Documento del Banco Interamericano de Desarrollo

**URUGUAY**

**Programa de Fortalecimiento de la Ciberseguridad**

**(UR-L1152)**

**Plan de Monitoreo y Evaluación**

Este documento fue elaborado por: Harold Villalba (SPD/SDV)

# Introducción

* 1. El objetivo de este documento es describir el plan de monitoreo y evaluación para la implementación del programa de fortalecimiento de la ciberseguridad en Uruguay (UR‑L1152).
  2. El BID y el gobierno de Uruguay están de acuerdo con los arreglos de seguimiento y evaluación detallados en este documento, que incorporan sistemas y metodologías múltiples para poder cumplir con los objetivos del mismo. La responsabilidad del cumplimiento de estos arreglos será del Organismo Ejecutor (OE).

# Monitoreo

* 1. **Seguimiento por parte del OE.** Para realizar el seguimiento del programa el OE utilizará los siguientes documentos: (i) la Matriz de Resultados (MR); (ii) el Plan de Ejecución del Programa (PEP); (iii) el Plan de Adquisiciones del Programa (PA); (iv) este mismo Plan de Monitoreo y Evaluación (PME); (v) el Plan Operativo Anual; (vi) la Matriz de Gestión de Riesgo; y (vii) el Informe de Monitoreo del Progreso (PMR, por sus siglas en ingles). La Unidad de Proyectos de AGESIC preparará informes semestrales de avance para su revisión por el Banco.
  2. **Seguimiento por parte del Banco.** El Banco realizará Misiones de Administración y Visitas de Inspección Técnica, siguiendo el cronograma definido en el PEP. Además, el Banco utilizará el PMR, que recoge la estimación temporal de los desembolsos y del cumplimiento de metas físicas y de costos de los productos programados, así como los resultados alcanzados; y un mecanismo para evaluar el desempeño del programa.
  3. Los contenidos principales y características de cada uno de los instrumentos detallados anteriormente se describen a continuación:

1. **Matriz de Resultados (MR).** que se presenta como parte del documento principal, se focaliza en los: (i) productos; y (ii) resultados de cada componente; y (iii) impactos del Programa. La MR es una herramienta fundamental para guiar la planificación, monitoreo y evaluación del Programa.
2. **Plan de Ejecución del Programa** **(PEP).** El PEP deberá comprender la planificación completa del Proyecto, de conformidad con la estructura de los productos esperados según la Matriz de Resultados del Proyecto, y la ruta crítica de hitos o acciones críticas que deberán ser ejecutadas para que el Préstamo sea desembolsado en el plazo previsto. El PEP deberá ser actualizado cuando fuere necesario, en especial, cuando se produzcan cambios significativos que impliquen o pudiesen implicar demoras en la ejecución del Programa o cambios en las metas de producto de los períodos intermedios.
3. **Plan de Adquisiciones del Programa (PA).** Enumera y programa las contrataciones de consultoría y las compras de bienes y servicios que se van a realizar para generar los productos previstos en la MR y PEP, junto con los procedimientos de adquisiciones y contrataciones a ser utilizados. Deberá ser actualizado por el OE como mínimo cada 12 meses, o antes de dicho plazo si fuera necesario debido a modificaciones sustanciales en la planificación de las adquisiciones. Será presentado junto con el POA (ver Numeral 2.3.e).
4. **Plan de Monitoreo y Evaluación (PME).** Describe instrumentos, responsables y presupuesto para las acciones de seguimiento a la ejecución del programa, así como de la medición de sus resultados e impactos.
5. **Plan Operativo Anual (POA).** Constituye el instrumento privilegiado de planificación de las actividades del proyecto para cada año. El POA debe ser presentado cada 30 de noviembre para la ejecución el siguiente año-calendario. Deben incluirse: (i) el presupuesto estimado, (ii) los resultados y productos esperados para los indicadores de la Matriz de Resultados, (iii) las adquisiciones y contrataciones previstas; (iv) el cronograma de ejecución y (v) el pronóstico de desembolsos de los recursos del Banco.
6. **Matriz de Gestión de Riesgo del Programa** **(MGR).** Enumera y ranquea los riesgos identificados para la implementación del programa. Define medidas de mitigación para cada uno de ellos y sus respectivos indicadores de seguimiento.
7. **Informes Semestrales de Progreso.** Son elaborados por el OE y resumen los avances del proyecto en el semestre respectivo. Incluyen: (i) valores de los indicadores de resultados que hayan sido medidos; (ii) valores de los indicadores de productos; (iii) costo de los productos; (iv) análisis de los riesgos y reporte de las acciones de mitigación realizadas; y (v) ejecución financiera global del proyecto. Los informes semestrales serán presentados al Banco hasta 2 meses después de la culminación del respectivo semestre (28 de Febrero y 30 de Agosto de cada año). El reporte del 30 de Agosto de cada año contendrá la generación de productos, sus respectivos costos, así como la ejecución financiera general correspondientes al primer semestre, mientras que el reporte del 28 de Febrero incluirá los productos y costos del segundo semestre y del acumulado del año calendario.
8. **Informe de Monitoreo del Progreso** **(PMR).** Recoge la estimación temporal de los desembolsos y del cumplimiento de las metas físicas y de costos de los productos programados, así como los resultados alcanzados, y es un mecanismo para evaluar el desempeño del programa. Se nutre del contenido de los Informes Semestrales de Progreso y otras informaciones puntuales solicitadas al OE por el Banco.
9. **Misiones de Administración o Visitas de Inspección.** El Banco realizará dichas Misiones de Administración o Visitas de Inspección, dependiendo de la complejidad y otras circunstancias de la ejecución del proyecto.

