

DOCUMENTO DEL BANCO INTERAMERICANO DE DESARROLLO

URUGUAY

FORTALECIMIENTO DE LA CIBERSEGURIDAD EN URUGUAY

(UR-L1152)

PROPUESTA DE PRÉSTAMO

Este documento fue preparado por el equipo de proyecto integrado por: Miguel Porrúa (IFD/ICS), Jefe de Equipo; Roberto Fernández, Jefe de equipo alterno; Alejandro Pareja, Ariel Nowersztern, Benjamin Roseth, Dario Kagelmacher, Sonia Rojas (IFD/ICS); Harold Villalba (SPD/SDV); Abel Cuba, Emilie Chapuis (FMP/CUR); y Krysia Avila (LEG/SGO).

De conformidad con la Política de Acceso a Información el presente documento se divulga al público de forma simultánea a su distribución al Directorio Ejecutivo del Banco. El presente documento no ha sido aprobado por el Directorio. Si el Directorio lo aprueba con modificaciones, se pondrá a disposición del público una versión revisada que sustituirá y reemplazará la versión original.

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	8
C. Indicadores claves de resultados.....	10
II. ESTRUCTURA DE FINANCIAMIENTO Y PRINCIPALES RIESGOS	11
A. Instrumentos de financiamiento	11
B. Riesgos ambientales y sociales.....	11
C. Riesgos fiduciarios.....	12
D. Otros riesgos y temas claves.....	12
III. PLAN DE IMPLEMENTACIÓN Y GESTIÓN.....	13
A. Resumen de los arreglos de implementación	13
B. Resumen de los arreglos para el monitoreo de resultados.....	16

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) y Plan Operativo Anual (POA)
EER#2	Plan de Monitoreo y Evaluación (PME)
EER#3	Plan de Adquisiciones (PA)

ENLACES ELECTRÓNICOS OPCIONALES (EEO)	
EEO#1	Análisis Económico del Proyecto 1.A. Informe 1.B. Hoja de Cálculo
EEO#2	Agenda Uruguay Digital 2020
EEO#3	Internet Security Threat Report, February 2019
EEO#4	Impacto de los Incidentes de Seguridad Digital en Colombia 2017
EEO#5	Marco para la Mejora de la Seguridad Cibernética en Infraestructuras Críticas, 2018
EEO#6	Informe Seguridad 2016
EEO#7	Filtro de Política de Salvaguardias (SPF) y Formulario de Evaluación de Salvaguardia (SSF)

ABREVIATURAS	
AGESIC	Agencia para el Desarrollo de Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento
ALC	América Latina y el Caribe
BID	Banco Interamericano de Desarrollo
CERT.uy	Centro Nacional de Respuesta a Incidentes de Seguridad Informática
DDoS	Ataque de Denegación de Servicio
FMI	Fondo Monetario Internacional
GSOC	<i>Government Security Operation Center</i>
IGAS	Informe de Gestión Ambiental y Social
ITU	<i>International Telecommunications Union</i>
NIST	<i>National Institute of Standards and Technology</i>
OE	Organismo Ejecutor
OEA	Organización de Estados Americanos
PA	Planes de Adquisiciones
PEP	Plan de Ejecución Plurianual
PIB	Producto Interno Bruto
PMR	Informes de Monitoreo del Progreso
POA	Planes Operativos Anuales
SIEM	<i>Security Information Event Management</i>
SOC	Centro de Operaciones de Seguridad
TCR	Tribunal de Cuentas de la República
TIC	Tecnologías de la Información y la Comunicación
UTEC	Universidad Tecnológica

RESUMEN DEL PROYECTO
URUGUAY
FORTALECIMIENTO DE LA CIBERSEGURIDAD EN URUGUAY
(UR-L1152)

Términos y Condiciones Financieras				
Prestatario:			Facilidad de Financiamiento Flexible^(a)	
República Oriental del Uruguay			Plazo de amortización:	25 años
Organismo Ejecutor:			Período de desembolso:	4 años
República Oriental del Uruguay, a través de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)			Período de gracia:	5,5 años ^(b)
Fuente	Monto (US\$)	%	Tasa de interés:	Basada en LIBOR
BID (Capital Ordinario):	8.000.000	80	Comisión de crédito:	^(c)
Local:	2.000.000	20	Comisión de inspección y vigilancia:	^(c)
			Vida Promedio Ponderada (VPP):	15,25 años
Total:	10.000.000	100	Moneda de aprobación:	Dólares de los Estados Unidos de América
Esquema del Proyecto				
Objetivo/descripción del proyecto: El programa contribuirá a fortalecer la capacidad del país para proteger su espacio digital mejorando la prevención, detección y respuesta a los ataques cibernéticos.				
Condiciones contractuales especiales previas al primer desembolso del financiamiento: Será condición contractual especial previa al primer desembolso del financiamiento que el Prestatario, por sí o por intermedio del Organismo Ejecutor (OE), haya presentado al Banco evidencia de: (i) la designación, como coordinador general del programa, del Director de la Dirección de Seguridad de la Información de AGESIC; y (ii) el nombramiento del coordinador operativo del programa (¶3.5).				
Excepciones a las políticas del Banco: Ninguna.				
Alineación Estratégica				
Desafíos^(d):	SI	<input checked="" type="checkbox"/>	PI	<input checked="" type="checkbox"/>
Temas Transversales^(e):	GD	<input checked="" type="checkbox"/>	CC	<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 y de productos básicos. 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) GD (Igualdad de Género y Diversidad); CC (Cambio Climático y 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.** Uruguay es uno de los países más desarrollados en la región en términos de gobierno digital¹, comercio electrónico y uso de Tecnologías de la Información y la Comunicación (TIC). Entre los avances en cuanto a desarrollo de gobierno electrónico destacan: (i) el 95% de los trámites del gobierno nacional pueden ser iniciados en línea²; (ii) cuenta con documento de identidad con chip e información biométrica; y (iii) ha iniciado la implementación de la ficha médica digital. Tanto la agenda de gobierno electrónico³ como la política de ciberseguridad⁴ son responsabilidad de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC).
- 1.2 La elevada penetración de las TIC en todos los ámbitos de la sociedad incrementa tanto el número de posibles vulnerabilidades como de incidentes potenciales, y del impacto que los mismos pueden generar al aumentar lo que los expertos denominan superficie de ataque⁵. Este escenario enfrenta una situación en la que, a pesar de que tanto gobierno digital como ciberseguridad son regulados por AGESIC, los esfuerzos por proteger el espacio digital no han avanzado al mismo ritmo que el proceso de digitalización lo cual deja el espacio cibernético uruguayo vulnerable a posibles ataques⁶. El Informe Ciberseguridad 2016 muestra que Uruguay no alcanza la mitad de la puntuación del modelo de madurez que representa una adecuada política de ciberseguridad para países con un desarrollo comparable⁷.
- 1.3 Uruguay ha llevado a cabo numerosas iniciativas para proteger su ciberespacio que lo posicionan como uno de los países más avanzados de América Latina y el Caribe (ALC) en materia de ciberseguridad. Sin embargo, como refleja el informe Ciberseguridad 2016, presenta algunas debilidades importantes. En el año 2008, AGESIC lanzó el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERT.uy)⁸ y en el año 2017 el *Government Security Operation Center* (GSOC)⁹. La capacidad técnica y el equipamiento tecnológico del CERT.uy no han sido actualizados al ritmo que demandan los rápidos cambios que se

¹ [e-Government Readiness Survey 2018](#). United Nations.

² [El fin del trámite eterno: ciudadanos, burocracia y gobierno digital](#). BID 2017.

³ [La Ley 17.930 de 19 de diciembre de 2005](#), art. 72 crea la AGESIC como institución responsable de las políticas de gobierno electrónico.

⁴ La Ley 18.719 de 27 de diciembre de 2010, art. 149 crea, dentro de la AGESIC, la Dirección de Seguridad de la Información.

⁵ [Cybersecurity Ventures](#).

⁶ [Informe Ciberseguridad 2016: ¿Estamos preparados en América Latina y el Caribe? BID/OEA. 2016](#). Este informe analiza todos los países ALC con base en una metodología de la Universidad de Oxford que incluye 49 indicadores agrupados en cinco dimensiones.

⁷ Uruguay obtiene 149 puntos de 245 posibles.

⁸ *Computer Emergency Response Team*. Es el centro responsable de la respuesta a incidentes cibernéticos en el país. Fue creado por el Artículo 73 de la Ley 18.362, de 6 de octubre de 2008 (cf. artículo 73), siendo su funcionamiento y organización regulados por el Decreto No. 451/009 del 28 de septiembre de 2019.

⁹ GSOC es la instancia responsable de monitorear, analizar y defender todos los incidentes que tienen lugar en la infraestructura TIC del gobierno. En el organigrama de ciberseguridad de la AGESIC, el GSOC opera como parte de la estructura de CERT.uy.

producen en el mundo digital, y el GSOC no ha sido equipado con todos los recursos que precisa para cumplir adecuadamente su función. Sin embargo, el gobierno está comprometido con la seguridad de su entorno digital como se refleja en la Agenda Uruguay Digital que tiene como uno de sus objetivos la “Confianza y seguridad en el uso de las tecnologías digitales”¹⁰. Este objetivo se complementa con la Política de Gestión de Incidentes de Seguridad de la Información y sus guías de implementación¹¹.

- 1.4 Esta falta de capacidad en el CERT.uy y en el GSOC hace que sea difícil detectar los ataques cibernéticos o que la detección se produzca de forma tardía y por tanto los daños ya se hayan producido. Los análisis realizados por el propio CERT.uy muestran que a medida que se incrementa su capacidad tecnológica y humana, crece su habilidad para detectar incidentes cibernéticos. En el año 2017, Uruguay lanza su GSOC y la detección de incidentes se incrementa en un 69%¹².
- 1.5 De acuerdo al *International Telecommunications Union* (ITU), Uruguay es el país de América Latina donde la agenda digital está más avanzada¹³, posición 42 de 176. Asimismo, según Naciones Unidas, Uruguay es el país con el mayor desarrollo del gobierno digital en ALC, ubicándose en la posición 34 de 193 a nivel mundial y primero en la región. Uruguay es, además, el primer exportador de *software* per cápita de América Latina, con más 300 empresas que exportan a 52 países¹⁴. Los ataques cibernéticos se han convertido en el riesgo que más preocupa a las empresas, situándose por encima de los ataques terroristas, las burbujas financieras o las crisis fiscales¹⁵. Estos ataques cibernéticos tienen consecuencias económicas importantes y están costando en promedio el 0,5% del Producto Interno Bruto (PIB) mundial¹⁶. Un estudio realizado en Colombia por el Gobierno de Colombia, el BID y la Organización de Estados Americanos (OEA), muestra que el costo del cibercrimen puede llegar a alcanzar hasta el 5% de las ventas en las microempresas y el 1% de las ventas en las pequeñas y medianas empresas¹⁷. Este mismo estudio indica que en el sector público los incidentes de ciberseguridad cuestan en promedio el 0,5% del presupuesto de inversión y el 17% de las instituciones reportaron costos superiores a los US\$200.000 por daños a los activos e infraestructura. Asimismo, un reciente estudio del Fondo Monetario Internacional (FMI) estima que las pérdidas promedio en el sector financiero debidas a ciberataques alcanzan el 9% de los ingresos netos¹⁸.
- 1.6 En el caso de Uruguay, la repercusión económica de su actual política de seguridad tiene dos vertientes que son analizadas en profundidad en el [análisis](#)

¹⁰ [Agenda Uruguay Digital](#), Transformación con equidad 2020. Objetivo viii. Pág. 18.

