

DOCUMENTO DEL BANCO INTERAMERICANO DE DESARROLLO

ARGENTINA

PROGRAMA DE CIBERSEGURIDAD PARA INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN (ICI)

(AR-L1343)

PROPUESTA DE PRÉSTAMO

Este documento fue preparado por el equipo de proyecto integrado por: Mauricio García (ICS/CAR), Jefe de Equipo; Santiago Paz (IFD/ICS), Jefe Alterno de Equipo; Krysia Ávila (LEG/SGO); Guillermo Laffaye (CSC/CAR); Pablo Libedinsky, Ariel Nowersztern, Alejandra Aguilar, y Benjamin Roseth (IFD/ICS); Manuel Fernandini (IFD/CMF); Virginia Snyder (INE/ENE); Andrea Bergamaschi (SCL/EDU); Gabriel Casaburi (IFD/CTI); Juliana Almeida (CSD/CCS); Juan Gomez (IFD/FMM); Ana Niubó, Diana de León, Natalia Pérez y Roberto Laguado (VPC/FMP); Gastón Pierri (SPD/SDV); Florencia Méndez, Roberto Fernández y Raimundo Arroio (Consultores).

El presente documento contiene información confidencial comprendida en una o más de las diez excepciones de la Política de Acceso a Información e inicialmente se considerará confidencial y estará disponible únicamente para empleados del Banco. Se divulgará y pondrá a disposición del público una vez aprobado.

ÍNDICE

RESUMEN DEL PROYECTO	1
I. DESCRIPCIÓN DEL PROYECTO Y MONITOREO DE RESULTADOS.....	2
A. Antecedentes, problemática y justificación.....	2
B. Objetivos, componentes y costo	11
C. Indicadores clave de resultados.....	12
II. ESTRUCTURA DE FINANCIAMIENTO Y PRINCIPALES RIESGOS	14
A. Instrumentos de financiamiento	14
B. Riesgos ambientales y sociales	15
C. Riesgos fiduciarios.....	15
D. Otros riesgos y temas clave.....	15
III. PLAN DE IMPLEMENTACIÓN Y GESTIÓN.....	16
A. Resumen de los arreglos de implementación	16
B. Resumen de los arreglos para el monitoreo de resultados	18

ANEXOS	
Anexo I	Matriz de Efectividad en el Desarrollo (DEM) - Resumen
Anexo II	Matriz de Resultados
Anexo III	Acuerdos y Requisitos Fiduciarios

ENLACES ELECTRÓNICOS REQUERIDOS (EER)	
EER#1	Plan de Ejecución Plurianual (PEP) / Plan Operativo Anual (POA)
EER#2	Plan de Monitoreo y Evaluación
EER#3	Plan de Adquisiciones

ENLACES ELECTRÓNICOS OPCIONALES (EEO)	
EEO#1	Análisis Económico del Programa A. Hoja de Cálculo
EEO#2	Lógica Vertical
EEO#3	Reglamento Operativo del Programa (ROP)
EEO#4	Anexo de Género
EEO#5	Anexo Técnico G-SOC: ¿qué es y para qué sirve?
EEO#6	Diseño de Alto Nivel G-SOC
EEO#7	Evaluación de Impacto Ciber Funcionarios
EEO#8	Análisis del Marco Jurídico y de Gobernanza
EEO#9	Filtro de Evaluación Ambiental y Social

ABREVIATURAS	
AD	Agenda Digital Argentina
AFIP	Administración Federal de Ingresos Públicos
AGN	Auditoría General de la Nación
ALC	América Latina y el Caribe
APN	Administración Pública Nacional
BCP	Plan de Continuidad de Negocio (por sus siglas en inglés)
BID	Banco Interamericano de Desarrollo
CC	Comité de Ciberseguridad
CERT	Centro de Respuesta a Incidentes de Ciberseguridad
DIPROSE	Dirección de Programas y Proyectos Sectoriales y Especiales
DNCP	Dirección Nacional de Contrataciones Públicas
DPSSYRI	Dirección de Prevención en Seguridad de Sistemas y Redes Informáticas de la SSTI
DRP	Plan de Recuperación de Desastres
ENC	Estrategia Nacional de Ciberseguridad
FMI	Fondo Monetario Internacional
GDE	Gestión Documental Electrónica
G-SOC	Centro de Operaciones de Ciberseguridad del Gobierno
G+T	Centro de Géneros en Tecnología
ICI	Infraestructuras Críticas de Información
ISP	Informe Semestral de Progreso
JGM	Jefatura de Gabinete de Ministros de la Presidencia de la Nación
LPI	Licitación Pública Internacional
LPN	Licitación Pública Nacional
MiPyMEs	Micro, Pequeñas y Medianas Empresas
MR	Matriz de Resultados
OE	Organismo Ejecutor
OEA	Organización de los Estados Americanos
PA	Plan de Adquisiciones
PCR	Informe de Terminación del Proyecto (por sus siglas en inglés)
PIB	Producto Interno Bruto
PEP	Plan de Ejecución Plurianual
PME	Plan de Monitoreo y Evaluación
POA	Plan Operativo Anual
ROP	Reglamento Operativo del Programa
SBCC	Selección Basada en Calidad y Costo
SCA	Secretaría de Coordinación Administrativa de Jefatura de Gabinete
SCC	Selección Basada en las Calificaciones de los Consultores
SIEM	Sistema de Gestión de Eventos de Seguridad (por sus siglas en inglés)
SIP	Secretaría de Innovación Pública
SOC	Centros de Operación de Ciberseguridad (por sus siglas en inglés)

ABREVIATURAS	
SSTI	Subsecretaría de Tecnologías de la Información de la SIP
TDR	Términos de Referencia
TI	Tecnologías de la Información
TIC	Tecnologías de la Información y la Comunicación
TIR	Tasa Interna de Retorno
UEPEX	Unidades Ejecutoras de Préstamos Externos
VPN	Valor Presente Neto

RESUMEN DEL PROYECTO
ARGENTINA
PROGRAMA DE CIBERSEGURIDAD PARA INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN (ICI)
(AR-L1343)

Términos y Condiciones Financieras				
Prestatario:			Facilidad de Financiamiento Flexible ^(a)	
República Argentina			Plazo de amortización:	25 años
Organismo Ejecutor (OE):			Período de desembolso:	5 años
República de Argentina, a través de la Jefatura de Gabinete de Ministros (JGM) de la Presidencia de la Nación			Período de gracia:	5,5 años ^(b)
Fuente	Monto (US\$)	%	Tasa de interés:	Basada en SOFR
BID (Capital Ordinario):	30.000.000	100	Comisión de crédito:	^(c)
			Comisión de inspección y vigilancia:	^(c)
Total:	30.000.000	100	Vida Promedio Ponderada (VPP):	15,25
			Moneda de aprobación:	Dólares de los Estados Unidos de América
Esquema del Proyecto				
Objetivo/descripción del proyecto: El objetivo general de desarrollo consiste en contribuir a la reducción de los costos por incidentes de ciberseguridad para el Estado y la ciudadanía; y los objetivos de desarrollo específicos son: (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 de las ICI priorizadas.				
Condiciones contractuales especiales previas al primer desembolso del financiamiento: El OE deberá presentar al Banco evidencia de la aprobación y entrada en vigencia del Reglamento Operativo del Programa (ROP), en los términos previamente acordados con el Banco (¶3.6).				
Excepciones a las políticas del Banco: Ninguna.				
Alineación Estratégica				
Desafíos ^(d) :	SI <input type="checkbox"/>		PI <input checked="" type="checkbox"/>	EI <input type="checkbox"/>
Temas Transversales ^(e) :	GE <input checked="" type="checkbox"/> y DI <input type="checkbox"/>		CC <input checked="" type="checkbox"/> y ES <input type="checkbox"/>	IC <input checked="" type="checkbox"/>

- (a) Bajo los términos de la Facilidad de Financiamiento Flexible (documento FN-655-1) el Prestatario tiene la opción de solicitar modificaciones en el cronograma de amortización, así como conversiones de moneda, de tasa de interés, de productos básicos y de protección contra catástrofes. En la consideración de dichas solicitudes, el Banco tomará en cuenta aspectos operacionales y de manejo de riesgos.
- (b) Bajo las opciones de reembolso flexible de la Facilidad de Financiamiento Flexible (FFF), cambios en el periodo de gracia son posibles siempre que la Vida Promedio Ponderada (VPP) Original del préstamo y la última fecha de pago, documentadas en el contrato de préstamo, no sean excedidas.
- (c) La comisión de crédito y la comisión de inspección y vigilancia serán establecidas periódicamente por el Directorio Ejecutivo como parte de su revisión de los cargos financieros del Banco, de conformidad con las políticas correspondientes.
- (d) SI (Inclusión Social e Igualdad); PI (Productividad e Innovación); y EI (Integración Económica).
- (e) GE (Equidad de Género) y DI (Diversidad); CC (Cambio Climático) y ES (Sostenibilidad Ambiental); y IC (Capacidad Institucional y Estado de Derecho).

I. DESCRIPCIÓN DEL PROYECTO Y MONITOREO DE RESULTADOS

A. Antecedentes, problemática y justificación

- 1.1 **Contexto macroeconómico.** La actividad económica en Argentina cayó fuertemente entre 2018 y 2020 (14% acumulado), agravada por el COVID-19. Si bien se recuperó 10,3% en 2021, el Producto Interno Bruto (PIB) aún estaba 5,2% por debajo de 2017. Se espera un crecimiento de 4,1% para 2022. La inflación alcanzó 50,9% anual en 2021 y el mercado proyecta una aceleración hasta 100,3 % para 2022. El déficit fiscal primario alcanzó el 6,4% del PIB en 2020, se redujo a 3% en 2021 y acordó con el Fondo Monetario Internacional (FMI) que alcance el 2,5% en 2022. En marzo se firmó un nuevo acuerdo con el FMI para refinanciar los vencimientos del programa anterior y brindar financiamiento adicional, y las dos primeras revisiones del programa fueron aprobadas. En línea a las necesidades de financiamiento externo del país y tras el cumplimiento de la segunda revisión del acuerdo con el FMI, se contó con la aprobación de un Financiamiento Especial para el Desarrollo (SDL) con el BID por US\$700 millones, que se suma al apoyo de otros organismos internacionales de crédito al financiamiento comprometido en el acuerdo con el FMI.
- 1.2 Según el [Foro Económico Mundial](#), la rápida digitalización expone a las economías a vulnerabilidades cibernéticas nuevas y más intensas, ya que las nuevas tecnologías y una superficie de ataque en constante expansión permiten una gama más diversa y peligrosa de delitos cibernéticos. Esto puede tener efectos económicos graves y dificultar la recuperación post pandemia, por lo que los ataques cibernéticos constituyen el séptimo riesgo más importante que enfrentan las economías del mundo (por debajo del deterioro en salud mental y por encima de crisis de deuda). También, son costosos: el costo del cibercrimen a nivel mundial superó los [US\\$6 billones](#) en 2021. En este contexto, América Latina y el Caribe (ALC) no está preparada para enfrentar estos riesgos: según el informe Banco Interamericano de Desarrollo (BID) - Organización de los Estados Americanos (OEA) (2020), su capacidad de ciberseguridad tiene un nivel apenas de “formativo”, es decir, que se ha comenzado a crecer en algunos aspectos, pero de forma desorganizada y/o con procesos poco definidos¹.
- 1.3 En el caso de Argentina, 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 tecnológicas 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 telecomunicaciones; (ii) desarrollar habilidades digitales; (iii) adoptar nuevas tecnologías en el sector productivo; y (iv) gestionar correctamente la ciberseguridad².
- 1.4 En esta línea, el país ha llevado a cabo numerosas iniciativas para proteger su ciberespacio. En 2011 crea el [Programa Nacional de Infraestructuras Críticas de](#)

¹ [Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en ALC.](#)

² [Agenda Digital Argentina](#) (AD).

