROYECTO

### ARGENTINA

#### I. DATOS BÁSICOS

|                                 |   |                                      |            |
|---------------------------------|---|--------------------------------------|------------|
| <b>Nombre del Proyecto:</b>     | Programa de Ciberseguridad para Infraestructuras Críticas de Información (ICI)  |                                      |            |
| <b>Número de Proyecto:</b>      | AR-L1343  |                                      |            |
| <b>Equipo de Proyecto:</b>      | Mauricio García (IFD/ICS), Jefe de Equipo; Santiago Paz (IFD/ICS), Jefe Alternativo de Equipo; Krysia Avila (LEG/SGO); Guillermo Laffaye (CSC/CAR); Pablo Libedinsky, Ariel Nowersztern, y Alejandra Aguilar (IFD/ICS); Ana Niubó, Natalia Perez y Roberto Laguado (VPC/FMP); Florencia Méndez (SCL/GDI); Gastón Pierri (SPD/SDV) y Raimundo Arroio (Consultor) |                                      |            |
| <b>Prestatario:</b>             | República Argentina   |                                      |            |
| <b>Organismo Ejecutor (OE):</b> | República Argentina, a través de Jefatura de Gabinete de Ministros (JGM) de la Presidencia de la Nación   |                                      |            |
| <b>Plan Financiero:</b>         | BID (Capital Ordinario):  | US\$                                 | 30.000.000 |
|                                 | Total:  | US\$                                 | 30.000.000 |
| <b>Salvaguardias:</b>           | Políticas activadas:  | Marco de Política Ambiental y Social |            |
|                                 | Clasificación:  | "C"                                  |            |

#### II. JUSTIFICACIÓN GENERAL Y OBJETIVOS

- 2.1 **Antecedentes y justificación.** La Administración Pública Nacional (APN) está en un proceso de mejora de los servicios que provee, haciéndolos más eficientes, accesibles y transparentes. Para ello, se han incorporado plataformas de gestión en los organismos, generando nuevos canales digitales con los ciudadanos y el sector privado. Sin embargo, para aprovechar las oportunidades que ofrece la digitalización, se requiere también: (i) mejorar la calidad de las comunicaciones; (ii) desarrollar habilidades digitales; (ii) adoptar nuevas tecnologías en el sector productivo; y gestionar correctamente la ciberseguridad<sup>1</sup>.
- 2.2 En este sentido, Argentina ha llevado a cabo numerosas iniciativas para proteger su ciberespacio. En 2011 crea el [Programa Nacional de Infraestructuras Críticas de Información \(ICI\)](#)<sup>2</sup> y [Ciberseguridad](#), en 2017 el Comité de Ciberseguridad (CC) para desarrollar una estrategia nacional de seguridad cibernética; y en 2019 aprueba su Estrategia Nacional de Ciberseguridad ([ENC](#)) incluyendo la protección de ICI.

<sup>1</sup> [Agenda Digital Argentina](#) (AD).

<sup>2</sup> Infraestructuras que habilitan la prestación de servicios esenciales para la sociedad y la economía. [Resolución 829/2019](#).

- 2.3 Esto ha permitido que se ubique por encima del valor promedio de América Latina y el Caribe (ALC), con un puntaje de 50,12 en el Índice Global de Ciberseguridad del *International Telecommunication Union (ITU)* y en la posición 13 en la región. Sin embargo, ALC es la segunda región menos preparada, después de África, para afrontar desafíos de ciberseguridad. Si comparamos el desempeño de Argentina con el promedio de la Organización para la Cooperación y el Desarrollo Económicos, éste queda debajo de la media. Ello está relacionado con que los esfuerzos por proteger el espacio digital no han avanzado al mismo ritmo que el proceso de digitalización<sup>3</sup>. En efecto, la elevada penetración de las Tecnologías de la Información y la Comunicación (TIC)<sup>4</sup>, incrementa vulnerabilidades, incidentes potenciales, e impacto que pueden generar al aumentar la “superficie de ataque”<sup>5</sup>.
- 2.4 La implementación de la ENC es incipiente. Si bien la JGM y el CC han definido lineamientos para identificar una ICI<sup>6</sup>, sólo el Sistema de Gestión Documental Electrónica (GDE)<sup>7</sup> ha sido identificado y aún no se ha desarrollado ningún plan de protección. Por el sector privado, 53% de las empresas no tienen estrategias de ciberseguridad y el 61% ni planes de contingencias ante incidentes<sup>8</sup>.
- 2.5 Desarrollar capacidades en ciberseguridad requiere la correcta gestión<sup>9</sup> de: (i) identificar qué debo proteger y su nivel de riesgo; (ii) proteger dichos activos implementando acciones defensivas; (iii) detectar posibles fallas en dichos sistemas de defensa; (iv) responder los ataques que hayan eludido dichas medidas; y (v) recuperarse ante los daños causados por estos incidentes. Una correcta implementación de estas funciones genera la robustez necesaria para que los sistemas e infraestructuras tecnológicas puedan brindar los servicios esperados.
- 2.6 **Problema y desafíos.** El principal problema identificado es el alto costo de los incidentes de ciberseguridad para el Estado y la ciudadanía<sup>10</sup>. Efectivamente, según [datos de la SIP](#), el 81,7% de los incidentes procesados durante 2021 fueron de severidad alta o crítica, que tienen un costo 100 veces mayor que los de severidad baja. Países de la región como Uruguay no alcanzan el 2% en esta categoría<sup>11</sup>. Esto se debe a la limitada capacidad del país para gestionar las funciones básicas de la ciberseguridad de las ICI, asociado a los siguientes factores:

---

<sup>3</sup> Entre 2016 y 2022 el número de usuarios de trámites a distancia incrementó 220% ([20.793.925 trámites digitales](#)).

<sup>4</sup> Decreto [733/2018](#) establece la obligación de la APN de digitalizar todos los trámites relacionados con el ciudadano.

<sup>5</sup> En 2021 son 27,1 billones los dispositivos conectados y el tráfico per cápita es de 35 GB/mes, aumentando la [superficie de ataque](#). <https://qblogs.cisco.com/>.

<sup>6</sup> <https://www.argentina.gob.ar/normativa/nacional/>.

<sup>7</sup> [GDE](#) es una plataforma que agiliza los procesos internos del Estado, incluyendo caratulación, numeración, seguimiento y registro de movimientos de todas las actuaciones y expedientes de la APN. Todos los ministerios nacionales y 86% de organismos públicos utilizan GDE. En 2019 se habían creado 10.538.180 expedientes electrónicos (BID-EVERIS, 2019). Para enero 2022, ya son 35.998.117.

<sup>8</sup> <https://www.pwc.com.ar/>.

<sup>9</sup> <https://www.nist.gov/cyberframework>.

<sup>10</sup> [En 2020 la Oficina Nacional de Migraciones sufrió un ciberataque que afectó sus servicios digitales impidiendo ingresos y egresos de personas al país. En 2021 el Registro Nacional de las Personas sufrió un el robo de información sensible de millones de argentinos.](#)

<sup>11</sup> <https://www.gub.uy/>.

- 2.7 **Baja cobertura de la SIP para identificar y proteger ICI.** De los 11 sectores clasificados como críticos<sup>12</sup>, desde 2019, solo el sistema GDE<sup>13</sup> fue identificado como ICI. Esto impide determinar los riesgos cibernéticos y definir planes de protección, pues: (i) los mecanismos de gobernanza<sup>14</sup> no logran priorizar los activos a proteger según su nivel de riesgo; y (ii) la SIP tiene limitaciones para coordinar transversalmente el diseño e implementación de planes de protección de ICI. Por ejemplo, la unidad a cargo del Ecosistema de GDE no cuenta con capacidades para desarrollar un plan para protegerlo, según últimos informes de auditoría<sup>15</sup>.
- 2.8 **Baja productividad en la gestión de incidentes cibernéticos (detección, respuesta y recuperación).** Por ejemplo, durante 2020 en [Argentina](#) solamente se procesaron 226 incidentes, mientras, que países como [Uruguay](#) y [Chile](#) procesaron 2.798 y 15.321 respectivamente ese año. Esto se debe a que: (i) no se cuenta con un centro de operaciones en ciberseguridad del gobierno (G-SOC)<sup>16</sup> que permita monitorear, en tiempo real, ataques y amenaza a las ICI; (ii) el Centro de Respuesta a Incidentes de Ciberseguridad Nacional (CERT)<sup>17</sup> no dispone de herramientas y capacidades para gestionar las respuestas a incidentes; y (iii) no existe un mecanismo seguro y confidencial para intercambiar información con el ecosistema nacional relativo a ataques e incidentes.
- 2.9 **Oferta reducida de personal capacitado en ciberseguridad.** Entre 2016 y 2020 las capacidades de formación se mantuvieron prácticamente estancadas<sup>18</sup>, y las universidades argentinas no cuentan con la infraestructura tecnológica adecuada para el dictado de cursos especializados<sup>19</sup>. El rápido crecimiento en su demanda (¶2.3) produjo una brecha con su oferta educativa, generándose una importante escasez, impactando la capacidad de gestión del ciberespacio. Asimismo, se observa una baja participación de mujeres en el sector y en la inscripción en carreras afines: en 2020 solo 15% eran mujeres<sup>20</sup>.
- 2.10 **Objetivo general:** Contribuir a la reducción de los costos por incidentes de ciberseguridad para el Estado y la ciudadanía.
- 2.11 **Objetivos específicos:** (i) aumentar la cobertura de gestión para la identificación y protección de las ICI; (ii) mejorar la productividad en la gestión de incidentes cibernéticos; y (iii) mejorar la eficacia en la gestión de la ciberseguridad para el GDE. Contará con los siguientes componentes:
- 2.12 **Componente 1. Fortalecimiento de las capacidades institucionales y tecnológicas de la SIP (US\$20 millones).** Financiará: (i) mejoras del marco institucional y normativo para la identificación y protección de ICI; (ii) creación de un G-SOC para el monitoreo y detección de ataques, dotándolo de herramientas

