

DOCUMENTO DEL BANCO INTERAMERICANO DE DESARROLLO

URUGUAY

FORTALECIMIENTO DE LA CIBERSEGURIDAD EN URUGUAY

(UR-L1152)

PERFIL DE PROYECTO

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

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

PERFIL DE PROYECTO

URUGUAY

I. DATOS BÁSICOS

Nombre del Proyecto:	Fortalecimiento de la ciberseguridad en Uruguay		
Número de Proyecto:	UR-L1152		
Equipo de Proyecto:	Miguel Porrúa (IFD/ICS), Jefe de equipo; Roberto Fernández, Jefe de equipo alternativo, Alejandro Pareja, Ariel Nowersztem, Benjamin Roseth, Dario Kagelmacher, Sonia Rojas (IFD/ICS), Harold Villalba (SPD/SDV); Abel Cuba, Emilie Chapuis (VPC/FMP); y Krysia Avila (LEG/SGO).		
Prestatario:	República Oriental del 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)		
Plan Financiero:	BID (Capital Ordinario):	US\$	8 millones
	Local:	US\$	2 millones
	Total:	US\$	10 millones
Salvaguardias:	Políticas activadas:	B.01; B.02; B.03; B.07; B.17	
	Clasificación:	C	

II. JUSTIFICACIÓN GENERAL Y OBJETIVOS

- 2.1 **Antecedentes y justificación.** Uruguay es uno de los países más desarrollados en la región en términos de gobierno digital¹, comercio electrónico y uso de TIC (Tecnologías de la Información y la Comunicación). 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 AGESIC (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento).
- 2.2 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

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.

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 digital comparable.

- 2.3 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 CERT.uy (Centro Nacional de Respuesta a Incidentes de Seguridad Informática)⁷ y en el año 2017 el GSOC (*Government Security Operation Center*)⁸. La capacidad técnica y el equipamiento tecnológico del CERTuy no han sido actualizados al ritmo que demandan los rápidos cambios que se 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 objetivo (viii) la “Confianza y seguridad en el uso de las tecnologías digitales”⁹. Este objetivo se complementa con la Política de Gestión de Incidentes de Seguridad de la Información y sus guías de implementación¹⁰.
- 2.4 Esta falta de recursos 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%¹¹.
- 2.5 De acuerdo al ITU (*International Telecommunications Union*) Uruguay es el país de América Latina donde la agenda digital está más avanzada¹², posición 42 de 176. Asimismo, como se indicó en el párrafo inicial, 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

⁵ [Blog Seguridad.](#)

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 5 dimensiones.

⁷ *Computer Emergency Response Team*. Es el centro responsable de la respuesta a incidentes cibernéticos en el país y se crea mediante Decreto 451-009 de 2008.

⁸ 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.

⁹ [Agenda Uruguay Digital](#), Transformación con equidad 2020. Pág. 18.

¹⁰ Resoluciones 59/010 y 62/010 del Consejo Directivo Honorario de AGESIC.

¹¹ [Estadísticas CERT.uy.](#)

¹² [ICT Development Index 2017.](#) ITU.

Latina, con más 300 empresas que exportan a 52 países¹³. Los ataques cibernéticos se han convertido en el riesgo que más preocupa a los hombres de negocios situándose por encima de los ataques terroristas, las burbujas financieras o las crisis fiscales¹⁴. Estos ataques cibernéticos tienen consecuencias económicas importantes y están costando en promedio el 0,5% del PIB mundial¹⁵. Un estudio realizado en Colombia por el Gobierno de Colombia, el BID y la 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 empresas¹⁶. 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 estima que las pérdidas promedio en el sector financiero debidas a ciberataques alcanzan el 9% de los ingresos netos¹⁷.