## Recopilación de datos e instrumentos

* 1. La División de Gestión Estratégica de AGESIC con el apoyo del Coordinador del Programa y el Coordinador Operativo, asegurará que los instrumentos y datos necesarios para efectuar el seguimiento estén disponibles de forma tal que este se pueda realizar sin contratiempos. Asimismo, preparará los Informes Semestrales de Progreso mencionados en 2.3(g), para su revisión por el Banco.
  2. Toda la información pertinente y adecuada para lograr un entendimiento cabal de la actividad de seguimiento, se encuentra recogida en los documentos referidos en el párrafo 2.3 anterior.

#### Presentación de informes

* 1. Los mecanismos e instrumentos que se usarán para informar acerca de los resultados del seguimiento serán la principal fuente de información para el PMR.

#### Coordinación, plan de trabajo y presupuesto del monitoreo

* 1. El Banco utilizará el PMR que recoge la estimación temporal de los desembolsos y del cumplimiento esperado de metas físicas y resultados, y es un mecanismo para evaluar el desempeño del programa.
  2. Las tareas de monitoreo del Proyecto de actividades y productos, serán realizadas por la División de Gestión Estratégica de AGESIC, unidad ya existente, que realiza la planificación y seguimiento de todos los proyectos BID de esta Agencia. Para la obtención de datos esta División se apoyará en insumos que le proveerán el Coordinador General y el Coordinador Operativo. Además, hará uso de información relativa a la ejecución de actividades que se encuentra registrada en el Sistema de Información y Gestión de Proyectos (SIGES) de AGESIC.
  3. La División de Gestión Estratégica de AGESIC será responsable de acompañar la ejecución de todas las actividades previstas, de acuerdo al PEP y POA, señalar las posibles desviaciones a partir de un sistema diseñado y puesto en marcha para tal fin y mantener informado al Gerente del Proyecto acerca de la ejecución de la operación.
  4. La División de Gestión Estratégica utilizará como guía para su labor los productos detallados en la MR (Cuadro 2) y en el PMR, así como las actividades explicitadas en el PEP y POAs.
  5. Plan y cronograma de tareas de Monitoreo. La División de Gestión Estratégica de AGESIC realizará el monitoreo de productos y actividades del programa de acuerdo con el siguiente esquema de tareas:

**Cuadro 1: Plan de trabajo y presupuesto de monitoreo**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Principales actividades y productos de monitoreo (año y semestre)** | **Año 1** | | **Año 2** | | **Año 3** | | | **Año 4** | | **Responsable** | **Costo (US$)** | **Financiamiento** | |
| 1 | 2 | 1 | 2 | 1 | 2 | 1 | | 2 |  |  |  |
| MdR, MGR e Informes semestrales de ejecución. |  |  |  |  |  |  |  | |  | OE | NA | NA |
| PEP, PA y POA |  |  |  |  |  |  |  | |  | OE | NA | NA |
| Misiones de Supervisión y Visitas técnicas y fiduciarias de seguimiento |  |  |  |  |  |  |  | |  | Equipo del proyecto - BID | NA | Recursos de Supervisión del Banco |
| Apoyo de M&E (medio tiempo) a la División e Gestión Estratégica | x | x | x | x | x | x | x | | x | OE | NA | UR-L1152 |
| Auditorías |  | x |  | x |  | x |  | | x | Consultoría supervisada por OE | 40.000 | UR-L1152 |
| Costo Total Monitoreo |  | 15.000 |  | 15.000 |  | 15.000 |  | | 30.000 |  | 75.000 | UR-L1152 |

* 1. Las tareas de monitoreo verificarán la entrega de los productos establecidos en la Matriz de Resultados, los cuales se detallan en el Cuadro 3 . En el siguiente cuadro se presentan los impactos y resultados esperados de la Matriz de Resultados del programa

**Cuadro 2: Matriz de Resultados Del proyecto**

**Impacto Esperado**

| **Indicadores** | **Unidad de Medida** | **Línea de Base** | **Año**  **Línea de Base** | **Año 1** | **Año 2** | **Año 3** | **Año 4** | **Meta Final** | **Medios de Verificación** | **Comentarios** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Impacto #1:** Madurez de Capacidad de Seguridad Cibernética aumentada | | | | | | | | | | |
| Madurez de capacidad de seguridad cibernética nacional | Puntaje | 149 | 2016 |  |  |  | 165 | 165 | Informe OEA BID | 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*”](https://publications.iadb.org/en/advanced-experiences-cybersecurity-policies-and-practices-overview-estonia-israel-south-korea-and) estudia Estados Unidos, Estonia, Korea del Sur e Israel con base en el modelo de madurez elegido para medir el impacto de esta operación. El documento muestra que las inversiones realizadas por 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, Estados Unidos pg 48-49. |
| Nivel de madurez promedio en ciberseguridad de las organizaciones públicas | Puntaje | 1,5 | 2018 |  |  |  | 2,5 | 2,5 | Auditoría externa de marco de ciberseguridad | Este es un indicador que refleja las capacidades de 10 entidades públicas más digitalizadas de Uruguay, el puntaje máximo posible es 4. |