<sup>12</sup> <https://www.argentina.gob.ar/>.

<sup>13</sup> <http://www.saij.gob.ar/>.

<sup>14</sup> No existe un protocolo para identificación de estos ni su nivel de riesgo.

<sup>15</sup> Auditoría General de la Nación, 2018-2019, y Fundación Sadosky, 2020.

<sup>16</sup> Unidad técnica especializada en la detección y primera respuesta a incidentes de ciberseguridad.

<sup>17</sup> Funciona como una dependencia de la Dirección Nacional de Ciberseguridad ([CERT.ar](#)), y se especializa en la respuesta a incidentes complejos.

<sup>18</sup> BID-OEA (2020). Ciberseguridad: Riesgos, Avances y el camino a seguir en ALC.

<sup>19</sup> Red de Excelencia de Ciberseguridad de Latinoamérica y el Caribe (CIBERLAC.ORG).

<sup>20</sup> Informe de universidades de Buenos Aires y La Plata.

SIEM<sup>21</sup> y sensores; (iii) fortalecimiento de las capacidades operativas del CERT; y (iv) desarrollo de plataformas para el análisis de amenazas e intercambio de información con el sector privado<sup>22</sup>.

- 2.13 **Componente 2. Consolidación del talento humano en ciberseguridad (US\$5 millones).** Financiará el desarrollo de habilidades a nivel nacional y subnacional, incluyendo: (i) plataforma de simulación de ataques cibernéticos para capacitación especializada ([CyberRange](#)); (ii) programas técnicos y de certificación en ciberseguridad<sup>23</sup>, priorizando mujeres; (iii) plataforma de *e-Learning* para formar profesionales, considerando accesibilidad para personas con discapacidad; y (iv) planes de gestión del cambio y desarrollo curricular en ciberseguridad.
- 2.14 **Componente 3. Mejoramiento de la protección del ecosistema GDE (US\$3 millones).** Financiará: (i) análisis de brecha de ciberseguridad del GDE; (ii) desarrollo de capacidades técnico-operativas para que la Subsecretaría de Innovación Administrativa (SIA) brinde ciberseguridad; (iii) implementación de tecnologías de prevención y protección de infraestructuras a cargo de la SIA.
- 2.15 **Administración.** Se han identificado costos de administración, evaluación y auditorías por US\$2 millones.
- 2.16 **Resultados esperados.** El principal impacto será el ahorro en los costos por incidentes de ciberseguridad para el Estado y la sociedad, derivado de mejoras en: (i) la identificación y protección de las ICI; (ii) las capacidades de detección, respuesta y recuperación a incidentes; (iii) la consolidación del talento humano capacitado, priorizando la participación de las mujeres; y (iv) la eficacia en la gestión de la ciberseguridad del GDE.
- 2.17 **Beneficiarios.** Los directos serán ciudadanos y empresas usuarias del GDE y las organizaciones operadoras de ICI que verán mejorados los servicios de ciberseguridad ofrecidos por la SIP; particularmente las mujeres, al incentivarse su ingreso y participación en el sector, reduciendo las brechas de género. Los indirectos serán las instituciones públicas en general porque su infraestructura tecnológica estará más protegida y tendrán más profesionales capacitados en ciberseguridad.
- 2.18 **Alineación estratégica.** El programa es consistente con la Segunda Actualización de la Estrategia Institucional 2020-2023 (UIS) (AB-3190-2) y se alinea al desafío de desarrollo Productividad e Innovación, al promover una nueva área de alto valor añadido como la ciberseguridad; y el desarrollo de métodos más eficientes para la provisión de servicios de ciberseguridad. También se alinea con los temas transversales (i) Igualdad de Género y Diversidad, a través de la inclusión de acciones destinadas a aumentar la participación de las mujeres en el sector y la accesibilidad de las plataformas a personas con discapacidad; y (ii) Capacidad Institucional y Estado de Derecho, al fortalecer la capacidad para proteger el espacio digital y la expansión segura

---

<sup>21</sup> *Security Information Event Management*: integra el análisis de incidentes con su gestión.

<sup>22</sup> El marco normativo no los obliga a compartir información con el CERT.