- 2.6 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; (ii) daño reputacional a organizaciones y al gobierno; (iii) daño a la privacidad de los ciudadanos; (iv) daño a la inclusión digital y financiera por menor uso de tecnología; y (v) daño a la democracia y a la cohesión social.
- 2.7 **El principal desafío.** El problema general es el bajo nivel de implantación de la política de ciberseguridad del país que lo deja vulnerable ante un eventual ataque cibernético¹⁸.
- 2.8 **Los problemas específicos** relacionados con el problema general son:
- 2.9 **Falta de capacidades operativas de monitoreo, detección y respuesta de incidentes**¹⁹. No se detectan o se detectan en forma tardía los ataques de ciberseguridad que se producen y por ende no es posible responder en forma oportuna incrementando el nivel de vulnerabilidad²⁰. 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. 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

¹³ [ADAU](#).

¹⁴ [Cyber attacks are shutting down countries, cities and companies. Here's how to stop them.](#) World Economic Forum. 2018.

¹⁵ "Net Losses: Estimating the global cost of cybercrime". [Center for Strategic International Studies \(CSIS\) and McAfee](#). 2014.

¹⁶ [Impacto de los incidentes de Seguridad Digital en Colombia 2017](#). Ministerio de Tecnologías de la Información y las Comunicaciones, OEA y BID. 2017.

¹⁷ [Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment](#). Antoine Bouveret. IMF. 2018. WP/18/143.

¹⁸ Según el Reporte Ciberseguridad 2016 mencionado anteriormente, Uruguay obtiene 149 puntos de 245 posibles. Como referencia, Israel obtiene 200.

¹⁹ En el estudio realizado por SecurePro, el SOC de Uruguay no alcanza ni la puntuación media del *Cybersecurity Maturity Model*.

²⁰ Información ciberseguridad Uruguay 2018. En la actualidad, de los 2000 incidentes detectados anualmente, más de 40 generan alto impacto debido a que se detectan tardíamente.

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; y (iii) no existe un mecanismo seguro y confidencial para compartir información con el sector privado relativo a ataques e incidentes.

- 2.10 **Baja oferta 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 escasez²¹. Se estima que Uruguay cuenta actualmente con 650 profesionales en ciberseguridad y precisa duplicar esa cifra en los próximos dos años²². 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 tema²³; (ii) el número de docentes en la temática es insuficiente para atender la demanda formativa de profesionales en ciberseguridad²⁴; (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 escasa²⁵.
- 2.11 **Objetivo del programa.** El programa contribuirá a fortalecer la capacidad del país para proteger su espacio digital contribuyendo a la prevención, detección y respuesta a los ataques cibernéticos. Para ello, el programa se estructurará en los siguientes componentes:
- 2.12 **Componente 1. Mejoramiento de las capacidades operativas y herramientas del CERT.uy (US\$4.275.000 BID/Local US\$950.000).** Se llevarán a cabo las siguientes actividades: (i) actualización de las herramientas tecnológicas de análisis y gestión de eventos de ciberseguridad, SIEM²⁶; (ii) expansión del sistema de detección de intrusiones NGIPS²⁷ 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

²¹ 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.

²² *Cybersecurity Excellence Framework*. Octubre 2018. Avnet. Pág. 37.

²³ Formación Académica en TIC: Informe 2017. Cámara Uruguaya de Tecnologías de la Información

²⁴ El país cuenta únicamente con 22 docentes en el ámbito de ciberseguridad que se reúnen periódicamente en el grupo *Hack and Beer*.

²⁵ Conversación con el grupo de docentes en el ámbito de *Hack and Beer*.

²⁶ *Security Information Event Management*. 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.

²⁷ *Next Generation Intrusion Prevention System*. Un Sistema de sensores ubicados estratégicamente que permite mejorar la capacidad de detectar intrusiones en el sistema.

información con el sector privado²⁸ y el análisis inteligente de amenazas²⁹; (iv) herramientas de laboratorio del CERT.uy (forense, prueba de concepto, desarrollo de sensores y gestión de incidentes, entre otros); (v) servicios especializados relacionados con la instalación y operación del SIEM; (vi) capacitación relacionada con todas actividades de este componente; (vii) investigación de tecnologías emergentes e innovadoras; y (viii) incorporación de Recursos Humanos con las cualificaciones necesarias para operar las nuevas herramientas introducidas.