[Información \(ICI\)](#)³ [y Ciberseguridad](#); en 2017 el Comité de Ciberseguridad (CC) para desarrollar una estrategia nacional de seguridad cibernética⁴; y en 2019, aprueba su Estrategia Nacional de Ciberseguridad ([ENC](#))⁵ incluyendo la protección de ICI, regulaciones sobre privacidad en el uso de datos personales en la APN y buenas prácticas en el uso de las Tecnologías de la Información y la Comunicación (TIC)⁶, entre otros.

- 1.5 Esto ha permitido que Argentina se ubique por encima del valor promedio de ALC en el Índice Global de Ciberseguridad del *International Telecommunication Union* (ITU), con un puntaje de 50,12, ocupando 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 (OCDE), 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 digitalización⁷. En efecto, la elevada penetración de las TIC⁸, incrementa vulnerabilidades, incidentes potenciales, e impactos que pueden generarse al aumentar la “superficie de ataque”⁹. Por el lado del sector privado, 53% de las empresas no tienen estrategias de ciberseguridad y el 61% no cuentan con planes de contingencias ante incidentes¹⁰.
- 1.6 Desarrollar capacidades en ciberseguridad requiere la correcta gestión¹¹ de cinco funciones básicas: (i) identificar qué activos 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 medidas¹²; y (v) recuperarse ante los daños causados por estos incidentes. Para todo ello es indispensable contar con organización, políticas, procesos, personas y tecnologías especializados.
- 1.7 **Gobernanza de la ciberseguridad en Argentina.** El marco normativo argentino da las atribuciones de protección de ICI a la Secretaría de Innovación Pública¹³

³ Creado mediante Resolución 580/2011. Infraestructuras Críticas son aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, tales como la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, y cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente. En tanto que las ICI son aquellas tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas. Resolución 1523/19, (ex) Secretaría de Gobierno de Modernización.

⁴ [Decreto 577/2017](#). Ver ¶3.4.

⁵ Aprobada mediante Resolución 829/2019 de la Secretaría de Gobierno de Modernización, y es producto de la operación [4755/OC-AR](#) (¶1.16).

⁶ Resolución No. 40/2018 de la Agencia de Acceso a la Información Pública. Disposición No. 2/2018 y No. 3/2018 de la ONTI (“Decálogo Tecnológico”).

⁷ Entre 2016 y 2022 el número de usuarios de trámites a distancia incrementó 220% ([20.793.925 trámites digitales](#)).

⁸ Decreto [733/2018](#) establece la obligación de la APN de digitalizar todos los trámites relacionados con el ciudadano.

⁹ En 2021 fueron 27,1 billones los dispositivos conectados y el tráfico per cápita era de 35 GB/mes, aumentando la [superficie de ataque](#). <https://gblogs.cisco.com/>.

¹⁰ <https://www.pwc.com.ar/>.

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

¹² Son acciones que se implementan cuando se ha detectado un incidente de ciberseguridad para contener su potencial impacto.

¹³ En ese año se trataba del Ministerio de Modernización. Actualmente la SIP depende de la Jefatura de Gabinete de Ministros (JGM). Ver Decreto 123/2022, como normativa vigente reglando la SIP y SSTI en la estructura de JGM.

(SIP) mediante el decreto 577/2017 y sus modificatorias y la resolución 141/2019, quien como presidente del CC¹⁴ debe desarrollar e implementar la ENC y fijar los lineamientos y criterios para la definición, identificación y protección de las ICI. En particular, la SIP es responsable de “entender en la ciberseguridad y protección de ICI y comunicaciones asociadas del Sector Público Nacional y de los servicios de información y comunicaciones” A su vez, la Subsecretaría de Tecnologías de la Información de la SIP (SSTI), perteneciente a la SIP, tiene entre sus funciones “proponer a la Secretaría estrategias, estándares y regulaciones para la ciberseguridad y protección de ICI y las comunicaciones asociadas del Sector Público Nacional y de los servicios de información y comunicaciones”¹⁵. Sin embargo, estas agencias aún carecen de recursos financieros, humanos y tecnológicos especializados para cumplir cabalmente con estas funciones.

- 1.8 **Problema y desafíos.** El principal problema identificado es el alto costo de los incidentes de ciberseguridad para el Estado¹⁶ y la ciudadanía¹⁷. 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 categoría¹⁸. Esto se debe a la limitada capacidad del país para gestionar las funciones básicas de la ciberseguridad de las ICI¹⁹, asociado a los siguientes factores:
- 1.9 **Limitaciones en los esquemas de gobernanza.** Según el diagnóstico presentado en [EEO#8](#), destacan una serie de limitaciones institucionales y normativas relacionadas principalmente con²⁰:
 - (i) la SIP posee atribuciones centradas exclusivamente en los aspectos normativos y procedimentales de la ciberseguridad pública, por lo que en la práctica la dirección operativa nacional de la ciberseguridad es débil;

¹⁴ A partir de 2019 (Resolución 141) el CC pasa a depender del Secretario de Gobierno de Modernización, que a su vez depende de la JGM.

¹⁵ Definidos en el artículo primero de la Ley N° 27.078 (objetivo incorporado por art. 4° del Decreto N° 139/2021 B.O. 5/3/2021. Ver [EEO#8](#).

¹⁶ 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.

¹⁷ Los impactos económicos estimados de incidentes cibernéticos en Argentina en 2021 fueron equivalentes US\$1.141 millones, siendo US\$4.434,4 del sector público y US\$700,6 de la ciudadanía ([EEO#1](#)).

¹⁸ <https://www.gub.uy/>.

¹⁹ Según el Modelo de Madurez de Capacidad de Ciberseguridad para las Naciones de los 24 factores que conforman sus cinco dimensiones ((i) política y estrategia de ciberseguridad; (ii) cultura cibernética y sociedad; (iii) educación, capacitación y habilidades en ciberseguridad; (iv) marcos legales y regulatorios; y (v) estándares, organizaciones y tecnologías), en Argentina 5% de ellos estaban en la etapa “inicial”; 50% en la “formativa”; 40% en la “consolidada”; 5% en la “estratégica” y ninguno en la “dinámica”. www.observatoriociberseguridad.com. Ibid1.

²⁰ “El modelo actual carece de una entidad de gobierno central de la ciberseguridad desde el punto de vista operativo. Es decir, una entidad que se responsabilice de la adecuada dirección centralizada (atendiendo siempre a la estrategia marcada por los órganos superiores) en materia de recursos, métodos, procedimientos, herramientas, sensibilización, formación y cooperación nacional e internacional en materia de ciberseguridad, sus tecnologías y sus condicionantes jurídicos”. Idem, págs 91 a 93.

- (ii) frágil capacidad de análisis del ecosistema nacional de la ciberseguridad²¹, comprensivo de todos los actores implicados: sector público, privado y ciudadanos;
 - (iii) dispersión organizacional ante amenazas de incidentes y procedimientos de prevención y respuesta, afectando su eficacia e inmediatez, incrementando así las consecuencias de los ataques;
 - (iv) limitados mecanismos de intercambio de información sobre riesgos e incidentes que permitan articular métodos, procedimientos y herramientas para garantizar que lo que es conocido por una entidad pueda, de manera inmediata, ser conocido por todas aquellas entidades que puedan ser afectadas; y
 - (v) los organismos públicos con competencias en la provisión de servicios de ciberseguridad suelen hacer uso de herramientas individuales propietarias que impiden o dificultan una postura común a las amenazas del ciberespacio, sin ningún tipo de estandarización en las herramientas, métodos y procedimientos²² utilizados para la defensa.
- 1.10 Estas limitaciones dificultan: (i) priorizar los activos a proteger según su nivel de riesgo; (ii) coordinar transversalmente el diseño e implementación de planes de protección de ICI; y (iii) la implementación rápida de la ENC ya que, si bien la JGM y el CC han definido lineamientos para identificar una ICI²³, sólo el Sistema de Gestión Documental Electrónica (GDE)²⁴ ha sido identificado y aún no se ha desarrollado ningún plan para su protección.
- 1.11 **Baja cobertura de la SIP para identificar y proteger ICI.** De los 11 sectores clasificados como críticos desde 2019, a saber, Energía, TIC, Transportes, Hídrico, Salud, Alimentación, Finanzas, Nuclear, Químico, Espacio y Estado²⁵, solo el sistema GDE²⁶ del Sector Estado fue declarado como ICI, lo que impide determinar los riesgos cibernéticos y definir planes de protección para los sistemas de información del resto de los sectores. Países como Israel han identificado 40 ICI y 300 sistemas de información anexos a las mismas.
- 1.12 **Baja productividad en la gestión de incidentes cibernéticos (detección, respuesta y recuperación).** Cuando estas capacidades son limitadas, los incidentes se detectan una vez que ya han iniciado la producción de daño y este tiende a aumentar mientras sigan sin solucionarse. 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 año²⁷. Esto se debe a que: (i) actualmente no es posible monitorear, en tiempo real, ataques y amenaza a las ICI, actividad que en otros contextos se realiza a través de un

²¹ Se entiende por ecosistema nacional de ciberseguridad, al conjunto de organizaciones públicas, privadas, académicas y de sociedad civil, que intervienen de forma coordinada en el desarrollo de la ciberseguridad de un país.

²² Por ejemplo, no existe un protocolo para identificación de activos informáticos a proteger ni su nivel de riesgo.

²³ Aprobada mediante Resolución 1523/2019. <https://www.argentina.gob.ar/normativa/nacional/>.

²⁴ Es un sistema para la gestión de los procesos internos del Estado, desplegada en el gobierno federal, 18 provincias y 80 municipios.

²⁵ <https://www.argentina.gob.ar/>.

²⁶ Resolución 36/2020 declaró el GDE como ICI del Estado. <http://www.saij.gob.ar/>.

²⁷ Se estima que en Argentina ocurre un número elevado de incidentes que no son detectados CERT Nacional, y que también generan impactos y costos de ciberseguridad.

Centro de Operaciones de Ciberseguridad del Gobierno (G-SOC)²⁸ (§1.20); (ii) la plataforma tecnológica con que cuenta el Centro de Respuesta a Incidentes de Ciberseguridad ([CERT.ar](#)) Nacional²⁹ solo permite el registro de incidentes y el seguimiento de los mismos, sin contar con capacidades para la prevención y gestión de su respuesta³⁰; y (iii) los mecanismos de intercambio de información relativa a ataques e incidentes de ciberseguridad no ofrecen la confidencialidad y seguridad requerida por los actores para colaborar oportunamente, dificultando la capacidad de prevención y respuesta ante dichos ataques.

- 1.13 **Escasez de profesionales en ciberseguridad** que es considerada como uno de los obstáculos globales en la materia³¹ y, particularmente en la región³². En Argentina se observa un estancamiento de la capacidad de formación de profesionales especialistas en esta materia, pese a la gran demanda de formación de los funcionarios en estas temáticas. En efecto, las universidades con carreras oficiales en ciberseguridad cuentan con una matriculación que no se ha incrementado significativamente en los últimos años, y actualmente es inferior a 400 estudiantes, de los cuales se identifica una brecha de género, ya que solo el 15% de las estudiantes son mujeres ([EEO#4](#))³³. Ello se refleja en los indicadores de madurez, en la dimensión de Desarrollo de Conocimiento y Capacidades, del [Reporte Regional de Ciberseguridad](#) realizado por la OEA y el BID, que se mantuvieron prácticamente estancados, en la etapa “formativa” (segundo nivel de cinco). Como contracara, el rápido crecimiento en la demanda de estos especialistas (§1.5) produjo una brecha con su oferta educativa, generándose una importante escasez, lo que a su vez impacta la capacidad de gestión del ciberespacio³⁴. Mientras que las buenas prácticas internacionales muestran que las agencias más maduras en ciberseguridad ocupan aproximadamente entre 5% y 10% de su personal de Tecnologías de la Información (TI) a la ciberseguridad³⁵, en la APN Argentina solo organizaciones maduras como la Administración Federal de Ingresos Públicos (AFIP)³⁶ o la Empresa Argentina de Soluciones Satelitales (ARSAT)³⁷, cumplen con esta relación. A esta falta de especialistas en la materia se suman los problemas de competencias en ciberseguridad de los empleados en

²⁸ Unidad técnica especializada en la detección y primera respuesta a incidentes de ciberseguridad.