<sup>23</sup> Priorizando instituciones que tengan alguna ICI.

del sector digital. Además, contribuirá a los indicadores del nivel 2 del Marco de Resultados Corporativos (CRF) 2020-2023 (GN-2727-12) de: (i) instituciones con capacidades gerenciales y de tecnología digital reforzadas, ya que contribuye a elevar el número de agencias gubernamentales beneficiadas por instrumentos tecnológicos y de gestión; y (ii) beneficiarios designados de servicios públicos que han sido adaptados para grupos diversos, mediante plataforma para formación accesible para personas con discapacidad. El programa está alineado con la Estrategia de País del Grupo BID con Argentina 2021-2023 (GN-3051) específicamente con los objetivos estratégicos de: (i) mejorar la empleabilidad de la población, por las inversiones en capacitaciones en ciberseguridad en función de la demanda laboral actual y futura; y (ii) gobierno digital, al dar mayor seguridad a la expansión del sector.

- 2.19 Este programa está diseñado como un préstamo de inversión específico, que será financiado por un total de US\$30 millones, con cargo a recursos del Capital Ordinario del Banco y con un plazo de desembolso de cinco años. Esta modalidad se justifica ya que las actividades del proyecto se encuentran claramente definidas. El OE será la JGM, con experiencia con proyectos con el Banco y otros multilaterales, a quien se aplicará el análisis de capacidad institucional (PACI) para definir y presupuestar las necesidades de asistencia técnica especializada que faciliten una eficiente gestión del programa.

### III. ASPECTOS TÉCNICOS Y CONOCIMIENTO DEL SECTOR

- 3.1 **Experiencia del Banco.** El Banco cuenta con amplia experiencia en el diseño e implementación de proyectos relacionados con el uso de TIC y con la protección del espacio digital, tales como: Fortalecimiento de la Ciberseguridad en Uruguay (4843/OC-UR), Panamá en Línea (3683/OC-PN), Transformación Digital del Gobierno para Fortalecer la Competitividad (4549/OC-BH), Programa de Apoyo a la Implementación de la AD (4650/OC-PR). Además, el Banco ha contado con el apoyo técnico y financiero de los gobiernos de Israel y España a través de las cooperaciones técnicas *Improving Human Resources Capacity in Cybersecurity* (ATN/CF-15598-RG) y Fortalecimiento de la Ciberseguridad en América Latina y el Caribe (ATN/FG-16633-RG), que han financiado la realización de actividades de capacitación y estudios que constituyen un insumo fundamental para el diseño de esta operación.
- 3.2 **Lecciones aprendidas.** En la preparación del programa se consideran lecciones aprendidas de operaciones similares del Banco en la región (§3.1), la importancia de: fortalecer la institucionalidad y liderazgo del organismo responsable de la ciberseguridad en el país (SIP); lo estratégico de la coordinación interinstitucional; la participación y trabajo en equipo desde su diseño; y la formación de talento para asegurar la disponibilidad de profesionales y servicios. Además, adelantar durante la preparación del programa los procesos de compras estratégicas de tecnologías y servicios complejos, realizando procesos de *request for information*, a partir de términos de referencia y especificaciones técnicas, según estándares internacionales.

#### IV. RIESGOS AMBIENTALES Y ASPECTOS FIDUCIARIOS

- 4.1 En atención al Nuevo Marco de Política Ambiental y Social (GN-2965-23), la operación fue clasificada como Categoría “C”. No se prevén efectos negativos ambientales o sociales significativos.
- 4.2 **Financiamiento retroactivo y reconocimiento de gastos.** El Banco podrá financiar retroactivamente con cargo a los recursos del préstamo, gastos elegibles efectivamente pagados por el prestatario antes de la fecha de aprobación del préstamo hasta por el 15% del monto propuesto, para pagos efectuados correspondientes a las contrataciones anticipadas de consultorías y bienes y servicios para el diseño e implementación rápida de actividades críticas del programa; siempre que se hayan cumplido los requisitos sustancialmente análogos a los establecidos en el contrato de préstamo. Dichos gastos deberán haberse efectuado a partir de la fecha de aprobación de este perfil de proyecto, pero en ningún caso se incluirán gastos efectuados más de 18 meses antes de la fecha de aprobación del préstamo.
- 4.3 Se identificó preliminarmente como riesgo fiduciario medio-alto, relacionado con los procesos internos que, si existieran demoras entre la identificación de una necesidad y el tiempo de gestión para la efectiva adquisición del bien o servicio, podría impactar negativamente en el avance del proyecto. Para mitigarlo se tiene previsto habilitar y contratar personal calificado, con experiencia en procedimientos de organismos multilaterales para la gestión de adquisiciones; y, el Banco brindará apoyo y capacitación en temas fiduciarios.