¹¹ Resoluciones 59/010 y 62/010 del Consejo Directivo Honorario de AGESIC.

¹² [Estadísticas CERT.uy](#).

¹³ [ICT Development Index 2017](#). ITU.

¹⁴ [Asociación de Despachantes de Aduanas del Uruguay](#).

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

¹⁶ “Net Losses: Estimating the global cost of cybercrime”. [Center for Strategic International Studies \(CSIS\) and McAfee](#). 2014.

¹⁷ [Impacto de los incidentes de Seguridad Digital en Colombia 2017](#). Ministerio de Tecnologías de la Información y las Comunicaciones, OEA y BID. 2017.

¹⁸ [Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment](#). Antoine Bouveret. FMI. 2018. WP/18/143.

económico. Por un lado, el costo económico para el país en su conjunto que en un escenario moderado podría alcanzar los US\$24 millones por año. Por otro la potencial actividad económica que el país puede generar exportando a la región servicios de formación y consultoría relacionados con ciberseguridad. Resulta difícil estimar con precisión el valor económico de este impacto positivo en la mejora de la ciberseguridad, pero dado el dinamismo del sector TIC uruguayo, que ha experimentado un crecimiento promedio del 11,55% (periodo 2007-2017) y el bajo desarrollo de la ciberseguridad en toda América Latina, este fortalecimiento de la ciberseguridad en Uruguay abre importantes posibilidades de actividad económica.

- 1.7 El cibercrimen se ha convertido en una poderosa industria que ha sobrepasado al tráfico de droga en volumen de recursos financieros generados¹⁹. Como muestra de que estamos ante una industria organizada y desarrollada, una de las reuniones más importantes de hackers a nivel mundial, DEFCON Las Vegas, reúne a más de 20.000 personas todos los años²⁰. Y quienes operan en la industria criminal de los ciberataques pueden acceder a un desarrollado mercado de productos y servicios que apoyan el ciberdelito haciéndolo fácil y de bajo costo²¹. Por ejemplo, un Ataque de Denegación de Servicio (DDoS)²² por una hora cuesta entre US\$5 y US\$20, y un kit de *ransomware*²³ menos de US\$250.
- 1.8 De acuerdo a *National Institute of Standards and Technology* (NIST) ²⁴, el marco de referencia más utilizado a nivel internacional para el diseño de políticas de ciberseguridad, un buen modelo de gestión del riesgo cibernético debe cumplir adecuadamente cinco funciones: identificar, proteger, detectar, responder y recuperar. Este marco permite además la definición de un modelo de gobernanza y de un lenguaje común que facilita la gestión del riesgo, su distribución entre las entidades relevantes para la protección del ciberespacio y la definición de las inversiones en ciberseguridad en función de las áreas en las que se desee disminuir el riesgo.
- 1.9 Las consecuencias de los incidentes digitales incluyen: (i) daño económico, responder y mitigar, impacto a disponibilidad de servicio, compensar los afectados, daño por menor uso de los servicios por menor confianza, como ejemplo un solo ataque llamado NotPetya generó costos por valor de US\$10.000 millones²⁵; (ii) daño reputacional a organizaciones y al gobierno, como ocurrió recientemente con varios websites gubernamentales, incluidos algunos de Presidentes; (iii) daño a la privacidad de los ciudadanos, en el caso del hackeo de la compañía financiera Equifax, los datos de 143 millones de clientes fueron

¹⁹ [How Cyber attacks became more profitable than drug trade](#), Revista Fortune.

²⁰ [DEFCON. Ver datos de asistencia aquí.](#)

²¹ [Information Security Report 2019: Volume 24. February 2019. Symantec.](#)

²² Un ataque DDoS, consiste en la solicitud simultánea de múltiples servicios de un *website* lo que cual supera su capacidad de responder y lo vuelve inoperativo.

²³ Un ransomware es un virus informático sofisticado que bloquea el acceso de los usuarios a los archivos de su dispositivo tecnológico. Con frecuencia, la única forma de rescatar los archivos es pagando un rescate a los ciberatacantes.

²⁴ [NIST](#) es una institución dependiente del Departamento de Comercio del Gobierno de los Estados Unidos que ha desarrollado un [marco de políticas de ciberseguridad](#) de uso generalizado a nivel mundial.

²⁵ [Notpetya](#).

expuestos²⁶; (iv) daño a la inclusión digital y financiera por menor uso de tecnología, como muestra un estudio de FireEye que indica que el 75% de los ciudadanos dejarían de comprar en una empresa en la que se descubre un robo de datos por negligencia en su política de ciberseguridad²⁷; y (v) daño a la democracia y a la cohesión social, como ilustró la experiencia en algunas de las últimas elecciones presidenciales tanto en América como en Europa, cuando varios *gygabites* de correos electrónicos de algunos de los partidos participantes en los procesos electorales fueron expuestos por *hackers* pocos días antes de la votación.

- 1.10 **El principal desafío.** El problema general es el bajo nivel de implantación de la política de ciberseguridad del país que lo deja en situación de vulnerabilidad ante un eventual ataque cibernético²⁸. Los problemas específicos relacionados con el problema general son:
- 1.11 **Falta de capacidades operativas de monitoreo, detección y respuesta de incidentes**²⁹. El hecho de detectar en forma temprana los incidentes permitirá manejarlos de una manera más eficiente, lo que resultará en menores daños y en menor costo de respuesta, ya que los ataques se detectarán en estado menos avanzado. Cuando no existen sistemas de monitoreo o el sistema no es muy sofisticado, los incidentes se detectan una vez que ya han iniciado la producción de daño y este daño crece en progresión geométrica con cada hora que pasa sin solucionarse. En Uruguay, los incidentes de severidad alta o muy alta³⁰ tienen un costo aproximado de remediación de US\$48.000³¹. Este problema específico está relacionado con los siguientes factores causales: (i) actualmente el GSOC solo cuenta con monitoreo perimetral para los Organismos de la Administración Pública, lo cual deja fuera del monitoreo los sistemas internos de cada Institución; (ii) existen limitadas capacidades en el GSOC de analizar las alertas que se generan, entre otros aspectos el sistema actual de monitoreo no cuenta con funcionalidades de *Big Data*, *information sharing* e inteligencia de amenazas³²; y (iii) no existe un mecanismo seguro y confidencial para compartir información con el sector privado relativo a ataques e incidentes.
- 1.12 **Falta de profesionales capacitados en ciberseguridad.** El rápido crecimiento en la necesidad de profesionales en ciberseguridad produjo una brecha entre la oferta y la demanda de los mismos que ha generado una importante escasez³³. Se estima que Uruguay cuenta actualmente con 650 profesionales en

²⁶ [The Washington Post](#). Septiembre 2017.

²⁷ [Security Magazine](#). May 2016.

²⁸ Según el Reporte Ciberseguridad 2016 mencionado anteriormente, Uruguay obtiene 149 puntos de 245 posibles. Como referencia, Israel obtiene 200.

²⁹ Estudio realizado por SecurePro como input para el diseño del proyecto. El Centro de Operaciones de Seguridad (SOC) de Uruguay no alcanza la puntuación media del *Cybersecurity Maturity Model*.

³⁰ AGESIC cuenta con un procedimiento de clasificación de incidentes basado en los estándares *European Union Agency for Network and Information Security*. La clasificación se basa en el impacto institucional, el impacto económico y la cantidad de horas de respuesta al incidente. Los incidentes de severidad alta o muy alta requieren más de 640 horas de experto senior para dar respuesta.

³¹ Dato suministrado por AGESIC con base en la experiencia de los últimos 10 años.

³² Ibid. Nota al pie 30 sobre SecurePro.

³³ A nivel mundial el gap de profesionales de ciberseguridad se estima en 1,5 millones de profesionales para el 2010. [Harvard Business Review](#). Mayo 2017.

ciberseguridad y precisa duplicar esa cifra en los próximos dos años³⁴. Esta brecha de profesionales tiene además un importante elemento de género. Menos del 10% de los profesionales de ciberseguridad del país son mujeres de acuerdo con AGESIC. En AGESIC, de 27 personas que integran el equipo, sólo 3 son mujeres, y en Deloitte Ciberseguridad, de un equipo de 10 personas sólo 1 es mujer. Este problema específico está relacionado con los siguientes factores causales: (i) la oferta formativa en seguridad informática es escasa, poco variada y se reduce al ámbito presencial. De las cuatro universidades uruguayas, sólo la Universidad de la República ofrece un curso de especialización en seguridad de la información. De la oferta formativa de grado y posgrado en el ámbito TIC, solamente el 1% se ofrece en el interior, lo que obliga a la mitad del país a desplazarse a la capital si desea formarse en este tema³⁵; (ii) el número de docentes en la temática es insuficiente para atender la demanda formativa de profesionales en ciberseguridad³⁶; (iii) no existe una estandarización temática en el contenido de la formación que permita definir perfiles profesionales; y (iv) la posibilidad de participar en instancias internacionales de intercambio de conocimiento profesional es escasa³⁷.

- 1.13 **Experiencia del Banco y lecciones aprendidas.** El Banco cuenta con amplia experiencia en el diseño e implementación de proyectos relacionados con el uso de las TIC en la administración pública y en particular con la incorporación de componentes relacionados con la protección del espacio digital tales como: Panamá en Línea (3683/OC-PN), Transformación Digital del Gobierno para Fortalecer la Competitividad (4549/OC-BH), 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), Programa de Apoyo a la Implementación de la Agenda Digital (4650/OC-PR). Además, el Banco ha contado con el apoyo técnico y financiero de los gobiernos de Israel y España a través de las cooperaciones técnicas *Improving Human Resources Capacity in Cybersecurity* (ATN/CF-15598-RG) y Fortalecimiento de la Ciberseguridad en América Latina y el Caribe (ATN/FG-16633-RG). Estas cooperaciones técnicas han financiado la realización de actividades de capacitación de funcionarios y la realización de estudios que constituyen un insumo fundamental para el diseño de esta operación. Asimismo, el Banco ha venido apoyando a AGESIC, la institución responsable de ciberseguridad en Uruguay, durante los últimos diez años a través las siguientes operaciones de gobierno digital: Proyecto para Gestión de Gobierno Electrónico en el Sector Salud (3007/OC-UR); Programa de Mejora de los Servicios Públicos y de la Interacción Estado-Ciudadano (3625/OC-UR); Proyecto para Gestión de Gobierno Electrónico en el Sector Salud II (4300/OC-UR); Programa de Apoyo a la Gestión del Gobierno Electrónico en Uruguay II (2591/OC-UR); Programa para el Fortalecimiento de la Gestión Presupuestaria (3398/OC-UR). Actualmente se encuentra en diseño una operación de préstamo para apoyar el gobierno digital por los próximos cuatro años. Este proyecto es particularmente importante para proteger el trabajo apoyado por el Banco a través de la operación 2591/OC-UR que ha puesto en línea todos los trámites del país e incluye una actividad para crear la figura del

³⁴ *Cybersecurity Excellence Framework*. Octubre 2018. Avnet. Pág. 37.

³⁵ Formación Académica en TIC: Informe 2017. Cámara Uruguaya de Tecnologías de la Información.

³⁶ El país cuenta únicamente con 22 docentes en el ámbito de ciberseguridad que se reúnen periódicamente en el grupo *Hack and Beer*.

³⁷ Conversación con el grupo de docentes en el ámbito de *Hack and Beer*.

Embajador Digital que será especialmente relevante para el manejo internacional de los temas de ciberseguridad del país, además de la operación 4300/OC-UR que pone en funcionamiento la ficha médica digital en el país. Asimismo, actualmente se encuentra en diseño una operación de préstamo para apoyar el fortalecimiento de la gestión estratégica de la seguridad pública en Chile, que incluye un componente de ciberseguridad, que incorpora algunas actividades similares a las de este programa, lo cual permite compartir lecciones aprendidas tanto en la fase de diseño como en la futura implementación de los programas.