²⁹ Funciona como una dependencia de la Dirección Nacional de Ciberseguridad ([CERT.ar](#)), y se especializa en la respuesta a incidentes complejos.

³⁰ Por ejemplo, a causa de esto no fue posible detectar de forma temprana la filtración de datos del Registro Nacional de las Personas (RENAPER) en el año 2021, generando esto un alto impacto negativo en su rol de resguardo de datos de ciudadanos.

³¹ La oferta de profesionales en ciberseguridad a nivel mundial debería aumentar en un 65% para poder cubrir la necesidad. <https://www.cyberseek.org/heatmap.html>.

³² Según el Estudio de la Fuerza Laboral en Ciberseguridad realizado en 2021 (ICS2, 2021), se estima que en la región hacen falta más de 500 mil profesionales en ciberseguridad para satisfacer las necesidades que los empleadores tienen actualmente.

³³ Datos obtenidos de las universidades: Universidad de Buenos Aires, Universidad de la Plata, Universidad de Defensa y Universidad Nacional Escalabrini Ortiz.

³⁴ A pesar de que los profesionales de ciberseguridad ganan considerablemente más que los programadores: 11% más en Estados Unidos, según cifras del [Bureau of Labor Statistics](#) (2021), y hasta 50% más en Uruguay, según la Cámara Uruguaya de Tecnologías de la Información (2019), hay una escasez de demanda de parte de los estudiantes que pocas veces es rentable emplear a profesores especializados (UDELAR, 2019).

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

³⁶ Cuenta con 986 funcionarios en TI (27% femenino) de los cuales 121 (28% femenino) están en ciberseguridad. SIP, 2022.

³⁷ Tiene 761 funcionarios. De estos, 143 trabajan en áreas de TI (18% femenino), siendo 27 los que están en ciberseguridad. ARSAT, 2022.

general, que son los usuarios de los diferentes sistemas y plataformas sujetas a ciberataques. Más de dos tercios de los ciberataques en las organizaciones se producen como resultado de negligencia de parte de un empleado³⁸.

- 1.14 **Diagnóstico de género en el mercado laboral de la ciberseguridad.** A nivel global, las mujeres representan solo el 25% de la fuerza de ciberseguridad (Microsoft, 2021)³⁹. Al analizar las brechas de género de profesionales en TI en el Estado Nacional Argentino, observamos por ejemplo que, en AFIP dentro de la Dirección de Seguridad de la Información, las mujeres solo representan el 28,1% del total de trabajadores. En la empresa de telecomunicaciones estatal ARSAT se mantiene esta brecha, donde las mujeres representan el 27% de la nómina laboral. La SSTI cuenta con un total de 34 agentes⁴⁰, de los cuales el 40% son mujeres. El abordaje de la ciberseguridad y el género en el país se encuentra en una etapa incipiente, en la que resalta la experiencia del Centro de Géneros en Tecnología (G+T)⁴¹, del que forma parte la SSTI junto al Instituto Nacional de Educación Tecnológica (INET) del Ministerio de Educación. Dentro de los diversos ejes temáticos que componen al centro, uno que se enfoca en Ciberseguridad busca promover iniciativas para potenciar la capacitación a mujeres, en seguridad digital, así como la reducción de la brecha de géneros en ciencia, tecnología, ingeniería y matemáticas.
- 1.15 **Baja eficacia en la gestión de la ciberseguridad de la ICI priorizada.** En 2019, a través del [GDE](#)⁴² se habían testeado 10.538.180 expedientes electrónicos⁴³, incluyendo caratulación, numeración, seguimiento y registro de movimientos de todas las actuaciones y expedientes de la APN. Para enero 2022, ya eran 35.998.117. Pese a la importancia de esta ICI, las últimas dos auditorías integrales realizadas⁴⁴ sobre su ecosistema⁴⁵ indican incumplimientos graves como: (i) una política de ciberseguridad inadecuada; (ii) incorrecta gestión de riesgos cibernéticos; (iii) planes de continuidad de negocio y recuperación ante desastres defectuosos; y (iv) una estructura organizacional incorrecta para gestionar la ciberseguridad; entre otros hallazgos.
- 1.16 **Experiencia del Banco en la región, el país y el sector.** El Banco cuenta con amplia experiencia en el diseño e implementación de proyectos relacionados con transformación digital y ciberseguridad. En Argentina, el Programa para el Fortalecimiento de la Agenda Digital, la Conectividad, el Gobierno Electrónico y la

³⁸ *Cybintsolutions*, 2020.

³⁹ En una encuesta realizada por *Microsoft* para indagar sobre las razones de la brecha de género existente, resultó que 56% de las mujeres consultadas respondieron no estar debidamente representadas en la industria. Las mujeres visualizan en mayor medida la existencia de un sesgo de género en la industria que resulta en salarios y apoyos desiguales.

⁴⁰ Incluyendo personal administrativo, asistentes técnicos y profesionales.

⁴¹ Se trata de un consorcio de organismos públicos, empresas TIC y organizaciones de la sociedad civil para la promoción de políticas de inclusión que buscan reducir la brecha de géneros en el sector TIC mediante colaboración público-privada. [Centro-gt](#).

⁴² Todos los ministerios y 86% de organismos públicos nacionales utilizan GDE.

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

⁴⁴ Auditorías realizadas por la Auditoría General de la Nación (AGN) en 2019 y por la Fundación Sadosky en 2020.

⁴⁵ El ecosistema del GDE incluye módulos como Comunicaciones Oficiales, Generador Electrónico de Documentos Oficiales y Expediente Electrónico, Trámites a Distancia, Legajo Único Electrónico, Locación de Obras y Servicios, Registro Legajo Multipropósito, Gestor de Asistencias y Transferencias, Registro Integral de Destinatarios, Registro Civil Electrónico, Firma Digital, Autenticación Electrónica, entre otros.

Transformación Productiva ([4755/OC-AR](#)) aprobado en 2019 por US\$300 millones y actualmente cerrado, apoyó al gobierno en la implementación de políticas relacionadas con ICI y seguridad de datos, y tuvo como uno de sus productos la ENC y Protección de ICI (§1.4). Siguiendo lo recomendado en el [Informe de Terminación del Proyecto](#) (PCR, por sus siglas en inglés) de dicho programa, la presente operación da continuidad a la implementación de la agenda digital del país, en particular respecto a las políticas de seguridad de datos, fortaleciendo la resiliencia digital de los actores económicos y mejorando la calidad de vida y el bienestar de las personas. A nivel regional, proyectos tales como Fortalecimiento de la Ciberseguridad en Uruguay ([4843/OC-UR](#)) aprobado en 2019, primer proyecto específico de ciberseguridad de la región; proyectos de transformación digital con grandes componentes de ciberseguridad, como: Panamá en Línea ([3683/OC-PN](#)) de 2016, Transformación Digital del Gobierno para Fortalecer la Competitividad ([4549/OC-BH](#)) de 2018, Proyecto de mejoramiento y ampliación de los servicios de soporte para la provisión de servicios a los ciudadanos y las empresas a nivel nacional ([4399/OC-PE](#)) de 2017, Programa de Apoyo a la Implementación de la AD ([4650/OC-PR](#)) de 2018, Programa de Gestión Estratégica de la Seguridad en Chile ([4891/OC-CH](#)) de 2019, Programa de Fortalecimiento del Poder Judicial de Ceará ([5248/OC-BR](#)) de 2020, Programa de Transformación Digital del Estado de Ceará ([5516/OC-BR](#)) de 2022. Además, el Banco ha contado con el apoyo técnico y financiero de los gobiernos de España e Israel a través de las cooperaciones técnicas: (i) de investigación y diseminación: que ya cerraron “Mejora de la Capacidad de los Recursos Humanos en Ciberseguridad” ([ATN/CF-15598-RG](#)) aprobada en 2016 por US\$3 millones, y Fortalecimiento de la Ciberseguridad en ALC ([ATN/FG-16633-RG](#)) de 2018 por US\$500.000, y su continuación con el mismo título, ([ATN/CF-19154-RG](#)) de 2022 por US\$2 millones y aún en ejecución; y (ii) de apoyo al cliente: “Digitalización para el Desarrollo Socioeconómico inclusivo en tiempos de COVID-19” ([ATN/FG-18691-RG](#)) de 2021 por US\$3 millones; que han financiado la realización de actividades de capacitación y estudios que constituyen un insumo fundamental para el diseño de esta operación.

- 1.17 **Complementariedad con otras operaciones del Banco en Argentina.** Este proyecto complementa al: (i) Programa para el Desarrollo de la Red Federal de Fibra Óptica (REFEFO) ([5364/OC-AR](#)) de 2021 por US\$100 millones, con 5,4% desembolsado y en ejecución, que impulsará el acceso a internet y la digitalización de Argentina; (ii) Programa de Apoyo a la Gestión Integrada del Gasto Público ([4802/OC-AR](#)) de 2019 por US\$40 millones, con 18,2% desembolsado y en ejecución, que financia el desarrollo y renovación de ICI para la mejora de la eficiencia y transparencia del gasto público; y (iii) Transformación Digital ([ATN/OC-17583-AR](#)) de apoyo operativo, aprobada en 2019 por US\$300.000, que apoya la implementación de la Agenda Digital, incluyendo el plan de protección de ICI. También se complementa con operaciones en preparación, como: (i) Línea de Crédito Condicional para Proyectos de Inversión (CCLIP): Inversiones para promover la descarbonización del sector energético en Argentina ([AR-O0020](#)) por US\$1.140 millones y su primera operación individual Programa Federal de Transporte de Energía Eléctrica ([5564/OC-AR](#)) aprobada en julio de 2022 por US\$200, pendiente de firma, que financiará la introducción de sistemas de información innovadores para la modernización de los sistemas de transporte de energía eléctrica (energía es sector crítico, §1.11), el presente programa favorecerá la ciberseguridad de las ICI

que se financiarán con estos programas; y (ii) Programa de Apoyo a Micro, Pequeñas y Medianas Empresas (MiPyMEs) para la Transformación Digital hacia Industria 4.0 ([5570/OC-AR](#)), aprobada en agosto de 2022 por US\$80 millones, pendiente de firma, pues al mejorar el entorno de ciberseguridad del país, favorecerá la transformación digital de estas.