- 2.13 **Componente 2. Potenciar el uso de tecnología avanzada para la formación de recursos humanos (US\$1.900.000 BID).** Se llevarán a cabo las siguientes actividades: (i) puesta en funcionamiento de una Plataforma de Simulación de ataques cibernéticos con múltiples escenarios³⁰ que podrán utilizar las instituciones que realicen formación en ciberseguridad; (ii) capacitación para el uso de la Plataforma; y (iii) puesta en funcionamiento de una plataforma de *e-Learning* para la formación de profesionales en ciberseguridad.
- 2.14 **Componente 3. Fortalecimiento del ecosistema de conocimiento de ciberseguridad a nivel nacional (US\$1.425.000 BID/Local US\$950.000).** Se llevarán a cabo las siguientes actividades: (i) apoyar el desarrollo de *curricula* de formación en ciberseguridad que pueda ser utilizada por diferentes centros académicos del país; (ii) formación de docentes en ciberseguridad; (iii) creación de una red nacional de expertos con activas vinculaciones internacionales; y (iv) actividades de difusión nacional e internacional incluyendo intercambios y eventos de difusión y comunicación.
- 2.15 A los montos indicados en los párrafos precedentes se debe agregar los costos de administración del proyecto estimados en US\$500.000 (US\$400.000 BID/Local US\$100.000).
- 2.16 **Alineamiento estratégico.** 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. El programa es consistente con la Estrategia del Banco con el País (EBP) con Uruguay 2016-2020 (GN-2836) en su área prioritaria de “mayor eficiencia de las instituciones públicas”, en su objetivo de “fortalecer los sistemas de gestión pública”. También es consistente con la actualización de la Estrategia Institucional 2010-2020 (AB-3008) por contribuir al reto “bajos niveles de productividad e

²⁸ 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. 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.

²⁹ 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*”.

³⁰ 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.

innovación" y aportar al tema transversal relativo a "fortalecer la capacidad institucional y el Estado de derecho" y con el Marco de Resultados Corporativos 2016-2019 (GN-2727-6), ya que contribuye a elevar el "número de agencias gubernamentales que son beneficiadas mediante el fortalecimiento de sus instrumentos tecnológicos y de gestión para mejorar los servicios públicos". 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.

III. ASPECTOS TÉCNICOS Y CONOCIMIENTO DEL SECTOR

- 3.1 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 la operación UR-L1159 Estrategia de Gobierno Digital. 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, así como la operación 4300/OC-UR que pone en funcionamiento la ficha médica digital en el país.
- 3.2 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.

- 3.3 **Ejecución, administración y riesgos.** La operación será un préstamo de inversión con un período de ejecución de cuatro años, a ser ejecutado por la República Oriental del Uruguay a través de AGESIC, institución responsable de gobierno electrónico y sociedad de la información en Uruguay. AGESIC cuenta con una comprobada y positiva experiencia como ejecutor de programas con el Banco y con las capacidades técnicas y administrativas para ello. Se han detectado, en forma preliminar, los siguientes riesgos de nivel medio y bajo: (i) demoras en los acuerdos interinstitucionales con los centros académicos; (ii) resistencia al cambio por parte de gestores públicos de los ministerios en los que se instalarán las sondas de monitoreo y de los funcionarios públicos que realizan su trabajo con base en sistemas de información y su actividad estará ahora sometida a un mayor monitoreo; y (iii) cambio de gobierno como resultado de las elecciones que tendrán lugar en octubre del presente año.
- 3.4 **Resultados esperados y Análisis económico.** Este programa fortalecerá la capacidad del Uruguay para detectar tempranamente y responder a los ataques cibernéticos mediante: (i) aumentar la detección y respuesta de los incidentes de ciberseguridad, reduciendo de esta manera su impacto (ii) incrementar la cantidad y calidad de técnicos especializados en ciberseguridad; y (iii) fortalecer la capacidad del ecosistema digital de formar profesionales en ciberseguridad. Los principales beneficiarios del programa serán las instituciones gubernamentales que tendrán más protegida su infraestructura TIC, el sector académico que verá fortalecida su oferta formativa en ciberseguridad, el sector privado que accederá más fácilmente a profesionales cualificados en el ámbito de la ciberseguridad y los ciudadanos en general que contarán con una institución responsable de ciberseguridad con mayor capacidad de defenderlos de los ataques cibernéticos.