#### V. OTROS TEMAS

- 5.1 **Otros riesgos.** Se consideraron dos riesgos de nivel medio-alto. Uno sobre entorno institucional que, si hubiese resistencia al cambio por parte de las organizaciones públicas y los operadores de ICI para aceptar las actividades de implementación del proyecto, podría no lograrse una adecuada apropiación de las medidas de protección y se continuaría la exposición a incidentes cibernéticos. Para mitigarlo se establecerán estrategias de gestión del cambio, implementando actividades de capacitación, comunicación y sensibilización. Otro de recursos humanos que, si existieran dificultades para retener a profesionales técnicos capacitados, podría no lograrse el cumplimiento en tiempo y/o calidad en los entregables del proyecto. Para mitigarlo se prevé dotar a estos técnicos de cursos avanzados, poner a su disposición las herramientas más modernas; y hacerlos partícipes en los procesos de decisión sobre las políticas y medidas de protección a las ICI.
- 5.2 **Complementariedad con otras operaciones del Banco en Argentina.** Complementa el Programa para el Fortalecimiento de la AD, la Conectividad, el Gobierno Electrónico y la Transformación Productiva (4755/OC-AR) de 2019 en que se apoyó al gobierno en la implementación de políticas relacionadas con ICI y seguridad de datos. Asimismo, la ATN/OC-17583-AR Transformación Digital en ejecución, que apoya la implementación de la AD, incluyendo el plan de protección de ICI.

- 5.3 **Sostenibilidad.** A nivel financiero, el programa prevé importantes ahorros derivados de menores costos para responder a ciberataques, y el aumento de capacidades de recuperación ante los daños causados por estos. A nivel tecnológico, las inversiones se harán con previsión del servicio de mantenimiento para darles mayor sostenibilidad. A nivel de capacidades, se fortalecerá a la SIP y APN con la profesionalización e incremento de funcionarios en ciberseguridad. Finalmente, a nivel institucional, el programa se encuentra alineado con la AD, con la ENC y el Plan de Protección de ICI, que son compromisos políticos asumidos por el gobierno, lo que también fortalece su sostenibilidad.

## **VI. RECURSOS Y CRONOGRAMA DE PREPARACIÓN**

- 6.1 Se prevé la distribución del POD al QRR para 16 de mayo de 2022; del Borrador de Propuesta de Préstamo al Comité de Políticas Operativas para 22 de junio de 2022; y la consideración de la Propuesta de Préstamo por el Directorio Ejecutivo el 27 de julio de 2022. El total de los recursos para la preparación se estiman en US\$131.200 (US\$81.200 de fondos transaccionales y US\$50.000 con recursos de ATN/FG-18691-RG y ATN/OC-17583-AR). El tiempo de personal requerido para la preparación del préstamo será de 1,12 FTE.



# CONFIDENCIAL

<sup>1</sup> La información contenida en este Anexo es de carácter deliberativo, y por lo tanto confidencial, de conformidad con la excepción relativa a "Información Deliberativa" contemplada en el párrafo 4.1 (g) de la "Política de Acceso al Información" del Banco (Documento GN-1831-28).

## Operation Information

|  |                 |
|--|-----------------|
| Operation Name   |                 |
| <b>Strengthening of Cybersecurity in the National Government</b> |                 |
| Operation Number   | <b>AR-L1343</b> |

## Operation Details

|   |   |
|---|---|
| Organizational Unit                                   | IDB Sector/Subsector  |
| <b>IFD/ICS</b>  | <b>E-GOVERNMENT</b>   |
| Type of Operation & Modality                          | Original IDB Amount   |
| <b>LON / ESP</b>                                      | <b>\$30,000,000.00</b>  |
| Environmental and Social Impact Categorization (ESIC) | Disaster and Climate Change Risk Classification (DCCRC)       |
| <b>C</b>  | <b>Low</b>  |
| Environmental and Social Risk Rating (ESRR)           |   |
| <b>Moderate</b>                                       |   |
| Executing Agency                                      | Borrower  |
| <b>AR-JGM</b>   | <b>NACION ARGENTINA</b>                                       |
| ESG Primary Team Member                               | Team Leader   |
|   | <b>Mauricio Garcia Mejia</b>                                  |
| Toolkit Completion Date                               | Author  |
| <b>08/02/2022</b>                                     | <b>Tapia Alba, Mauricio Alejandro (Esg Guidance Services)</b> |
| Applicable ESPs                                       |   |
| <b>ESPS 1; ESPS 2; ESPS 10</b>                        |   |

## Operation Classification Summary

|                |                              |
|----------------|------------------------------|
| Overriden ESIC | Overriden ESIC Justification |
|                |                              |
| Comments       |                              |
|                |                              |

|                 |                               |
|-----------------|-------------------------------|
| Overriden DCCRC | Overriden DCCRC Justification |
|                 |                               |

| Comments |
|----------|
|          |

## Summary of Impacts / Risks and Potential Solutions

The project has no environmental and social impacts and/or risks therefore no Environmental and Social Assessment (ESA) or Environmental and Social Impact Assessment (ESIA) process will be conducted for the project during preparation.