- 1.18 **Lecciones aprendidas.** En la preparación del programa se consideran mejores prácticas internacionales en seguridad, [productos de conocimiento](#) y lecciones aprendidas de operaciones similares del Banco en la región (§1.16). Entre ellas se encuentra la importancia de: (i) fortalecer la institucionalidad y liderazgo del organismo responsable de la ciberseguridad en el país (SIP) dotándolo de los marcos regulatorios, herramientas tecnológicas y talento humano necesario para dirigir el proyecto en el país; (ii) la coordinación interinstitucional y el enfoque en el ecosistema considerando instituciones públicas, privadas, académicas y de la sociedad civil; y (iii) la formación de talento para asegurar la disponibilidad de profesionales y servicios durante la ejecución y al finalizar el proyecto. Todas estas fueron incorporadas a las diferentes actividades previstas en los componentes del programa (ver §1.25, §1.26 y §1.27).
- 1.19 Además, por lo innovador del tipo de tecnologías y servicios que componen el programa, adelantar los procesos de compras estratégicas de tecnologías y servicios complejos, realizando procesos de *request for information*, con Términos de Referencia (TDR) y especificaciones técnicas según estándares internacionales -para ajustar los requerimientos junto con los líderes de la industria-, colaborará para que el ecosistema de empresas del rubro instaladas en el país se pueda preparar mejor para el diseño y entrega de servicios de manera local. Esto se realizará con el apoyo de consultores expertos, que serán financiados con asistencia técnica no reembolsable ([ATN/OC-17583-AR](#)) (§1.17). En cuanto a capacitación y entrenamiento, el uso de plataformas de simulación ha demostrado ser rápido y efectivo en operaciones de ciberseguridad⁴⁶. En este sentido, la simulación de operaciones de ciberseguridad ya sea con el objetivo de aprendizaje, o de evaluación, se utilizan plataformas *CyberRange*⁴⁷. Estas plataformas virtuales simulan escenarios complejos de TIC donde se ejecutan ataques complejos en entornos controlados. Los principales beneficios de estas plataformas son la generación de habilidades operativas de ciberseguridad mediante el uso de técnicas de simulación⁴⁸.
- 1.20 **La experiencia y buenas prácticas internacionales** también resaltan la importancia de los Centros de Operación de Ciberseguridad (SOC, por sus siglas en inglés) ([EEO#5](#)) como una herramienta fundamental. Tienen como principal función la gestión de incidentes informáticos⁴⁹. Los SOC específicos para

⁴⁶ El mismo efecto se produce la incorporación de competencias o juegos, lo que se conoce como “Edutainment” donde combinando actividades de entrenamiento con componentes lúdicos se consiguen buenos resultados de aprendizaje. [Simulating Cyber Operations: A Cyber Security Training Framework](#), SANS Bryan K. Fite, 2014.

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

⁴⁸ De esta manera, sus usuarios pueden analizar y entrenarse en la forma de detectar y solucionar estos problemas, e incluso en desarrollar herramientas tanto defensivas como ofensivas. El concepto de simulación es bien conocido en el mundo aeronáutico o militar, por ejemplo, donde se simulan escenarios, pero en caso de un fallo no produce impacto real y se vuelve a comenzar la prueba. Estas plataformas hacen lo mismo, pero en el contexto de ciberseguridad. [SANS Bryan K. Fite, 2014](#).

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

gobiernos se conocen como G-SOC y monitorean, en tiempo real, los sistemas informáticos detectando, respondiendo y recuperando dichos sistemas ante incidentes de manera muy efectiva. Ejemplos de estos G-SOC podemos encontrarlos en países avanzados como España⁵⁰ e Israel⁵¹. Los G-SOC ofrecen una gran diversidad de servicios de ciberseguridad, pero su principal función es la detección y respuesta a incidentes de ciberseguridad. Para esto utilizan “sondas”⁵² distribuidas en los diferentes sistemas de información a ser monitoreados, las cuales analizan todos los eventos del sistema buscando actividad sospechosa que podría tratarse de un ataque. Toda la información analizada es enviada a un sistema central llamado Sistema de Gestión de Eventos de Seguridad (SIEM, por sus siglas en inglés) el cual la procesa, correlaciona y en tiempo real indica si se trata de un ataque. En ese momento comienza el proceso de respuesta, el cual puede ser automatizado o con intervención humana.

- 1.21 **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 (§1.25). También se alinea con los temas transversales: (i) Equidad de Género, a través de la inclusión de acciones destinadas a aumentar la participación de las mujeres en el sector (§1.14, §1.22, §1.26); (ii) Cambio Climático, ya que el 8,57% de los recursos de la operación se invierten en actividades de mitigación al cambio climático por la adquisición de equipos informáticos de alta eficiencia energética ([categoría A](#)), según la [Metodología conjunta de los Bancos Multilaterales de Desarrollo](#), contribuyendo así a la meta de financiamiento climático del BID (30% del volumen de aprobaciones anual); y (iii) Capacidad Institucional y Estado de Derecho, al fortalecer la capacidad para proteger el espacio digital y la expansión segura del sector digital (§1.25, §1.26, §1.27). Además, contribuirá al indicador del nivel 2 del Marco de Resultados Corporativos (CRF) 2020-2023 (GN-2727-12) de: 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. 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 (§1.26); y (ii) gobierno digital, al dar mayor seguridad a la expansión del sector (§1.27). Finalmente, la operación se encuentra incluida en la Actualización del Anexo III del Informe sobre el Programa de Operaciones de 2022 (GN-3087-2).
- 1.22 **Acciones de género.** Se incorporarán a través de: (i) desarrollo de programas técnicos y de certificación en ciberseguridad, donde se priorizará la inclusión de mujeres, en coordinación con el G+T; y (ii) asistencia técnica para elaborar un diagnóstico y plan de acción de género que permita trazar un curso de diferentes acciones para reducir brechas de género en Ciberseguridad dentro de la SSTI.

⁵⁰ <https://www.ccn-cert.cni.es/>.

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

⁵² Se trata de un sistema tecnológico que tiene la capacidad de monitorear los eventos de ciberseguridad, alertar y/o actuar para evitar un posible ataque.

B. Objetivos, componentes y costo

- 1.23 **Objetivo general de desarrollo:** Consiste en contribuir a la reducción de los costos por incidentes de ciberseguridad para el Estado y la ciudadanía.
- 1.24 **Objetivos de desarrollo 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 de las ICI priorizadas. Contará con los siguientes componentes:
- 1.25 **Componente 1. Fortalecimiento de las capacidades institucionales y tecnológicas de la SIP (US\$20 millones).** Financiará: (i) mejoras en el diseño e implementación del marco institucional y normativo para la identificación y protección de ICI⁵³; (ii) creación de un G-SOC⁵⁴ para el monitoreo y detección de ataques, dotándolo de herramientas SIEM⁵⁵ y sensores⁵⁶; (iii) fortalecimiento de las capacidades operativas del CERT Nacional⁵⁷; y (iv) desarrollo de plataformas para el análisis de amenazas e intercambio de información dentro del sector público y con el sector privado⁵⁸.
- 1.26 **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 ciberseguridad⁵⁹, priorizando mujeres; (iii) *software* de *e-Learning* para formar profesionales, considerando capacitación básica para funcionarios usuarios de los sistemas institucionales⁶⁰ y accesibilidad para personas con

⁵³ Se realizará un análisis del programa nacional de protección de ICI (2011) para evaluar los resultados y en función de ello proponer, desarrollar e implementar un nuevo programa que se ejecutará a través de los entes reguladores. Se diseñarán planes de protección para cada ICI identificada, esperando contar con al menos una en la mitad de los sectores al final del proyecto. Esto, puesto que actualmente la única ICI identificada es el GDE. Ver ¶1.10 y ¶1.15.

⁵⁴ Se creará una unidad organizacional. Se apoyará con el diseño de esta, así como el desarrollo de sus políticas y procesos, capacitación del personal, contratación de empresas de servicios profesionales (i.e. servicios de monitoreo, respuesta a incidentes, análisis de vulnerabilidades, entre otros) e infraestructura tecnológica.

⁵⁵ Son herramientas que integran el análisis de incidentes con su gestión, al mostrar anomalías en el comportamiento del usuario y utilizar inteligencia artificial para automatizar muchos de los procesos manuales asociados con la detección de amenazas y la respuesta a incidentes. [What is Security Information and Event Management \(SIEM\)? | IBM](#).

⁵⁶ Todas las adquisiciones de herramientas tecnológicas (*hardware* y *software*) considerarán una cláusula de mantenimiento de las mismas.

⁵⁷ Las acciones de fortalecimiento del G-SOC y del CERT Nacional permitirán la detección de más incidentes. Al detectarlos de forma temprana y centralizada, estos incidentes finalmente no lograrían generar daño en la organización atacada, por lo que la misma no incurrirá en ningún gasto de recuperación. Entre las acciones a financiar se incluyen: consultorías para el diseño, producción y mantenimiento, despliegue y operación del Programa Nacional de Sondas y la Plataforma de Agregación de Eventos; servicios de ciberseguridad preventiva, servicios avanzados en ciberseguridad, y la adquisición de equipos informáticos con sello de eficiencia energética.

⁵⁸ Actualmente el marco normativo no los obliga a compartir información con el CERT Nacional.

⁵⁹ Priorizando instituciones que tengan alguna ICI, se desarrollará al menos un programa de formación técnica por año bajo estándares ISO 17024 que permita la certificación de los profesionales. Se incluirán acciones de promoción de género para aumentar la participación de mujeres a través de campañas y espacios de difusión en alrededor de 30 ciudades del país donde operen eventuales ICI, así como el apoyo a nuevas ediciones del programa [Cyberwomen Challenge](#). Ver ¶1.22.

⁶⁰ Se realizará una evaluación del estado de conocimiento de los funcionarios públicos (a través de campañas de *phishing*) y se desarrollarán programas en distintas temáticas de ciberseguridad para los usuarios de la administración pública, incluyendo un sistema de soporte y consulta de contenidos.

discapacidad; y (iv) planes de gestión del cambio y desarrollo curricular en ciberseguridad, incluyendo una propuesta de alineación entre el desempeño del funcionario como un buen vigilante de la ciberseguridad, e incentivos tangibles relacionados a su carrera⁶¹.

- 1.27 **Componente 3. Mejoramiento de la protección del ecosistema del GDE (US\$3 millones).** Financiará: (i) la formulación e implementación de una política de ciberseguridad considerando: análisis de brechas de ciberseguridad del GDE; Plan de Continuidad de Negocio (BCP); y Plan de Recuperación de Desastres (DRP); (ii) implementación de tecnologías de respaldo de información para el GDE; y (iii) desarrollo de capacitaciones y entrenamientos sobre ciberseguridad para el personal técnico y usuarios del ecosistema del GDE⁶².
- 1.28 **Administración, supervisión, evaluaciones y auditoría (US\$2 millones).** Con estos fondos se financiarán gastos administrativos, seguimiento, evaluaciones, incluyendo la evaluación estratégica y auditoría del programa. Se prevé también la evaluación de impacto del programa.
- 1.29 Los gastos elegibles que financiará el programa contemplan consultorías especializadas, y bienes y servicios distintos de consultorías (incluyendo la adquisición de equipamiento, *software* y capacitación)⁶³.

C. Indicadores clave de resultados

- 1.30 **Resultados esperados.** El objetivo general de desarrollo “Ahorro en los costos de gestión por incidentes de ciberseguridad para el Estado y la sociedad” se derivará de un aumento del nivel de madurez de capacidad de seguridad cibernética nacional y una reducción de costos anuales de gestión de incidentes cibernéticos. El logro de los objetivos de desarrollo específico se medirán a través de: (i) aumento de la cobertura de gestión para la identificación y protección de las ICI y de los ministerios monitoreados a través del G-SOC, medido mediante la cobertura de sectores con ICI identificadas y cantidad de ministerios monitoreados; (ii) mejoras en la productividad en la gestión de ciberseguridad derivada del incremento de incidentes gestionados y la reducción en la proporción de los mismos clasificados con severidad alta o crítica; (iii) mujeres de la SIP certificadas en ciberseguridad e instituciones con capacidades gerenciales y de tecnología digital reforzadas; y (iv) mejoras en la eficacia en la gestión de la ciberseguridad en las ICI priorizadas, derivadas del aumento de los hallazgos resueltos y la realización de pruebas exitosas ante problemas informáticos.
- 1.31 **Beneficiarios.** Los directos serán los ciudadanos, empresas y las organizaciones operadoras de ICI, entre ellos el GDE, con un aproximado de 3.300.000 usuarios, que al ver mejorados los servicios de ciberseguridad ofrecidos por la SIP, verán incrementados sus ahorros ante incidentes de ciberseguridad y una mayor

⁶¹ La estrategia de gestión del cambio permitirá: (i) la generación y difusión de conocimiento específicos en ciberseguridad a través de eventos de alto impacto a nivel nacional e internacional; (ii) una mayor retención y estímulo de los profesionales en ciberseguridad mediante planes de incentivos; y (iii) mayor oferta de programas de formación en instituciones académicas que permitan también una mayor disponibilidad de profesionales formados en estas áreas de experiencia.