**Resultados Esperados**

| **Indicadores** | **Unidad de Medida** | **Línea de Base** | **Año**  **Línea de Base** | **Año 1** | **Año 2** | **Año 3** | **Año 4** | **Meta Final** | **Medios de Verificación** | **Comentarios** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **resultado #1:** Capacidades operativas de monitoreo, detección y respuesta de incidentes de ciberseguridad mejorada | | | | | | | | | | |
| Número de organizaciones públicas monitoreadas a través del SOC | Número de ministerios | 2 | 2018 | 2 | 5 | 11 | 17 | 17 | Reporte anual de la dirección de ciberseguridad informática | Este indicador no refleja el flujo anual sino la cantidad de instituciones acumuladas. |
| Número de incidentes cibernéticos detectados anual | Número de incidentes | 2.043 | 2018 | 2.250 | 3.267 | 6.889 | 10.000 | 10.000 | Reporte anual de la dirección de ciberseguridad informática | Se entiende como incidente “una violación o una amenaza inminente de violación a una política de seguridad de la información implícita o explícita, así como un hecho que compromete la seguridad de un sistema (confidencialidad, integridad o disponibilidad). (Decreto N° 451/009 de 28 de Setiembre 2009- Art.3).  El reporte [“Informe de Incidentes. *Activity Report*” del Centro Criptológico Nacional](https://www.ccn-cert.cni.es/documentos-publicos/2157-memoria-de-actividad-2015-2016-version-imprimible/file.html) 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. |
| Porcentaje de incidentes cibernéticos de alto impacto | Porcentaje | 2,1 | 2018 | 2,25 | 1,84 | 1,51 | 1,24 | 1 | Reporte anual de la dirección de ciberseguridad informática | De acuerdo al documento de procedimiento de clasificación de incidentes de AGESIC, son de alto impacto los que precisan más de 640 horas de experto *senior* para su solución. |
| **resultado #2:** Capital humano capacitado en ciberseguridad aumentado | | | | | | | | | | |
| Número de personas que han tomado al menos 40 horas de capacitación en ciberseguridad anual | Número de personas | 50 | 2018 | 0 | 0 | 150 | 150 | 350 | Registros de estudiantes de las entidades de educación terciaria | Este es indicador que mide el flujo de personas capacitadas en ciberseguridad de manera anual. |
| Mujeres que han tomado al menos 40 horas de capacitación en ciberseguridad anual | Porcentaje | 0 | 2018 | 0 | 0 | 15 | 20 | 25 | Registros de estudiantes de las entidades de educación terciaria | Pro-*Gender*  Este es el indicador que mide el flujo de personas capacitadas en ciberseguridad de manera anual. |

**Cuadro 3: Costeo de Productos del Proyecto**

| **Productos** | **Unidad de Medida** | **Línea de Base** | **Año**  **Línea de Base** | **Año 1** | **Año 2** | **Año 3** | **Año 4** | **Meta Final** | **Medios de Verificación** | **Comentarios** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Componente #1:** Mejoramiento de las capacidades operativas y herramientas del CERT.uy | | | | | | | | | | |
| 1.1 Licencia de Qradar actualizadas | Licencia | 0 | 2018 | 1  (915.000) | 0 | 0 | 0 | 1  (915.000) | Contrato de licencia de Qradar |  |
| 1.2 Sistema NIGPS de detección de intrusiones en funcionamiento | Sistema | 0 | 2018 | 0 | 0  (166.667) | 1  (166.667) | 0  (136.667) | 1  (500.000) | AGESIC Informes de programa |  |
| 1.3 Plataforma de *Big Data* en funcionamiento | Plataforma | 0 | 2018 | 0 | 0  (30.000) | 1  (270.000) | 0 | 1  (300.000) | AGESIC Informes de programa |  |
| 1.4 Laboratorio del CERT Instalado | Laboratorio | 0 | 2018 | 0 | 0  (10.000) | 1  (90.000) | 0 | 1  (100.000) | AGESIC Informes de programa | Este producto incluye: forense, pruebas de concepto, desarrollo de sensores y gestión de incidencias. |
| 1.5 Sistema SIEM implementado | Sistema | 0 | 2018 | 0  (120.000) | 1  (760.000) | 0  (560.000) | 0  (560.000) | 1  (2.000.000) | Reporte SIEM elaborado por AGESIC |  |
| **Componente #2:** Potenciación del uso de tecnología avanzada para la formación de recursos humanos | | | | | | | | | | |
| 2.1 Plataforma de simulación de ataques cibernéticos instalada | Plataforma | 0 | 2018 | 1  (360.000) | 0  (720.000) | 0  (360.000) | 0  (360.000) | 1  (1.900.000) | AGESIC Informes de programa |  |
| 2.2 Plataforma de *e-learning* instalada | Plataforma | 0 | 2018 | 0 | 0  (58.333) | 1  (41.667) | 0 | 1  (100.000) | AGESIC Informes de programa |  |
| **Componente #3:** Fortalecimiento del ecosistema de conocimiento de ciberseguridad a nivel nacional | | | | | | | | | | |
| 3.1.a Currículade formación en ciberseguridad diseñada | Currícula | 0 | 2018 | 0 | 0  (135.000) | 1  (157.500) | 0  (157.500) | 1  (450.000) | AGESIC Informes de programa | La currícula incluye los programas de formación para los diferentes grados y perfiles, así como el contenido de los mismos. |
| 3.1.b Profesores formados en la nueva currícula de formación en ciberseguridad | Profesores | 0 | 2018 | 0 | 0 | 110  (450.000) | 110  (450.000) | 220  (900.000) | AGESIC Informes de programa | En cada año, 10 profesores de cada uno de los 5 centros académicos de formación superior, más 3 profesores de cada uno de los 19 de departamentos del país, más 3 personas de AGESIC. |
| 3.2 Red de expertos en funcionamiento | Red de expertos | 0 | 2018 | 1 | 0  (85.000) | 0  (170.000) | 0  (85.000) | 1  (340.000) | AGESIC Informes de programa |  |
| 3.3 Plan de difusión nacional e internacional implementado | Plan | 0 | 2018 | 0 | 1  (25.000) | 0  (50.000) | 0  (25.000) | 1  (100.000) | AGESIC Informes de programa |  |
| 3.4 Estrategia de gestión del cambio | Documento | 0 | 2018 | 1  (6.000) | 0  (36.000) | 0  (18.000) | 0 | 1  (60.000) | Documento de estrategia de gestión del cambio |  |