- 1.14 Este proyecto es la primera operación dedicada íntegramente a ciberseguridad que el Banco apoya. Dada la necesidad de los países de América Latina y el Caribe de fortalecer sus políticas de ciberseguridad, esta operación es una valiosa oportunidad de aprendizaje, generación de método y replicabilidad en otros países de la región. Uruguay, de acuerdo con el Informe Ciberseguridad 2019, es el país más avanzado de la ALC, a pesar de estar en la mitad del modelo de madurez. Uruguay cuenta con un SOC, un CERT, un equipo de profesionales en ciberseguridad y un marco operativo de ciberseguridad fruto de su propia traducción y adaptación de NIST. Las operaciones previamente ejecutadas con AGESIC han dejado lecciones aprendidas acerca del liderazgo, la coordinación institucional, la participación, el trabajo en equipo y el rol del sector privado que han sido incorporadas en el diseño de esta operación. AGESIC ha involucrado al sector privado del área tecnológica en el diseño de la operación con fin de que pueda contribuir a generar una nueva área de actividad tecnológica de exportación. En el resto de América Latina y el Caribe, sólo 13 países cuentan con una estrategia de ciberseguridad y la mayor parte de ellos no llegan al 40% de la puntuación del modelo de madurez que recoge el Informe Ciberseguridad 2016, lo cual ofrece un gran potencial de trabajo para el Banco y de exportación de conocimiento para Uruguay con base en el trabajo que se llevará a cabo en este programa.
- 1.15 **Alineación estratégica.** El programa está alineado con la Actualización de la Estrategia Institucional (UIS) 2010-2020 (AB-3008) y se alinea estratégicamente con los desafíos de desarrollo de: (i) Inclusión Social e Igualdad, al promover la oferta de formación presencial en ciberseguridad en el interior del país a través de la Universidad Tecnológica (UTEC) acercando esta formación a ciudadanos de escasos recursos económicos; y (ii) Productividad e Innovación, por contribuir al reto “bajos niveles de productividad e innovación” al promover una nueva área de actividad económica de alto valor añadido como la ciberseguridad. El programa también está alineado con las áreas transversales de: (i) Igualdad de Género y Diversidad, a través de la promoción de mujeres para recibir capacitación en temas de ciberseguridad (¶1.19 – Actividad ii); y (ii) Capacidad Institucional y Estado de Derecho, relativo a fortalecer la capacidad de AGESIC para defender el espacio digital del país. Adicionalmente, el programa contribuirá con el Marco de Resultados Corporativos 2016-2019 (GN-2727-6), en los siguientes indicadores: (i) “número de agencias gubernamentales beneficiadas mediante el fortalecimiento de sus instrumentos tecnológicos y de gestión para mejorar la provisión de servicios públicos”; (ii) “número de maestros capacitados”; (iii) “países que usan sistemas nacionales fiduciarios”; (iv) “sistemas de información del delito fortalecidos”; y (v) “proyectos que apoyan los sistemas de innovación”. Además, está alineado con la Estrategia Sectorial sobre las Instituciones para el Crecimiento y el Bienestar Social (GN-2587-2) por aportar al

tema “Instituciones para la Innovación y el Desarrollo Tecnológico” en particular a los objetivos: (i) mejorar las políticas y la acción gubernamental en el sector de las TIC; (ii) desarrollar un capital humano de avanzada; y (iii) fortalecer instituciones y redes. El programa es consistente con el Marco Sectorial de Seguridad y Justicia (GN-2771-7), contribuyendo a la meta de mejorar la eficiencia y la efectividad de las políticas públicas en seguridad ciudadana y justicia en la región, con el propósito de contribuir a la reducción del delito y la violencia³⁸. El programa también está alineado con la Estrategia del Banco con el País con Uruguay 2016-2020 (GN-2836) en su área prioritaria de “mayor eficiencia de instituciones públicas”, en su objetivo estratégico de “fortalecer los sistemas de gestión pública”. Asimismo, la operación se encuentra alineada en el Programa de Operaciones de 2019 (GN-2948). Finalmente, el programa colaborará con la implementación de la Iniciativa “Trámites 100% en Línea”, que forma parte del Programa de Gobierno 2015-2019 de Uruguay y con el cumplimiento del objetivo viii “Confianza y seguridad en el uso de las tecnologías digitales” de la [Agenda Uruguay Digital 2020](#).

B. Objetivos, componentes y costo

1.16 Objetivo del programa. El programa contribuirá a fortalecer la capacidad del país para proteger su espacio digital mejorando la prevención, detección y respuesta a los ataques cibernéticos. Para ello, el programa se estructurará en los siguientes componentes:

1.17 Componente 1. Mejoramiento de las capacidades operativas y herramientas del CERT.uy (US\$5.415.000). Se llevarán a cabo las siguientes actividades: (i) actualización de las herramientas tecnológicas de análisis y gestión de eventos de ciberseguridad, *Security Information Event Management* (SIEM)³⁹; (ii) expansión del sistema de detección de intrusiones NGIPS⁴⁰ incrementando tanto el número de instituciones monitoreadas como las funcionalidades de la herramienta; (iii) incorporación de una plataforma de *Big Data* que permita el intercambio de información con el sector privado⁴¹ y el análisis

³⁸ Contribuye en particular a la dimensión 2 de éxito “La policía actúa basada en resultados y en estrecha colaboración con la comunidad para prevenir, atender y resolver el crimen”.

³⁹ SIEM. Es una herramienta tecnológica que permite integrar las funciones de análisis de información sobre incidentes de ciberseguridad con la gestión de los mismos, contribuyendo a mejorar la capacidad de detección y la eficiencia en el manejo de las respuestas. Actualmente el SIEM tiene una capacidad 4500 EPS (eventos por segundo) y 2 nodos remotos. Tras la implementación del proyecto tendrá una capacidad de 20.000 EPS y 17 nodos remotos.

⁴⁰ *Next Generation Intrusion Prevention System*. Un sistema de sensores ubicados estratégicamente que permite mejorar la capacidad de detectar intrusiones en el sistema.

⁴¹ El marco normativo actual no obliga al sector privado a compartir información de incidentes cibernéticos con CERT.uy, sin embargo, varias empresas ya lo están haciendo con el fin de recibir apoyo para mejorar su protección. Contar con un mecanismo que facilite que esta información se comparta de forma sencilla y segura facilitará que más empresas se sumen a la práctica de compartir con el CERT.uy. AGESIC planea reforzar su apoyo técnico al sector privado y generar instancias de diálogo continuo en las que presente a los expertos del sector privado el trabajo de análisis forense que se realiza con los datos compartidos, de forma que sirva para prevenir incidentes futuros. En esta actividad, el sector privado se refiere fundamentalmente a empresas, con especial atención a aquellas que operan en áreas relacionadas con la infraestructura crítica como la energía o la salud, así como en sectores clave para la economía como las finanzas, la agricultura o el turismo.

inteligente de amenazas⁴²; (iv) herramientas de laboratorio del CERT.uy (forense, pruebas de concepto, desarrollo de sensores y gestión de incidentes, entre otros); (v) servicios especializados relacionados con la instalación y operación del SIEM, los cuales incluirán la parametrización y configuración del SIEM así como los servicios de despliegue y operación de todos los nodos; y (vi) incorporación de actividades de investigación de tecnologías emergentes e innovadoras tales como inteligencia artificial, criptografía y *threat intelligence* con el fin de identificar amenazas y optimizar las respuestas, e incorporación de Recursos Humanos con las cualificaciones necesarias para operar las nuevas herramientas introducidas, especialmente gerentes de proyectos especializados en ciberseguridad y técnicos especialistas de nivel 1, 2, y 3.

- 1.18 **Componente 2. Potenciación del uso de tecnología avanzada para la formación de recursos humanos (US\$1.900.000).** Se llevarán a cabo las siguientes actividades: (i) puesta en funcionamiento de una Plataforma de Simulación de ataques cibernéticos con múltiples escenarios⁴³ que podrán utilizar las instituciones que realicen formación en ciberseguridad con el fin de proporcionar capacitación avanzada y especializada gracias al uso de escenarios sectoriales incluyendo la capacitación al equipo de CERT.uy, a docentes del sector académico y a desarrolladores de *software* para el uso de la Plataforma; y (ii) puesta en funcionamiento de una plataforma de *e-Learning* para la formación de profesionales en ciberseguridad que permita el acceso a formación práctica especializada y la difusión de conocimiento acerca de las políticas, metodologías y estándares de ciberseguridad promovidos por AGESIC.
- 1.19 **Componente 3. Fortalecimiento del ecosistema de conocimiento de ciberseguridad a nivel nacional (US\$1.850.000).** Se llevarán a cabo las siguientes actividades: (i) apoyar el desarrollo de curricula de formación en ciberseguridad tanto a nivel técnico como de grado y posgrado, que pueda ser utilizada por diferentes centros académicos del país, para la cual se contratará el apoyo de un centro académico internacional de prestigio en el ámbito de la ciberseguridad, y la formación de docentes en ciberseguridad para la impartición de la curricula; (ii) creación de una red nacional de expertos con activas vinculaciones internacionales y en la que se promoverá activamente la incorporación de la mujer al ámbito profesional de la ciberseguridad⁴⁴; (iii) actividades de difusión nacional e internacional incluyendo intercambios y

⁴² La capacidad de prevención será fortalecida por la combinación de la actualización de los sistemas SIEM (actualmente AGESIC utiliza la herramienta QRadar), la instalación de sondas en los ministerios más importantes y la incorporación de una plataforma de "*Big Data*".

⁴³ Las plataformas de simulación se utilizan frecuentemente en los países más avanzados en ciberseguridad con el fin de poner a los profesionales en la situación de gestionar ciberataques que operan como en la realidad en cuanto a su funcionamiento y a sus efectos.

⁴⁴ Los miembros femeninos de la Red realizarán actividades voluntarias de promoción de la ciberseguridad en centros de formación secundaria y universidades, con el fin de interesar al género femenino en la profesión. Además, se llevarán a cabo iniciativas de promoción de la ciberseguridad como profesión entre las mujeres probando el impacto de diferentes estrategias de atracción y documentando la efectividad de cada una de ellas. Estas estrategias incluyen el uso de argumentos económicos, de flexibilidad laboral y de motivación a través de profesionales femeninas de prestigio en la profesión que puedan servir como referencia (Ver [PME](#) ¶3.17, 3.20 y 3.22, así como el Cuadro 7).

eventos de promoción y comunicación; y (iv) diseño de una estrategia de gestión del cambio⁴⁵.

- 1.20 **Principales beneficiarios.** Los principales beneficiarios serán la población en general y, en particular, las empresas que verán sus espacios digitales más protegidos. Además, como se desprende la matriz de resultados, las instituciones públicas serán directamente beneficiadas porque su infraestructura tecnológica estará más protegida. Asimismo, las cinco universidades públicas y privadas, que representan la totalidad del universo de universidades que ofrecen formación sobre sistemas de información en Uruguay, se verán beneficiadas porque introducirán la ciberseguridad en su oferta formativa y sus docentes actualizarán su conocimiento en seguridad. Además, el sector privado se beneficiará por la mayor disponibilidad de profesionales en ciberseguridad y el sector empresarial TIC del país se beneficiará por el reposicionamiento de Uruguay como un país avanzado en ciberseguridad con una oferta de profesionales y servicios que puede atender necesidades regionales. Como colectivo beneficiario de esta operación, es especialmente destacable el género femenino que está subrepresentado en el colectivo de profesionales de ciberseguridad y recibirá acciones específicas de motivación para incorporarse a este ámbito profesional.

