Gobierno de la República del Uruguay

PROGRAMA DE FORTALECIMIENTO DE LA CIBERSEGURIDAD EN URUGUAY (UR-L1152)

PRÉSTAMO NO. 4843/OC-UR

BANCO INTERAMERICANO DE DESARROLLO (BID)

AGENCIA DE GOBIERNO ELECTRÓNICO Y SOCIEDAD DE LA INFORMACIÓN Y DEL CONOCIMIENTO (AGESIC)

Evaluación Intermedia

Informe Final

Sebastián Rocha

Agosto 2023

El presente documento ha sido elaborado en colaboración con el Lic. Manuel Maffe. Se agradece a la Coordinación del Programa y al equipo de la AGESIC por la amplia colaboración brindada durante el desarrollo de la evaluación. En el documento final, se mencionan los funcionarios y técnicos que han colaborado con la presente evaluación, así como los referentes que fueran entrevistados.

Abreviaturas y Acrónimos

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	Government Security Operation Center
IGAS	Informe de Gestión Ambiental y Social
ITU	International Telecommunications Union
NIST	National Institute of Standards and Technology
OE	Organismo Ejecutor
OEA	Organización de Estados Americanos
PA	Planes de Adquisiciones
PEP	Plan de Ejecución Plurianual
PIB	Producto Interno Bruto
PMR	Progress Monitoring Reports
POA	Planes Operativos Anuales
SIEM	Security Information Event Management
SOC	Security Operations Center
TCR	Tribunal de Cuentas de la República
TIC	Tecnologías de la Información y la Comunicación
UTEC	Universidad Tecnológica

Información Básica

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	☑	PI	☑	EI	☐
Temas Transversales[e]:	GD	☑	CC	☐	IC	☑

[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 período 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).

Tabla de Contenidos

Presentación

En el año 2019 se aprobó el programa de Fortalecimiento de la Ciberseguridad en Uruguay, a cargo de la Agencia de Gobierno electrónico y Sociedad de la Información y del Conocimiento (AGESIC) y financiado por el Banco Interamericano de Desarrollo (BID) mediante el contrato de préstamo No. 4843/OC-UR, por un monto de US$ 8.000.000 y el aporte local del Gobierno Uruguayo de US$ 2.000.000.

El objetivo de la Consultoría es proporcionar una evaluación integral del Programa de Fortalecimiento de Ciberseguridad de las actividades llevadas a cabo desde el inicio del programa hasta fin del año 2022[1] (Evaluación de Medio Término), a través de la recolección y sistematización de información que contribuya a documentar lecciones aprendidas y recomendaciones de política pública que permitan ajustes y mejoras en la implementación.

Como objetivos específicos se identificaron: i) la evaluación del progreso del programa hacia la consecución de metas, objetivos, resultados y productos declarados, así como resultados no esperados, que se han alcanzado durante el período que lleva siendo implementado el Programa, ii) la evaluación de la fidelidad del programa, contemplando el diseño inicial, evaluar la concordancia en términos de procesos y sistemas de implementación, iii) el establecimiento de hipótesis que en lo posible sean comprobables demostrando el cumplimiento de resultados previstos (definidos en la Matriz de Resultados de la Operación), iv) la identificación de evidencia y contribución del programa en la calidad y eficiencia del ecosistema de Ciberseguridad, v) la realización de un análisis de eficiencia del Programa hasta la fecha que permita constatar lo planteado en el análisis ex ante de la operación[2], vii) el análisis de la estructura institucional del Programa que permita identificar los elementos claves de la coordinación durante la ejecución e implementación de este, viii) la elaboración de un documento que pueda ser utilizado para involucrar a un grupo más amplio de partes interesadas.

Los resultados de la consultoría tienen que arrojar lecciones aprendidas para mejorar la ejecución desde esta evaluación hacia el final del Programa, reflejando los desvíos para poder corregirlos antes de finalizada la operación.

El presente Informe de avance resume las actividades pautadas en los Términos de Referencia de la consultoría para la evaluación intermedia en el marco del Préstamo BID 4843/OC-UR.

Durante el mes de febrero de 2023, se trabajó en el Plan de Trabajo que fuera consensuado con las autoridades de la AGESIC. A partir del mes de marzo de 2023 se iniciaron las actividades relativas a la Evaluación Intermedia del Proyecto, profundizándose el análisis a través de entrevistas que se han realizado con los diferentes actores del Gobierno de Uruguay y a las consultoras que han participado activamente en la ejecución de la operación.

El documento está organizado en cuatro (V) SECCIONES y cinco (V) ANEXOS. En la Sección primera, Antecedentes, se describe el marco contextual sobre el que se basó la ejecución del Programa, las relaciones vinculares entre los distintos organismos del sector público y el marco legal que rigió durante el diseño y su posterior ejecución. En la siguiente Sección, se analiza el Desempeño del Programa, tanto en materia de su efectividad en relación al cumplimiento de los objetivos del programa, como en términos de eficiencia. La sección tercera versa sobre la implementación del Programa. Se analizan los factores críticos que incidieron en la implementación (describiéndose las principales implementaciones), así como el desempeño de la AGESIC y el del Banco durante todo el período de ejecución. En la Sección cuarta se exponen las consideraciones de acerca de este primer informe, y un resumen de las primeras lecciones aprendidas, y en la última describe la bibliografía y los actores críticos entrevistados

Se han considerado -para el análisis- los documentos relativos al Programa BID, la información que surge de los PMRs (Progress Monitoring Reports), los Informes de Avance Semestrales que

[1] La evaluación es llevada a cabo para el periodo considerado entre octubre de 2019 (inicio de ejecución) y diciembre de 2022.

[2] Ver detalle de estos tópicos en el capítulo II sección 2 “Eficiencia”

realiza el organismo ejecutor, el marco normativo del Gobierno Electrónico del Uruguay, la documentación interna de la AGESIC y los informes específicos solicitados a la citada Agencia, asociados al Proyecto que nos ocupa y a otros afines[3].

[3] Al personal de la AGESIC y de las Dependencias Estatales que colaboraron con sus opiniones como resultados de las entrevistas, se les hace saber el más sincero agradecimiento por la excelente calidez humana y disposición manifestada, así como por la calidad de la información aportada. Sobre el final del documento se cita la bibliografía y los agentes públicos y privados entrevistados durante la evaluación. Finalmente, se deja constancia de que cualquier eventual inexactitud del presente Informe, corresponde al autor y refleja un error involuntario de interpretación de los mismo

I. Antecedentes

Contexto previo al diseño. El Gobierno de Uruguay es uno de los países con mayor desarrollo relativo en relación al resto de los países de la región en términos de gobierno digital[4]. Para el año 2020 ya contaba con la posibilidad de iniciar el 95% de los trámites del gobierno nacional en forma digital (en línea), la portabilidad de documento de identidad con chip e información biométrica, un sistema de historia clínicas electrónicas en red entre establecimiento públicos y privados, entre otras.

Este avance en la materia, conlleva una elevada penetración de las TIC en la sociedad, que incrementa el número de posibles vulnerabilidades e incidentes potenciales, que amenazan los entornos mediante la generación de ciberataques: intentos no deseados de robar, exponer, alterar, deshabilitar o destruir información mediante el acceso no autorizado a los sistemas informáticos

Tanto Gobierno Digital como Ciberseguridad son regulados por la AGESIC. Sin embargo, como los avances en el proceso de digitalización han tenido un ritmo de crecimiento exponencial en el país, es necesario el diseño de herramientas que no dejen tan vulnerable el espacio digital a posibles ataques cibernéticos[5].

Desde la creación de la AGESIC[6], el gobierno ha llevado a cabo muchas acciones para proteger su ciberespacio que lo posicionan como uno de los países más avanzados de América Latina y el Caribe (ALC): en el año 2008, AGESIC lanzó el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy), en el año 2017 el Security Operation Center (SOC) (dentro del cual fue creado el Government Security Operation Center -GSOC- como programa).

A pesar de ello, la falta de capacidad en el CERTuy y en el SOC hace que sea difícil detectar los ataques cibernéticos o que la detección se produzca de forma tardía. Los análisis realizados por el propio CERTuy muestran que a medida que se incrementa su capacidad tecnológica y humana, crece su habilidad para detectar incidentes cibernéticos. En efecto, cuando se lanza la iniciativa GSOC la detección de incidentes se incrementa en un 69%.

El principal desafío que tiene en adelante el Gobierno de Uruguay es llevar adelante políticas de ciberseguridad, que profundicen las capacidades operativas de monitoreo, detección y respuesta de incidentes. Asimismo, es fundamental capacitar a los agentes públicos en estas temáticas y trabajar con las instituciones de formación para incrementar la oferta de profesionales en esta especialidad. De las seis universidades uruguayas, sólo la Universidad de la República y la ORT ofrecen 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 tema. En cuanto a los docentes, se visualiza una dotación insuficiente para atender la demanda formativa de profesionales.

En este contexto, el BID ha decidido apoyar la iniciativa del Gobierno Uruguayo a través del diseño de una operación dedicada íntegramente a ciberseguridad. Dada la necesidad de los países de

---

[4] *"In addition to developing "Digital Government Plan 2020", the Government of Uruguay has created "Agenda Uruguay Digital 2020", a plan built on four key pillars: i) social policy and inclusion, ii) sustainable economic development, iii) government management, and iv) governance for the information society. Objective VI of the Agenda, on "Proximity government", aims to improve transparency, accountability, citizen participation and services through increased focus on citizens' interaction with the Government. Specific goals include the establishment of "Citizen Response Centres" portals, which will allow citizens to complete all transactions related to select services online*".e-Government Readiness Survey 2018, . United Nations

[5] 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 comparable. Uruguay obtiene 149 puntos de 245 posibles. En 2020 el país calificó con el más alto puntaje en 4 de las 4 categorías (Modelo BID-OEA https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe)

[6] "La Ley 17.930 de 19 de diciembre de 2005, art. 72 crea la AGESIC como institución responsable de las políticas de gobierno electrónico. La Ley 18.719 de 27 de diciembre de 2010, art. 149 crea, dentro de la AGESIC, la Dirección de Seguridad de la Información.

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.

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. El programa también está alineado con las áreas transversales referidas a la Igualdad de Género y Diversidad, a través de la promoción de mujeres para recibir capacitación en temas de ciberseguridad; 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 violencia Además, 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).

Asimismo, cabe mencionar que el Programa se encuentra alineado con la Agenda de Uruguay Digital 2025, donde la ciberseguridad se establece como uno de los principales pilares de desarrollo. Particularmente, en el contexto de la Meta IV de dicha agenda “Potenciar infraestructura de telecomunicaciones, conectividad y ciberseguridad”, se destaca como objetivo X el “incrementar la ciberseguridad para prevenir y mitigar riesgos en el ciberespacio y avanzar en el cumplimiento del marco nacional de ciberseguridad, basado en la cooperación público y privada, garantizando la disponibilidad de los activos críticos de información”, donde aparecen puntos de acción directamente relacionados a los objetivos del Programa, a saber: (i) Adoptar el Marco de Ciberseguridad en servicios, infraestructura y redes críticas para el país, otorgando mayor seguridad, estandarización y confianza a todos los actores del desarrollo digital; (ii) Desarrollar e impulsar trayectorias de formación en ciberseguridad para el desarrollo de capacidades a través de la educación formal y no formal, y (iii) Mejorar la eficiencia en la detección y respuesta a incidentes cibernéticos, mediante la implementación de nuevas tecnologías que permitan aplicar análisis predictivo y automatización de respuestas, entre otras[7].

[7] Fuente: Agenda Uruguay Digital 2025. Link.