There are no contextual risks associated with the project (e.g. political instability, oppression of communities, armed forces in the project area).

The operation will not have direct impacts associated with child labor or forced labor in the workforce.

The operation will not have significant indirect and/or cumulative impacts associated with child labor or forced labor in the workforce.

The Executing Agency or other relevant entity (in relation to the operation) has a proven track record to respect and protect the fundamental principles and rights of workers (including fair treatment, commitment to non-discrimination, equal opportunity, protection of workers including workers in vulnerable situations, work accommodations, migrant workers' rights, collective bargaining and rights of association) and compliance with national employment and labor laws.

The operation will not result in the direct loss of employment (i.e. retrenchment).

The operation will not result in the indirect and/or cumulative loss of employment (i.e. retrenchment).

The Borrower will prepare and operate a Grievance Redress Mechanism for all workers (direct and contracted).

The operation will not cause direct impacts associated with accidents, injury, and attraction disease arising from, associated with, or occurring in the course of work.

The operation will not cause indirect and/or cumulative impacts associated with accidents, injury, and attraction disease arising from, associated with, or occurring in the course of work.

The operation will promote a sustainable use of resources including energy, water and raw materials.

The operation will not have direct adverse impacts on human health and the environment due to pollution from project activities.

The operation will not have indirect and/or cumulative adverse impacts on human health and the environment due to pollution from project activities.

The operation will not generate direct impacts generated by solid waste (hazardous and/or non-hazardous).

The operation will not generate indirect and/or cumulative impacts generated by solid waste (hazardous and/or non-hazardous).



## E&S Screening Filter

The operation will not have direct negative impacts to the environment and human health and safety due to the production, procurement, use, and disposal of hazardous materials such as PCBs, Radiological Waste, Mercury, CFCs, etc.

The operation will not have indirect and/or cumulative negative impacts to the environment and human health and safety due to the production, procurement, use, and disposal of hazardous materials such as PCBs, Radiological Waste, Mercury, CFCs, etc.

The operation will not have direct negative impacts to the environment and human health and safety due to the production, procurement, use, and disposal of pesticides.

The operation will not have indirect and/or cumulative negative impacts to the environment and human health and safety due to the production, procurement, use, and disposal of pesticides.

The operation is not expected to or currently produce directly GHG emissions.

The operation is not expected to or currently produce indirectly-cumulatively GHG emissions.

The operation is not considering alternatives to implement technically and financially feasible and cost-effective options to avoid or minimize project-related GHG emissions during the design and operation of the project.

The operation has no exposure to climate transition risks related with a loss of value of a project driven by the transition to a lower-carbon economy, result from extensive policy, legal, technology, and/or market changes to address climate change.

There are no direct health and safety risks associated with the design of structural elements or components of the operation (e.g. existing or new buildings, earthworks, bridges, drainage, roadways, power stations, transmission and distribution poles, underground utilities, and dams), and/or road transport activities (e.g. transport of heavy or over-sized equipment) which could result in health and safety impacts to third parties and project-affected people.

There are no indirect and/or cumulative health and safety risks associated with the design of structural elements or components of the operation (e.g. existing or new buildings, earthworks, bridges, drainage, roadways, power stations, transmission and distribution poles, underground utilities, and dams), and/or road transport activities (e.g. transport of heavy or over-sized equipment) which could result in health and safety impacts to third parties and project-affected people.

The project will not directly affect the public (including workers and their families) by exposing them to hazardous materials released by the project, particularly those that may be life threatening.

The project will not indirectly-cumulatively affect the public (including workers and their families) by exposing them to hazardous materials released by the project, particularly those that may be life threatening.

There is no potential for the project or project-related activities (e.g. the influx of temporary or permanent project labor, among others) to directly result in or exacerbate community exposure to water-related (i.e., waterborne, water-based, and vector-borne diseases) and/or communicable diseases (e.g. COVID).

There is no potential for the project or project-related activities (e.g. the influx of temporary or permanent project labor, among others) to indirectly-cumulatively result in or exacerbate community exposure to water-related (i.e., waterborne, water-based, and vector-borne diseases) and/or communicable diseases (e.g. COVID).



The project's direct impacts on priority ecosystem services will not result in adverse health and safety risks and impacts to the project-affected people.

The project's indirect and/or cumulative impacts on priority ecosystem services will not result in adverse health and safety risks and impacts to the project-affected people.