⁶² El fortalecimiento de las capacidades de gestión del personal del Ecosistema del GDE es indispensable para asegurar el éxito de los sistemas de respaldo de información que financiará el componente. Tanto la tecnología como el entrenamiento del equipo que la opera permitirán aumentar el número exitoso de pruebas de recuperación efectuadas y, por lo tanto, mejorar la eficacia de la gestión del ecosistema del GDE, única ICI actualmente identificada.

⁶³ Se estima un 40% para consultorías y 60% para bienes y servicios.

protección de sus datos. Los indirectos serán los agentes públicos, en particular mujeres (aproximadamente 80 agentes de la SIP serán certificadas en ciberseguridad), debido a que su capacidad profesional en ciberseguridad se verá mejorada. También, las instituciones públicas en general ya que su infraestructura tecnológica estará más protegida como resultado del proyecto.

- 1.32 **Evaluación económica.** La evaluación económica, realizada mediante un análisis costo-beneficio ([EEO#1](#)), considera dos tipos de beneficios⁶⁴: disminución (i) de los costos operativos en remediación de los daños causados por ciberataques a las instituciones públicas, por una reducción en el número de incidentes que son de alta severidad, que son los que conllevan un mayor costo operativo unitario; y (ii) en el impacto económico negativo causado por los ciberataques a las instituciones públicas, gracias a una mayor capacidad de prevención y respuesta. Cada segmento del análisis y estimación de beneficios cuenta con supuestos y metodología propia. Para el cálculo de la rentabilidad, se utilizó una tasa de descuento del 12%, estándar para el Banco, y un plazo de contabilización de beneficios de ocho años, esto es, cinco años de implementación del proyecto y tres años adicionales post implementación. El análisis arroja una adecuada rentabilidad esperada: en el escenario Base, se ha estimado una Tasa Interna de Retorno (TIR) de 36%, un Valor Presente Neto (VPN) de US\$14,6 millones, y una Razón Costo-Beneficio (RBC) de 1,71. A partir del año final de implementación del programa, se proyectan ahorros anuales en los costos operativos de gestión de incidentes por valor de US\$4,8 millones, e impactos negativos evitados para organismos y ciudadanos por un valor anual de US\$8,5 millones por año.
- 1.33 El análisis de sensibilidad muestra que el proyecto tendría una rentabilidad económica aceptable, aún dentro de escenarios y supuestos adversos. En la hipótesis que el proyecto tuviese una menor efectividad para reducir la proporción de incidentes de severidad alta o crítica en el total de incidentes gestionados anualmente por el CERT Nacional, y que solo alcanzase a reducir esta participación de su valor inicial de 81,7% a 10% (en lugar del valor meta de 5% previsto en la Matriz de Resultados - MR), el VPN del proyecto sería US\$11,2 millones y la TIR 34%. En la hipótesis que el proyecto no tuviese éxito en aumentar a 10.000 incidentes el número total gestionado anualmente por el CERT Nacional, y solo alcanzase a 6.000 incidentes/año, el VPN sería US\$12,5 millones y la TIR 33%. Finalmente, si el proyecto no lograra la efectividad marcada en el escenario base en cuanto a evitar daños a las instituciones y personas gracias a una más temprana detección y defensa de los datos y los sistemas, y sólo obtuviese una reducción de 1% en el valor del impacto económico negativo anual a partir del quinto año, el VPN sería US\$3,0 millones y la TIR 17%. Esto es indicativo de una destacable robustez de la rentabilidad económica del proyecto.

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

II. ESTRUCTURA DE FINANCIAMIENTO Y PRINCIPALES RIESGOS

A. Instrumentos de financiamiento

- 2.1 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 por la integralidad de la lógica de intervención prevista, porque se cuenta con una estimación técnica y económica, y por el tipo de inversiones a ser financiadas⁶⁵.

Cuadro 1. Costos estimados del programa (US\$)⁶⁶

Concepto	Total	%
Componente 1. Fortalecimiento de las capacidades institucionales y tecnológicas de la SIP	20.000.000	66,7
IP 1. Marco institucional y normativo para la identificación y protección de ICI aprobado	920.000	3,1
IP 2. Acciones de fortalecimiento de monitoreo y detección de ataques (G-SOC) con herramientas SIEM y sensores	12.955.000	43,2
IP 3. Acciones de fortalecimiento de las capacidades operativas del CERT	4.375.000	14,6
IP 4. Plataformas para el análisis de amenazas e intercambio de información con el sector privado implementado	1.750.000	5,8
Componente 2. Consolidación del talento humano en ciberseguridad	5.000.000	16,7
IP 5. Plataforma de simulación de ataques cibernéticos instalada	2.000.000	6,7
IP 6. Programas técnicos y de certificación en ciberseguridad (priorizando mujeres) desarrollados	1.025.000	3,4
IP 7. <i>Software</i> de <i>e-learning</i> instalado y operando	875.000	2,9
IP 8. Plan de gestión del cambio y desarrollo curricular en ciberseguridad implementada	1.100.000	3,7
Componente 3. Mejoramiento de la protección del ecosistema del GDE	3.000.000	10,0
IP 9. Política de ciberseguridad desarrollado (incluyendo plan de continuidad de negocio -BCP- y recuperación ante desastres -DRP)	500.000	1,7
IP 10. Tecnología de <i>backup</i> implementadas (<i>hardware</i> y <i>software</i>)	2.000.000	6,6
IP 11. Personal de la SIA con capacidades en ciberseguridad del GDE fortalecidas	500.000	1,7
Administración, supervisión, evaluaciones y auditoría	2.000.000	6,6
Gestión	1.300.000	4,3
Monitoreo	300.000	1,0
Evaluaciones: intermedia; final, estratégica, antes y después, y de impacto	300.000	1,0
Auditorías	100.000	0,3
Totales	30.000.000	100,0

- 2.2 **Cronograma de desembolsos.** El plazo de desembolso de cinco años (ver Cuadro 2), se definió principalmente por: (i) el tiempo promedio que conlleva el diseño e implementación de las actividades que se proponen en el programa; (ii) la alineación con la ENC; y (iii) la solicitud de la contraparte de ejecutar la mayor cantidad de actividades posibles en ese período para aprovechar sinergias con otras intervenciones del gobierno en materia de digitalización de trámites.

⁶⁵ Ver Plan de Ejecución Plurianual (PEP).

⁶⁶ Los montos a nivel de producto son indicativos.

Cuadro 2. Cronograma de desembolso (US\$ miles)

Componentes	Año 1	Año 2	Año 3	Año 4	Año 5	Total
BID	3.295	5.505	5.650	7.660	7.890	30.000
%	11,0	18,4	18,8	25,5	26,3	100,0

B. Riesgos ambientales y sociales

- 2.3 En atención al Nuevo Marco de Política Ambiental y Social (GN-2965-23), la operación fue clasificada como Categoría “C”. Durante la aplicación del análisis de la capacidad institucional se analizó el Sistema de Gestión Ambiental y Social del Organismo Ejecutor (OE) y se prevén impactos ambientales o sociales negativos mínimos o nulos. La JGM a través de la Dirección de Programas y Proyectos Sectoriales y Especiales (DIPROSE) ha implementado un mecanismo para la gestión de quejas, incluyendo los temas socioambientales y laborales⁶⁷. Los Procedimientos de Gestión Laboral que regirán durante el ciclo de vida de la operación serán los establecidos por la legislación nacional del país. Asimismo, el país es firmante de los Convenios multilaterales celebrados en el marco de la Organización Internacional del Trabajo (OIT) y la Organización de las Naciones Unidas (ONU), que a su vez se hallan internalizados en la legislación nacional.

C. Riesgos fiduciarios

- 2.4 Se identificó preliminarmente como riesgo fiduciario medio-alto, relacionado con los procesos internos en materia de adquisiciones, tal que, si existieran demoras entre la identificación de una necesidad y el tiempo de incorporación de los distintos bienes y servicios, podría impactar negativamente en el avance del proyecto. Para mitigarlo se tiene previsto habilitar y contratar, en caso de ser necesario y en acuerdo con el Banco, personal calificado con experiencia en procedimientos de organismos multilaterales para la gestión de adquisiciones; y el Banco brindará apoyo y capacitación en temas fiduciarios.

D. Otros riesgos y temas clave

- 2.5 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 (§1.26). 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 (§1.26).
- 2.6 **Sostenibilidad del programa.** 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

⁶⁷ Descripción completa del mecanismo disponible en: https://www.argentina.gob.ar/quejas_y_reclamos.pdf.

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 que rigen desde la gestión anterior, lo que también fortalece su sostenibilidad.

III. PLAN DE IMPLEMENTACIÓN Y GESTIÓN

A. Resumen de los arreglos de implementación

- 3.1 **Prestatario y Organismo Ejecutor.** El Prestatario será la República Argentina. El OE del programa será el Prestatario a través de la JGM, a través de la DIPROSE, que actuará como responsable de la coordinación administrativa y financiera; y la Dirección de Prevención en Seguridad de Sistemas y Redes Informáticas de la SSTI (DPSSYRI), que actuará como área sustantiva del programa^{68, 69}. Adicionalmente, la evaluación estratégica (¶3.15) tendrá al OE como responsable de la ejecución fiduciaria, y a la Subsecretaría de Relaciones Financieras Internacionales para el Desarrollo del Ministerio de Economía de la Nación (SSRFID) como responsable de la ejecución técnica-metodológica⁷⁰.
- 3.2 **ROP.** El [ROP](#) se referirá a la estrategia de ejecución de la operación e incluirá, entre otros: (i) el esquema organizacional del proyecto; (ii) los arreglos técnicos y operativos para su ejecución; (iii) el esquema de programación, seguimiento y evaluación de los resultados; (iv) los lineamientos para los procesos financieros, de auditoría y de adquisiciones y contrataciones; (v) los detalles de las funciones del OE así como las responsabilidades de otras instancias relevantes de los Ministerios en los procesos previstos en el programa; y (vi) los detalles de las actividades comprendidas en los distintos componentes y sub componentes del programa.
- 3.3 **Análisis de la capacidad institucional.** El Banco aplicó en 2022 un análisis de capacidad institucional a la JGM. Encontró que cuenta con experiencia en proyectos con el Banco y otros multilaterales, y consideró que la capacidad institucional para asumir la responsabilidad de la gestión de los recursos del programa, incluyendo la administración financiera y contable, las adquisiciones y contrataciones, y la planeación de sus actividades y monitoreo de su ejecución, necesitan ser reforzadas. Para ello el programa financiará la contratación de personal de apoyo técnico y un equipo de consultores administrativo-financieros para complementar las capacidades de la JGM y, a la vez, apoyar a la dirección de la SIP.
- 3.4 **Funciones y responsabilidades del OE.** Como se detallará en el [ROP](#), el OE deberá: (i) coordinar los procedimientos financieros y administrativos relacionados con el programa; (ii) coordinar, consolidar, preparar y presentar al Banco toda la información y documentación de la gestión integral del programa; y (iii) velar por la articulación, coherencia y cumplimiento de lo planificado en las herramientas de gestión del programa, a fin de contribuir con el cumplimiento de los resultados esperados. Entre sus funciones, se destacan las siguientes: (i) colaborar en la

⁶⁸ Ver la composición y responsabilidades del OE en el Reglamento Operativo del Programa ([ROP](#)).

