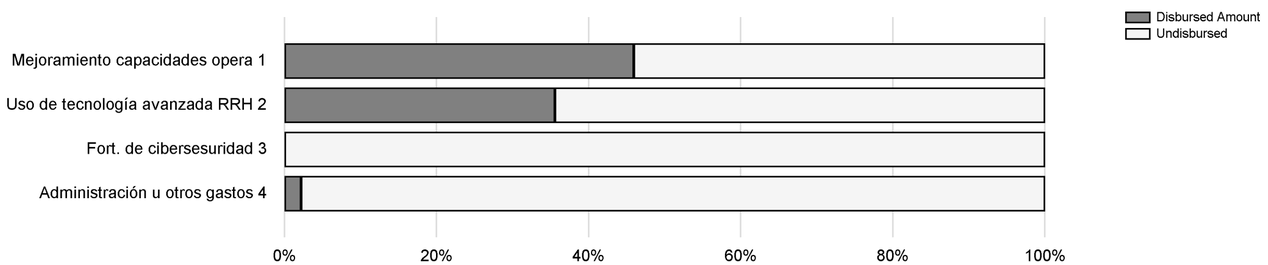
PMR Public Report

Operation Number	UR-L1152	**Chief of Operations Validation Date**	03/29/23
Year- PMR Cycle	Second period Jan-Dec 2022	**Division Chief Validation Date**	05/05/23
Last Update	03/25/23	**Country Representative Validation Date**	05/08/23
PMR Validation Stage	Validated by Representative		
Basic Data			
Operation Profile			
Operation Name	Strengthening Cybersecurity in Uruguay	**Loan Number**	4843/OC-UR
Executing Agency	AGENCIA DE GOBIERNO ELECTRONICO Y SOCIEDAD DE LA INFORMACION Y DEL CONOCIMIENTO	**Sector/Subsector**	REFORM / MODERNIZATION OF THE STATE-E-GOVERNMENT
Team Leader	PAREJA GLASS, ALEJANDRO	**Overall Stage**	Disbursing (From eligibility until all the Operations are closed)
Operation Type	Loan Operation	**Country**	Uruguay
Lending Instrument	Investment Loan	**Convergence related Operation(s)**	
Borrower	REPUBLICA ORIENTAL DE URUGUAY		
Environmental and Social Safeguards			
Impacts Category	C	**Was/Were the objective(s) of this operation reformulated?**	NO
Safeguard Performance Rating		**Date of approval**	
Safeguard Performance Rating - Rationale			

Financial Data

	Total Cost and Source					Available Funds (US$)			
Operations	**Original IDB**	**Current IDB**	**Local Counterpart**	**Co-Financing / Country**	**Total Original Cost**	**Current IDB**	**Disb. Amount to Date**	**% Disbursed**	**Undisbursed Amount**
UR-L1152	8,000,000	8,000,000	2,000,000	0	10,000,000	8,000,000	4,050,000	50.63%	3,950,000
Aggregated	**8,000,000**	**8,000,000**	**2,000,000**	**0**	**10,000,000**	**8,000,000**	**4,050,000**	**50.63%**	**3,950,000**

Expense Categories by Loan Contract (cumulative values)



Please note that inactive indicators and outputs are not displayed; totals in the actual cost table may not match the sum of the cost of the outputs displayed, due to the cost of inactive outputs.

RESULTS MATRIX

General Development Objectives

General Development Objectives Nbr. 1: Madurez de Capacidad de Seguridad Cibernética aumentada

Observation:

	Indicator	Unit of Measure	Baseline	Baseline Year	Expected Year of Achievement		EOP 2025
1.0	Madurez de capacidad de seguridad cibernética nacional.	Puntaje	149	2016	2024	P	165
						A	-

Details

Means of Verification: Informe OEA BID

Observations: Este es un indicador que refleja las capacidades a nivel nacional, el máximo puntaje posible es 245 puntos. El documento “Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States” estudia EEUU, Estonia, Korea del Sur e Israel con base en el modelo de madurez elegido para medir el impacto de esta operación. El documento muestra que las inversiones realizadas por estos países en fortalecimiento de su capacidad tecnológica y en la formación de recursos humanos ha contribuido a posicionarlos como países avanzados en la protección de sus ciberespacios. De hecho en este modelo de madurez, de 49 indicadores, 5 tienen que ver con educación y 9 con fortalecimiento de capacidades tecnológicas incluidas en este programa. Los esfuerzos de educación de cada país pueden verse en las siguientes páginas: Estonia pg 15-16, Israel pg 27-28, Korea pg 38-39, EEUU pg 48-49.