There is no potential for an emergency or unanticipated event to occur in the project area of influence that demands immediate action to prevent or reduce harm to people, property, and/or the environment.

Natural hazards, such as earthquakes, droughts, landslides, floods, wildfires, or others, including those caused or exacerbated by climate change, are not likely to occur in the project area, and there will be no impact the project, and/or the project will not exacerbate the risk from natural hazards to human life, property, and/or the environment.

There is no potential direct impacts to workers and project-affected people related to the use or arrangement of security services to safeguard personnel and/or property.

There is no potential indirect and/or cumulative impacts to workers and project-affected people related to the use or arrangement of security services to safeguard personnel and/or property.

The project will not lead to direct impacts related to land acquisition - Impacts include, and are not limited to, relocation; loss of shelter; loss of land; loss of assets; restrictions on land and natural resources; loss of income; loss of livelihoods; loss of social safety net.

The project will not lead to indirect and/or cumulative impacts related to land acquisition - Impacts include, and are not limited to, relocation; loss of shelter; loss of land; loss of assets; restrictions on land and natural resources; loss of income; loss of livelihoods; loss of social safety net.

Vulnerable people will not be disproportionately affected by direct impacts related to land acquisition - people may be considered vulnerable by virtue of disability, state of health, indigenous status, gender identity, sexual orientation, religion, race, color, ethnicity, age, language, political or other opinion, national or social origin, property, birth, economic disadvantage, or social condition. Other vulnerable people include the elderly, children, single-headed households, refugees, internally displaced persons, natural resource dependent communities.

Vulnerable people will not be disproportionately affected by indirect and/or cumulative impacts related to land acquisition - people may be considered vulnerable by virtue of disability, state of health, indigenous status, gender identity, sexual orientation, religion, race, color, ethnicity, age, language, political or other opinion, national or social origin, property, birth, economic disadvantage, or social condition. Other vulnerable people include the elderly, children, single-headed households, refugees, internally displaced persons, natural resource dependent communities.

The operation doesn't have the potential to directly impact modified habitat that include significant biodiversity value.

The operation doesn't have the potential to indirectly-cumulatively impact modified habitat that include significant biodiversity value.

The operation doesn't have the potential to directly convert or degrade natural habitat.

The operation doesn't have the potential to indirectly-cumulatively convert or degrade natural habitat.



## E&S Screening Filter

The operation doesn't have the direct potential to implement project activities in critical natural habitat.

The operation doesn't have the indirect and/or cumulative potential to implement project activities in critical natural habitat.

The operation is not expected to directly impact a legally protected area or an internationally recognized area.

The operation is not expected to indirectly-cumulatively impact a legally protected area or an internationally recognized area.

The project will not directly introduce (intentionally or accidentally) alien, or non-native, species of flora and fauna that have the potential for invasive behavior in areas where they are not normally found.

The project will not indirectly-cumulatively introduce (intentionally or accidentally) alien, or non-native, species of flora and fauna that have the potential for invasive behavior in areas where they are not normally found.

The project is not likely to adversely directly impact ecosystem services.

The project is not likely to adversely indirectly-cumulatively impact ecosystem services.

The project is not expected to cause adverse direct impact on Indigenous Peoples. FPIC is required when there will be (i) impacts on lands and natural resources subject to traditional ownership or under customary use; (ii) Relocation of Indigenous Peoples from lands and natural resources subject to traditional ownership or under customary use; or (iii) significant impact on Cultural Heritage.

The project is not expected to cause adverse indirect/cumulative impact on Indigenous Peoples. FPIC is required when there will be (i) impacts on lands and natural resources subject to traditional ownership or under customary use; (ii) Relocation of Indigenous Peoples from lands and natural resources subject to traditional ownership or under customary use; or (iii) significant impact on Cultural Heritage.

Indigenous Peoples are not expected to be adversely impacted by direct project related land-acquisition or access restrictions. Note that all impacts on lands and natural resources subject to traditional ownership or under customary law requires FPIC.

Indigenous Peoples are not expected to be adversely impacted by indirect/cumulative project related land-acquisition or access restrictions. Note that all impacts on lands and natural resources subject to traditional ownership or under customary law requires FPIC.

The project doesn't have the potential to cause adverse direct impacts on Indigenous Peoples who live in isolation and initial contact.

The project doesn't have the potential to cause adverse indirect and/or cumulative impacts on Indigenous Peoples who live in isolation and initial contact.

The project is not expected to directly damage or negatively impact cultural heritage.

The project is not expected to indirectly-cumulatively damage or negatively impact cultural heritage.

The project is not expected to directly damage or negatively impact critical cultural heritage.



## E&S Screening Filter

The project is not expected to indirectly-cumulatively damage or negatively impact critical cultural heritage.

The project will not negatively directly affect people due to their gender, sexual orientation or gender identity.