II. Desempeño del Programa

II.1. Efectividad[8]

II.1.1. Objetivos y Componentes del Programa

Se definió como objetivo general del Programa contribuir 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.

Para alcanzar el objetivo indicado, el Programa comprende los siguientes componentes:

Componente 1. Mejoramiento de las capacidades operativas y herramientas del CERT.uy (US$5.415.000) contemplando las siguientes actividades: (i) actualización de las herramientas tecnológicas de análisis y gestión de eventos de ciberseguridad *Security Information Event Management (SIEM)*; (ii) expansión del sistema de detección de intrusiones *Next Generation Intrusion Prevention System (NGIPS)*, (iii) incorporación de una plataforma de *Big Data* , (iv) herramientas de laboratorio del *CERT.uy*, (v) servicios especializados relacionados con la instalación y operación del *SIEM*, (vi) incorporación de actividades de investigación de tecnologías emergentes e innovadoras tales como inteligencia artificial, criptografía y *threat intelligence.*

Componente 2. Potenciación del uso de tecnología avanzada para la formación de recursos humanos (US$1.900.000)., cuyas actividades identificadas fueron: (i) puesta en funcionamiento de una Plataforma de Simulación de ataques cibernéticos mediante capacitaciones a usuarios, (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.

Componente 3. Fortalecimiento del ecosistema de conocimiento de ciberseguridad a nivel nacional, financiando las siguientes actividades (US$1.850.000): (i) apoyar el desarrollo de curricula de formación en ciberseguridad tanto a nivel técnico como de grado y posgrado, 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, incorporando a la mujer al ámbito profesional de la ciberseguridad; (iii) actividades de difusión nacional e internacional incluyendo intercambios y eventos de promoción y comunicación; y (iv) diseño de una estrategia de gestión del cambio.

II.1.2. Calidad de Diseño y Análisis de Lógica Vertical

El diseño original del Programa responde a las problemáticas que se buscaban resolver en a inicios de la ejecución. De hecho, la Propuesta de Préstamo establece que “El problema general [en Uruguay] es el bajo nivel de implantación de la política de ciberseguridad del país que lo deja en situación de vulnerabilidad ante un eventual ataque cibernético” (Documento “Propuesta de Préstamo. Fortalecimiento de la Ciberseguridad en Uruguay”, p. 5), encontrando las causas de este desafío en:

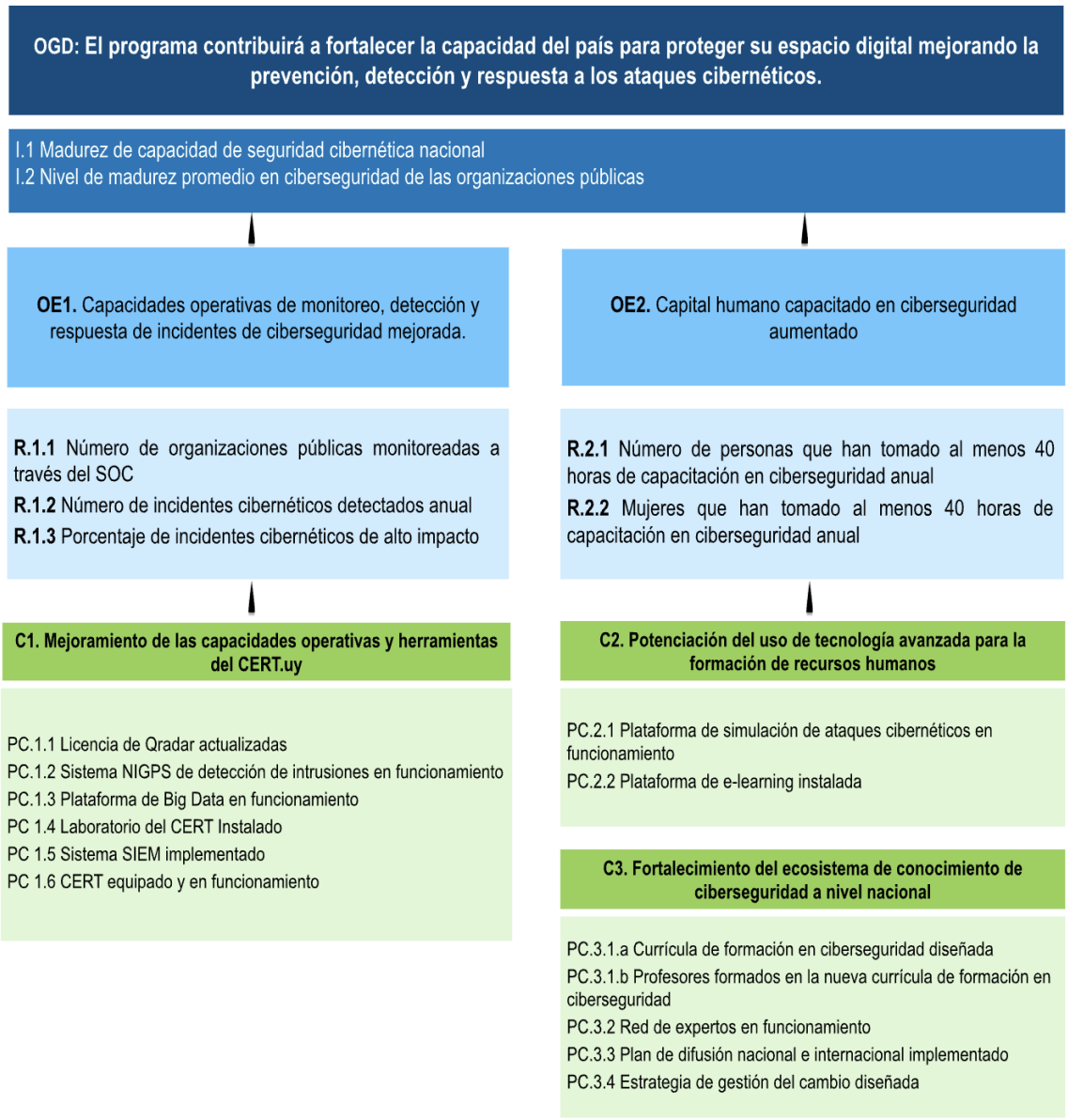
1. La *falta de capacidades operativas de monitoreo, detección y respuesta de incidentes*, producido por la falta de sistemas de monitoreo y/o su bajo nivel de desarrollo;

[8] En esta sección se analizan los resultados que el Programa alcanzó, en base a los indicadores definidos en el Documento de Proyecto original, sobre la base de la información expuesta en la Matriz de Resultados (MdR) y contemplándose las modificaciones en los indicadores y métricas durante la ejecución de la operación, en acuerdo con el Banco.

2. La *falta de profesionales capacitados en ciberseguridad***,** expresada en la creciente brecha entre oferta y demanda de profesionales en el sector, producto del rápido crecimiento de este último.

Tanto la problemática general como sus especificidades han sido validadas por todos los actores clave entrevistados durante la presente evaluación, incluso en aquellos casos donde la colaboración con la intervención ha iniciado ya en la fase de adquisición y/o implementación del Programa.

En términos de diseño y lógica vertical del Programa, dichas problemáticas encuentran estrecha relación con los Componentes, Resultados y Productos Clave definidos. Dicha relación se expresa en el cuadro que sigue:



Nota: OGD: Objetivo General de Desarrollo. OE: Objetivo Específico. C: Componente. I: Indicador. PC: Producto clave.

En el marco de los Productos Clave, todas las metas definidas de cara al cierre del año 2022 fueron alcanzadas (ver sección II.1.3), con la única excepción del PC.3.3. De manera similar, en términos de Resultados, se evidencia un logro en el Resultado 2, aunque los valores alcanzados respecto a las metas, para el Resultado 1, presentan ciertos desvíos (ver sección II.1.4).

Cabe mencionar que no se han realizado cambios en los indicadores de resultados ni en los productos críticos, en relación a la matriz de resultados originalmente presentada. Los cambios evidenciados se refieren a la planificación ajustada, con miras a la consecución de los mismos. En este sentido, la lógica vertical establecida por el diseño original del Programa, ha sido respetado hasta el momento de la presente evaluación intermedia.

II.1.3. Productos Ejecutados

En este acápite se describen los productos alcanzados por la ejecución del Proyecto, sobre la base de los indicadores identificados en la MdR[9], en referencia a los informes semestrales de avance en la ejecución, sobre los registros de los sistemas de la AGESIC. Además, se revisan uno a uno los productos a ser ejecutados con la operación según lo establecido en el PEP de la operación y en el Plan de Adquisiciones (PA).

Respecto a los Productos establecidos por el Programa, durante la ejecución fueron modificadas algunas metas y plazos para los indicadores que se consideraron en la matriz original. Se hacen las siguientes aclaraciones al respecto:

Componente 1:

Producto 1.2. Sistema NGIPS de detección de intrusiones en funcionamiento. La meta referida a la implementación del sistema ha sido planificada para el año 2022, aunque en el último informe de avance disponible (correspondiente al segundo semestre del año 2022), se propone diferir la meta para el año 2024. Cabe señalar que a la fecha de elaboración de la presente evaluación intermedia, no se cuenta con un documento respaldatorio por parte del Directorio del Banco Interamericano de Desarrollo que refleje la aceptación del Banco de dicha propuesta. No obstante, cabe mencionar que en el Informe de Avance presentado al cierre de Diciembre de 2022, dicha modificación es presentada y aprobada por el BID junto con el resto de la información presentada en dicho documento[10].

Componente 2:

Producto 2.2. Plataforma de e-learning instalada. La meta referida a la implementación de la plataforma se encuentra planificada para el año 2023 en el marco del diseño inicial del Programa, aunque en el último informe de avance disponible se propone diferirla hacia el año 2024. Si bien no es objeto de la presente evaluación, este diferimiento puede afectar evaluaciones futuras del Programa, en caso de no contar con un documento respaldatorio por parte del Banco Interamericano de Desarrollo que dé aceptación y formalidad a dicha propuesta. No obstante, cabe mencionar que en el Informe de Avance presentado al cierre de Diciembre de 2022, dicha modificación es presentada y aprobada por el BID junto con el resto de la información presentada en dicho documento[11].

Producto 2.3. Cursos de ciberseguridad disponibilizados por AGESIC y de acceso libre. Se ha incorporado dicho indicador de producto como complemento del indicador 2.2, siendo esta propuesta presentada y aprobada con el último informe de avance presentado al momento del

[9] La evaluación se realiza conforme a los informes semestrales de avance del programa desde el inicio de la ejecución hasta la finalización.
[10] Informe de avance al 31 de diciembre de 2022
[11] Informe de avance al 31 de diciembre de 2022

presente análisis[12]. Cabe mencionar que el primer producto a entregar (tomando como unidad de medida “cursos”) se planifica para el año 2023, por lo que queda por fuera del alcance del presente documento (ver Cuadro 2).

Componente 3:

Producto 3.1b. Profesores formados en la nueva currícula de formación en ciberseguridad. La meta definida establece capacitar a 60 docentes en 2022, con el objetivo de llegar a 220 hacia el final del Programa. En la meta ajustada, estos 60 docentes han sido desconsiderados, previendo un impacto sobre 160 educadores hacia el final de la intervención. Complementariamente, en el último informe de avance disponible, se requiere una replanificación de esta última meta, proponiendo llegar a 35 docentes, tanto en el año 2023 como en el año 2024[13].