The General Development Objective indicator target is expected to be observed by the operation's "Fully Justified" date in Convergence (CO): No

Pro-Gender	No	**Pro-Ethnicity**	No	CRF indicator	

	Indicator	Unit of Measure	Baseline	Baseline Year	Expected Year of Achievement		EOP 2025
1.2	Nivel de madurez promedio en ciberseguridad de las organizaciones públicas.	Puntaje	1.5	2018	2024	P	2.5
						A	-

Details

Means of Verification: Auditoría externa de marco de ciberseguridad.

Observations: Este es un indicador que refleja las capacidades de diez entidades públicas más digitalizadas de Uruguay, el puntaje máximo posible es 4.

The General Development Objective indicator target is expected to be observed by the operation's "Fully Justified" date in Convergence (CO): No

Pro-Gender	No	**Pro-Ethnicity**	No	CRF indicator	

RESULTS MATRIX

Specific Development Objectives

Specific Development Objectives Nbr. 1: Capacidades operativas de monitoreo, detección y respuesta de incidentes de ciberseguridad mejorada

Observation:

	Indicator	Unit of Measure	Baseline	Baseline Year		2020	2021	2022	2023	2024	EOP 2025
1.0	Número de organizaciones públicas monitoreadas a través del SOC	Número de ministerios	2	2018	P	2	5	11	15	17	17
					A	2	6	11	-	-	-

Details

Means of Verification: Reporte anual de la dirección de ciberseguridad informática.

Observations: Este indicador no refleja el flujo anual sino la cantidad de instituciones acumuladas.

Evaluation Methodology: -

Pro-Gender	No	**Pro-Ethnicity**	No	CRF indicator	

	Indicator	Unit of Measure	Baseline	Baseline Year		2020	2021	2022	2023	2024	EOP 2025
1.2	Número de incidentes cibernéticos detectados anual.	Número de incidentes	2043	2018	P	2,500	4,000	6,000	8,500	10,000	10,000
					A	2,761	3,948	4,169	-	-	-

Details

Means of Verification: Reporte anual de la dirección de ciberseguridad informática.

Observations: Se entiende como incidente “una violación o una amenaza inminente de violación a una política de seguridad de la información implícita o explícita, así como un hecho que compromete la seguridad de un sistema (confidencialidad, integridad o disponibilidad). (Decreto N° 451/009 de 28 de Setiembre 2009- Art.3). El reporte “Informe de Incidentes. Activity Report” del Centro Criptológico Nacional del Gobierno de España, muestra que a medida que el gobierno invirtió en su capacidad de monitoreo, se incrementó la cantidad de incidentes detectados en todos los niveles de peligrosidad, ver página 41.

Evaluation Methodology: -

Pro-Gender	No	**Pro-Ethnicity**	No	CRF indicator	

	Indicator	Unit of Measure	Baseline	Baseline Year		2020	2021	2022	2023	2024	EOP 2025
1.3	Porcentaje de incidentes cibernéticos de alto impacto	Porcentaje	2.1	2018	P	2	1.84	1.51	1.24	1	1
					A	2.1	1.27	3	-	-	-

Details

Means of Verification: Reporte anual de la dirección de ciberseguridad informática.

Observations: De acuerdo al documento de procedimiento de clasificación de incidentes de AGESIC, son de alto impacto los que precisan más de 640 horas de experto senior para su solución.