The project will not negatively indirectly-cumulatively affect people due to their gender, sexual orientation or gender identity.

The project is not expected to lead to direct risks and impacts associated with Sexual and Gender-based Violence.

The project is not expected to lead to indirect and/or cumulative risks and impacts associated with Sexual and Gender-based Violence.

The project will not potentially face direct barriers to equitable gender-based participation.

The project will not potentially face indirect and/or cumulative barriers to equitable gender-based participation.

The project will not deal with a subject matter and/or be implemented in an area where the manipulation, interference, coercion, discrimination, and intimidation of stakeholders has been documented.

### ESPS 1 - Assessment and Management of Environmental and Social Risks and Impacts

The project has no environmental and social impacts and/or risks therefore no Environmental and Social Management System (ESMS) will be prepared for the operation as defined under ESPS 1.

### ESPS 2 - Labor and Working Conditions

The Executing Agency will partially prepare and maintain an Environmental and Social Management System (ESMS) for the operation with specific elements related to Labor and Working Conditions under ESPS 2.

### ESPS 10 - Stakeholder Engagement and Information Disclosure

The Borrower will operate a Grievance Redress Mechanism at the Project level (direct and contracted).

## **ESTRATEGIA AMBIENTAL Y SOCIAL**

- 1.1 Considerando que la operación tendrá impactos ambientales y sociales mínimos o nulos, que no se conlleva riesgos socioambientales sustanciales o altos y que el riesgo de desastres naturales y cambio climático es bajo, no existen requerimientos específicos derivados del Marco de Política Ambiental y Social (MPAS).
- 1.2 Para dar cumplimiento con los requisitos del MPAS y especialmente aquellos de las Normas de Desempeño Ambiental y Social 1, 2 y 10, se revisará el Sistema de Gestión Ambiental y Social ya existente en la Unidad Ejecutora y la normativa local aplicable. En base al nivel de los riesgos e impactos de la operación, se determinará el grado de concordancia del sistema de gestión, de los procesos de gestión laboral, de los mecanismos de participación con partes interesadas y de los mecanismos de quejas y reclamos. Asimismo, de ser el caso, se definirá la estrategia para abordar cualquier brecha identificada frente a estas normas y otras que pudiesen ser relevantes durante la preparación y ejecución de la operación. En el POD, en caso de ser necesario, se acordará un Plan de Acción Ambiental y Social (PAAS) con el Prestatario que establezca las acciones requeridas durante el ciclo de vida la operación para que esta se mantenga en cumplimiento con el MPAS.



## Índice de Trabajo Sectorial Realizado y Propuesto

| Tema  | Tipo de Referencia | Descripción  | Estado de Preparación | Referencias e Hipervínculos |
|---|--------------------|--|-----------------------|-----------------------------|
| Preparación de Perfil de Proyecto (PP) y estudios necesarios para la elaboración del PP | Normativa          | Agenda Digital Argentina   | Terminado             | <a href="#">Enlace</a>      |
|   | Normativa          | Estrategia Nacional de Ciberseguridad de la República Argentina  | Terminado             | <a href="#">Enlace</a>      |
|   | Publicación        | Índice de Madurez de Ciberseguridad: Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. BID, OEA, 2020  | Terminado             | <a href="#">Enlace</a>      |
| Preparación del POD   | Estudio            | Actualización de la Evaluación del Nivel de Madurez de Ciberseguridad de Argentina y hoja de ruta para cierre de brechas   | En Proceso            |                             |
|   | Estudio            | Evaluación de riesgos de ciberseguridad del ecosistema de gestión documental electrónica   | En Proceso            |                             |
|   | Estudio            | Consultoría para el análisis y dimensionamiento del Centro de Operaciones de Ciberseguridad del Gobierno (GSOC)  | En proceso            |                             |
|   | Estudio            | Preparación del Manual Operativo del Programa, el Plan de Adquisiciones, el Informe de Monitoreo del Programa (PMR), el Mecanismo de Monitoreo y Evaluación y apoyo en la preparación del Plan de Ejecución Plurianual (PEP) | En Proceso            |                             |
|   | Estudio            | Análisis económico ex ante del proyecto  | En Proceso            |                             |
|   | Estudio            | Anexo sobre género y diversidad en ciberseguridad  | En Proceso            |                             |
| Recolección de información y análisis para concluir los resultados                      | Estudio            | Elaboración de la Matriz de Resultados   | En Proceso            |                             |

# CONFIDENCIAL

<sup>1</sup> La información contenida en este Anexo es de carácter deliberativo, y por lo tanto confidencial, de conformidad con la excepción relativa a "Información Deliberativa" contemplada en el párrafo 4.1 (g) de la "Política de Acceso al Información" del Banco (Documento GN-1831-28).