C. Indicadores claves de resultados

- 1.21 **Resultados esperados.** El impacto de este programa será el aumento de la madurez de la capacidad de seguridad cibernética de Uruguay y el aumento del nivel de madurez promedio en ciberseguridad de las organizaciones públicas. Los resultados esperados serán: (i) la mejora de las capacidades operativas de monitoreo, detección y respuesta a incidentes de ciberseguridad; y (ii) el aumento del capital humano capacitado en ciberseguridad, incluyendo un indicador *pro-gender* para medir el porcentaje de mujeres que reciben entrenamiento en el tema.
- 1.22 **Evaluación económica.** La [evaluación económica](#), realizada a través de un análisis costo-beneficio, incluye tres formas en las cuales se espera que el programa genere retornos monetarios: (i) la disminución de costos operativos en remediación de los daños causados por ciberataques a las instituciones públicas, a través de una disminución en la proporción de ataques que son de alta severidad; (ii) la disminución en el impacto económico causado por los ciberataques a las instituciones públicas, gracias a una mayor capacidad de prevención y respuesta; y (iii) la generación de actividad económica a través de la formación de profesionales en ciberseguridad y su subsecuente inserción al mercado laboral. Los costos considerados son los gastos del programa abarcando tanto el aporte BID como la contrapartida local. Cada segmento del análisis de beneficios cuenta con supuestos y metodología propia, que se describen en el anexo. Los únicos supuestos compartidos entre ellos son el de la tasa de descuento del 12%, estándar para el Banco, y el plazo de contabilización de beneficios de 10 años. Se espera que el programa tenga una alta rentabilidad, aun

⁴⁵ La estrategia incluirá actividades de información, comunicación y participación para lograr la implicación y el apoyo de los funcionarios públicos hacia las actividades de ciberseguridad propuestas por el programa.

en el escenario conservador, se estima una tasa interna de retorno del 45%, un valor presente neto de más de US\$40 millones, y una razón costo-beneficio de 7,07.

II. ESTRUCTURA DE FINANCIAMIENTO Y PRINCIPALES RIESGOS

A. Instrumentos de financiamiento

- 2.1 El presente programa, con un costo total de US\$10 millones, se estructura bajo la modalidad de préstamo de inversión específica, con cargo al Capital Ordinario del Banco por US\$8 millones. La operación tendrá contrapartida local por U\$2 millones. El Cuadro 1 describe el presupuesto consolidado por componente, cuyo detalle se muestra en el [presupuesto detallado](#). El Organismo Ejecutor (OE) ha planificado ejecutar todas las actividades del proyecto en cuatro años (ver Cuadro 2) sobre la base de los siguientes criterios: (i) la demostrada capacidad de ejecución de AGESIC en las cinco operaciones de préstamo que ha ejecutado previamente⁴⁶; y (ii) el avance en el trabajo previo de consultoría y recopilación de información para los dos procesos de compra más complejos, el relacionado con el sistema de monitoreo y el relativo al simulador de entrenamiento.

Cuadro 1. Presupuesto del proyecto (US\$)

Componentes	BID	Local	Total	%
Componente 1. Mejoramiento de las capacidades operativas y herramientas del CERT.uy	4.438.525	976.475	5.415.000	54
Componente 2. Potenciación del uso de tecnología avanzada para la formación de recursos humanos	1.557.377	342.623	1.900.000	19
Componente 3. Fortalecimiento del ecosistema de conocimiento de ciberseguridad a nivel nacional	1.516.393	333.607	1.850.000	19
Administración u otros gastos contingentes	487.705	347.295	835.000	8
Total	8.000.000	2.000.000	10.000.000	100

Cuadro 2. Programa tentativo de desembolsos (US\$)

Fuente	Año 1	Año 2	Año 3	Año 4	TOTAL
BID	1.606.595	2.102.496	2.328.589	1.962.319	8.000.000
Local	368.451	477.549	527.290	626.711	2.000.000
%	20	26	28	26	100

B. Riesgos ambientales y sociales

- 2.2 De acuerdo con la Política de Medio Ambiente y Cumplimiento de Salvaguardias del Banco (GN-2208-20, OP-703), la operación fue clasificada como Categoría

⁴⁶ AGESIC ha venido ejecutando de acuerdo a los planes establecidos las siguientes actividades: Proyecto para Gestión de Gobierno Electrónico en el Sector Salud (3007/OC-UR); Programa de Mejora de los Servicios Públicos y de la Interacción Estado-Ciudadano (3625/OC-UR); Proyecto para Gestión de Gobierno Electrónico en el Sector Salud II (4300/OC-UR); Programa de Apoyo a la Gestión del Gobierno Electrónico en Uruguay I y II (1970/OC-UR y 2591/OC-UR).

“C”. El programa no financiará ningún componente de infraestructura física, por lo cual no se prevén riesgos ambientales o sociales asociados.

C. Riesgos fiduciarios

- 2.3 La AGESIC ha tenido una amplia y positiva experiencia como OE de operaciones con el Banco. Durante el taller de riesgos no se han identificado riesgos fiduciarios y de acuerdo con el Anexo de Acuerdos y Requisitos Fiduciarios (Anexo III), el riesgo fiduciario es evaluado como bajo, teniendo en cuenta sus antecedentes en el rol de organismo ejecutor corroborado por los sucesivos informes de auditoría externa que anualmente el Tribunal de Cuentas de la República (TCR) emite con opinión favorable sobre la ejecución de los proyectos que administra.

D. Otros riesgos y temas claves

- 2.4 Se identificaron los siguientes riesgos:

- a. **Gobernanza.** Se identificaron dos riesgos medios: (i) demoras en los acuerdos institucionales, este riesgo podría afectar la implementación de los Componentes 1 y 3, en la medida que gran parte de la implementación del componente requiere de la participación activa de instituciones externas a AGESIC. Con el fin de mitigarlo, se creará un Comité Asesor integrado por todas las instituciones académicas participantes en el cual se consultarán las decisiones más importantes relacionadas con la ejecución del proyecto y se definirán los planes de trabajo; y (ii) resistencia al cambio, aunque AGESIC cuenta con 10 años de experiencia desarrollando proyectos tecnológicos en la Administración Central, es la primera vez que se va a hacer una actividad de este tipo que concederá un importante control de la infraestructura tecnológica de los Ministerios más importantes a una institución central. Esto puede generar algunas resistencias a nivel de gerentes sectoriales y de tecnología en estos Ministerios. Con el fin de mitigar esta resistencia, se han incorporado al proyecto actividades de gestión del cambio que pondrán énfasis en la comunicación y la participación. Además, se incluye un importante esfuerzo de capacitación.
- b. **Gestión pública y gobernabilidad.** Se identificó como riesgo medio el cambio de gobierno que puede afectar a la prioridad de la ciberseguridad en la agenda del sector público. A pesar de que hay un proceso electoral en octubre de 2019, la Agenda Digital es política de Estado y varios partidos políticos han dado mensajes positivos acerca del trabajo de AGESIC. Con el fin de mitigarlo, se mantendrá un diálogo con las diferentes fuerzas políticas acerca de la importancia de mantener protegido el espacio digital uruguayo, y se involucrará el sector privado en el diseño y ejecución del proyecto.
- c. **Sostenibilidad fiscal.** Se identificó como riesgo medio, restricciones fiscales que pueden limitar la disponibilidad de recursos de contrapartida y el espacio fiscal para la ejecución. Uruguay vive un momento de restricciones fiscales que está obligando al gobierno a contener el gasto y la inversión públicas lo cual puede afectar doblemente la ejecución del proyecto, tanto a los recursos de contrapartida como a la disponibilidad de espacio fiscal para la ejecución de los componentes financiados con recursos BID. Para mitigar este riesgo

AGESIC presentará al MEF, Ministerio responsable de la asignación presupuestaria, de forma detallada la importancia económica de esta operación con el fin de asegurar comprenda la magnitud del impacto económico que podría derivarse de tener un espacio digital desprotegido.

- 2.5 **Propiedad intelectual y sostenibilidad.** Cerca de la mitad de la inversión incluida en este proyecto se enfoca en la compra de bienes o servicios de tecnología. AGESIC, cuenta con una amplia experiencia en la compra y gestión de tecnología. Actualmente gestiona más de 60 aplicaciones tanto de *software* libre como propietario y cuenta con un área de tecnología y otra de operaciones con dilatada experiencia en la operación de soluciones tecnológicas. Algunas de estas aplicaciones requieren relaciones contractuales con reconocidos proveedores del sector⁴⁷. En su arquitectura de nube presta servicios relacionados con más de 20 aplicaciones a numerosas dependencias de la administración pública. AGESIC, tiene además una política relacionada con *software* público⁴⁸ y su reutilización en la administración pública, ofreciendo más de 25 aplicaciones para uso tanto por parte del Gobierno Uruguayo como por el resto de los gobiernos de ALC a través de licencia GNU GPL 3⁴⁹. Los 12 años de experiencia de AGESIC como responsable de la Agenda Digital de Uruguay le han permitido desarrollar una política de gestión de la tecnología que incluye *software* público y propietario, que prevé presupuestariamente la renovación periódica de aplicaciones y equipos y que cuenta con un equipo humano cualificado⁵⁰ para gestionarla como indica su posición como el país más digitalizado de la región. Además, la agenda digital se ha consolidado como una política del país como muestra el hecho de que Uruguay esté implementando actualmente la tercera versión de su agenda en los últimos 10 años⁵¹. La sostenibilidad técnica y financiera de las soluciones tecnológicas, por tanto, está basada en la estabilidad que tiene la agenda digital que gestiona AGESIC tras 12 años de operación, la calidad del servicio que AGESIC presta al resto las instituciones del gobierno, el buen trabajo de comunicación de resultados que realiza AGESIC y la participación del sector privado.

III. PLAN DE IMPLEMENTACIÓN Y GESTIÓN

A. Resumen de los arreglos de implementación

- 3.1 **Mecanismo de ejecución.** El prestatario será la República Oriental del Uruguay y el OE será la República Oriental del Uruguay por intermedio de AGESIC. Esta agencia tendrá la responsabilidad básica ante el Banco por la ejecución, manteniendo la relación directa con éste. El programa se alinea con el mandato

⁴⁷ En la actualidad, AGESIC tiene relaciones contractuales con Microsoft, IBM y Oracle, entre otras reconocidas empresas TIC.

⁴⁸ [Software Público Uruguayo](#).

⁴⁹ Uruguay ha liderado y participa activamente en la iniciativa de *software* público de ALC financiada por el un Bien Público Regional del BID. Ver [aquí](#).

⁵⁰ AGESIC cuenta con más de 300 funcionarios de los cuales casi un tercio tiene formación en sistemas.

⁵¹ [Uruguay Digital: 10 años de política digital](#).

legal y la estructura administrativa y operacional existentes en la AGESIC⁵². La normativa aplicable establece que la AGESIC es responsable de regir la ejecución de todo lo vinculado con la implementación de planes y proyectos específicos en materia de gobierno electrónico y seguridad de la información.