A continuación, se detalla el grado de avance de los productos correspondientes a cada uno de los Componentes del Programa:

Cuadro 1. Productos Ejecutados Componente 1 – Meta planeada vs meta alcanzada, por año

Componente / Producto	Unidad de Medida				
			2020	2021	2022
Componente 1. Mejoramiento de las capacidades operativas y herramientas del CERT.uy					
1.1 Licencia de Qradar actualizadas	Licencia	**P**	1	0	0
		P(a)	1	0	0
		A	1	0	0
1.2 Sistema NGIPS de detección de intrusiones en funcionamiento	Sistema	**P**	0	0	1
		P(a)	0	0	0
		A	0	0	0
1.3 Plataforma de Big Data en funcionamiento	Plataforma	**P**	0	0	0
		P(a)	0	0	0
		A	0	0	0
1.4 Laboratorio del CERT instalado	Laboratorio	**P**	0	0	1

[12] Informe de avance al 31 de diciembre de 2022

[13] Cabe mencionar que el logro de dicha meta excede al alcance del presente informe, el cual considera el logro de los objetivos y metas establecidos hasta el cierre del año 2022.

		P(a)	0	0	1
		A	0	0	1
1.5 Sistema SIEM implementado	Sistema	**P**	0	1	0
		P(a)	0	1	0
		A	0	1	0
1.6 CERT equipado y en funcionamiento	Sistema	**P**	0	0	0
		P(a)	1	1	1
		A	1	1	1

Fuente: Matriz de Resultados del Programa, Informe de Avance, 2do semestre de 2022

El análisis de los productos identificados en el Componente 1 del programa permiten verificar un **cumplimiento del 100%** en la comparación de las metas Planificadas (ajustadas) y la meta alcanzada.

Cabe señalar que el cumplimiento de las metas respecto a la terminación del Programa, para el Componente 1, es del 100% para los productos 1.1 y 1.5, encontrándose el producto 1.6 con un nivel de completitud del 60% (3 de 5 sistemas instalados).

Cuadro 2. Productos Ejecutados Componente 2 – Meta planeada vs meta alcanzada, por año

Componente / Producto	**Unidad de Medida**				
			2020	**2021**	**2022**
Componente 2. Potenciación del uso de tecnología avanzada para formación de recursos humanos					
2.1 Plataforma de simulación de ataques cibernéticos en funcionamiento	Plataforma	**P**	0	0	1
		P(a)	0	1	0
		A	0	1	0
2.2 Plataforma de e-learning instalada	Plataforma	**P**	0	0	0
		P(a)	0	0	0
		A	0	0	0

2.3 Cursos de ciberseguridad disponibilizados por AGESIC y de acceso libre	Cursos	**P**	0	0	0
		P(a)	0	0	0
		A	0	0	0

Fuente: Matriz de Resultados del Programa, Informe de Avance, 2do semestre de 2022

El análisis de los productos identificados en el Componente 2 del programa permiten verificar un **cumplimiento del 100%** en la comparación de las metas Planificadas (ajustadas) y la meta alcanzada.

Cabe señalar que el cumplimiento de las metas respecto a la terminación del Programa, es del 100% para el producto 2.1 (1 de 1 plataforma de simulación de ataques cibernéticos instalada).

Cuadro 3. Productos Ejecutados Componente 3 – Meta planeada vs meta alcanzada, por año

Componente / Producto	**Unidad de Medida**				
			2020	**2021**	**2022**
Componente 3. Fortalecimiento del ecosistema de conocimiento de ciberseguridad a nivel nacional					
3.1 a Currícula de formación en ciberseguridad diseñada	Currícula	**P**	0	0	1
		P(a)	0	0	1
		A	0	0	1
3.1 b Profesores formados en la nueva currícula de formación en ciberseguridad	Profesores	**P**	0	0	60
		P(a)	0	0	0
		A	0	0	0
3.2 Red de expertos en funcionamiento	Red de expertos	**P**	0	1	0
		P(a)	0	1	0
		A	0	1	0
3.3 Plan de difusión nacional e internacional implementado	Plan	**P**	0	1	0
		P(a)	0	0	1

		A	0	0	0
3.4 Estrategia de gestión del cambio diseñada	Documento	**P**	1	0	0
		P(a)	1	1	1
		A	1	1	1

Fuente: Matriz de Resultados del Programa, Informe de Avance, 2do semestre de 2022

El análisis de los productos identificados en el Componente 3 del programa permiten verificar un **cumplimiento del 100%** en la comparación de las metas Planificadas (ajustadas) y la meta alcanzada, con excepción del producto 3.3, donde se ha planificado implementar un Plan de difusión nacional e internacional hacia el año 2022, pero donde no se encuentra registro de dicha implementación en los últimos informes de avance analizados.

Cabe señalar que el cumplimiento de las metas respecto a la terminación del Programa, para el Componente 3, es del 100% para los productos 3.1, 3.2 y 3.4.

En función de lo analizado previamente, se presenta a continuación un resumen de los productos alcanzados en relación a lo planificado, tomando como referencia la planificación ajustada. Tal como puede observarse, 7 de las 12 metas definidas en relación a los productos del Programa se encuentran en un 100% de completitud hacia el año 2022.

Cuadro 4. Productos - Meta planeada vs meta alcanzada - Resumen general

	Meta (2022)	**Alcanzado (2022)**	**% logro**	**Meta (Fin del Proyecto)**	**% logro**
Componente 1. Mejoramiento de las capacidades operativas y herramientas del CERT.uy					
1.1 Licencia de Qradar actualizadas	1	1	100%	1	100%
1.2 Sistema NGIPS de detección de intrusiones en funcionamiento*	0	0	-	1	0%
1.3 Plataforma de Big Data en funcionamiento	0	0	-	1	0%
1.4 Laboratorio del CERT instalado	1	1	100%	1	100%
1.5 Sistema SIEM implementado	1	1	100%	1	100%
1.6 CERT equipado y en funcionamiento	3	3	100%	5	60%
Componente 2. Potenciación del uso de tecnología avanzada para formación de recursos humanos					
2.1 Plataforma de simulación de ataques cibernéticos en funcionamiento	1	1	100%	1	100%
2.2 Plataforma de e-learning instalada	0	0	-	1	0%

Componente 3. Fortalecimiento del ecosistema de conocimiento de ciberseguridad a nivel nacional					
3.1 a Currícula de formación en ciberseguridad diseñada	1	1	100%	1	100%
3.1 b Profesores formados en la nueva currícula de formación en ciberseguridad	0	0	-	160	0%
3.2 Red de expertos en funcionamiento	1	1	100%	1	100%
3.3 Plan de difusión nacional e internacional implementado	1	0	0%	1	0%
3.4 Estrategia de gestión del cambio diseñada	3	3	100%	3	100%

Fuente: Elaboración propia en base a Matriz de Resultados del Programa

II.1.4. Resultados logrados y atribución

El Programa plantea 2 resultados a ser alcanzados, con 5 indicadores diferentes para corroborar su cumplimiento. Particularmente, como resultados del Programa, se define: (1) Capacidades operativas de monitoreo, detección y respuesta de incidentes de ciberseguridad mejorada, y (2) Capital humano capacitado en ciberseguridad aumentado.

A continuación, es posible observar el grado de avance de cada resultado, a la fecha del último informe semestral presentado:

Cuadro 5. Resultado 1. Capacidades operativas de monitoreo, detección y respuesta de incidentes de ciberseguridad mejorada - Meta planeada vs meta alcanzada

Indicador	Unidad de Medida	Línea de base	Año Línea de base		2020	2021	2022
Número de organizaciones públicas monitoreadas a través del SOC	Número de ministerios	2	2018	P	2	5	11
				A	2	6	11
Número de incidentes cibernéticos detectados anual	Número de incidentes	2.043	2018	P	2500	4000	6000
				A	2761	3948	4169
Porcentaje de incidentes cibernéticos de alto impacto	Porcentaje	2.1	2018	P	2	1,84	1,51
				A	2,10	1,27	3,00

Fuente: Matriz de Resultados del Programa, Informe de Avance, 2do semestre de 2022

Cuadro 6. Resultado 2. Capital humano capacitado en ciberseguridad aumentado - Meta planeada vs meta alcanzada

Indicador	Unidad de Medida	Línea de base	Año Línea de base		2020	2021	2022
Número de personas que han tomado al menos 40 horas de capacitación en ciberseguridad anual	Número de personas	50	2018	P	0	0	150
				A	0	674	1510
Mujeres que han tomado al menos 40 horas de capacitación en ciberseguridad anual	Porcentaje	0	2018	P	0	0	15
				A	0	15	47

Fuente: Matriz de Resultados del Programa, Informe de Avance, 2do semestre de 2022

Tal como puede observarse, el indicador 1 del Resultado 1, se encuentra cumplido en su meta parcial para el año 2022. Sin embargo, los indicadores 2 y 3 no se encuentran cumplidos según las metas establecidas para el año analizado. Para el Resultado 2, en cambio, los dos indicadores definidos se encuentran ampliamente cumplidos, teniendo en cuenta las metas parciales establecidas para el año 2022.

A continuación, se expresa la tasa de logro para cada uno de los indicadores de contraste para los resultados establecidos, en base a la última información compartida por parte del Programa[14]. Para el cálculo de la tasa de logro de los resultados esperados, se utilizan las siguientes fórmulas, siguiendo las buenas prácticas establecidas por el Banco Interamericano de Desarrollo para la elaboración de Informes de Terminación de Programas (PCR, por sus siglas en inglés):

i) Para calcular la tasa de logro de aquellos indicadores de resultado cuyo valor se espera que sea inferior a la línea de referencia:

$$\frac{Línea\ de\ referencia\ P\ -\ Logro\ Registrado\ (EOP)}{Línea\ de\ referencia\ (P) - Meta\ Definida\ (P)}$$

ii) Para calcular la tasa de logro de aquellos indicadores de resultado cuyo valor se espera que sea superior a la línea de referencia:

$$\frac{Línea\ de\ referencia\ P\ -\ Logro\ Registrado\ (EOP)}{Línea\ de\ referencia\ (P) - Meta\ Definida\ (P)}$$

iii) Para calcular la tasa de logro en casos excepcionales en los que se espera que un indicador de resultado mantenga el valor de la línea de referencia:

[14] Informe de Avance, 2do semestre de 2022

$$1 - \frac{\text{Línea de referencia } P - \text{ Logro Registrado } (EOP)}{\text{Línea de referencia } (P) - \text{Meta Definida } (P)}$$

Tomando estas definiciones, si el valor final del indicador del proyecto muestra una mejora respecto a la línea de referencia la tasa de logro es automáticamente igual al valor unitario (1).

Cuadro 7. Resultados Esperados – Tasa de Logro

Resultado 1: Capacidades operativas de monitoreo, detección y respuesta de incidentes de ciberseguridad mejorada.							
Indicador	**Unidad de Medida**	**Línea de Base**	**Meta (2022)**	**Meta (Fin del Programa)**	**Logro registrado**	**Tasa de Logro (2022)**	**Tasa de Logro (Fin del Programa)**
Número de organizaciones públicas monitoreadas a través del SOC	Número de ministerios	2	11	17	11	1,0	0,6
Número de incidentes cibernéticos detectados anual	Número de incidentes	2043	6000	10000	4169	0,5	0,3
Porcentaje de incidentes cibernéticos de alto impacto	Porcentaje	2,1	2	1	3	-1,5	-0,8
Resultado 2: Capital humano capacitado en ciberseguridad aumentado.							
Indicador	**Unidad de Medida**	**Línea de Base**	**Meta (2022)**	**Meta (Fin del Programa)**	**Logro registrado**	**Tasa de Logro**	**Tasa de Logro (Fin del Programa)**
Número de personas que han tomado al menos 40 horas de capacitación en ciberseguridad anual	Número de personas	50	150	350	1510	14,6	4,9
Mujeres que han tomado al menos 40 horas de capacitación en ciberseguridad anual	Porcentaje	0	15	25	47	3,1	1,9

Fuente: Elaboración Propia a partir de Matriz de Resultados del Programa, Informe de Avance, 2do semestre de 2022

Resultado Esperado 1. Capacidades operativas de monitoreo, detección y respuesta de incidentes de ciberseguridad mejorada.. Para dicho el monitoreo de dicho resultado se han establecido 3 indicadores, de los cuales solo 1 se encuentran cumplido al 100% en términos de la meta definida para el año 2022, considerando el alcance de la presente evaluación. En este sentido, puede afirmarse que se han alcanzado el número de organizaciones públicas monitoreadas mediante el SOC, gracias a la intervención del Programa.