⁶⁹ Se entiende por área sustantiva: el área con liderazgo en los aspectos técnicos, no fiduciarios, del programa.

⁷⁰ En caso de modificaciones en la estructura organizativa del OE, el mismo podrá actuar a través de aquellas áreas o dependencias con atribuciones y competencias semejantes que en el futuro las reemplacen, con la previa conformidad del Banco para efectos de este programa.

preparación y aprobación de los TDR para contrataciones; (ii) elaborar la documentación técnica y administrativa pertinente a los procesos de licitación y contratación según corresponda; y (iii) coordinar los procesos de contrataciones instruidos por el Director General.

- 3.5 **Mecanismos de coordinación interinstitucional.** La ciberseguridad requiere, para ser efectiva, considerar todas las instituciones responsables por ICI y, por ello, es necesariamente multisectorial. El país, desde 2017, cuenta con un CC⁷¹ (§1.4, §1.6) que, entre sus principales funciones, además que desarrolla la ENC, está la de “elaborar el plan de acción necesario para implementar la ENC, convocar a otros organismos para que participen en la implementación de medidas en el marco del plan de acción elaborado, y fijar los lineamientos y criterios para la definición, identificación y protección de las infraestructuras críticas nacionales”⁷². En este sentido, el CC cuenta con todo el respaldo legal para fungir como responsable de la coordinación interinstitucional de la ENC. Específicamente para las ICI, la SIP es la responsable directa de la coordinación interinstitucional (§1.7) y será reforzada con recursos de esta operación para que pueda ejercerla cabalmente (§1.26).
- 3.6 **Condición contractual especial previa al primer desembolso del financiamiento.** El OE deberá presentar al Banco evidencia de la aprobación y entrada en vigencia del [ROP](#), en los términos previamente acordados con el Banco. Esta medida es necesaria dado que la aprobación del [ROP](#) previamente al primer desembolso contribuye a la organización de los aspectos operativos para la implementación exitosa de la operación.
- 3.7 **Financiamiento retroactivo.** De acuerdo con la Política del Banco sobre Financiamiento Retroactivo y Adquisiciones Anticipadas (GN-2259-1/OP-507), el Banco podrá financiar retroactivamente con cargo a los recursos del préstamo, gastos elegibles efectuados por el Prestatario antes de la fecha de aprobación del préstamo hasta por la suma de US\$3.000.000 (10% del préstamo), para pagos 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 del 07 de abril de 2022 (fecha de aprobación del Perfil de Proyecto), pero en ningún caso se incluirán gastos efectuados más de 18 meses antes de la fecha de aprobación del préstamo por el Directorio Ejecutivo del Banco. El monto del financiamiento retroactivo estará sujeto a las limitaciones aplicables a los desembolsos.
- 3.8 **Adquisición de bienes y servicios.** Las adquisiciones financiadas, total o parcialmente, con recursos del préstamo se realizarán de conformidad con la Política para la Adquisición de Obras y Bienes Financiados por el BID (GN-2349-15) y la Política para la Selección y Contratación de Consultores Financiados por el BID (GN-2350-15).
- 3.9 **Gestión financiera.** Los recursos del préstamo podrán desembolsarse mediante las modalidades de anticipos, reembolso y/o pagos directos, modalidades establecidas en la Guía OP-273-12. Los anticipos de fondos se realizarán basados

⁷¹ Está conformado por los Secretarios de Gobierno de Modernización y el de Asuntos Estratégicos de la JGM y por los Ministerios de Defensa, Seguridad, Relaciones Exteriores y Culto, y Justicia y Derechos Humanos.

⁷² Art. 2, Decreto 480/2019.

en un plan financiero a fin de cubrir las necesidades del programa para los próximos seis meses u otro período razonable. Exceptuado el primer anticipo de fondos, los subsiguientes podrán tramitarse al haber justificado el 80% del saldo total acumulado pendiente de justificación. El OE utilizará el sistema de Unidades Ejecutoras de Préstamos Externos (UEPEX) como sistema de administración financiera.

- 3.10 **Auditoría.** Durante la ejecución, el OE presentará anualmente los estados financieros auditados del programa, en los términos requeridos por el Banco en sus políticas (OP-273-12). Dichos estados financieros auditados deberán presentarse al Banco dentro de un plazo no mayor a los 120 días siguientes al cierre de cada ejercicio financiero fiscal, debidamente dictaminados por una firma de auditoría independiente elegible para el Banco o por la AGN. Los estados financieros auditados finales deberán presentarse dentro de los 120 días posteriores a la fecha de último desembolso del programa.

B. Resumen de los arreglos para el monitoreo de resultados

- 3.11 **Monitoreo.** El OE, realizará el monitoreo y control de todos los procesos de gestión de proyectos, que incluyen al menos los siguientes: (i) seguimiento y reporte del avance en la ejecución del programa; (ii) seguimiento y reporte del desempeño del programa hacia el cumplimiento de las metas anuales físicas y financieras; (iii) seguimiento a la ejecución del Plan de Adquisiciones ([PA](#)); (iv) el seguimiento a los documentos de gestión de riesgos; (v) el seguimiento a la trazabilidad de productos y resultados; (vi) la realización de los Informes Semestrales de Progreso (ISP); (vii) la actualización del [PEP](#) del programa que se remitirá al Banco como parte de cada ISP; (viii) la elaboración del Informe de Terminación del Proyecto; y (ix) la sistematización de buenas prácticas y lecciones aprendidas de cara al cierre del programa. El Banco realizará una reunión de seguimiento anual con el OE, donde se discutirá, entre otros aspectos: (i) el avance de las actividades identificadas en su Plan Operativo Anual ([POA](#)); (ii) el nivel de cumplimiento de los indicadores establecidos para cada componente; (iii) el [POA](#) para el año siguiente; (iv) el PA para los próximos 18 meses; y (v) las posibles modificaciones de las asignaciones presupuestarias por componente ([PME](#)).
- 3.12 **Evaluación.** Para realizar la evaluación del programa se utilizarán la MR y el [PME](#) entre otras herramientas. El programa tiene previsto realizar una evaluación intermedia, una final, y una de impacto que abarquen los aspectos técnicos, administrativos y financieros. La intermedia se realizará a los 90 días contados a partir de la fecha en que se haya desembolsado el 50% de los recursos del préstamo o cuando hayan transcurrido dos años y medio de ejecución, lo que ocurra primero. Esa evaluación tendrá como principales objetivos revisar el avance de todas las actividades programadas para ese momento, las posibles desviaciones ocurridas, las causas de éstas y proponer medidas correctivas a ser aplicadas, además de verificar los productos intermedios generados, la ocurrencia de los riesgos previstos en la matriz correspondiente y la aplicación de las medidas para mitigarlos.
- 3.13 La evaluación final se presentará al Banco a los 90 días contados a partir del término del plazo original de desembolsos o sus extensiones. Incluirá: (i) los resultados de la ejecución físico-financiera; (ii) el grado de cumplimiento de las metas de la MR, incluyendo un resumen de los resultados en contraste con la línea de base elaborada en el primer año de ejecución; (iii) una síntesis de los

resultados de las auditorías realizadas y de la implementación de los planes de mejora; (iv) un análisis de la sostenibilidad de las inversiones del programa, en particular a nivel de costo y de la gestión del capital humano; y (v) un resumen de las principales lecciones aprendidas. Incluirá también la evaluación con metodología “antes y después” y la evaluación económica, que se hará a través de un análisis costo beneficio ex post que replicará el ejercicio realizado para el análisis económico ex ante del programa, utilizando datos recopilados durante la ejecución y actualizando los datos relacionados con los comparadores ([PME](#)). Estos análisis se reflejarán además en el PCR que elaborará el Banco.

- 3.14 Finalmente, la evaluación de impacto tiene como objetivo generar conocimiento sobre la mejor forma de promover buenas prácticas de comportamiento de ciberseguridad entre los funcionarios públicos. Ejemplos de dichas buenas prácticas incluyen: no abrir enlaces sospechosos, no compartir información sensible con personas desconocidas, y cambiar las contraseñas periódicamente. Se buscará lograr este objetivo mediante un experimento de campo que prueba una serie de estrategias, incluyendo: (i) “aprender haciendo”: exposición repetida a intentos de ataques, seguido por retroalimentación del desempeño del funcionario; y (ii) capacitación, con diferentes tipos de incentivos. La teoría de cambio en la que subyace la evaluación es que una proporción importante, y creciente, de los ciberataques a las instituciones ocurre a través de los empleados (§1.13). Esto se debe a que es más costo-efectivo para los cibercriminales tratar de explotar fallas en el conocimiento o la atención de los empleados, que de superar las barreras protectoras instaladas en el *software* o *hardware*. El indicador de resultado principal para la evaluación, que también aparece en la MR del programa, es el porcentaje de funcionarios públicos que caen en una trampa de *phishing* enviado de manera controlada por el gobierno al finalizar los diferentes tratamientos ([EEO#7](#)).
- 3.15 Adicionalmente, el Prestatario a través del OE, realizará una evaluación estratégica del programa, a los efectos de generar información sobre la contribución del préstamo a los logros de las prioridades estratégicas de gestión. Los arreglos y metodología del diseño e implementación de la evaluación estratégica deberán contar con la no objeción del Banco.

Matriz de Efectividad en el Desarrollo		
Resumen AR-L1343		
I. Prioridades corporativas y del país		
1. Prioridades Estratégicas del Grupo BID e Indicadores del CRF		
Retos Regionales y Temas Transversales	-Productividad e Innovación -Equidad de Género y Diversidad -Cambio Climático -Capacidad Institucional y Estado de Derecho	
Nivel 2 del CRF: Contribuciones del Grupo BID a los Resultados de Desarrollo	-Instituciones con capacidades gerenciales y de tecnología digital reforzadas (#)	
2. Objetivos de desarrollo del país		
Matriz de resultados de la estrategia de país	GN-3051	(i) mejorar la empleabilidad de la población; y (ii) gobierno digital
Matriz de resultados del programa de país	GN-3087-2	La intervención está incluida en el Programa de Operaciones de 2022.
Relevancia del proyecto a los retos de desarrollo del país (si no se encuadra dentro de la estrategia de país o el programa de país)		
II. Development Outcomes - Evaluability		Evaluable
3. Evaluación basada en pruebas y solución		8.4
3.1 Diagnóstico del Programa		1.9
3.2 Intervenciones o Soluciones Propuestas		3.5
3.3 Calidad de la Matriz de Resultados		3.0
4. Análisis económico ex ante		7.5
4.1 El programa tiene una TIR/VPN, o resultados clave identificados para ACE		1.5
4.2 Beneficios Identificados y Cuantificados		3.0
4.3 Supuestos Razonables		0.0
4.4 Análisis de Sensibilidad		2.0
4.5 Consistencia con la matriz de resultados		1.0
5. Evaluación y seguimiento		10.0
5.1 Mecanismos de Monitoreo		4.0
5.2 Plan de Evaluación		6.0
III. Matriz de seguimiento de riesgos y mitigación		
Calificación de riesgo global = magnitud de los riesgos*probabilidad		Medio Alto
Clasificación de los riesgos ambientales y sociales		C
IV. Función del BID - Adicionalidad		
El proyecto se basa en el uso de los sistemas nacionales		
Fiduciarios (criterios de VPC/FMP)	Si	Administración financiera: Presupuesto, Contabilidad y emisión de informes, Controles externos. Adquisiciones y contrataciones: Sistema de información.
No-Fiduciarios		
La participación del BID promueve mejoras adicionales en los presuntos beneficiarios o la entidad del sector público en las siguientes dimensiones:		
Antes de la aprobación se brindó a la entidad del sector público asistencia técnica adicional (por encima de la preparación de proyecto) para aumentar las probabilidades de éxito del proyecto	Sí	Transformación Digital (ATN/OC-17583-AR) en ejecución, que apoya la implementación de la Agenda Digital, incluyendo el plan de protección de ICI

Nota de valoración de la evaluabilidad: El objetivo general de desarrollo del programa es contribuir a la reducción de costos para el estado y la ciudadanía atribuidos a incidentes de ciberseguridad. Para conseguir este fin, el préstamo define un enfoque en tres áreas específicas en las que el proyecto interviene.