IV. RIESGOS AMBIENTALES Y ASPECTOS FIDUCIARIOS

- 4.1 No se prevén efectos negativos ambientales o sociales. De acuerdo con la política de medio ambiente y cumplimiento de salvaguardas (OP-703), la operación fue clasificada como categoría "C" (ver Anexos II y III). Las adquisiciones financiadas con recursos del préstamo se harán de acuerdo con las Políticas GN-2349-9 y GN-2350-9.
- 4.2 A solicitud del prestatario y debido a que se realizarán actividades prioritarias relacionadas con este programa, se permitirá el financiamiento retroactivo de gastos hasta el 20% del total de los recursos del crédito que se hagan desde la fecha de aprobación del Perfil de Proyecto hasta la fecha de aprobación del préstamo por el Directorio del Banco, y que cumplan con requisitos sustancialmente análogos a los que se establecerán en el contrato de préstamo. La gestión financiera seguirá lo previsto en la Guía OP-273-6. No se prevén excepciones a las políticas del Banco.

V. RECURSOS Y CRONOGRAMA DE PREPARACIÓN

- 5.1 Se prevé la distribución del POD al QRR para el 7 de marzo de 2019, la distribución del Borrador de Propuesta de Préstamo al OPC para el 10 de abril de 2019 y la consideración por el Directorio de la operación para el 15 de mayo

de 2019. El total de recursos transaccionales necesarios para la preparación se estiman en US\$60.360 (US\$8.000 para honorarios de consultores y US\$52.360 para misiones). El tiempo de personal requerido para la preparación del préstamo será 1,24 FTE.

CONFIDENCIAL

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



Safeguard Policy Filter Report

Operation Information

Operation		
UR-L1152 Strengthening Cybersecurity in Uruguay		
Environmental and Social Impact Category	High Risk Rating	
C		
Country	Executing Agency	
URUGUAY	UR-AGESIC - AGENCIA PARA EL DESARROLLO DEL GOBIERNO DE GESTIÓN ELECTRÓNICA Y LA SOCIEDAD DE	
Organizational Unit	IDB Sector/Subsector	
Innovation in Citizen Services Division	E-GOVERNMENT	
Team Leader	ESG Primary Team Member	
MIGUEL ANGEL PORRUA VIGON		
Type of Operation	Original IDB Amount	% Disbursed
Loan Operation	\$8,000,000	0.000 %
Assessment Date	Author	
16 Jan 2019	srojas Project Assistant	
Operation Cycle Stage	Completion Date	
ERM (Estimated)	29 Jan 2019	
QRR (Estimated)	15 Mar 2019	
Board Approval (Estimated)	15 May 2019	
Safeguard Performance Rating		
Rationale		



Safeguard Policy Filter Report

Potential Safeguard Policy Items

[No potential issues identified]

Safeguard Policy Items Identified

B.1 Bank Policies (Access to Information Policy– OP-102)

The Bank will make the relevant project documents available to the public.

B.2 Country Laws and Regulations

The operation is expected to be in compliance with laws and regulations of the country regarding specific women's rights, the environment, gender and indigenous peoples (including national obligations established under ratified multilateral environmental agreements).

B.3 Screening and Classification

The operation (including [associated facilities](#)) is screened and classified according to its potential environmental impacts.

B.7 Supervision and Compliance

The Bank is expected to monitor the executing agency/borrower's compliance with all safeguard requirements stipulated in the loan agreement and project operating or credit regulations.