En línea con lo mencionado previamente, en las entrevistas a referentes realizadas, tanto de la misma AGESIC como de organismos gubernamentales y agentes privados que han participado del Programa, se destaca la implementación del GSOC como uno de los principales logros de la intervención. Se considera valioso dado que ha brindado una capacidad de monitoreo a los organismos beneficiarios que no hubieran podido obtener mediante recursos propios, y asociado

a las auditorías iniciales que han posibilitado la implementación, sienta las bases para el desarrollo futuro en materia de ciberseguridad para los organismos públicos a nivel nacional. En base a estas observaciones, se evidencia la atribución del logro descrito a las acciones del Programa, con un gran valor agregado en la articulación de las partes involucradas tanto en las tareas de auditoría, como de planificación e implementación.

No obstante el logro del indicador de resultado, se evidencian ciertos desafíos en el marco de las entrevistas, que vale la pena mencionar:

a. En el marco de las auditorías iniciales, los agentes privados participantes de las entrevistas mencionan la oportunidad de haber conocido mejor la infraestructura y problemáticas de los organismos públicos antes del relevamiento , para lograr una colaboración más fructífera entre ambos. Sin embargo, la falta de recursos por parte de los organismos (ya sea en términos de recursos humanos o en tiempo de dedicación a las iniciativas desarrolladas), no permiten tener este conocimiento hasta no comenzadas las actividades de relevamiento. En este sentido, se destaca que en muchos casos los puntos de partida establecidos para el monitoreo no han sido los de mayor impacto, como monitorear correos electrónicos, aunque esto resultaba difícil de estimar en el comienzo de la intervención (asimismo, vale la pena mencionar que los casos de uso son definidos por el mismo organismo beneficiario, no teniendo ni AGESIC ni el agente privado la potestad de decidir sobre esta implementación). AGESIC esta trabajando en mejorar este tipo de trabajo, ofreciendo a los organismos un “menú” de opciones que sean relevantes.
b. De cara a la implementación, se destaca el valor para los organismos de contar con un recursos como el GSOC sin considerar inversión propia, aunque desde el punto de vista del proceso de implementación, se ha destacado la necesidad de demostrar con mayor anticipación el valor del GSOC, con el fin que los organismos dispongan más rápida y efectivamente de los recursos con los cuales colaborarían durante el mismo (es decir, infraestructura propia y recursos humanos). Cabe mencionar que desde el accionar de la AGESIC se ha desarrollado, en cada caso, un Acuerdo de Adhesión para incentivar el compromiso por parte de cada uno de los organismos involucrados. Esto enmarca las acciones desarrolladas por el Programa de cara al desarrollo del GSOC. En este sentido, el Acuerdo de Adhesión firmado con cada organismo tiene como objeto que la AGESIC “brinde apoyo a la entidad en el fortalecimiento de sus capacidades en ciberseguridad”[15], mediante el cual en el Anexo se provee de un listado de obligaciones que el organismo beneficiario debe cumplir, entre las cuales se destacan “1. Proporcionar la infraestructura, en ambiente de producción, para la implantación de los sensores y colectores de datos”, “3. Incluir este contrato en las metas y/o planificación anual del organismo en lo que respecta al proyecto de implantación y sostenibilidad del mismo”, “4. Designar un responsable técnico que será el interlocutor entre CERTuy y las diferentes áreas del organismo (...)”, “5. Designar un equipo técnico, para poder llevar adelante esta implantación, en los tiempos acordados en el Plan de Trabajo”, “6. Brindar la información necesaria de los activos a monitorear”, y “7. Brindar la información necesaria para poder analizar los eventos generados por los activos que son monitoreados (...)”. A su vez, allí se especifican los tiempos estipulados para la mitigación o remediación de las vulnerabilidades detectadas, además de declarar las responsabilidades correspondientes al CERT.uy durante la implantación.
c. Partiendo de las alertas que el GSOC genera en base a la información compartida por los

[15] Fuente: Contrato de Adhesión para el Fortalecimiento de Capacidades en Seguridad de la Información. Implantación de Gsoc. Ver Anexos.

organismos respecto a los activos a monitorear y los eventos generados por dichos activos, algunos de los organismos entrevistados mencionan que las notificaciones sobre actividad crítica brindadas resultan en ocasiones genéricas, sin aplicar a las herramientas que usa el organismo. Cabe mencionar, no obstante, que las alertas generadas por el GSOC para organismos participantes son alertas específicas sobre el equipamiento o software afectado, pudiendo tratarse esto de cierta confusión con las alertas generales brindadas por CERTuy como parte de su comunicación con los organismos frente a amenazas o vulnerabilidades.

d. Si bien no es parte integrante de las acciones del préstamo, cabe mencionar que diversos organismos y actores privados entrevistados toman como punto de partida de su relación con AGESIC, en pos de realizar mejoras en materia de ciberseguridad, las auditorías iniciales realizadas. En este sentido, si bien el marco utilizado aquí resulta ampliamente reconocido y es tomado como referencia en la región, algunos actores destacan que el mismo no termina de adaptarse a la realidad de América Latina y el Caribe, tomando parámetros de evaluación de alta especificidad, que pierden valor al no estar cumplidos los criterios de evaluación básicos para la materia. De esta manera, se destaca que el marco para realizar la evaluación es de calidad, consistente y completo, aunque invita a realizar acciones de mejora muy específicas que no se termina de corresponder con las necesidades básicas de muchos organismos.

Las oportunidades mencionadas pueden explicar el cumplimiento parcial de los restantes indicadores. Tal como puede verse en el cuadro previo, el indicador 2 “Número de incidentes cibernéticos detectados anual” se encuentra a un nivel de logro del 50%, habiendo detectado 2.126 incidentes de los 3.957 nuevos incidentes a detectar planificados. Por su parte , el indicador 3 “Porcentaje de incidentes cibernéticos de alto impacto” no solo no cumple la meta parcial establecida, sino que ha incrementado su valor respecto a la línea de base correspondiente al año 2018. En este sentido, cabe mencionar que las personas de AGESIC entrevistadas mencionan que el indicador presenta limitaciones al no poder delimitarse efectivamente cuáles de los incidentes detectados resultan “graves” o se vuelven “graves” durante el ciclo, tendiendo a errores de cálculo en el indicador. Se destaca que dicho indicador debería buscar medir la eficacia del Programa en base a la cantidad de incidentes que se transforman en “graves” y permiten así la detección temprana de vulnerabilidades. Otra limitación relacionada, mencionada durante las entrevistas, es que el Programa prevé incorporación del personal al SOC para actividades de detección y monitoreo, pero no lo hace para el CERTuy con la finalidad de contener un incidente declarado, limitando la capacidad de acción frente a un incremento real de incidentes graves declarados[16].

Resultado Esperado 2. Capital humano capacitado en ciberseguridad aumentado. El cumplimiento de este resultado se evaluó mediante 2 indicadores. Para el primer indicador “Número de personas que han tomado al menos 40 horas de capacitación en ciberseguridad anual”, se evidencia un logro de 14,6 veces sobre la meta parcial establecida, llegando a cumplir también en 4,9 veces la meta establecida para el cierre de la operación. Esto implica haber capacitado, hacia el año 2022, a 1.510 personas en materia de ciberseguridad.

Para el segundo indicador “Mujeres que han tomado al menos 40 horas de capacitación en ciberseguridad anual”, se evidencia un logro en 3,1 veces sobre la meta parcial establecida para el año 2022, significando esto un logro en 1,9 veces de la meta establecida para el fin del Programa. En este sentido, se observa un 47% de mujeres capacitadas en materia de

[16] Al momento de elaborar el presente informe, la AGESIC se encuentra en el marco de la elaboración de nuevos indicadores para considerar como alternativa a los mencionados.

ciberseguridad, sobre un 15% establecido para el año 2022 (25% para el fin de la operación).

El logro de este resultado resulta más que relevante frente a los desafíos mencionados, en materia de ciberseguridad, por parte de los actores entrevistados. En relación a este último punto, se ha mencionado que los principales problemas con los que cuentan los organismos son la falta de recursos humanos capacitados en la materia, siendo que ésta no se percibe como un área de especialización dentro de la propia formación universitaria en Tecnología de la Información. Frente a esto, los recursos disponibles y compartidos como material de capacitación, incluso en la misma web de AGESIC, aparecen como un recurso valioso para los organismos. Asimismo, se han considerado las siguientes oportunidades por parte de las personas entrevistadas, que pueden señalar nuevos desafíos para el Programa, así como lecciones aprendidas:

a. Si bien el plan de formación desarrollado mediante el diplomado resulta útil y necesario, al no estar centrado en graduados universitarios de las carreras en ingeniería y sistemas de información, los conocimientos técnicos de la audiencia suelen ser iniciales, lo que dificulta la aprehensión de los conocimientos impartidos y su puesta en práctica. En este sentido, durante la entrevistas se destaca la necesidad de especializar a perfiles profesionales afines, en asociación con instituciones educativas.
   En este sentido, resulta relevante mencionar que, durante las entrevistas realizadas a personas de la AGESIC, se destaca que las acciones en materia de educación por parte del Programa han tenido dos vertientes: una primera acción ligada a la actualización profesional mediante becas para programas de posgrado, centradas en graduados universitarios que busquen especializarse, y que justamente aborda esta oportunidad mencionada previamente por los organismos entrevistados; y una segunda línea de acción ligada a la currícula técnica que permite que tanto jóvenes que terminan la educación secundaria como profesionales que busquen desarrollar otro perfil o revalidar sus conocimientos, y se encuentren interesados en ciberseguridad, puedan contar con las herramientas para dedicarse a ellos. Esta última currícula se encuentra a disposición de todas las instituciones educativas del país hoy en día, estando así en proceso de puesta en marcha[17].
b. Se considera que la capacitación de recursos humanos podría haber empezado con anticipación, en tanto que proceso, para poder aprovechar el impacto del conocimiento impartido durante la implementación del Programa. El plazo invertido en la planificación de dichas actividades se traduce hoy en un bajo uso de dichos conocimientos, en relación al grado de avance de las actividades correspondientes a la intervención en los organismos y la implementación de los sistemas ya mencionados. Complementariamente, cabe mencionar que en las entrevistas realizadas a personal de la AGESIC, se aclara que este efecto es principalmente producto de la pandemia y el descalce presupuestario que este factor contextual ha generado.