La primera área de enfoque busca aumentar la cobertura de gestión para la identificación y protección de las ICI; la segunda se enfoca en mejorar la productividad en la gestión de incidentes cibernéticos, mientras que la tercera busca hacer mejoras en la eficacia de la gestión de ciberseguridad de las ICI priorizadas.

La propuesta de préstamo presenta un diagnóstico del problema basado en los efectos económicos relacionados con los ciberataques y el alto costo de procesamiento de incidentes de ciberseguridad para el estado y los ciudadanos. Se consideran también brechas de género en la fuerza laboral de ciberseguridad. Las soluciones propuestas se enfocan en la mejora de la capacidad tecnológica e institucional, recursos humanos, la coordinación interinstitucional, y la interacción del ecosistema de actores.

Dichas soluciones son apropiadas para dar respuesta a los problemas identificados y a sus factores contribuyentes. La matriz de resultados (MR) es congruente con la lógica vertical del proyecto. Los indicadores de resultado están definidos apropiadamente para medir los logros alcanzados por el programa y el cumplimiento de sus objetivos específicos. Los indicadores de impacto se alinean al objetivo general de desarrollo.

El análisis económico ex-ante de la operación es apropiado bajo los supuestos aplicables a este tipo de proyectos, así como de acuerdo a análisis de sensibilidad razonable. Este se basa en los beneficios potenciales de generar una capacidad mejorada de prevención y respuesta a ataques cibernéticos. El análisis muestra un valor presente neto positivo en el escenario central, así como bajo varias condiciones incluidas en el análisis de sensibilidad.

El plan de monitoreo y evaluación incluye una metodología experimental con miras a generar evidencia sobre la efectividad de promover buenas prácticas de comportamiento de ciberseguridad. Para todas las variables de línea de base se utilizarán datos administrativos. Las actividades de monitoreo y evaluación serán realizadas por la Jefatura de Gabinete de Ministros (JGM) de la Presidencia de Argentina en coordinación con el Banco.

MATRIZ DE RESULTADOS

Objetivo del proyecto:	Los objetivos de desarrollo específicos son: (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 de las Infraestructuras Críticas de Información (ICI) priorizadas. El logro de estos objetivos contribuirá al objetivo general de desarrollo que consiste en contribuir a la reducción de los costos por incidentes de ciberseguridad para el Estado y la ciudadanía.
-------------------------------	--

Objetivo General de Desarrollo

Indicadores	Unidad de Medida	Valor de Línea de Base	Año Línea de Base	Año Esperado para el Logro	Meta	Medios de Verificación	Comentarios
Objetivo general de desarrollo: Ahorro en los costos de gestión por incidentes de ciberseguridad para el Estado y la sociedad							
1. Nivel de madurez de capacidad de seguridad cibernética nacional	Puntaje	125	2020	2027	165	Informe OEA BID	Ver PME
2. Costos anuales de gestión de incidentes cibernéticos	US\$ Millones	8,2	2021	2027	3,4	Evaluación costo-beneficio ex post	Ver PME

Objetivos de Desarrollo Específicos

Indicadores	Unidad de Medida	Valor Línea de Base	Año Línea de Base	Meta Final	Medios de Verificación	Comentarios
Objetivo específico de desarrollo 1: Aumento de la cobertura de gestión para la identificación y protección de las ICI						
1.1. Cobertura de sectores con ICI identificadas	%	9	2021	50	Informe Semestral de Progreso (ISP) de SIP	Ver PME
1.2. Cobertura de ministerios monitoreados a través del G-SOC	%	0	2021	60	ISP de SIP	Ver PME
1.3. Equipos informáticos con sello de eficiencias energética adquiridos	%	0	2021	90	ISP de SIP, incluyendo Reporte anual de Dirección Nacional de Contrataciones Públicas (DNCP)	Indicador Pro-Cambio Climático Ver PME

Indicadores	Unidad de Medida	Valor Línea de Base	Año Línea de Base	Meta Final	Medios de Verificación	Comentarios
Objetivo específico de desarrollo 2: Mejora de la productividad en la gestión de incidentes cibernéticos						
2.1. Incidentes cibernéticos gestionados anualmente	Número	591	2021	10.000	ISP de SIP	Ver PME
2.2. Incidentes cibernéticos gestionados que son clasificados como altos o críticos (de alto impacto)	%	81,7	2021	5	ISP de SIP	Ver PME
2.3. Mujeres de la SIP certificadas en ciberseguridad	%	28	2021	34	ISP de SIP	Indicador Pro-Género Ver PME
2.4. Instituciones con capacidades gerenciales y de tecnología digital reforzadas	Número	0	2021	2	ISP de SIP	Ver PME
Objetivo específico de desarrollo 3: Mejora de la eficacia en la gestión de la ciberseguridad de las ICI priorizadas						
3.1. Hallazgos de ciberseguridad de GDE resueltos	%	0	2021	50	ISP de SIP e Informe de auditoría 2021	Ver PME
3.2. Pruebas de recuperación exitosas ante problemas informáticos	Número	0	2021	4	ISP de SIP incluyendo reporte de performance de ejercicios de restauración	Ver PME

Productos

Indicadores	Unidad de Medida	Valor Línea de Base	Año Línea de Base	Año 1	Año 2	Año 3	Año 4	Año 5	Fin del Proyecto	Medios de Verificación	Comentarios
Componente 1. Fortalecimiento de las capacidades institucionales y tecnológicas de la SIP											
1.1. Marco institucional y normativo para la identificación y protección del ICI aprobado	Marco institucional	0	2021	0	1	0	0	0	1	ISP de SIP y Acto administrativo de JGM aprobatorio del Marco Institucional	Ver PME

Indicadores	Unidad de Medida	Valor Línea de Base	Año Línea de Base	Año 1	Año 2	Año 3	Año 4	Año 5	Fin del Proyecto	Medios de Verificación	Comentarios
1.2. Acciones de fortalecimiento de monitoreo y detección de ataques (G-SOC) con herramientas SIEM y sensores	Acciones	0	2021	1	1	1	1	1	5	ISP de SIP	Ver PME
1.3. Acciones de fortalecimiento de las capacidades operativas del CERT Nacional	Acciones	0	2021	1	1	1	1	1	5		
1.4. Plataformas para el análisis de amenazas e intercambio de información con el sector privado implementado	Plataforma	0	2021	0	1	0	0	0	1	ISP de SIP y reporte de uso de la plataforma	Ver PME
Componente 2. Consolidación del talento humano en ciberseguridad											
2.1. Plataforma de simulación de ataques cibernéticos instalada	Plataforma	0	2021	0	1	0	0	0	1	ISP de SIP y reporte de uso de la plataforma de simulación	
2.2. Programas técnicos y de certificación en ciberseguridad (priorizando mujeres) desarrollados	Programas	0	2021	1	1	1	1	1	5	ISP de SIP incluyendo Informe de inscripciones	Indicador Pro-Género Ver PME
2.3. <i>Software</i> de <i>e-learning</i> instalado y operando	<i>Software</i>	0	2021	0	1	0	0	0	1	ISP de SIP incluyendo reporte sobre uso del <i>software</i>	Ver PME
2.4. Plan de gestión del cambio y desarrollo curricular en	Documento	0	2021	0	1	0	0	0	1	ISP de SIP incluyendo documento aprobado	

Indicadores	Unidad de Medida	Valor Línea de Base	Año Línea de Base	Año 1	Año 2	Año 3	Año 4	Año 5	Fin del Proyecto	Medios de Verificación	Comentarios
ciberseguridad implementada											
Componente 3. Mejoramiento de la protección del ecosistema del GDE											
3.1. Política de ciberseguridad desarrollada	Documento	0	2021	0	1	0	0	0	1	ISP de SIP incluyendo Documento aprobado por autoridad competente	Ver PME
3.2. Tecnología de <i>backup</i> implementada (<i>hardware y software</i>)	Sistema	0	2021	0	0	1	0	0	1	ISP de SIP incluyendo reportes del sistema	Ver PME
3.3. Capacitaciones sobre ciberseguridad del GDE implementadas	Talleres	0	2021	2	2	2	2	2	10	ISP de SIP incluyendo reportes de asistencia	

País: Argentina

División: IFD/ICS

No. de operación: AR-L1343

Año: 2023

ACUERDOS Y REQUISITOS FIDUCIARIOS

Organismo Ejecutor (OE): República de Argentina, a través de la Jefatura de Gabinete de Ministros (JGM) de la Presidencia de la Nación

Nombre de la Operación: Programa de Ciberseguridad para Infraestructuras Críticas de Información (ICI)

I. CONTEXTO FIDUCIARIO DEL ORGANISMO EJECUTOR

1. Uso de sistema de país en la operación

<input checked="" type="checkbox"/> Presupuesto	<input checked="" type="checkbox"/> Reportes	<input checked="" type="checkbox"/> Sistema Informativo	<input type="checkbox"/> Licitación Pública Nacional (LPN)
<input type="checkbox"/> Tesorería	<input type="checkbox"/> Auditoría Interna	<input type="checkbox"/> Comparación de Precios	<input type="checkbox"/> Otros
<input checked="" type="checkbox"/> Contabilidad	<input checked="" type="checkbox"/> Control Externo	<input type="checkbox"/> Consultores Individuales	

2. Mecanismo de ejecución fiduciaria

<input checked="" type="checkbox"/>	Particularidades de la ejecución fiduciaria	El Prestatario será la República Argentina. El OE será el Prestatario a través de la JGM, a través de la DIPROSE, que actuará como responsable de la coordinación administrativa y financiera; y la Dirección de Prevención en Seguridad de Sistemas y Redes Informáticas de la SSTI (DPSSYRI), que actuará como área sustantiva del programa. Para ello contará con el apoyo de un equipo integrado experto con roles diversos.
-------------------------------------	---	--

3. Capacidad fiduciaria

Capacidad fiduciaria del OE	Al llevarse a cabo el análisis institucional se concluyó que la capacidad institucional para asumir la responsabilidad de la gestión de los recursos del programa, incluyendo la administración financiera y contable, las adquisiciones y contrataciones, y la planeación de sus actividades y monitoreo de su ejecución, necesitan ser reforzadas. Para ello el programa financiará la contratación de personal de apoyo técnico y un equipo de consultores administrativo-financieros para complementar las capacidades de la JGM y, a la vez, apoyar a la dirección de la SIT.
-----------------------------	--

4. Riesgos fiduciarios y respuesta al riesgo

Área (Gestión Financiera/ Adquisiciones)	Riesgo	Nivel de Riesgo	Respuesta al Riesgo
Procesos internos	Si existieran demoras entre la identificación de una necesidad y el tiempo de incorporación de los distintos bienes y servicios, podría impactar negativamente en el avance del proyecto.	Medio-Alto	Habilitar y contratar, en caso de ser necesario y en acuerdo con el Banco, personal calificado, con experiencia en procedimientos de organismos multilaterales para la gestión de adquisiciones; y el Banco brindará apoyo y capacitación en temas fiduciarios.

5. Políticas y Guías aplicables a la operación: En materia de adquisiciones, para la adquisición de bienes y obras se aplicarán las Políticas para la Adquisición de Bienes y Obras Financiados por el BID (GN-2349-15) y para la selección y contratación de consultores se aplicarán las Políticas para la Selección y Contratación de Consultores Financiados por el BID (GN-2350-15). En materia de gestión financiera se aplicará la Guía de Gestión Financiera para Proyectos Financiados por el BID (OP-273-12) o sus actualizaciones correspondientes.