- 3.2 **Mecanismo de coordinación interna.** El programa estará a cargo de la Dirección de Seguridad de la Información de AGESIC. Su Director/a, actuará como coordinador/a general del programa y será responsable de la conducción del mismo y mantendrá las reuniones estratégicas y de planificación con el Banco. Para el ejercicio de su función el coordinador general contará con el siguiente apoyo: (i) un coordinador operativo que se encargará de implementar el plan operativo anual, solicitar desembolsos, proponer las contrataciones y adquisiciones, informar sobre el uso de los recursos, y remitir al Banco los Planes Operativos Anuales (POA), Planes de Adquisiciones (PA) e informes de progreso; (ii) un consultor senior de administración y finanzas; y (iii) consultor *senior* de adquisiciones.
- 3.3 **Mecanismo de coordinación externa.** Con el fin de facilitar el diálogo y la coordinación con los actores más relevantes relacionados con la ejecución de esta operación, AGESIC establecerá un Comité Asesor que estará integrado por representantes de las seis universidades que ofrecen formación sobre sistemas de información en Uruguay⁵³. A este Comité Asesor se irán incorporando instituciones del ámbito público y privado en función de las necesidades que se identifiquen en el marco de este Comité durante el proceso de implementación de las actividades.
- 3.4 Para las relaciones de trabajo con las instituciones públicas que se beneficiarán de esta operación, AGESIC ya cuenta con convenios marco firmados⁵⁴ con todas las instituciones públicas como parte de la agenda de trabajo de gobierno digital. Bajo estos convenios marco, AGESIC y cada institución pública firmarán acuerdos específicos, con el fin de incorporar al plan de trabajo las acciones relacionadas con ciberseguridad. Para la relación con los centros académicos que participarán en el programa, AGESIC establecerá un convenio de adhesión estándar que establecerá los beneficios que recibirán las instituciones y los compromisos que deben asumir para participar.
- 3.5 **Condiciones contractuales especiales previas al primer desembolso del financiamiento. Será condición contractual especial previa al primer**

⁵² Como se indica en el pie de página 3, AGESIC fue creada por Ley No. 17.930 (arts. 72) 19 de diciembre de 2005 como entidad responsable de gobierno electrónico. Como se indica en pie de página 4, la ley 18.719 de 27 de diciembre de 2010, crea dentro de la AGESIC la Dirección de Seguridad de la Información con la función de proteger la seguridad cibernética del sector público. La normativa asociada a AGESIC puede consultarse [aquí](#).

⁵³ Universidad de la República, UTEC, Universidad ORT Uruguay, Universidad Católica, Universidad de la Empresa y Universidad de Montevideo.

⁵⁴ Desde el año 2009 a la fecha AGESIC ha suscripto convenios y planes de trabajo con los distintos organismos estatales para el desarrollo e implementación de 90 soluciones y aplicaciones de gobierno electrónico, financiados con recursos de los préstamos 1970/OC-UR y 2591/OC-UR mediante un mecanismo de fondos concursables. Los convenios marco definen como objetivo general el interés de ambas instituciones en colaborar en el desarrollo de actividades relacionadas con la agenda digital. Los convenios específicos detallan actividades particulares que se desarrollarán en el marco del convenio marco, definen las responsabilidades de cada una de las partes y regulan la transferencia de conocimiento y capacitación. Se adjuntan [aquí](#) ejemplos de ambos convenios.

desembolso del financiamiento que el Prestatario, por sí o por intermedio del OE, haya presentado al Banco evidencia de: (i) la designación, como coordinador general del programa, del Director de la Dirección de Seguridad de la Información de AGESIC; y (ii) el nombramiento del coordinador operativo del programa. Estos dos roles son críticos para revisar la planificación de la operación e iniciar la implementación de la misma.

- 3.6 Los Acuerdos y Requisitos Fiduciarios establecen el marco de gestión financiera y de planificación, al igual que de supervisión y ejecución de adquisiciones aplicables para la ejecución del programa.
- 3.7 El desarrollo de las actividades del programa seguirá una programación instrumentada a través del Plan de Ejecución Plurianual (PEP) (el cual contiene el detalle para la ejecución de la totalidad del programa). Su revisión anual se plasmará en el respectivo POA. El PEP deberá ser modificado cada año teniendo en cuenta el avance real del programa. Las revisiones anuales del PEP y del POA deberán ser remitidas al Banco para aprobación.
- 3.8 **Adquisición de obras, bienes y servicios distintos de consultorías y servicios de consultoría.** Las adquisiciones financiadas total o parcialmente con recursos del Banco serán realizadas de acuerdo con las Políticas para la Adquisición de Obras y Bienes Financiados por el BID (GN-2349-9) y las Políticas para la Selección y Contratación de Consultores Financiados por el BID (GN-2350-9).
- 3.9 **Selección directa.** El programa estará contratando a los consultores individuales identificados en el PA de la operación. Debido a la necesidad de mantener la continuidad del enfoque técnico durante la ejecución del proyecto, en el PA acordado se prevé la recontractación de consultores individuales que previamente fueron contratados con recursos de los préstamos 3007/OC-UR y 3625/OC-UR que continuarán prestando servicios para la presente operación, lo que se encuentra en conformidad con lo dispuesto en la sección 5.4(a) de la Sección V de las Políticas GN-2350-9, entendiéndose que las condiciones contractuales de los consultores identificados permanecen idénticas y el desempeño satisfactorio de cada consultor será medido anualmente. Estos consultores cumplirán funciones técnicas relacionadas con el CERT.uy y el SOC, así como funciones de coordinación técnica del proyecto, análisis presupuestal y financiero, monitoreo, gestión financiero-contable y de adquisiciones, y los contratados serán por un monto aproximado de hasta US\$1.361.000 durante los cuatro años de duración del programa⁵⁵. El [PA](#) contiene el detalle de las adquisiciones que se implementarán durante la ejecución, así como los procedimientos aplicados por el Banco para su examen. Las contrataciones de consultorías y servicios distintos de consultoría que se realizarán mediante los servicios de la *United Nations Office for Project Services, United Nations Development Programme* o Fundación Julio Ricaldoni, de acuerdo a los convenios que AGESIC mantiene serán sujetas a las Políticas del Banco.

⁵⁵ Estos consultores fueron seleccionados inicialmente por comparación de calificaciones, con no objeción previa del Banco en todos los casos.

- 3.10 **Desembolsos.** La principal modalidad de desembolsos será la de “anticipos” basado en las necesidades reales de liquidez. Preferentemente, estos anticipos se harán en forma semestral, una vez se haya hecho la rendición de cuentas de por lo menos el 70% del monto anticipado⁵⁶. Como documentación se requerirá la presentación de los formularios de rendición y la planilla de planificación financiera. La revisión de la documentación se hará en forma ex post.
- 3.11 **Auditorías.** Durante la ejecución el OE presentará al Banco anualmente los estados financieros auditados del programa, de conformidad con la Política de Gestión Financiera OP-273-6, dentro de los 120 días posteriores a la finalización del año fiscal. Los estados financieros auditados de cierre del programa serán presentados dentro de los ciento veinte (120) días siguientes al vencimiento del plazo original de desembolso o sus extensiones. La auditoría de dichos estados financieros podrá ser realizada por el TCR o por una firma de auditoría.

B. Resumen de los arreglos para el monitoreo de resultados

- 3.12 **Monitoreo por parte del OE.** Entre otros se utilizarán los siguientes documentos: (i) Matriz de Resultados (MdR); (ii) [PEP](#); (iii) [POA](#); (iv) Plan de Monitoreo y Evaluación ([PME](#)); (v) [PA](#); (vi) Matrices de Riesgo; (vii) Plan de Desembolsos; y (viii) Informes de Monitoreo del Progreso (PMR). El OE enviará informes semestrales de avance para la revisión del Banco.
- 3.13 **Monitoreo por parte del Banco.** Se realizarán misiones de supervisión o visitas de inspección, dependiendo de la importancia y complejidad de la ejecución, siguiendo el cronograma definido en el PEP. A los efectos del seguimiento, el Banco utilizará el sistema PMR, que recoge la estimación de los desembolsos y del cumplimiento de metas físicas y resultados.
- 3.14 Se realizará anualmente al menos una reunión conjunta con el OE y el Banco, para discutir, entre otros aspectos: (i) el avance de las actividades identificadas en el POA; (ii) el nivel de cumplimiento de los indicadores establecidos en la MdR; (iii) el POA para el año siguiente; y (iv) el PA para los próximos 18 meses y las posibles modificaciones de las asignaciones presupuestarias por componente.
- 3.15 **Evaluación.** Para realizar la evaluación del programa se utilizará la MdR y el [PME](#). Dado el carácter innovador de esta operación, se contempla realizar una serie evaluaciones y productos de conocimiento que tienen como objetivo la generación de evidencia y aprendizajes sobre la costo-efectividad de invertir en ciberseguridad. En efecto, se tiene previsto realizar una evaluación intermedia, una final, una evaluación de impacto y el desarrollo de una metodología que permita medir el impacto económico de los ciberataques en Uruguay. La evaluación intermedia se realizará una vez transcurridos 24 meses luego de la entrada en vigencia del contrato de préstamo o cuando se haya comprometido el 50% del monto total del préstamo, lo que ocurra primero. Esa evaluación tendrá como principales objetivos revisar el avance de todas las actividades programadas

⁵⁶ Conforme a la Política de Gestión Financiera OP-273-6, se justifica la aplicación de este porcentaje debido a que las Entidades de la Administración Central, a la que pertenece AGESIC, deben disponer del financiamiento en cuentas del Banco Central para comprometer nuevas obligaciones. Asimismo, el procesamiento de pagos requiere la intervención preventiva del TCR y la Contaduría General de la Nación.

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. La evaluación final se realizará cuando haya concluido el plazo original de desembolsos o sus extensiones, o se haya comprometido el 90% del monto del préstamo, lo que ocurra primero; y sus objetivos serán verificar el avance en el cumplimiento de las metas previstas para cada uno de los resultados esperados y la generación de los productos por componente.

- 3.16 **Evaluación de impacto.** Se llevará a cabo una evaluación de impacto bajo la metodología de estudio aleatorizado controlado que tiene como objetivo principal responder las siguientes preguntas: (i) ¿Existe una manera efectiva y costo-eficiente de aumentar la demanda por cursos de ciberseguridad?; y (ii) ¿Cuál es la estrategia más efectiva y costo-eficiente para cerrar la brecha de género en ciberseguridad? Para lograr este objetivo, la evaluación se apoyará en las actividades del Componente 3, que se alinean con la generación de capital humano y con el cierre de la brecha de género de profesionales en ciberseguridad, se espera obtener evidencia causal que brinde recomendaciones de política pública sobre la implementación de programas que promueven la demanda por cursos y carreras profesionales en TIC.
- 3.17 **Estimación del impacto económico de ciberataques.** Este documento de evaluación tendrá como objetivo generar conocimiento sobre el impacto económico de los ciberataques y los beneficios económicos de invertir en la protección del espacio digital. Para lograr este objetivo se pretende formular una metodología que considere un sistema de clasificación de ciberataques y un protocolo de respuestas ante incidentes, asimismo, en acuerdo con la AGESIC ésta se aplicará de manera piloto en un conjunto de instituciones públicas uruguayas y se espera tener como resultado un mejor dimensionamiento de la magnitud y la probabilidad de los riesgos que se evitan bajo la implementación de una política pública de ciberseguridad.