En este sentido, para el primer resultado se identifica un grado de avance parcial, mientras que para el segundo la meta se encuentra alcanzada. No obstante, para ambos se mencionan desafíos y aprendizajes durante los primeros años de implementación, que involucran tanto a la planificación de las actividades que hacen a la intervención, como también al involucramiento de

[17] Como punto de referencia de estas acciones puede ser considerada la currícula de nivel técnica implementada en la Universidad del Trabajo de Uruguay (UTU). Link. (https://www.utu.edu.uy/noticias/tecnologo-en-ciberseguridad-preinscripciones-abiertas-hasta-el-lunes-22-de-mayo)

las diferentes partes durante la ejecución y las capacidades que los beneficiarios tienen de cara a la sostenibilidad de los logros alcanzados. En este sentido, cabe mencionar que durante las entrevistas a AGESIC se destaca la buena recepción de las acciones emprendidas por parte del sistema educativo, a la vez que la buena ejecución que están teniendo dichas acciones. De esta manera, puede verse que los desafíos mencionados se encuentran siendo abordados en el marco de la ejecución actual.

II.1.5. Impacto

El impacto del Programa fue definido como **"**Madurez de Capacidad de Seguridad Cibernética aumentada**".** Para su demostración se propusieron 2 indicadores en la MdR original, a saber:

1. Madurez de capacidad de seguridad cibernética nacional;
2. Nivel de madurez promedio en ciberseguridad de las organizaciones públicas.

A continuación, se muestra su valor en la medición de línea de base realizada, en contraste con su valor actual según lo informado en el último informe de avance disponible:

Cuadro 8. Indicadores de Impacto – Metas Planeadas vs Alcanzadas

Impacto 1: Madurez de Capacidad de Seguridad Cibernética aumentada							
Indicador	**Unidad de Medida**	**Línea de Base**	**Meta (2022)**	**Meta (Fin del Programa)**	**Logro registrado**	**Tasa de Logro (2022)**	**Tasa de Logro (Fin del Programa)**
Madurez de capacidad de seguridad cibernética nacional	Puntaje	149	s/d	165	s/d	s/d	s/d
Nivel de madurez promedio en ciberseguridad de las organizaciones públicas	Puntaje	1,5	s/d	2,5	s/d	s/d	s/d

Fuente: Elaboración Propia a partir de Documento de Propuesta de Préstamo

Tal como puede observarse, no se han establecido metas intermedias para los Indicadores de Impacto del Programa, por lo cual tampoco son informados en los Informes de Avance consultados. Esto puede deberse a dos factores: en el caso del Indicador 1, se trata de una fuente externa de la cual se tiene una dependencia (Informe OEA BID); en el caso del segundo Indicador, el resultado registrado depende de la realización de una auditoría externa, no realizada nuevamente, luego de la medición de la línea de base, al momento de la realización del presente informe. En este sentido, desde la AGESIC se destaca que las auditorías realizadas inicialmente han sido llevadas a cabo mediante contrataciones externas realizadas por la Agencia, se realizan anualmente y que lo mismo será realizado hacia el fin de la ejecución también. Durante dicha ejecución, las auditorías en base al marco de ciberseguridad del país son realizadas por consultoras externas contratadas por la misma AGESIC.

II.2. Eficiencia

II.2.1. Análisis de costos y ejecución presupuestaria

Los costos y ejecución del programa pueden expresarse de distintas maneras a fin de entender la evolución y el estado de situación actual.

Según el Contrato de Préstamo, el presupuesto para el Programa fue establecido en **US$ 10 millones**, financiado con fuente BID por **US$ 8 millones** y fuente local por **US$ 2 millones**[18]. Sobre dicho monto, un 47% (US$ 4,7 millones) se encontraban dentro de la planificación de la ejecución presupuestaria hacia cierre del año 2022.

Cabe mencionar que dicha planificación fue ajustada durante la ejecución del Programa, teniendo como resultado un monto total presupuestado para el Programa de US$ 10,4 millones, sobre lo que se estimó ejecutar un 49% (US$ 5,2 millones) hacia el cierre del año 2022[19]. Sobre dicha planificación ajustada, el cumplimiento del plan de ejecución es del 100% por parte del Programa[20].

A continuación, se expresan los costos incurridos según cada componente y producto, informados en los sucesivos informes semestrales, por parte del Programa:

Cuadro 8. Ejecución Financiera. Componente 1

Componente / Producto	Unidad de Medida		Año			
			2019	2020	2021	2022
Componente 1. Mejoramiento de las capacidades operativas y herramientas del CERT.uy						
1.1 Licencia de Qradar actualizadas	Licencia	**P**	0	824	0	0
		P(a)	0	802	0	0
		A	0	802	0	0
1.2 Sistema NGIPS de detección de intrusiones en funcionamiento	Sistema	**P**	0	68	75	61
		P(a)	0	68	129	62
		A	0	68	129	62
1.3 Plataforma de Big Data en funcionamiento	Plataforma	**P**	0	43	70	90
		P(a)	0	35	70	172
		A	0	35	70	172
1.4 Laboratorio del CERT instalado	Laboratorio	**P**	0	0	222	114

[18] Contrato de Préstamo No. 4843/OC-UR

[19] En el Informe de Avance presentado al cierre de Diciembre de 2022, dicha modificación es presentada y aprobada por el BID junto con el resto de la información presentada en dicho documento.

[20] Matriz de Costos del Programa, Informe de Avance, 2do semestre de 2022

		P(a)	13	110	166	331
		A	13	110	166	331
1.5 Sistema SIEM implementado	Sistema	**P**	0	175	465	465
		P(a)	28	205	376	619
		A	28	205	376	619
1.6 CERT equipado y en funcionamiento	Sistema	**P**	0	134	408	481
		P(a)	0	204	508	421
		A	0	204	508	421

(*) Todos los costos están expresados en miles de dólares estadounidenses e incluyen contrapartida local.

Fuente: Matriz de Resultados del Programa, Informe de Avance, 2do semestre de 2022

Cuadro 9. Ejecución Financiera. Componente 2

Componente / Producto	**Unidad de Medida**	**Año**			
		2019	**2020**	**2021**	**2022**
Componente 2. Potenciación del uso de tecnología avanzada para formación de recursos humanos					
2.1 Plataforma de simulación de ataques cibernéticos en funcionamiento	Plataforma	**P**	0	0	183	300
		P(a)	0	0	493	117
		A	0	0	493	117
2.2 Plataforma de e-learning instalada	Plataforma	**P**	0	0	0	0
		P(a)	0	0	0	0
		A	0	0	0	0

(*) Todos los costos están expresados en miles de dólares estadounidenses e incluyen contrapartida local.

Fuente: Matriz de Resultados del Programa, Informe de Avance, 2do semestre de 2022

Cuadro 10. Ejecución Financiera. Componente 3

Componente / Producto	Unidad de Medida		Año			
			2019	2020	2021	2022
Componente 3. Fortalecimiento del ecosistema de conocimiento de ciberseguridad a nivel nacional						
3.1 a Currícula de formación en ciberseguridad diseñada	Currícula	**P**	0	0	6	1
		P(a)	0	0	0	110
		A	0	0	0	110
3.1 b Profesores formados en la nueva currícula de formación en ciberseguridad	Profesores	**P**	0	0	122	134
		P(a)	0	0	0	0
		A	0	0	0	0
3.2 Red de expertos en funcionamiento	Red de expertos	**P**	0	0	37	49
		P(a)	0	0	8	0
		A	0	0	8	0
3.3 Plan de difusión nacional e internacional implementado	Plan	**P**	0	0	0	0
		P(a)	46	38	5	0
		A	46	38	5	0
3.4 Estrategia de gestión del cambio diseñada	Documento	**P**	0	14	12	12
		P(a)	0	0	0	0
		A	0	0	0	0

(*) Todos los costos están expresados en miles de dólares estadounidenses e incluyen contrapartida local.

Fuente: Matriz de Resultados del Programa, Informe de Avance, 2do semestre de 2022

Cuadro 11. Ejecución Financiera. Administración del Programa

Componente / Producto		Año			
		2019	2020	2021	2022
Componente 4. Administración del Programa					
4.1 Administración u otros gastos contingentes	**P**	0	45	15	55
	P(a)	0	0	13	0
	A	0	0	13	0

(*) Todos los costos están expresados en miles de dólares estadounidenses e incluyen contrapartida local.

Fuente: Matriz de Resultados del Programa, Informe de Avance, 2do semestre de 2022

Tal como puede observarse, en todos las líneas de gasto discriminadas en el Plan de Ejecución Presupuestaria, el cumplimiento respecto a la planificación ajustada es del 100%, sin presentar desvíos de ningún tipo.

Respecto a la planificación inicial, puede notarse que los desvíos se encuentran mayormente concentrados en el Producto 1.4 “Laboratorio del CERT instalado”, donde se ha decidido dedicar una mayor cantidad de recursos al mismo durante el año 2022, a la vez que en los productos 2.1 “Plataforma de simulación de ataques cibernéticos en funcionamiento”, donde se evidencia un mayor uso de los recursos hacia el año 2021 como contrapartida del menor presupuesto asignado a la ejecución del año 2022, y el Producto 3.1a “Currícula de formación en ciberseguridad diseñada”, donde se evidencia una significa asignación de recursos a la ejecución presupuestaria del año 2022, no contemplada en la planificación inicial del Programa. Complementariamente, cabe señalar que los recursos inicialmente destinados al Producto 3.1b “Profesores formados en la nueva currícula de formación en ciberseguridad” han sido postergados para los años 2023 y 2024, en línea con la dependencia que presenta respecto al Producto 3.1a. En este sentido, cabe mencionar que durante las entrevistas con AGESIC, se ha mencionado que este cambio en materia de metas y sus correspondientes fechas límite se deben a los cambios de asignación presupuestaria que la pandemia obligó a realizar, forzando a priorizar otro tipo de proyectos.

De manera complementaria, se presenta a continuación la evaluación del desempeño en la ejecución de los recursos del Programa discriminando por componente y fondos aportados por el Banco en relación a los recursos de contraparte.

Tal como puede observarse, la mayor ejecución presupuestaria se encuentra concentrada en el Componente 1 del Programa, el cual representa el componente más significativo respecto al gasto de la intervención. Esto demuestra una adecuada ejecución financiera por parte del mismo, mostrando principalmente desvíos en el Componente 3, frente al cual ya se ha mencionado la dependencia respecto al diseño de la nueva currícula en materia de ciberseguridad, producto

sobre el cual se han destinado recursos con anticipación con el fin de implementarlo adecuadamente. Cabe señalar, de manera complementaria, que los mayores desvíos en materia de ejecución presupuestaria se encuentran ligados a los costos administrativos de la intervención.

Cuadro 12. Resumen Ejecución del Préstamo por Componente y tipo de Aporte

Categoría de Inversión	Costo Total del Proyecto (US$)			Costo Total del Proyecto Ejecutado (US$)			Diferencia (%)		
	BID	Local	Total	BID	Local	Total	BID	Local	Total
Componente 1	4.438.525	976.475	5.415.000	2.951.401	1.366.367	4.317.769	-33,5%	39,9%	-20,3%
Componente 2	1.557.377	342.623	1.900.000	553.720	56.347	610.067	-64,4%	-83,6%	-67,9%
Componente 3	1.516.393	333.607	1.850.000	107.533	99.011	206.544	-92,9%	-70,3%	-88,8%
Componente 4	487.705	347.295	835.000	10.459	2.319	12.778	-97,9%	-99,3%	-98,5%
TOTAL	8.000.000	2.000.000	10.000.000	3.623.113	1.524.045	5.147.157	-54,7%	-23,8%	-48,5%

Fuente: Elaboración propia a partir de Ejecución Financiera, Informe de Avance, 2do semestre de 2022

II.2.2. Análisis económico del Programa

Con el fin de complementar el análisis de eficiencia sobre el Programa, se considera la evaluación económica realizada ex ante la implementación del mismo, a la vez que se resumen los supuestos sobre los cuales se han planteado los beneficios económicos de la intervención, con el fin de corroborar sus valores actuales y por ende su cumplimiento.