6. Excepciones a Políticas y Guías: Ninguna.

II. ASPECTOS A SER CONSIDERADOS EN LAS ESTIPULACIONES ESPECIALES DEL CONTRATO DE PRÉSTAMO

Tasa de cambio: Para efectos de lo estipulado en el Artículo 4.10 de las Normas Generales, las Partes acuerdan que la tasa de cambio aplicable será la indicada en el inciso (b)(i) de dicho Artículo. Para efectos de determinar la equivalencia de gastos incurridos en moneda local con cargo al aporte local o del reembolso de gastos con cargo al Préstamo, la tasa de cambio acordada será la tasa de cambio del primer día hábil del mes del pago en que el Prestatario, el OE o cualquier otra persona natural o jurídica a quien se le haya delegado la facultad de efectuar gastos, efectúe los pagos respectivos en favor del contratista, proveedor o beneficiario.

Informes Financieros Anuales Auditados: El OE presentará informes financieros anuales auditados relacionados con el uso de los recursos, de acuerdo con los TDR acordados con el Banco dentro de los 120 días posteriores al cierre del ejercicio fiscal. Los Informes financieros finales del proyecto se presentarán dentro del plazo de 120 días posteriores a la fecha de último desembolso. La auditoría externa del programa será realizada por una firma auditora independiente elegible para auditar operaciones financiadas por el Banco, seleccionada y contratada de acuerdo con los TDR y modelo de contrato previamente acordados con el Banco o por la AGN.

III. ACUERDOS Y REQUISITOS PARA LA EJECUCIÓN DE ADQUISICIONES

<input checked="" type="checkbox"/>	Documentos de Licitación	Para adquisiciones de Obras, Bienes y Servicios Diferentes de Consultoría ejecutadas de acuerdo con las Políticas para la Adquisición de Bienes y Obras Financiados por el BID (GN-2349-15), sujetas a Licitación Pública Internacional (LPI), se utilizarán los Documentos Estándar de Licitación (DEL) del Banco o los acordados entre el OE y el Banco para la adquisición particular. Así mismo, la selección y contratación de Servicios de Consultoría serán realizadas de acuerdo con las Políticas de Selección de y Contratación de Consultores Financiados por el BID (GN-2350-15) y se utilizará la Solicitud Estándar de Propuestas (SEP) emitida por el Banco o acordada entre el OE y el Banco para la selección particular. Para la adquisición de bienes y servicios se usará prioritariamente el sistema Compr.AR con documentos de licitación adaptados y aceptados por el Banco. La revisión de las especificaciones técnicas, así como de los TDR de las adquisiciones durante la preparación de procesos de selección, es responsabilidad del especialista sectorial del proyecto. Esta revisión técnica puede ser ex ante y es independiente del método de revisión de la adquisición.
<input checked="" type="checkbox"/>	Adquisiciones Anticipadas Financiamiento Retroactivo	De acuerdo con la Política del Banco sobre Financiamiento Retroactivo y Adquisiciones Anticipadas (GN-2259-1/OP-507), el Banco podrá financiar retroactivamente con cargo a los recursos del préstamo, gastos elegibles efectuados por el Prestatario antes de la fecha de aprobación del préstamo hasta por la suma de US\$3.000.000 (10% del préstamo), para pagos 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 del 07 de abril de 2022 (fecha de aprobación del Perfil de Proyecto), pero en ningún caso se incluirán gastos efectuados más de 18 meses antes de la fecha de aprobación del

		préstamo por el Directorio Ejecutivo del Banco. El monto del financiamiento retroactivo estará sujeto a las limitaciones aplicables a los desembolsos.						
<input checked="" type="checkbox"/>	Supervisión de las Adquisiciones	<p>El método de supervisión será ex post, salvo en aquellos casos en que se justifique una supervisión ex ante. El método (i) ex ante o (ii) ex post de supervisión se debe determinar para cada proceso de selección. Las revisiones ex post serán cada 18 meses de acuerdo con el plan de supervisión del proyecto, sujeto a cambios durante la ejecución. Los reportes de revisión ex post incluirán al menos una visita. Los montos referenciales para la revisión ex post son los siguientes:</p> <table border="1"> <tr> <th>Obras</th><th>Bienes/Servicios</th><th>Servicios de Consultoría</th></tr> <tr> <td>5.000.000</td><td>500.000</td><td>200.000</td></tr> </table>	Obras	Bienes/Servicios	Servicios de Consultoría	5.000.000	500.000	200.000
Obras	Bienes/Servicios	Servicios de Consultoría						
5.000.000	500.000	200.000						
<input checked="" type="checkbox"/>	Registros y Archivos	En el caso de adquisiciones con base en el Compr.AR, dicho sistema servirá de repositorio para la supervisión del Banco.						

Adquisiciones Principales

Descripción de la Adquisición	Método de Selección	Fecha Estimada	Monto Estimado (miles US\$)
Bienes			
Equipamiento básico	Licitación Pública Nacional (LPN)	Junio 2023	400
Software y hardware para SIEM, agregación, respaldo etc. (Varios)	LPI	Septiembre 2023	10.600
Servicios de no consultoría			
Servicios de ciberseguridad preventiva	LPN	Junio 2023	2.300
Organización de eventos y capacitación	Comparación de Precios (CP) por invitación abierta	Junio 2024	880
Firmas			
Análisis de brecha de ciberseguridad del GDE	Selección Basada en Calidad y Costo (SBCC)	Enero 2024	500
Programas académicos y cursos especializados (varios procesos)	Selección Basada en las Calificaciones de los Consultores (SCC)	Marzo 2024	740
Acciones de promoción de género en el sector	SCC	Febrero 2023	150
Consultorías para certificaciones varias	SCC	Febrero 2024	400
Fortalecimiento de capacidades operativas del CERT Nacional	SCC	Febrero 2023	200
Consultoría plataforma <i>e-learning</i>	SBCC	Junio 2023	625
Consultoría Plataformas Notificación y Coordinación de Incidentes y de Intercambio de Información de Amenazas	SBCC	Febrero 2024	320
Consultoría de Análisis de riesgos	SBCC	Marzo 2023	250
Consultorías para la operación L1-L2 del CERT.ar / G-SOC	SBCC	Marzo 2023	2.900
Servicios avanzados en ciberseguridad	SBCC	Junio 2023	980
Plataforma de Agregación de Eventos	SBCC	Junio 2023	675
Programa Nacional de Sondas	SBCC	Abril 2023	1.400
Consultoría de Detección e Identificación de Activos Tecnológicos y Humanos	SBCC	Abril 2023	450

Descripción de la Adquisición	Método de Selección	Fecha Estimada	Monto Estimado (miles US\$)
Consultoría para el diseño y puesta en marcha del G-SOC	SBCC	Enero 2023	600
Consultoría para la identificación de ICI y el diseño de sus planes de protección	SBCC	Enero 2023	320
Consultoría para el diseño del marco institucional y normativo	SBCC	Febrero 2023	600
Individuos			
Seguimiento a cursos académicos y certificaciones	Selección de Consultor Individual (3CV)	Enero 2023	275
Gestión de Comunicación	3CV	Enero 2023	250
Equipo CERT.ar G-SOC	3CV	Enero 2023	375
Consultorías especializadas para administración y fortalecimiento fiduciario	3CV	Enero 2023	1.300

Para acceder al PA, ver [link](#).

Procedimientos	Justificación del Uso
Contratación Electrónica de Bienes y Servicios	El Banco aprobó el uso de Compr.AR en 2018 siguiendo procedimientos establecidos.

IV. ACUERDOS Y REQUISITOS PARA LA GESTIÓN FINANCIERA

<input checked="" type="checkbox"/>	Programación y Presupuesto	El OE es responsable del proceso de formulación y programación del presupuesto anual, quien se encarga de realizar todos los procedimientos conducentes a la consolidación del presupuesto anual para su aprobación. A medida que surgen necesidades de ampliación o reasignaciones de partidas, la unidad ejecutora solicita las modificaciones encargándose de gestionar su aprobación. Los créditos presupuestarios se ejecutan mediante cuotas de compromiso trimestrales y mensuales de devengado, las cuales son asignadas por la Oficina Nacional de Presupuesto (Ministerio de Economía).
<input checked="" type="checkbox"/>	Tesorería y Gestión de Desembolsos	Cuentas bancarias: El OE mantendrá una cuenta especial en dólares y una cuenta en pesos en el Banco Nación separadas e identificadas contable y operacionalmente para la gestión exclusiva de los recursos del programa. Plan financiero: Los desembolsos se realizarán sobre la base de un plan financiero detallado basado en las necesidades reales de liquidez del programa. Método de desembolsos: El Banco desembolsará recursos bajo la modalidad de Anticipo de Fondos u otra modalidad establecida en la Guía OP-273-12. Los subsiguientes desembolsos posteriores al primer anticipo de fondos podrán tramitarse al haber justificado el 80% de los anticipos anteriores debido a que es un programa descentralizado y de ejecución compleja. Se utilizará la plataforma electrónica <i>Online Disbursement</i> para gestionar los desembolsos.
<input checked="" type="checkbox"/>	Contabilidad, Sistemas de Información y Generación de Reportes	El OE utilizará el sistema de UEPEX como sistema de administración financiera. Este permite identificar los fondos del programa y también las fuentes de financiamiento. UEPEX consigna, de conformidad con el catálogo de cuentas aprobado por el Banco, las inversiones del programa por componente del cuadro de costos. El registro de la contabilidad se hará con base de caja y se seguirán las Normas Internacionales de Información

		Financiera cuando aplique, de acuerdo con los criterios nacionales establecidos.
<input checked="" type="checkbox"/>	Control Externo e Informes Financieros	El Control Externo es desempeñado por la AGN, órgano rector de control externo, dependiente y de asistencia del Congreso Nacional en el control del estado de cuentas del Sector Público. Su creación y funcionamiento se encuentran reglamentados en el Título VII, Capítulo I de la Ley 24.156 de Administración Financiera y de los Sistemas del Control Externo. Los estados financieros anuales del programa, con base en los TDR previamente acordados con el Banco, deberán ser auditados por un auditor independiente aceptable para el Banco, pudiendo ser tanto la AGN como una Firma de Auditoría Independiente.
<input checked="" type="checkbox"/>	Supervisión Financiera de la Operación	El plan de supervisión financiera surgirá a partir de las evaluaciones de riesgo y capacidad fiduciaria realizadas al OE y considerará visitas de supervisión in situ y de “escritorio”, así como el análisis y seguimiento de los resultados y recomendaciones de las auditorías a los informes financieros anuales, del programa.

DOCUMENTO DEL BANCO INTERAMERICANO DE DESARROLLO

PROYECTO DE RESOLUCIÓN DE-___/23

Argentina. Préstamo ___/OC-AR a la República Argentina. Programa de
Ciberseguridad para Infraestructuras Críticas de Información (ICI)

El Directorio Ejecutivo

RESUELVE:

Autorizar al Presidente del Banco, o al representante que él designe, para que, en nombre y representación del Banco, proceda a formalizar el contrato o contratos que sean necesarios con la República Argentina, como Prestatario, para otorgarle un financiamiento destinado a cooperar en la ejecución del Programa de Ciberseguridad para Infraestructuras Críticas de Información (ICI). Dicho financiamiento será por una suma de hasta US\$30.000.000, que formen parte de los recursos del Capital Ordinario del Banco, y se sujetará a los Plazos y Condiciones Financieras y a las Condiciones Contractuales Especiales del Resumen de Proyecto de la Propuesta de Préstamo.

(Aprobada el ___ de _____ de 2023)