Matriz de Efectividad en el Desarrollo		
Resumen		
I. Prioridades corporativas y del país		
1. Objetivos de desarrollo del BID	Sí	
Retos Regionales y Temas Transversales	-Inclusión Social e Igualdad -Productividad e Innovación -Equidad de Género y Diversidad -Capacidad Institucional y Estado de Derecho	
Indicadores de desarrollo de países	-Agencias gubernamentales beneficiadas por proyectos que fortalecen los instrumentos tecnológicos y de gestión para mejorar la provisión de servicios públicos (#)* -Maestros capacitados (#)* -Países que usan sistemas nacionales fiduciarios (#)* -Sistemas de información del delito fortalecidos (#)* -Proyectos que apoyan los ecosistemas de innovación (#)*	
2. Objetivos de desarrollo del país	Sí	
Matriz de resultados de la estrategia de país	GN-2836	Fortalecer los sistemas de gestión pública
Matriz de resultados del programa de país	GN-2948	La intervención está incluida en el Programa de Operaciones de 2019.
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		8.2
3.1 Diagnóstico del Programa		1.8
3.2 Intervenciones o Soluciones Propuestas		4.0
3.3 Calidad de la Matriz de Resultados		2.4
4. Análisis económico ex ante		9.0
4.1 El programa tiene una TIR/VPN, o resultados clave identificados para ACE		3.0
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		8.5
5.1 Mecanismos de Monitoreo		2.2
5.2 Plan de Evaluación		6.4
III. Matriz de seguimiento de riesgos y mitigación		
Calificación de riesgo global = magnitud de los riesgos*probabilidad		Medio
Se han calificado todos los riesgos por magnitud y probabilidad		Sí
Se han identificado medidas adecuadas de mitigación para los riesgos principales		Sí
Las medidas de mitigación tienen indicadores para el seguimiento de su implementación		Sí
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)	Sí	Administración financiera: Presupuesto, Tesorería, Contabilidad y emisión de informes. 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		

Nota: (*) Indica contribución al Indicador de Desarrollo de Países correspondiente.

El objetivo principal de la operación es fortalecer la capacidad del país para proteger su espacio digital mejorando la prevención, detección y respuesta a los ataques cibernéticos. Para lograr esto, el proyecto define dos áreas específicas de intervención. La primera, propone una inversión tecnológica para mejorar la capacidad de monitorear incidentes a través un Sistema de Manejo de Eventos en Seguridad de la Información. La segunda, se concentra en la formación de capital humano a través de la creación de cursos, diseño de currículos y capacitación docente en ciberseguridad y la implementación de una plataforma virtual para estudiantes y servidores públicos.

El diagnóstico del proyecto describe que a pesar de que Uruguay tiene un alto desarrollo en gobierno digital, el país no tiene la misma fortaleza en la protección del espacio digital. Por esta razón, la gestión de los riesgos digitales es un reto importante para Uruguay y la región. En el mismo sentido, el diagnóstico identifica brechas de habilidades importantes. Actualmente, el mercado laboral demanda al menos 200 profesionales en ciberseguridad y las universidades solo ofrecen un curso de especialización, las soluciones se encuentran alineadas a los problemas, aunque no hay evidencia de la efectividad de estas, adicionalmente algunos indicadores de producto no son SMART.

El análisis económico provee una cuantificación de algunos beneficios económicos. Este cuantifica beneficios asociados con: (i) la reducción de costos de remediación por daños causados por ciberataques; (ii) una caída en el impacto económico causado por ciber ataques a las instituciones públicas y (iii) la generación de actividad económica a través del entrenamiento de profesionales en ciberseguridad y su subsecuente inserción al mercado laboral. Los supuestos d de los beneficios esperados están fundamentados en experiencias internacionales como Estados Unidos y Estonia. Los costos incluyen mantenimiento e inversiones asociados con el préstamo, este análisis concluye que el Proyecto tiene un valor presente neto de US\$40 millones.

El proyecto presenta un plan de monitoreo y evaluación robusto, este considera dos evaluaciones diferentes, la primera es una evaluación económica expost para medir los efectos del componente res en la creación de capital humano, empleo e inclusión de las mujeres en el área TICs.

MATRIZ DE RESULTADOS

Objetivo del Proyecto:	El programa contribuirá a fortalecer la capacidad del país para proteger su espacio digital mejorando la prevención, detección y respuesta a los ataques cibernéticos.
-------------------------------	--

IMPACTO ESPERADO

Indicadores	Unidad de Medida	Línea de Base	Año Línea de Base	Año 1	Año 2	Año 3	Año 4	Meta Final	Medios de Verificación	Comentarios
IMPACTO #1: Madurez de Capacidad de Seguridad Cibernética aumentada										
Madurez de capacidad de seguridad cibernética nacional	Puntaje	149	2016				165	165	Informe OEA BID	<p>Este es un indicador que refleja las capacidades a nivel nacional, el máximo puntaje posible es 245 puntos.</p> <p>El documento <i>“Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States”</i> estudia Estados Unidos, Estonia, Korea del Sur e Israel con base en el modelo de madurez elegido para medir el impacto de esta operación. El documento muestra que las inversiones realizadas por</p>

Indicadores	Unidad de Medida	Línea de Base	Año Línea de Base	Año 1	Año 2	Año 3	Año 4	Meta Final	Medios de Verificación	Comentarios
										<p>estos países en fortalecimiento de su capacidad tecnológica y en la formación de recursos humanos ha contribuido a posicionarlos como países avanzados en la protección de sus ciberespacios. De hecho, en este modelo de madurez, de 49 indicadores, 5 tienen que ver con educación y 9 con fortalecimiento de capacidades tecnológicas incluidas en este programa.</p> <p>Los esfuerzos de educación de cada país pueden verse en las siguientes páginas: Estonia pg 15-16, Israel pg 27-28, Korea pg 38-39, Estados Unidos pg 48-49.</p>
Nivel de madurez promedio en ciberseguridad de las organizaciones públicas	Puntaje	1,5	2018				2,5	2,5	Auditoría externa de marco de ciberseguridad	Este es un indicador que refleja las capacidades de 10 entidades públicas más

Indicadores	Unidad de Medida	Línea de Base	Año Línea de Base	Año 1	Año 2	Año 3	Año 4	Meta Final	Medios de Verificación	Comentarios
										digitalizadas de Uruguay, el puntaje máximo posible es 4.

RESULTADOS ESPERADOS

Indicadores	Unidad de Medida	Línea de Base	Año Línea de Base	Año 1	Año 2	Año 3	Año 4	Meta Final	Medios de Verificación	Comentarios
RESULTADO #1: Capacidades operativas de monitoreo, detección y respuesta de incidentes de ciberseguridad mejorada										
Número de organizaciones públicas monitoreadas a través del SOC	Número de ministerios	2	2018	2	5	11	17	17	Reporte anual de la dirección de ciberseguridad informática	Este indicador no refleja el flujo anual sino la cantidad de instituciones acumuladas.
Número de incidentes cibernéticos detectados anual	Número de incidentes	2.043	2018	2.250	3.267	6.889	10.000	10.000	Reporte anual de la dirección de ciberseguridad informática	Se entiende como incidente “una violación o una amenaza inminente de violación a una política de seguridad de la información implícita o explícita, así como un hecho que compromete la seguridad de un sistema (confidencialidad, integridad o disponibilidad). (Decreto No. 451/009 de 28 de

Indicadores	Unidad de Medida	Línea de Base	Año Línea de Base	Año 1	Año 2	Año 3	Año 4	Meta Final	Medios de Verificación	Comentarios
										<p>Setiembre 2009-Art.3).</p> <p>El reporte "Informe de Incidentes. Activity Report" del Centro Criptológico Nacional del Gobierno de España, muestra que a medida que el gobierno invirtió en su capacidad de monitoreo, se incrementó la cantidad de incidentes detectados en todos los niveles de peligrosidad, ver página 41.</p>
Porcentaje de incidentes cibernéticos de alto impacto	Porcentaje	2,1	2018	2,25	1,84	1,51	1,24	1	Reporte anual de la dirección de ciberseguridad informática	De acuerdo al documento de procedimiento de clasificación de incidentes de AGESIC, son de alto impacto los que precisan más de 640 horas de experto <i>senior</i> para su solución.
RESULTADO #2: Capital humano capacitado en ciberseguridad aumentado										
Número de personas que han tomado al menos 40 horas de capacitación en	Número de personas	50	2018	0	0	150	150	350	Registros de estudiantes de las entidades de educación terciaria	Este es indicador que mide el flujo de personas capacitadas en

Indicadores	Unidad de Medida	Línea de Base	Año Línea de Base	Año 1	Año 2	Año 3	Año 4	Meta Final	Medios de Verificación	Comentarios
ciberseguridad anual										ciberseguridad de manera anual.
Mujeres que han tomado al menos 40 horas de capacitación en ciberseguridad anual	Porcentaje	0	2018	0	0	15	20	25	Registros de estudiantes de las entidades de educación terciaria	<i>Pro-Gender</i> Este es el indicador que mide el flujo de personas capacitadas en ciberseguridad de manera anual.

PRODUCTOS

Productos	Unidad de Medida	Línea de Base	Año Línea de Base	Año 1	Año 2	Año 3	Año 4	Meta Final	Medios de Verificación	Comentarios
Componente #1: Mejoramiento de las capacidades operativas y herramientas del CERT.uy										
1.1 Licencia de Qradar actualizadas	Licencia	0	2018	1	0	0	0	1	Contrato de licencia de Qradar	
1.2 Sistema NIGPS de detección de intrusiones en funcionamiento	Sistema	0	2018	0	0	1	0	1	AGESIC Informes de programa	
1.3 Plataforma de <i>Big Data</i> en funcionamiento	Plataforma	0	2018	0	0	1	0	1	AGESIC Informes de programa	

Productos	Unidad de Medida	Línea de Base	Año Línea de Base	Año 1	Año 2	Año 3	Año 4	Meta Final	Medios de Verificación	Comentarios
1.4 Laboratorio del CERT Instalado	Laboratorio	0	2018	0	0	1	0	1	AGESIC Informes de programa	Este producto incluye: forense, pruebas de concepto, desarrollo de sensores y gestión de incidencias.
1.5 Sistema SIEM implementado	Sistema	0	2018	0	1	0	0	1	Reporte SIEM elaborado por AGESIC	
1.6 CERT equipado y en funcionamiento	Sistema	0	2018	0	0	1	0	1	AGESIC Informes de programa	Se entiende como sistema un conjunto de tecnologías, métodos y personas con las cualificaciones requeridas para gestionar los incidentes cibernéticos que llegan la CERT.
Componente #2: Potenciación del uso de tecnología avanzada para la formación de recursos humanos										
2.1 Plataforma de simulación de ataques cibernéticos en funcionamiento	Plataforma	0	2018	1	0	0	0	1	AGESIC Informes de programa	Para que la plataforma esté funcionamiento, se requiere que el <i>software</i> esté instalado y el equipo del CERT capacitado.
2.2 Plataforma de <i>e-learning</i> instalada	Plataforma	0	2018	0	0	1	0	1	AGESIC Informes de programa	

Productos	Unidad de Medida	Línea de Base	Año Línea de Base	Año 1	Año 2	Año 3	Año 4	Meta Final	Medios de Verificación	Comentarios
Componente #3: Fortalecimiento del ecosistema de conocimiento de ciberseguridad a nivel nacional										
3.1.a Currícula de formación en ciberseguridad diseñada	Currícula	0	2018	0	0	1	0	1	AGESIC Informes de programa	La currícula incluye los programas de formación para los diferentes grados y perfiles, así como el contenido de los mismos.
3.1.b Profesores formados en la nueva currícula de formación en ciberseguridad	Profesores	0	2018	0	0	110	110	220	AGESIC Informes de programa	En cada año, 10 profesores de cada uno de los 5 centros académicos de formación superior, más 3 profesores de cada uno de los 19 de departamentos del país, más 3 personas de AGESIC.
3.2 Red de expertos en funcionamiento	Red de expertos	0	2018	1	0	0	0	1	AGESIC Informes de programa	
3.3 Plan de difusión nacional e internacional implementado	Plan	0	2018	0	1	0	0	1	AGESIC Informes de programa	
3.4 Estrategia de gestión del cambio diseñada	Documento	0	2018	1	0	0	0	1	Documento de estrategia de gestión del cambio	