El análisis costo-beneficio realizado identificada tres factores sobre los cuales se esperaba que el proyecto genere retornos monetarios, a saber:

1. 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;
2. La disminución en el impacto económico causado por los ciberataques a las instituciones públicas, gracias a una mayor capacidad de prevención y respuesta;
3. La generación de actividad económica a través de la formación de profesionales en ciberseguridad y su subsecuente inserción al mercado laboral.

Sobre estas líneas de beneficios identificadas, la evaluación mencionada establece resultados económicos positivos para el Programa, con un Valor Presente Neto equivalente a US$ 40,334 millones, y una Tasa Interna de Retorno del 96%, en su escenario base.

Tal como puede observarse, las líneas de beneficio 1 y 3 identificadas en la evaluación, se corresponden directamente con Indicadores de Resultados planteados por el diseño del Programa. En este sentido, se expresa a continuación el valor actual de dichos Indicadores, en relación a los valores asumidos por la evaluación económica ex ante, para los tres escenarios considerados por el análisis:

Cuadro 13. Supuestos de Evaluación Económica Ex Ante vs Valor Registrado

Beneficio	Supuesto	Evaluación Económica Ex Ante			Valor Real (2do semestre 2022)
		Base	Conservador	Optimista	
Beneficio 1. Costo de Remediación	Porcentaje de ataques de severidad alta o muy alta	1%	1,5%	0,5%	3%
Beneficio 3. Actividad económica por formación de profesionales	Cantidad de profesionales nuevos formados en ciberseguridad	50 en 2022, 80 por año de ahí en adelante	20 en 2022, luego 40 en 2023, y 60 de 2024 en adelante	60 en 2021, luego 150 de 2022 en adelante	1510

Nota: no se presentan valores para el Beneficio 2 “Impacto económico de los ciberataques”, considerando que el indicador establecido como supuesto es *% del impacto económico evitado al final de la ejecución del proyecto*, y que dicho indicador requiere de una estimación propia por parte de la Agencia o los organismos beneficiarios, no registrada en el marco de los Resultados del Programa.

Fuente: Elaboración Propia a partir de Evaluación Económica Ex Ante y Matriz de Resultados del Programa, Informe de Avance, 2do semestre de 2022

Tal como puede observarse en el Cuadro previo, el valor real observado para el resultado asociado al Beneficio 1 no se encuentra dentro de los valores adoptados para calcular la rentabilidad social del Programa. Cabe mencionar que esto se encuentra alineado con el grado de cumplimiento de dicho resultado (ver sección II.1.4).

Complementariamente, se evidencia un valor real muy por encima del valor supuesto para el resultado asociado al Beneficio 3, al considerar el total de personas capacitadas en la materia. Sin embargo, cabe señalar que la evaluación económica ex ante supone una capacitación específica para profesionales ligados a la ingeniería y la tecnología de la información, brindada por instituciones universitarias, aspecto que no presenta una cobertura total entre el conjunto de la población abordada por los diplomados. Esto resulta relevante dado que estos aspectos formativos impactan en sus retornos salariales, y por ende en los beneficios económicos atribuibles al Programa. Asimismo, cabe mencionar que, tal como fue comentado previamente, unas de las acciones emprendidas por el Programa ligada a educación se centra en la actualización profesional mediante becas para programas de posgrado, centradas en graduados universitarios que busquen especializarse. En este sentido, es de esperarse que si la adopción de dicho contenido evoluciona favorablemente, dicho supuesto pueda llegar a cumplirse.

En este sentido, resulta importante, en el marco de la segunda mitad de la implementación, poder discriminar a la población beneficiaria en función de su nivel educativo y su formación de origen, con el fin de facilitar análisis ex post ligados a la rentabilidad económica de la intervención.

III. Implementación del Programa

III.1. Análisis de los factores críticos

Fortaleza Institucional. El rol de AGESIC fue clave para el éxito de la operación. Entre los actores entrevistados se destaca su disponibilidad y predisposición a la hora de diseñar e implementar soluciones para los problemas que afrontan diferentes organismos de la administración pública, desde un punto de vista integral.

Un aspecto destacado en su articulación con actores externos, lo cual siempre brinda credibilidad y solidez al curso de acción emprendido por la AGESIC. En este sentido, la auditoría externa que ha planteado un punto de partida para la intervención, ha significado una práctica de concientización sobre el tópico la ciberseguridad, pero también un punto de partida confiable con el cual contrastar los resultados de las acciones ligadas al Programa. Complementariamente, el apoyo siempre brindado por AGESIC en materia de capacitación y desarrollo de recursos educativos o pedagógicos, es uno de los aspectos más valorados de la intervención y ataca uno de los pilares fundamentales respecto al desarrollo de capacidades en materia de ciberseguridad, desde el punto de vista de las personas y organismos involucradas en el Programa y sus acciones.

Diagnóstico, priorización de problemas y diseño de la solución. Se evidencia una gran correspondencia entre los antecedentes planteados por el diseño del Programa, su lógica vertical y las acciones emprendidas, y la mirada sobre la situación local y regional en materia de ciberseguridad, por parte de los actores clave entrevistados. Ambas partes coinciden en la necesidad de hacer madurar las prácticas correspondientes a dicha disciplina, a la vez que concentrar los esfuerzos de la capacitación de los recursos humanos dedicados a la misma.

Complementariamente, cabe mencionar algunas lecciones aprendidas en relación a lo anterior: de las entrevistas cualitativas a actores involucrados en la intervención, surge la necesidad de revisar los tiempos de implementación en cuanto a recursos educativos, para futuras intervenciones, considerando que en esta oportunidad dichos recursos han sido desarrollados en paralelo a otras acciones que podrían haberse visto nutridas de una capacitación previa. Asimismo, si bien se destaca el hecho de haber focalizado las acciones en capacitar profesionales de otras disciplinas o jóvenes egresados de la educación secundaria en materia de ciberseguridad mediante diplomados técnicos, se plantea el desafío de capacitar recursos humanos profesionales provenientes de carreras de grado ligadas a la ingeniería y la tecnología de la información, dado que gracias al conocimiento técnico que ellos traen, pueden desarrollar un perfil profesional complementario a los primeros, muy alineado a las necesidades de los organismos beneficiarios. No obstante, es necesario mencionar que estas acciones se encuentran en vías de implementación por parte del Programa (primera línea de acción ligada a educación mencionada en los capítulos previos, ligada al incentivo de estudios de posgrado en la materia), por lo que se espera que esta percepción sobre la intervención se modifique en el tiempo y, gracias a la adopción favorable de los contenidos hasta ahora desarrollados, pueda ser sostenible en el tiempo.

Acceso a la tecnología y desarrollo de capacidades internas. La implementación del SIEM se destaca como uno de los puntos más importantes de la intervención, por parte de los organismos beneficiarios, considerando que con una baja inversión de recursos por su parte, sobre todo en materia de infraestructura, ha sido posible implementar una tecnología muy necesaria para los mismos.

Asimismo, se considera que la posibilidad de implementar dichas tecnologías ha permitido concientizar a las líneas de mando de dichos organismos sobre la relevancia del tema, aunque también ha planteado algunos desafíos, que pueden ser tomados como aprendizaje para la segunda etapa del Programa: en primer lugar, aparece el desafío de concientizar a los organismos beneficiarios sobre la necesidad de disponer y organizar sus recursos propios de cara a la implementación de las nuevas tecnologías, optimizando la colaboración con los actores privados que participan de dichos procesos; en segundo lugar, se menciona el desafío de optimizar el sistema de alertas para generar una máxima adopción del mismo, considerando que existen ciertas dependencias con los organismos beneficiarios (definición de eventos y reglas), que de no cumplirse pueden llegar a resultados genéricos que dificulten su adopción; por último, se plantea la necesidad de rediseñar el marco de referencia a partir del cual se han llevado a cabo las prácticas de auditoría, teniendo en cuenta el particular nivel de desarrollo en materia de ciberseguridad existente en Uruguay y la región. Esto último, permitiría adoptar un enfoque y diseñar acciones mucho más ajustadas a las necesidades básicas que debe cumplir el sistema,

antes que destinar recursos (al menos de relevamiento) a la obtención de aspectos parciales que no responden a las capacidades básicas de la materia.

Principales desarrollos e implementaciones.

Curricula Técnica. Tal como fue mencionado en el cuerpo del informe, el desarrollo de una currícula técnica para la especialización en materia de ciberseguridad, se encuentra satisfaciendo una demanda insatisfecha en el sector en el Uruguay. Dicho programa de formación se encuentra diseñado para jóvenes recientemente egresados de la educación secundaria que quieran formarse técnicamente en la materia y allí encontrar una salida laboral, como también profesionales de otras disciplinas que busquen reconvertirse profesionalmente. En este sentido, dicha currícula permite una rápida incorporación de personas capacitadas en la materia al sector, sin tener que atravesar previamente por una carrera universitaria relacionada, y de esta forma comenzar a satisfacer rápidamente la alta demanda existente.

Programa de Becas de Posgrado. De manera complementaria al desarrollo anterior, se considera relevante el programa de becas de posgrado llevado adelante. Dicho programa busca facilitar la especialización de profesionales provenientes de carreras ligadas a la tecnología de la información, en materia de ciberseguridad. En este sentido, se presenta como una acción complementaria a la anterior, y permite articular en el mediano plazo acciones realizadas por perfiles profesionales con conocimiento y know-how especializado, con acciones y posiciones técnicas a ser satisfechas por la currícula mencionada en el punto previo.

SIEM. El SIEM es una de las implementaciones mayormente valoradas por los organismos entrevistados durante la presente evaluación, dada la fácil integración que presenta (considerando que no se incurre en costos adicionales por su uso) y las ventajas que este brinda. De esta manera, se valora el hecho de contar con un sistema externo de fácil integración, que recibe información sobre eventos y permite analizar lo que los organismos tienen expuesto a internet. Complementariamente, es necesario mencionar que el SIEM adopta especial relevancia porque, junto con el SOC, sienta las bases para que el desarrollo del GSOC sea posible.

GSOC. El GSOC se presenta como una evolución del SOC, especializada y desarrollada sobre los cimientos establecidos tanto por este último como por el SIEM. En este sentido, busca monitorear a los organismos no desde una mirada externa, como lo hacen los otros desarrollos mencionados, sino internamente, desarrollando colectores en los organismos capaces de enviar información al SIEM central. De esta manera, el GSOC permite generar alertas especializadas sobre vulnerabilidades específicamente ligadas al sector público, en base a la información que los organismos participantes deseen compartir. Es importante destacar que el GSOC puede sentar antecedentes para contar con un SOC especializado para diferentes industrias, como actualmente se está realizando con los organismos de gobierno.

SOAR. La implementación de una solución de gestión de incidentes de seguridad de la información y Security Orchestration, Automation and Response (SOAR) fue licitada en el año 2021 (ver Anexo III), complementando la implementación del SIEM En el marco de dicha licitación, se solicita el licenciamiento de la solución y su entorno de pruebas, además de la implementación de la solución y servicios adicionales de consultoría y capacitación. Esta herramienta permitirá lograr por un lado medir correctamente los indicadores de resultado y por otra parte lograr automatizar respuesta a problemas conocidos y de esa forma mejorar la eficacia y eficiencia de los recursos humanos asignados al CERTuy.