Evaluation Methodology: -

Pro-Gender	No	**Pro-Ethnicity**	No	CRF indicator	

Specific Development Objectives Nbr. 2: Capital humano capacitado en ciberseguridad aumentado

Observation:

	Indicator	Unit of Measure	Baseline	Baseline Year		2020	2021	2022	2023	2024	EOP 2025
2.0	Número de personas que han tomado al menos 40 horas de capacitación en ciberseguridad anual.	Número de personas	50	2018	P	-	-	150	300	350	350
					A	-	674	1,510	-	-	-

Details

Means of Verification: Registros de estudiantes de las entidades de educación terciaria.

Observations: Este es indicador que mide el flujo de personas capacitadas en ciberseguridad de manera anual.

Evaluation Methodology: -

Pro-Gender	No	**Pro-Ethnicity**	No	CRF indicator	

	Indicator	**Unit of Measure**	**Baseline**	**Baseline Year**		**2020**	**2021**	**2022**	**2023**	**2024**	**EOP 2025**
2.2	Mujeres que han tomado al menos 40 horas de capacitación en ciberseguridad anual.	Porcentaje	0	2018	P	-	-	15	20	25	25
					A	-	15	47	-	-	-

Details

Means of Verification: Registros de estudiantes de las entidades de educación terciaria.

Observations: Este es el indicador que mide el flujo de personas capacitadas en ciberseguridad de manera anual.

Evaluation Methodology: -

Pro-Gender	Yes	**Pro-Ethnicity**	No	CRF indicator	

RESULTS MATRIX

OUTPUTS: ANNUAL PHYSICAL AND FINANCIAL PROGRESS

Component Nbr. 1 Mejoramiento de las capacidades operativas y herramientas del CERT.uy

				PHYSICAL PROGRESS		FINANCIAL PROGRESS	
	Output	Unit of Measure		2022	EOP 2025	2022	EOP 2025
1.01	1.1 Licencia de Qradar actualizadas	Licencia	P	-	1	-	1,068
			P (a)	-	1	-	1,046
			A	-	1	-	802
1.02	1.2 Sistema NIGPS de detección de intrusiones en funcionamiento	Sistema	P	1	1	61	387
			P (a)	1	1	37	527.1
			A	-	-	62.1	259.1
1.03	1.3 Plataforma de big data en funcionamiento	Plataforma	P	-	1	90	605
			P (a)	-	1	78	847
			A	-	-	172	277
1.04	1.4. Laboratorio del CERT Instalado	Laboratorio	P	1	1	114	678
			P (a)	1	1	472	1,443.49
			A	1	1	331	620
1.05	1.5 Sistema SIEM implementado	Sistema	P	-	1	465	1,842
			P (a)	-	1	711	2,062
			A	-	1	691	1,300
1.06	1.6 CERT equipado y en funcionamiento	Sistema	P	-	1	481	2,615
			P (a)	1	5	235	2,835
			A	1	3	421	1,133

Component Nbr. 2 Potenciación del uso de tecnología avanzada para la formación de recursos humanos

				PHYSICAL PROGRESS		FINANCIAL PROGRESS	
	Output	Unit of Measure		2022	EOP 2025	2022	EOP 2025
2.01	2.1 Plataforma de simulación de ataques cibernéticos en funcionamiento Plataforma	Plataforma	P	1	1	300	1,383
			P (a)	-	1	110	762.72
			A	-	1	116.72	609.72
2.02	2.2 Plataforma de e-learning instalada	Plataforma	P	-	1	-	90
			P (a)	-	1	-	63
			A	-	-	-	-

Component Nbr. 3 Fortalecimiento del ecosistema de conocimiento de ciberseguridad a nivel nacional

				PHYSICAL PROGRESS		FINANCIAL PROGRESS	
	Output	**Unit of Measure**		**2022**	**EOP 2025**	**2022**	**EOP 2025**
3.01	3.1.a Curricula de formación en ciberseguridad diseñada	curricula	P	1	1	1	10
			P (a)	1	1	127	261
			A	1	1	110	110
3.02	3.1.b Profesores formados en la nueva curricula de formación en ciberseguridad	Profesores	P	60	220	134	634
			P (a)	-	70	24	391
			A	-	-	-	-
3.03	3.2 Red de expertos en funcionamiento	Red de expertos	P	-	1	49	183
			P (a)	-	1	-	200
			A	-	1	-	127
3.04	3.3 Plan de difusión nacional e internacional implementado	Plan	P	-	1	-	-
			P (a)	1	1	-	-
			A	-	-	-	-
3.05	3.4 Estrategia de gestión del cambio diseñada	Documento	P	-	1	12	74
			P (a)	1	3	12	51
			A	1	3	-	-