ACUERDOS Y REQUISITOS FIDUCIARIOS

PAÍS	República Oriental del Uruguay
PROYECTO NO:	UR-L1152
NOMBRE:	Fortalecimiento de la Ciberseguridad en Uruguay
ORGANISMO EJECUTOR	República Oriental del Uruguay, a través de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)
EQUIPO FIDUCIARIO:	Abel Cuba y Emilie Chapuis (FMP/CUR)

I. RESUMEN EJECUTIVO

- 1.1 La presente operación es por US\$10.000.000, dónde US\$8.000.000 estarán financiados por el Banco y US\$2.000.000 por contraparte local. El prestatario es la República Oriental del Uruguay y el Organismo Ejecutor (OE) es AGESIC. Esta Agencia cuenta con una estructura organizacional y administrativa que será responsable por la ejecución de los recursos de la operación, así como de gestionar el oportuno financiamiento de los aportes de contrapartida local. El objetivo del préstamo es contribuir a fortalecer la capacidad del país para proteger su espacio digital mejorando la prevención, detección y respuesta a los ataques cibernéticos. La operación cuenta con tres componentes: (i) Componente 1 - Mejoramiento de las capacidades operativas y herramientas del CERT.uy (US\$5.415.000); (ii) Componente 2 - Potenciación del uso de tecnología avanzada para la formación de recursos humanos (US\$1.900.000 BID); y (iii) Componente 3 - Fortalecimiento del ecosistema de conocimiento de ciberseguridad a nivel nacional (US\$1.850.000).
- 1.2 Los ARF establecidos para el presente programa se fundamentan en los antecedentes de AGESIC como OE de los Préstamos 1970/OC-UR, 2591/OC-UR, 3007/OC-UR, 3625/OC-UR y 4300/OC-UR.

II. CONTEXTO FIDUCIARIO DEL ORGANISMO EJECUTOR

- 2.1 La AGESIC es una entidad modelo dentro de la administración pública. En los cuatro proyectos anteriores ejecutados por este OE, quedó demostrada su adecuada capacidad de ejecución en todos los ámbitos de la gestión. AGESIC posee una consolidada experiencia previa en materia de compras y contrataciones según normativas BID. Asimismo, sus procesos y su ambiente general de controles internos, se los considera adecuados, en su conjunto.
- 2.2 En cuanto a los sistemas nacionales, o sus equivalentes, que utilizaría en esta operación, son los siguientes:
- a. **Presupuesto.** Se utilizará el sistema nacional de presupuesto. Los recursos de esta operación quedarán inscritos en la nueva Ley de Presupuesto Quinquenal 2020-2025. Se espera que AGESIC cuente con la misma base presupuestal que la obtenida en 2019, suficiente a nivel global del programa y que contempla recursos del financiamiento y contraparte local.
 - b. **Tesorería.** Para administrar los recursos del programa se habilitará una cuenta especial en el Banco Central del Uruguay (BCU), cuenta que forma

parte de la Cuenta Única Nacional a nombre de AGESIC, especificando el nombre del programa.

- c. **Contabilidad y reportes financieros.** El OE utilizará el Sistema de Proyectos Internacionales (SPI), en coordinación con la Contaduría General de la Nación, administradora del SIIF.
- d. **Control interno.** AGESIC mantiene un sistema de controles internos para la gestión de sus operaciones, cuya efectividad es evaluada al momento de la intervención de los gastos y pagos que efectúa el Tribunal de Cuentas de la República (TCR) y el control de legalidad que realizan los contadores delegados.
- e. **Control externo.** Durante los últimos años, el TCR ha sido responsable de las auditorías anuales de los programas financiados por el Banco, cuyo trabajo se enmarcó en las normas internacionales de Auditoría emitidas por la Organización Internacional de las Entidades Fiscalizadoras Superiores (INTOSAI).

III. EVALUACIÓN DEL RIESGO FIDUCIARIO Y ACCIONES DE MITIGACIÓN

- 3.1 Según se identificó en el taller de riesgo relacionado a este programa y analizando los antecedentes de ejecución del OE, el riesgo fiduciario es evaluado como bajo. Este hallazgo se fundamenta en:
 - a. El hecho de que la AGESIC, siendo una Entidad de la Administración Central, se rige por procedimientos claros establecidos en normas legales y reglamentarias cuya aplicación se realiza bajo controles internos y externos estrictos previstos por ley, que atenúan los riesgos relacionados a los aspectos de gestión financiera.
 - b. Los antecedentes del OE, quien posee una consolidada experiencia previa en la gestión de la materia fiduciaria, de compras y contrataciones según la normativa del Banco, y de gestión financiera, considerando adicionalmente que el presente programa será administrado por el mismo equipo que está cargo de los préstamos actualmente en ejecución.
 - c. La experiencia específica de la AGESIC en la compra de tecnología en general y de aplicaciones relacionadas con ciberseguridad en particular, considerando que la institución cuenta ya con un CERT y un SOC en funcionamiento.
- 3.2 En virtud de lo anteriormente mencionado, se considera que el programa solo podrá requerir de medidas mitigatorias de importancia que serán identificadas a lo largo del ciclo de ejecución del préstamo mediante las actividades de supervisión realizadas por el Banco mismo o las auditorías requeridas en el marco de esta operación.

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

- 4.1 Los siguientes aspectos serán considerados en las estipulaciones especiales:
- a. **Tipo de cambio.** Para la rendición de cuentas en dólares se utilizará el tipo de cambio de la fecha efectiva de pago por parte de AGESIC a los Contratistas, especificando el método de conversión que menciona el Art.4.10 (b) (ii) de las Normas Generales del Contrato de Préstamo.
 - b. **Estados financieros auditados.** Se requiere su presentación dentro de los siguientes 120 días del cierre del ejercicio fiscal de cada año. La auditoría podrá ser realizada por el TCR o por una firma de auditoría. En caso de optar por una firma de auditoría, los términos de referencia deben ser acordados con el Banco y la firma auditora deberá ser aceptable para el Banco, especificando el plazo de presentación que menciona el Art. 7.03 de las Normas Generales del Contrato de Préstamo. El último de estos estados financieros auditados deberá presentarse al Banco dentro de los ciento veinte (120) días siguientes al vencimiento del plazo original de desembolso o sus extensiones.

V. ACUERDOS Y REQUISITOS PARA LA EJECUCIÓN DE LAS ADQUISICIONES

A. Ejecución de las adquisiciones

- 5.1 Las Políticas de Adquisiciones del Banco, GN-2349-9 (Políticas para las Adquisiciones de Obras y Bienes) y GN-2350-9 (Políticas para la Selección y Reclutamiento de Servicios de Consultoría) serán aplicables para todas las actividades de adquisiciones anticipadas en esta operación. Las mismas estarán incluidas en el Plan de Adquisiciones que deberá cubrir, como mínimo, un período inicial de 18 meses, y luego será actualizado anualmente. El mismo plan de adquisiciones deberá estar registrado, aprobado y publicado en SEPA (Sistema Electrónico de Planes de Adquisiciones – www.iniciativasepa.org) antes de iniciar las adquisiciones. Una vez registrado, estará actualizado anualmente o cada vez que sea necesario en caso de cambios sustanciales a la planificación original.
- 5.2 La pertinencia del gasto, es decir los Términos de Referencia (TdR), especificaciones técnicas y presupuesto, es responsabilidad del Especialista Sectorial (ES) del proyecto y necesita siempre de no-objeción previa, con respecto al inicio de la adquisición misma, y según criterios operacionales del Jefe de Equipo de Proyecto.
- 5.3 Las adquisiciones de menor cuantía serán realizadas de acuerdo con las Políticas del Banco y en conformidad con la Guía de Supervisión Expost para las compras de menor cuantía elaborado para las operaciones de AGESIC en base a su experiencia en la gestión de los procesos de adquisiciones bajo normativa del Banco.
- 5.4 No se prevén excepciones a las Políticas del Banco, ni se prevé financiamiento retroactivo. De acuerdo a la sección 1.9 del GN-2349-9 y 1.12 del GN-2350-9, el OE podrá realizar el proceso de licitación antes de la aprobación del préstamo. Conforme a lo dispuesto en las Políticas de Adquisiciones del Banco, “el

Prestatario realiza la contratación anticipada a su propio riesgo y el acuerdo del Banco respecto a los procedimientos, la documentación o la propuesta de adjudicación no lo compromete a otorgar un préstamo para el proyecto de que se trate”. Se podrá considerar elegible un proceso realizado en forma anticipada si se encuentra adecuadamente registrado y documentado en los sistemas del organismo ejecutor y si se ha realizado en conformidad con las Políticas del Banco o mediante procedimientos análogos que se encuentren conformes con las disposiciones aplicables de las políticas del Banco. Según indicado por AGESIC, no se anticipa el uso al mecanismo del financiamiento retroactivo.

- 5.5 **Adquisiciones de obras, bienes y servicios diferentes de consultoría.** Los contratos de Obras, Bienes y Servicios Diferentes de Consultoría¹ generados bajo el proyecto y sujetos a Licitación Pública Internacional (LPI) se ejecutarán utilizando los Documentos Estándar de Licitaciones (DELS) emitidos por el Banco. Las licitaciones sujetas a Licitación Pública Nacional (LPN) se ejecutarán usando Documentos de Licitación Nacional satisfactorios para el Banco. La revisión de las especificaciones técnicas de las adquisiciones durante la preparación de procesos de selección es responsabilidad del especialista sectorial del proyecto.
- 5.6 De acuerdo con el plan de adquisiciones relacionado a esta operación, no se anticipa la realización de ninguna obra. Se contratarán bienes por un valor estimativo de US\$3.315.000 y servicios diferentes a consultorías por un valor estimativo de US\$440.000. Estas adquisiciones serán sujetas a las disposiciones del GN-2349-9 – Políticas de Adquisición de Bienes y Obras.
- 5.7 **Selección y contratación de consultores.** Los contratos de Servicios de Consultoría generados bajo el proyecto se ejecutarán utilizando la Solicitud Estándar de Propuestas (SEPs) emitida por el Banco para todas licitaciones internacionales o satisfactoria para el Banco para las licitaciones nacionales. La revisión de términos de referencia para la contratación de servicios de consultoría es responsabilidad del especialista sectorial del proyecto.
- a. **Los procesos de selección y reclutamiento de servicios de firmas consultoras** serán procesos competitivos gestionados de acuerdo con las disposiciones aplicables del GN-2350-9 – Políticas de Selección y Reclutamiento de Servicios de Consultoría.
- b. **La selección de los consultores individuales.** El programa estará contratando a los consultores individuales identificados en el plan de adquisiciones de la operación. Debido a la necesidad de mantener la continuidad del enfoque técnico durante la ejecución del proyecto, en el PA acordado se prevé la selección directa de consultores individuales que previamente fueron contratados con recursos de los préstamos 3625/OC-UR y 2792/OC-UR que continuarán prestando servicios para la presente operación, lo que se encuentra en conformidad con lo dispuesto en la sección 5.4(a) de la Sección V de las Políticas GN-2350-9, entendiéndose que las condiciones contractuales de los consultores identificados permanecen idénticas y el desempeño satisfactorio de cada consultor será medido anualmente. Estos consultores cumplirán funciones técnicas

¹ Políticas para la Adquisición de Bienes y Obras financiadas por el Banco Interamericano de Desarrollo (GN-2349-9) párrafo 1.1: Los servicios diferentes a los de consultoría tienen un tratamiento similar a los bienes.

relacionadas con el CERT.uy y el SOC, así como funciones de coordinación técnica del proyecto, análisis presupuestal y financiero, monitoreo, gestión financiero-contable y de adquisiciones, y los contrataos serán por un monto aproximado de hasta US\$1.361.000 durante los cuatro años de duración del programa². El [PA](#) contiene el detalle de las adquisiciones que se implementarán durante la ejecución, así como los procedimientos aplicados por el Banco para su examen. Las contrataciones de consultorías y servicios distintos de consultoría que se realizarán mediante los servicios de la UNOPS, PNUD o Fundación Julio Ricaldoni, de acuerdo a los convenios que AGESIC mantiene serán sujetas a las Políticas del Banco.