Herramienta de Cyber Range. La herramienta de Cyber Range consta de una herramienta de entrenamiento en materia de ciberseguridad, en base a la simulación de escenarios y problemáticas a resolver por el usuario especializado. Si bien aún en proceso de instalación al momento de la elaboración del presente informe, este producto resulta relevante porque contribuye a satisfacer la demanda de profesionales especializados en ciberseguridad, mediante el desarrollo de conocimientos prácticos. Por otro lado, es importante destacar el carácter innovador del uso de

dicha herramienta, dado que no se registran usos de otras herramientas cyber range en la región. Su uso conlleva diferentes desafíos, que fundamentalmente están relacionados a la cantidad de tecnologías que el profesional usuario del sistema realmente debe conocer para poder hacer uso del mismo. En este sentido, el uso del sistema requiere de formación previa, lo cual puede llegar a retrasar su adopción, pero esta potencial limitación también se encuentra abordada actualmente por algunas acciones emprendidas por AGESIC, como el Programa de Formación inicial para estudiantes y docentes en Cyber Range en desarrollo junto con UTEC (ver Anexo).

III.2. Desempeño del Prestatario/Agencia Ejecutora

El modelo planteado por la AGESIC para la ejecución del Programa, ha demostrado ser exitoso durante la primera mitad de la implementación, tanto hacia adentro como hacia afuera de la organización.

Complementariamente a la ejecución de los fondos del Programa y la consecución de las metas establecidas en materia de productos, se destaca la participación y acompañamiento de la Agencia durante la ejecución de las actividades, además de su constante apoyo en materia de capacitación y desarrollo de colaboradores integrantes de la administración pública. Por otro lado, se destaca la capacidad técnica instalada por parte de la Agencia en las organizaciones involucradas, tanto desde el punto de vista de la Tecnología de la Información como desde el punto de gestión del cambio, que ha posibilitado instalar una temática en la gestión de dichos organismos de importante necesidad pero de bajo nivel de conocimiento.

Desde el punto de vista de los desafíos, es posible seguir trabajando sobre la articulación de los diferentes actores intervinientes, particularmente en la relación entre los organismos del Estado y los actores privados, en pos que los primeros logren organizar sus recursos de la manera más eficiente posible para que los segundos puedan implementar sus procesos y planes de trabajo de una manera eficiente y eficaz. En relación a los segundos, se destaca el hecho de permitirse flexibilizar los planes de trabajo y entregables a medida que los relevamientos avanzan, en pos de adaptarse a las necesidades de cada organismo y su contexto.

III.3. Desempeño del Banco

El organismo ejecutor, junto con el Jefe de Proyecto y el equipo del Banco, se encuentra logrando un efectivo trabajo en conjunto, logrando ejecutar con éxito las acciones del Programa hasta la fecha.

La continua comunicación y el permanente intercambio de información ha permitido, en tiempo y forma, evidenciar la necesidad de los cambios que se realizaron en algunos de los indicadores de producto y resultados, en caso de ser necesario. Esto se evidencia en la replanificación de metas para indicadores de producto o en la incorporación del Indicador de Producto 2.3 a la planificación.

Complementariamente, se han establecido diferentes colaboraciones entre el ejecutor y el banco, permitiendo ampliar el conjunto de acciones iniciadas. En este sentido, cabe destacar la colaboración establecida para poder ampliar el alcance a PYMEs y MIPYMEs, así como la coordinación en temas relacionados a capacitaciones, buscando sinergias con otros Programas del Banco.

IV. Sostenibilidad

IV.1. Análisis de Factores Críticos[21]

Continuidad Programática en Educación

Uno de los objetivos más ambiciosos del Programa se encuentra relacionado a la capacitación de recursos humanos en el Uruguay, ligados a la actividad profesional en ciberseguridad. Tal como puedo observarse en los capítulos anteriores, dicho objetivo se viene desarrollando de forma correcta y con buenos resultados, con respecto a lograr incrementar las capacitaciones en ciberseguridad y la cantidad de técnicos que se están formando actualmente. Asimismo, este objetivo se encuentra asociado a una de las metas establecidas por el Programa, tal como se evidencia con los indicadores de resultado correspondientes al *capital humano formado en ciberseguridad*, en particular al tema de los docentes[22]. Esto se debe a la escasez de técnicos en la materia y de docentes en las instituciones siendo poco atractivo desde el punto de vista salarial en el mercado.

Tal como se ha mencionado, esto se ha llevado a cabo mediante la implementación de programas de capacitación técnicos, permitiendo ensanchar la base de los técnicos en ciberseguridad del país, escasez fundamental hoy en día, así como también con una tecnicatura que de forma rápida logra colocar en condiciones laborales a técnicos en la materia. A su vez, gracias al Programa se han visto reforzados los programas de posgrado en una de las Universidades del Uruguay que ya contaba con un programa de posgrado tenia (FING), en base a otorgar becas para estudios, a la vez que se ha logrado el lanzamiento de un posgrado en otra universidad que no lo había implementado (ORT).

Las acciones anteriormente mencionadas han permitido, por una parte, un cambio en la tendencia en descenso de estudiantes de posgrado de ciberseguridad en el país, y aumentarlos de manera considerable en consecuencia. Adicionalmente, se logró incorporar una nueva especialización de posgrado en la UTEC en conjunto con una universidad española (Oberta de Catalunya). En este sentido, la evidencia muestra que a la fecha, el programa de Analista de Ciberseguridad (de nivel terciario no universitario) vigente en la Universidad del Trabajo de Uruguay (UTU) se encuentra operativo (con más de 70 alumnos cursando), así como los programas de posgrado, cuyas matrículas también han mejorado (+50 en los últimos 2 años y +30 a partir de agosto de este año, totalizando +80 alumno de posgrado)[23].

---

[21] Cabe mencionar que, al tratarse de una evaluación intermedia, parte o la totalidad de los factores críticos aquí analizados pueden tanto ser mitigados durante la ejecución de la segunda mitad del Programa, así como por las acciones de respuesta propuestas en función de los riesgos potenciales detectados en cada revisión semestral de la operación.

[22] Ver particularmente el indicador de resultados 2.1 “Número de personas que han tomado al menos 40 horas de capacitación en ciberseguridad anual”, con una tasa de logro de 14,6; y el indicador de resultados 2.2 “Mujeres que han tomado al menos 40 horas de capacitación en ciberseguridad anual” con una tasa de logro equivalente a 3,1.

[23] Con el fin de corroborar dicho impacto del Programa, el equipo de evaluación ha entrevistado a representantes de las Universidades con las cuales la Agencia a trabajado.
En este sentido, según la perspectiva de los entrevistados, de no haber existido el apoyo por parte del Programa, no hubiera existido el lanzamiento de los Diplomas. En base a su experiencia, al querer una institución educativa (pública o privada) lanzar un programa innovador como este, en materia de ciberseguridad, los costos de lanzarlos son altos y pocos actores en el mercado quieren hacerlo, asumiendo el riesgo que implica.
De la cuantificación de resultados, se estima que 50% más de los inscriptos pudieron hacerlo gracias al apoyo. Esto ha permitido que exista tanto la primera como segunda generación del Diploma, y el apoyo es tan relevante que actualmente se está buscando acompañamiento en el lanzamiento de la tercera generación. Asimismo, los entrevistados cuentan con información sobre la cantidad de interesados por el Diploma, datos sobre los cuales se encuentra demostrado que el interés en la formación incrementa al incorporar el beneficio de las becas posibilitadas por parte del Programa.

En este sentido, cabe mencionar que estos programas operan con total independencia de la Agencia luego de su creación e impulso, y no requerirán inversión adicional para mantener su capacidad operativa, pero se entiende que para terminar de lograr su consolidación y continuidad es probable que continúen requiriendo algún tipo de apoyo de menor cuantía, tanto para docentes nuevos como para programas de becas, ya no tan ambiciosos.

Empleabilidad en el Sector Público para perfiles especializados

Durante las entrevistas, fue mencionado el hecho de la migración del sector público al sector privado, en perfiles especializados en materia de ciberseguridad, producto de las brechas salariales existentes entre dichos sectores. Este es un fenómeno que pone en riesgo el retorno para el sector público en función de la inversión en formación para sus recursos, particularmente los mayormente especializados.

En este sentido, con el fin de evitar dicha migración mediante la reducción de las brechas mencionadas, se encuentra evidencia de acciones que permitirían mitigarlas. A modo de ejemplo, cabe mencionar la última Rendición de Cuentas por parte del Ministerio de Economía y Finanzas del Uruguay[24], donde se contempla un potencial régimen especial de contratación para dichos perfiles por parte del Estado. Complementariamente, dada la significativa cantidad de inscriptos que existen hoy en los programas de formación tanto técnicos como de posgrados, se debería estimar un incremento de la oferta profesional en materia de ciberseguridad, que en el largo plazo tienda a disminuir la remuneración promedio de dichos perfiles y así contribuya a la velocidad en la reducción de dicha brecha. Este fenómeno se va a seguir manteniendo en el corto y mediano plazo.

Continuidad Institucional

Entre los desafíos relevados durante el proceso de entrevistas, se encuentra el caracterizado por la capacidad de la Agencia para erigirse como entidad autónoma y certificadora en materia de ciberseguridad, así como su capacidad de sostener las acciones emprendidas en materia de desarrollo en ciberseguridad en el Uruguay.

En este sentido, cabe destacar las actuales negociaciones vigentes en torno a una nueva operación de financiamiento que permita continuar con las actividades aquí vigentes, tanto con el Banco Interamericano de Desarrollo como con el Ministerio de Economía y Finanzas del Uruguay. De manera complementaria, cabe mencionar que podrían buscarse mecanismos de financiamiento externo que no dependan de un organismo multilateral dependiendo del objeto del gasto, que pueda por ejemplo sostener determinadas acciones puntuales de capacitación o proyectos específicos. En este sentido, la Agencia dispone hoy del marco legal para cobrar por servicios al Sector Público, originario en la Rendición de Cuentas y Balance de Ejecución Presupuestal para el Ejercicio 2020[25], aunque aún no dispone de un espacio para generar ingresos que permitan sostener acciones desarrolladas en articulación con el Sector Privado. En este caso,

---

Si bien no se cuenta con una trazabilidad tal que permita dimensionar el impacto del apoyo dado por el Programa a partir de un análisis en base a un contrafactual, se considera un factor clave para el desarrollo del mismo. Desde el punto de vista de los entrevistados, sin el financiamiento mencionado, el Diploma no se hubiera lanzado, por lo que el apoyo por parte del Gobierno se ha transformado en un hito fundamental para la ejecución de dicho programa educativo. De hecho, este es el principal motivo por el cual no hay un análisis contrafactual que permita atribuir directamente resultados al Programa.
Complementariamente, los entrevistados han afirmado que el principal aporte del Diploma (y por ende del apoyo del Programa) es al desarrollo en materia de ciberseguridad, independientemente del ámbito de inserción laboral donde se inserte el profesional capacitado. Es un aporte al desarrollo social en general, en base a su contribución al desarrollo de la gestión de seguridad de la información, disciplina central en la estructura de las organizaciones tanto privadas como públicas.

[24] Fuente: Rendición de Cuentas 2023, Ministerio de Economía y Finanzas, Art. 69 a 75.

[25] Fuente: Rendición de Cuentas y Balance de Ejecución Presupuestal para el Ejercicio 2020, art. 49. Link.

el incentivo de las asociaciones público-privadas, tan exitosas en la región, podrían beneficiar a la Agencia en pos de la obtención de dichos recursos.

IV.2. Riesgos potenciales

En el último informe semestral del Programa, se mencionan los riesgos evaluados durante su ejecución, los cuales han sido clasificados mayoritariamente como medio a alto.