B.17. Procurement

Suitable safeguard provisions for the procurement of goods and services in Bank financed operations may be incorporated into project-specific loan agreements, operating regulations and bidding documents, as appropriate, to ensure environmentally responsible procurement.

Recommended Actions

Operation has triggered 1 or more Policy Directives; please refer to appropriate Directive(s). Complete Project Classification Tool. Submit Safeguard Policy Filter Report, PP (or equivalent) and Safeguard Screening Form to ESR.

Additional Comments

[No additional comments]



Safeguard Screening Form

Operation Information

Operation		
UR-L1152 Strengthening Cybersecurity in Uruguay		
Environmental and Social Impact Category	High Risk Rating	
C		
Country	Executing Agency	
URUGUAY	UR-AGESIC - AGENCIA PARA EL DESARROLLO DEL GOBIERNO DE GESTIÓN ELECTRÓNICA Y LA SOCIEDAD DE	
Organizational Unit	IDB Sector/Subsector	
Innovation in Citizen Services Division	E-GOVERNMENT	
Team Leader	ESG Primary Team Member	
MIGUEL ANGEL PORRUA VIGON		
Type of Operation	Original IDB Amount	% Disbursed
Loan Operation	\$8,000,000	0.000 %
Assessment Date	Author	
16 Jan 2019	srojas Project Assistant	
Operation Cycle Stage	Completion Date	
ERM (Estimated)	29 Jan 2019	
QRR (Estimated)	15 Mar 2019	
Board Approval (Estimated)	15 May 2019	
Safeguard Performance Rating		
Rationale		

Operation Classification Summary

Overriden Rating	Overriden Justification
Comments	



Safeguard Screening Form

Conditions / Recommendations

No environmental assessment studies or consultations are required for Category "C" operations.

Some Category "C" operations may require specific safeguard or monitoring requirements (Policy Directive B.3). Where relevant, these operations will establish safeguard, or monitoring requirements to address environmental and other risks (social, disaster, cultural, health and safety etc.)

The Project Team must send the PP (or equivalent) containing the Environmental and Social Strategy (the requirements for an ESS are described in the Environment Policy Guideline: Directive B.3) as well as the Safeguard Policy Filter and Safeguard Screening Form Reports.

Summary of Impacts / Risks and Potential Solutions

Disaster Risk Summary

Disaster Risk Level

C

Disaster / Recommendations

Disaster Summary

Details

Actions

Operation has triggered 1 or more Policy Directives; please refer to appropriate Directive(s). Complete Project Classification Tool. Submit Safeguard Policy Filter Report, PP (or equivalent) and Safeguard Screening Form to ESR.

ESTRATEGIA AMBIENTAL Y SOCIAL

- 1.1 **El objetivo del programa** es contribuir la capacidad del país para proteger su espacio digital contribuyendo a la prevención, detección y respuesta a los ataques cibernéticos.
- 1.2 No existen riesgos ambientales o sociales asociados con el programa. Según la directiva B.3 de la Política de Medio Ambiente y Cumplimiento de Salvaguardias del Banco (documento GN-2208-20 y manual OP-703), la operación fue clasificada como categoría “C”.

Índice de Trabajo Sectorial Realizado y Propuesto

Descripción	Estado de Preparación
Informe Ciberseguridad 2016: ¿Estamos preparados en América Latina y el Caribe? BID/OEA. 2016	Elaborado
El fin del trámite eterno: ciudadanos, burocracia y gobierno digital. BID 2017	Elaborado
Impacto de los incidentes de Seguridad Digital en Colombia 2017. Ministerio de Tecnologías de la Información y las Comunicaciones, OEA y BID. 2017	Elaborado
Cybersecurity Excellence Framework. Avnet	Elaborado
Security Test Lab. SecurePro	Elaborado
Practical SOC Operation. SecurePro	Elaborado
Incident Response. SecurePro	Elaborado
National Information Sharing Model. SecurePro	Elaborado
SOC-CERT. SecurePro	Elaborada
Support to Uruguay's GSC. SecurePro	Elaborado

CONFIDENCIAL

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