Cuadro 1. Montos Límites para Licitación Internacional y Lista Corta con Conformación Internacional (miles US\$)

Obras			Bienes y Servicios			Consultoría	
Licitación Pública internacional	Licitación Pública Nacional	Comparación de Precios	Licitación Pública internacional	Licitación Pública Nacional	Comparación de Precios	Publicidad Internacional al Consultoría	Lista Corta 100% Nacional
≥ 3.000.000	≤ 3.000.000 ≥ 250.000	≤ 100.000	≥ 250.000	≤ 250.000 ≥ 50.000	≤ 50.000	≥ 200.000	≤ 200.000

B. Adquisiciones principales

5.8 Según lo identificado, las principales actividades de adquisiciones para esta operación se dividirán como detallado en la tabla a continuación. El resto de las actividades planificadas se encuentra en el [PA](#) que figura en los enlaces electrónicos al documento principal.

Cuadro 2. Bienes

Número de Proceso	Actividad Asociada	Unidad Ejecutora	Actividad	Descripción adicional	Método de Adquisición (Seleccionar una de las opciones)	Monto Estimado US\$
B1	1.1.1	AGESIC	LPI_1 - Adquisición de Licencias Qradar	Licencias IBM	LPI	915.000
B2	1.2.1	AGESIC	LPI_2 - Adquisición de NGIPS (virtuales y físicos), HW servers y VMWare		LPI	500.000

² Estos consultores fueron seleccionados inicialmente por comparación de calificaciones, con no objeción previa del Banco en todos los casos.

Número de Proceso	Actividad Asociada	Unidad Ejecutora	Actividad	Descripción adicional	Método de Adquisición (Seleccionar una de las opciones)	Monto Estimado US\$
B4	2.1.1	AGESIC	LPI_3 - Adquisición de Plataforma de Simulación	Plataforma de Simulación de ataques cibernéticos con diferentes escenarios en funcionamiento	LPI	1.800.000

Cuadro 3. Consultoría Firmas

Número de Proceso	Actividad Asociada	Unidad Ejecutora	Actividad	Método de Adquisición (Seleccionar una de las opciones)	Monto Estimado (US\$)
CF4	1.5.1	AGESIC	SBCC_4: Contratación de Firma Consultora para la provisión de Ss. Operación y Mantenim.	SBCC	400.000
CF5	1.5.2	AGESIC	SBCC_5: Contratación de Firma Consultora para la provisión de asesoramiento y despliegue	SBCC	1.600.000
CF7	3.1.1	AGESIC	SBCC_7: Contratación de firma consultora para el desarrollo de currículas en ciberseguridad y entrenamiento de docentes	SBCC	1.350.000

C. Supervisión de adquisiciones

- 5.9 Considerando la experiencia y el desempeño del ejecutor, las actividades de adquisiciones estarán sujetas a revisión ex post, salvo en procesos bajo modalidad LPI o lista corta internacional, y en aquellos casos en que se justifique una supervisión ex ante según identificado en el PA. Las revisiones ex post serán cada 12 meses de acuerdo con el Plan de Supervisión del proyecto. La tabla a continuación identifica los umbrales aplicables en relación a lo anterior³.

Cuadro 4. Límite para revisión ex post (US\$)

Obras	Bienes	Servicios de Consultoría
<3.000.000	<250.000	<200.000

D. Registros y archivos

- 5.10 Para la preparación y archivo de los reportes del proyecto se deben utilizar los formatos o procedimientos que han sido acordados con el Banco para las anteriores operaciones y que sean conformes con los requerimientos de las Políticas al respecto. Cada archivo deberá ser autocontenido e incluir la totalidad

³ Los montos límites establecidos para revisión ex post se aplican en función de la capacidad fiduciaria de ejecución del OE y pueden ser modificados por el Banco en la medida que tal capacidad varíe.

de la documentación relacionada a los procesos de adquisiciones, incluyendo el plan de adquisiciones, los pliegos y toda información relacionada (avisos específicos, informes de evaluación y recomendación de adjudicación, entre otros), los documentos de gestión de contratos.

VI. ACUERDOS Y REQUISITOS DE GESTIÓN FINANCIERA

- 6.1 **Programación y presupuesto.** AGESIC, que es parte de la Presidencia de la República (PE), envía su propuesta de presupuesto al MEF, quien lo contempla dentro del Proyecto Consolidado de Presupuesto Nacional y lo eleva a la consideración de la PE, que lo envía al Poder Legislativo para análisis y aprobación legal.
- 6.2 AGESIC realizará la programación y formulación presupuestaria en base al plan operativo anual acordado, que toma como base el Plan de Ejecución del Programa. La gestión del presupuesto del proyecto se realiza a través del sistema nacional del país (Sistema Información Financiera -SIIF). Se prevé que el OE gestione los recursos de contraparte local oportunamente a efectos de cumplir con el *pari passu* respectivo.
- 6.3 **Contabilidad y sistemas de información.** El proyecto llevará la contabilidad del programa en el sistema nacional (SIIF), a través del cual se gestionan los créditos presupuestales aprobados por Ley de Presupuesto Quinquenal para el Proyecto, por lo tanto, para procesar los compromisos y pagos relacionados con el proyecto, se deberán seguir los procedimientos establecidos por la Contaduría General de la Nación (CGN) a tales efectos.
- 6.4 Los Estados Financieros del Proyecto se emitirán en forma periódica, de acuerdo con Normas Contables Aceptables, que serán auditados anualmente: Se presentarán los siguientes: (i) estado de efectivo recibido y desembolsos efectuados; y (ii) estado de inversiones acumuladas; acompañados por las correspondientes notas explicativas.
- 6.5 **Desembolsos y flujo de fondos.** Los recursos del proyecto serán gestionados a través de la Cuenta Única Nacional (CUN), para lo cual la Tesorería General de la Nación (TGN), a solicitud de la Unidad Ejecutora del Proyecto, deberá habilitar una cuenta especial en el BCU. Esta cuenta recibirá los fondos desembolsados por el Banco, pero al ser de carácter nominativo (no se pueden efectuar pagos) se deberá abrir una cuenta bancaria específica del proyecto en el banco comercial estatal (Banco de la República Oriental del Uruguay – BROU) a efectos de efectuar los pagos correspondientes.
- 6.6 La modalidad de desembolsos será la de anticipo de fondos basado en las necesidades reales de liquidez, sustentadas en una adecuada proyección financiera y de desembolsos. Preferentemente estos anticipos se harán en forma semestral, una vez que se haya hecho la rendición de cuentas de por lo menos el

70% del monto anticipado⁴. Junto con cada solicitud de desembolso se deberá adjuntar las planillas de planificación financiera y la conciliación de fondos. Para la tramitación de las solicitudes de desembolsos se utilizará el sistema *e-Disbursements*. El tipo de cambio para convertir los pagos efectuados en moneda local a la moneda del préstamo será de la fecha de pago.

- 6.7 **Control interno y auditoría interna.** El sistema de control interno está basado en el Sistema Nacional definido en la normativa legal vigente. De acuerdo con lo establecido en el Texto Ordenado de Contabilidad y Administración Financiera (TOCAF) el TCR debe realizar la intervención preventiva de todos los gastos relacionados con la ejecución del proyecto. Complementariamente y según la normativa legal vigente, AGESIC es un organismo que está bajo el control de la Auditoría Interna de la Nación (AIN). Durante la ejecución del programa se coordinará con la AIN en caso de que el programa sea sujeto de revisión.
- 6.8 En lo que respecta a los controles institucionales, el OE mantendrá las condiciones definidas para la ejecución de los proyectos financiados por el Banco, actualmente en ejecución, asegurando la permanencia y participación de responsables fiduciarios de dedicación a los mismos.
- 6.9 **Control externo e informes.** Para cumplir con el requerimiento contractual del Banco, las auditorías anuales del programa podrán ser efectuadas por el TCR o por una firma de auditoría independiente que sea elegible para el Banco. Para el caso del TCR, la relación con AGESIC se plasmará en una Carta Acuerdo de Servicios, que incluirá los términos de referencia acordados con el Banco.
- 6.10 Los informes de la auditoría financiera deberán presentarse anualmente durante la etapa de desembolso, hasta el 30 de abril y 120 días después de la fecha de último desembolso, de acuerdo con las normas internacionales de auditoría. La contratación de la firma auditora, así como los términos de referencia respectivos deben seguir los lineamientos de la Política de Gestión Financiera OP-273-6. Los costos de auditoría podrán ser financiados con recursos del financiamiento.
- 6.11 **Plan de supervisión financiera.** El plan de supervisión financiera considera los siguientes aspectos:
- Participación en el taller de arranque definido por el equipo de proyecto, realizando una presentación de los aspectos fiduciarios más relevantes.
 - Revisión del POA y plan financiero inicial preparado por la UE como respaldo del primer anticipo a solicitar luego de la elegibilidad del programa.
 - Con base a una evaluación de riesgos de la cartera se podrán definir visitas financieras in situ, durante la ejecución del proyecto, donde se evaluarán los principales aspectos financieros y de control y manejo de archivos del proyecto. La modalidad de revisión de los desembolsos será ex post.

⁴ Conforme a la Política de Gestión Financiera OP-273-6, se justifica la aplicación de este porcentaje debido a que las Entidades de la Administración Central, a la que pertenece AGESIC, deben disponer del financiamiento en cuentas del Banco Central para comprometer nuevas obligaciones. Asimismo, el procesamiento de pagos requiere la intervención preventiva del TCR y la CGN.

- 6.12 **Mecanismo de ejecución.** El prestatario será la República Oriental del Uruguay y el OE será la República por intermedio de AGESIC. Esta agencia tendrá la responsabilidad básica ante el Banco por la ejecución, manteniendo la relación directa con éste. El programa se alinea con el mandato legal y la estructura administrativa y operacional existentes en la AGESIC⁵. La normativa aplicable establece que la AGESIC es responsable de regir la ejecución de todo lo vinculado con la implementación de planes y proyectos específicos en materia de gobierno electrónico y seguridad de la información.

⁵ Como se indica en los pies de página 2, AGESIC fue creada por Ley No. 17.930 (arts. 72) 19 de diciembre de 2005 como entidad responsable de gobierno electrónico. Como se indica en pie de página 3, la ley 18.719 de 27 de diciembre de 2010, crea dentro de la AGESIC la Dirección de Seguridad de la Información con la función de proteger la seguridad cibernética del sector público. La normativa asociada a AGESIC puede consultarse [aquí](#).

DOCUMENTO DEL BANCO INTERAMERICANO DE DESARROLLO

PROYECTO DE RESOLUCIÓN DE-___/19

Uruguay. Préstamo ____/OC-UR a la República Oriental del Uruguay
Fortalecimiento de la Ciberseguridad en Uruguay

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 Oriental del Uruguay, como Prestatario, para otorgarle un financiamiento destinado a cooperar en la ejecución del programa de Fortalecimiento de la Ciberseguridad en Uruguay. Dicho financiamiento será hasta por la suma de US\$8.000.000, 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 del Proyecto de la Propuesta de Préstamo.

(Aprobada el __ de _____ de 2019)