Entre los principales riesgos que se toman en consideración, se destacan (ordenados de mayor riesgo a menor riesgo):

- Baja retención y baja capacidad de contar con mayor cantidad de personal especializado por parte de la Agencia, dada la escasez en el mercado de dichos recursos y la baja competitividad de las ofertas salariales propuestas por el sector público. Es importante tener en cuenta que las amenazas continúan incrementándose y así como también las nuevas potestades otorgadas a AGESIC en temas de ciberseguridad hace imprescindible contar con mayor cantidad de personal especializado, en un área donde la rotación es la más alta.
- Cambios en la visión nacional en materia de ciberseguridad, que derive en tiempos no acordes, tanto en la elaboración y aprobación de normativa acorde en dicha materia.
- No lograr una adecuada gestión del cambio en el marco del trabajo con los organismos asociados, que impacte en la implementación de los proyectos actuales.
- Restricción presupuestaria y en materia de recursos humanos para lograr una adecuada gestión en el proceso de Desarrollo de Capacidades, lo cual impacta en el desarrollo de cursos y talleres necesario para la formación de recursos humanos especializados.
- Baja participación de mujeres en temáticas de ciberseguridad.
- Incumplimiento en la planificación y ejecución del Plan de Difusión Nacional e Internacional.

Tal como puede observarse, los riesgos mencionados encuentran relación con las iniciativas mencionadas en el presente documento, así como con los factores críticos relacionados con la Sostenibilidad de las acciones emprendidas, ya mencionadas en la sesión previa. Complementariamente, cada uno de los factores de riesgo mencionados, ya encuentra una acción de respuesta identificada y en implementación[26].

IV.3. Capacidad Institucional

La capacidad institucional observada durante el proceso de implementación del Programa ha sido un factor clave y ha contribuido en forma exitosa para alcanzar los resultados obtenidos por parte de la presente operación, a la fecha del presente análisis.

Desde el punto de vista del Gobierno, se destaca no solo el apoyo y financiamiento a la Agencia, sino también el lineamiento estratégico definido para que estas actividades encuentren un marco sobre las cuales ser realizadas, donde un ejemplo a destacar es la Rendición de Cuentas para el ejercicio 2023, realizada por el Ministerio de Economía y Finanzas del Uruguay, que explicita dicho lineamiento.

A modo de ejemplo, es posible mencionar el Artículo 69 de dicho documento, donde se menciona explícitamente que “Las entidades públicas y las entidades privadas vinculadas a servicios o

[26] Fuente: Informe de Avance – Primer Semestre de 2022

sectores críticos del país (…) deberán adoptar medidas de seguridad eficaces para proteger sus activos de información críticos de conformidad con los lineamientos indicados por la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC)" así como "incorporar, en función de su nivel de madurez, el Marco de Ciberseguridad desarrollado por AGESIC". De manera complementaria, en el Artículo 70 de dicho documento se faculta a la AGESIC para "a) requerir el ajuste de los procedimientos a la normativa vigente en materia de ciberseguridad en los plazos que se definan por AGESIC; b) requerir el cumplimiento de medidas específicas para la prevención de riesgos vinculados al sector de la entidad; c) requerir informaciones complementarias vinculadas a la ocurrencia de incidentes de seguridad, las medidas adoptadas y a la aplicación de la normativa en materia de ciberseguridad en general; d) apercibir, considerando la gravedad o reiteración del incumplimiento por parte de la entidad".

Por último, en términos de continuidad presupuestaria, y si bien el Programa se encuentra en un punto intermedio en su ejecución, cabe mencionar que actualmente existen negociaciones iniciales en torno a una continuidad de las operaciones con el Banco Interamericano de Desarrollo y el Ministerio de Economía y Finanzas del Uruguay, lo cual posibilitaría la obtención de recursos por parte de la Agencia para la continuación de las actividades aquí mencionadas.

V. Conclusiones Finales y Lecciones aprendidas

Tal como puede verse a lo largo del documento, dada la etapa intermedia del Programa, el mismo ha logrado la consecución de prácticamente la totalidad de los indicadores de producto y resultados planteados al momento del diseño. En gran parte, esto es debido a la alineación estratégica del Programa con la estrategia país del Banco Interamericano de Desarrollo, así como la alineación con la Agenda Digital a nivel nacional para la República del Uruguay.

Particularmente, se evidencia para cada uno de los Componentes del Programa que:

- Los productos identificados en el Componente 1 del programa muestran un cumplimiento del 100% en la comparación de las metas Planificadas (ajustadas) y la meta alcanzada.
- Los productos identificados en el Componente 2 muestran un cumplimiento del 100% en la comparación de las metas Planificadas (ajustadas) y la meta alcanzada.
- Los productos identificados en el Componente 3 del programa muestran un cumplimiento del 100% en la comparación de las metas Planificadas (ajustadas) y la meta alcanzada, con la única excepción del producto 3.3 ("Plan de difusión nacional e internacional implementado"), aunque cabe mencionar que el Programa se encuentra realizando actualmente actividades de difusión ligados al mismo.

Asimismo, se evidencia un logro parcial para el Resultado 1 del Programa en relación a la meta correspondiente al año 2022 (solo se ve un cumplimiento del 100% en el indicador de resultado número 1, pero no así en los restantes), y un logro total de las metas de resultados para el Resultado 2 del Programa. En este sentido, cabe resaltar nuevamente las dificultades de medición que algunos de los indicadores del Resultado 1 encuentran asociadas, y las acciones de mitigación y evaluación de alternativas que la AGESIC ya se encuentra haciendo, de caras a su redefinición.

Complementariamente, en materia de eficiencia, se evidencia un cumplimiento del 100% en cuanto a la planificación vigente en materia de ejecución presupuestaria hacia la fecha (en base a la replanificación acordada con el Banco Interamericano de Desarrollo), sin presentar ningún tipo de desvío.

Por último, si bien se evidencian factores críticos y potenciales riesgos que podrían afectar a la consecución de los objetivos planteados y la sostenibilidad de los resultados ya obtenidos, es de destacar que el Programa ya tenga acciones de respuesta para cada uno de los riesgos identificados (sin discriminar por nivel de severidad), así como la posibilidad de identificar factores

que ya contribuyan a la Sostenibilidad de la operación y sus logros, tal como la continuidad programática en materia educativa.

En este sentido, el Programa logra demostrar antecedentes consistentes y resultados positivos en materia de efectividad y eficiencia, en relación a su calidad de diseño y consecuente desempeño. Complementariamente, se identifican algunas **lecciones aprendidas** de cara a la ejecución de la segunda mitad del Programa y futuras acciones a desarrollar, a saber:

- Es posible mejorar las estrategias de retención y captación de recursos humanos para atenuar el impacto de la rotación del personal en la operativa. Este factor continúa impactando en los proyectos, haciendo difícil su continuidad y seguir un correcto proceso. Asimismo, factores del mercado laboral que se han modificado en el marco de la pandemia hacen de este un problema complejo de abordar.
- Los tiempos para la ejecución de convenios e interacción con terceras partes resultan ser más largos de lo esperado. Esto podría ser contemplado en las etapas más tempranas de la ejecución.
- Los socios más relevantes poseen dificultades considerables con respecto a la capacidad operativa.
- Un desafío a considerar es el fortalecimiento de la relación con Organismos para el abordaje tanto de GSOC como de otros proyectos/servicios de CERTuy y de Seguridad en general. Este es un trabajo que , debido a la pandemia, no fue abordado de la forma en que debería haber sido.
- Es recomendable liderar y empoderar a técnicos de CERTuy para poder desarrollar adopción y cursos de Cyber Range. Sin embargo, debe considerarse dicho abordaje no sólo con técnicos del CERTuy sino con mayores recursos, ya que en el contexto de un área con una operativa compleja y demandante es difícil que pueda asumirse un proyecto educativo que difiere y tiene otros tiempos diferentes a los de su operativa técnica. También debe de considerar la forma de lograr acortar la brecha de conocimientos que poseen los estudiantes que pueden acceder a estas prácticas, para lograr que tengan una experiencia correcta en este tipo de herramienta, aspecto que debe de ser considerado casi en conjunto con su adquisición.
- Se recomienda trabajar sobre la comunicación del Programa y sus acciones, para que espontáneamente se identifique su área de incumbencia y se comprendan fácilmente las responsabilidades. Si bien documentos marco como los Acuerdos de Adhesión buscan cumplir este objetivo, estas acciones encuentran oportunidades durante el proceso dadas por cierta falta de información a la hora de compartirla o poca disponibilidad de recursos propios para las tareas a efectuar.
- Por último, dado el dinamismo de la actividad y el sector de la Tecnología de la Información en general y de la Ciberseguridad en particular, se recomienda tomar plazos de ejecución menores (por ejemplo, de 3 años mediante CCLIPs) con el fin de poder evaluar impactos más periódicamente y rediseñar objetivos con mayor dinamismo, de acuerdo a la evolución del sector y los recursos vigentes.

VI. Bibliografía consultada

- Contrato de Adhesión para Implantación del GSOC (modelo). AGESIC.
- Contrato de Préstamo No.4843/OC-UR. Fortalecimiento de la Ciberseguridad en Uruguay.
- Informe de Avance al 30 de Junio de 2020. Programa UR-L1152, Uruguay.
- Informe de Avance al 31 de Diciembre de 2020. Programa UR-L1152, Uruguay.
- Informe de Avance al 30 de Junio de 2021. Programa UR-L1152, Uruguay.
- Informe de Avance al 31 de Diciembre de 2021. Programa UR-L1152, Uruguay.
- Informe de Avance al 30 de Junio de 2022. Programa UR-L1152, Uruguay.
- Informe de Avance al 31 de Diciembre de 2022. Programa UR-L1152, Uruguay.
- Perfil de Proyecto. Fortalecimiento de la Ciberseguridad en Uruguay. (UR-L1152).
- Principales licitaciones Préstamo No.4843/OC-UR. 2020.
- Principales licitaciones Préstamo No.4843/OC-UR. 2021.
- Principales licitaciones Préstamo No.4843/OC-UR. 2022.
- Propuesta de Préstamo. Fortalecimiento de la Ciberseguridad en Uruguay. (UR-L1152).

Actores clave entrevistados y referentes de la Agencia Ejecutora

Nombre	Organismo / Consultora	Fecha Entrevista
Referentes de la AGENCIA y Programa		
Lorena Lacero	Coordinadora División Gestión Estratégica – AGESIC	Durante Evaluación
Cecilia Rossi	AGESIC	Durante Evaluación
Nicolas Correa	Gerente de SOC AGESIC	3 de abril de 2023
Mauricio Papaleo	Gerente de Seguridad Informática AGESIC	5 de mayo de 2023
Actores Entrevistados		
Alvaro Arias	Responsible de Ciberseguridad BPS	29 de marzo de 2023
Guillermo Freire	Responsable de Seguridad de la Información CGN Ministerio de Economía	29 de marzo de 2023
Carlos Berruti	Director de IT MINTUR	3 de abril de 2023
Reynaldo de la Fuente	Director DataSec	3 de abril de 2023
Gustavo Betarte	Profesor Grado 5 FING- UdelaR – Director del grupo de Seguridad Informática.	4 de abril de 2023
Luis Garcimartin	Gerente de Seguridad Informática Intendencia de Montevideo	5 de mayo de 2023
Roberto Ambrosini	Gestión de Seguridad de la Información (UNIT)	11 de septiembre de 2023
Andres Galiana	Facultad de Ingeniería - Universidad ORT Uruguay	11 de septiembre de 2023

Anexos

Anexo I. Informes semestrales de avance.

Anexo II. Modelo de Acuerdo de Adhesión para organismos.

Anexo III. Principales licitaciones realizadas.

Anexo IV. Programa Entry Level Cyber Range: plan de formación inicial para estudiantes y docentes.