Other Cost				
	Administración, evaluación e imprevistos	P	55	431
		P (a)	0	56
		A	0	13

Total Cost				
	Total Cost	P	1,762	10,000
		P (a)	1,806	10,545.31
		A	1,903.82	5,250.82

CHANGES TO THE MATRIX

Section	Name	Type of Change	Sub type	Modified By	Entered in System
Output	1.2 Sistema NIGPS de detección de intrusiones en funcionamiento	Modify Output	Modify Financial EOP P(a) value - caused by a change in the Financial P(a).	MARIADUT	3/24/2023
			Modify Physical EOP P(a) value - caused by a change in the Physical P(a).	MARIADUT	3/24/2023
	1.3 Plataforma de big data en funcionamiento	Modify Output	Modify Financial EOP P(a) value - caused by a change in the Financial P(a).	MARIADUT	3/24/2023
	1.4. Laboratorio del CERT Instalado	Modify Output	Modify Financial EOP P(a) value - caused by a change in the Financial P(a).	MARIADUT	3/24/2023
	1.5 Sistema SIEM implementado	Modify Output	Modify Financial EOP P(a) value - caused by a change in the Financial P(a).	MARIADUT	3/24/2023
	1.6 CERT equipado y en funcionamiento	Modify Output	Modify Financial EOP P(a) value - caused by a change in the Financial P(a).	MARIADUT	3/24/2023
	2.1 Plataforma de simulación de ataques cibernéticos en funcionamiento Plataforma	Modify Output	Modify Financial EOP P(a) value - caused by a change in the Financial P(a).	MARIADUT	3/24/2023
	2.2 Plataforma de e-learning instalada	Modify Output	Modify Financial EOP P(a) value - caused by a change in the Financial P(a).	MARIADUT	3/24/2023
	3.1.a Curricula de formación en ciberseguridad diseñada	Modify Output	Modify Financial EOP P(a) value - caused by a change in the Financial P(a).	MARIADUT	3/24/2023
	3.1.b Profesores formados en la nueva curricula de formación en ciberseguridad	Modify Output	Modify Financial EOP P(a) value - caused by a change in the Financial P(a).	MARIADUT	3/24/2023
			Modify Physical EOP P(a) value - caused by a change in the Physical P(a).	MARIADUT	3/25/2023
	3.2 Red de expertos en funcionamiento	Modify Output	Modify Financial EOP P(a) value - caused by a change in the Financial P(a).	MARIADUT	3/24/2023
	3.4 Estrategia de gestión del cambio diseñada	Modify Output	Modify Financial EOP P(a) value - caused by a change in the Financial P(a).	MARIADUT	3/24/2023

RISKS AND PLANNED RESPONSES

Risk ID	Risk Status	Risk Taxonomy
1	Active	Human Resources

Response Actions	Management Strategy	Status
1.01	MITIGATE	ACTIVE

Risk ID	Risk Status	Risk Taxonomy
2	Materialized	Governance Framework

Response Actions	Management Strategy	Status
2.01	MITIGATE	ACTIVE

Risk ID	Risk Status	Risk Taxonomy
3	Active	Governance Framework

Response Actions	Management Strategy	Status
3.01	MITIGATE	ACTIVE

Risk ID	Risk Status	Risk Taxonomy
4	Active	Institutional Environment

Response Actions	Management Strategy	Status
4.01	MITIGATE	COMPLETE

Risk ID	Risk Status	Risk Taxonomy
5	Active	Economic and Financial Environment

Response Actions	Management Strategy	Status
5.01	MITIGATE	COMPLETE

Risk ID	Risk Status		Risk Taxonomy
6	Inactive		Political Environment
	Response Actions		
	6	Management Strategy	Status

IMPLEMENTATION STATUS AND LEARNING

Lesson Learned - Categories