**Cuadro 4: Costo total del programa**

|  |  |
| --- | --- |
| Costo total estimado de los productos | US$9.165.000 |
| Administración, auditoria, monitoreo y evaluación | US$666.182 |
| Contingencias | US$168.818 |
| Costo total estimado del programa | US$10.000.000 |

# Evaluación

* 1. Por parte del Banco, se elaborará un **Informe de Terminación del Programa (PCR)**: Este informe se presentará dentro de los 180 días después de la realización del último desembolso y se basará en los informes semestrales de progreso del Organismo Ejecutor, los informes de monitoreo de progreso (PMR), la Matriz de Resultados, los Estados Financieros Auditados (EFA), los informes correspondientes a las evaluaciones intermedia y final, y en los resultados de los talleres de evaluación y posibles estudios, investigaciones y otras acciones que se consideren pertinentes.
  2. Se realizará una evaluación intermedia una vez transcurridos 24 meses luego de la entrada en vigencia del contrato de préstamo o cuando se haya comprometido el 50% de monto del préstamo, lo que ocurra primero; y una evaluación final, cuando haya concluido el plazo original de desembolsos o sus extensiones, o se haya comprometido el 90% del monto del préstamo, lo que ocurra primero. Dichas evaluaciones serán externas e independientes, en función de TdR acordados con el Banco, y financiadas con recursos del préstamo, previstos en el Plan de Ejecución Plurianual.
  3. La evaluación final, incluirá un **análisis económico ex post,** queseguirá la metodología propuesta en la evaluación económica ex ante, incluida en otro anexo al documento principal, cuando haya concluido el plazo original de desembolsos o sus extensiones, o cuando el Prestatario, por intermedio del Organismo Ejecutor, haya comprometido el noventa por ciento (90%) de los recursos del Préstamo, lo que suceda primero.
  4. Como complemento, a fin de generar conocimiento aplicado acerca del impacto económico real de los ciberataques, se diseñará una **metodología de estimación de impacto económico**, la cual **se aplicará de forma piloto** en una selección de instituciones públicas.
  5. Asimismo, se realizará una **evaluación de impacto** que tendrá como objetivo medir la efectividad de las actividades relacionadas con la generación de capital humano en ciberseguridad.
  6. La **evaluación intermedia** revisará el grado de avance y cumplimiento de los indicadores de resultado y producto previstos, así como formular recomendaciones, proponer acciones correctivas, y establecer buenas prácticas y lecciones aprendidas. Se revisará el cumplimiento de las metas que se establecieron en el plan inicial y en los Planes de Operativos Anuales, así como los avances en la Matriz de Resultados. Específicamente, las actividades serán las siguientes:

1. Llevar a cabo una revisión detallada de los **desembolsos y contrataciones** del Programa con referencia a la documentación aprobada como el Plan de Ejecución Plurianual (PEP) y los Planes Operativos Anuales (POA). Se identificará cualquier déficit o rezago y las causas de los mismos, a fin de proponer acciones correctivas (y generar lecciones aprendidas para futuros programas), así como cualquier ahorro en términos presupuestales o de tiempos.
2. Llevar a cabo una revisión detallada del avance de los **indicadores de la matriz de resultados**, incluyendo una revisión del soporte documental o físico de los mismos. Se identificará cualquier déficit o rezago de cumplimiento y analizará las causas del mismo, a fin de proponer acciones correctivas. Adicionalmente, se hará nota de cualquier ajuste que se haya hecho a la matriz de resultados durante la implementación del proyecto (del indicador mismo, su valor de línea de base o las metas) y la justificación por dicho ajuste. Finalmente, se debe analizar si las metas y los indicadores planteados (en la propuesta de préstamo) son adecuados para medir los objetivos declarados y si las metas fueron infundadamente optimistas o injustificadamente conservadoras. Entre otras fuentes, este ejercicio se beneficiará de la información contenida dentro de la herramienta de monitoreo del BID, *Project Monitoring Report (PMR).*
3. Identificar los **resultados imprevistos** (no incluidos en el objetivo declarado o la matriz de resultados) observados hasta la fecha y presentar evidencia de la influencia del proyecto sobre dichos resultados.
4. Llevar a cabo una revisión detallada de **la matriz de riesgos** del Programa y analizar el grado al cual se han materializado los riesgos identificados, las medidas de mitigación que se han implementado, la efectividad de las medidas tomadas, y el grado de riesgo a futuro. Adicionalmente, con base en una revisión documental y entrevistas con informantes clave, se identificarán riesgos no contemplados en la matriz de riesgos original y recomendadas acciones de mitigación.
5. Llevar a cabo una revisión de la **administración del proyecto** y su impacto en el éxito del proyecto hasta la fecha, incluyendo: (i) los mandatos, las relaciones, las estructuras, los recursos las capacidades del organismo ejecutor y su coordinación con otras entidades involucradas; (ii) la gestión fiduciaria (gestión financiera y de adquisiciones); (iii) cualquier conducta o acción de algún participante público o privado; (iv) aspectos jurídicos o normativos, del país o del Banco; y (v) otro factor influyente.
6. Elaborar una sección de conclusiones y recomendaciones con base en toda la evidencia recopilada.
   1. La **evaluación final** incluirá las mismas actividades que la evaluación intermedia y las siguientes actividades adicionales, siguiendo las directrices del Banco al respecto:
7. **Análisis de la lógica vertical**: la evaluación de la efectividad analiza la validez de los vínculos previstos entre los productos del proyecto, los efectos directos deseados y los impactos (la cadena de resultados). La evaluación procurará examinar la cadena de resultados y proporcionar elementos de prueba que determinen si se dio la vinculación prevista entre los productos y los efectos directos o impactos.
8. **Análisis de atribución de resultados**: debería analizar los elementos teóricos o pruebas de otro tipo sobre los que se apoye la atribución de los efectos directos. En este caso, el análisis de la consecución de los resultados esperados debería complementarse con una evaluación de “atribución teórica” basada en una cadena causal que sintetice los factores determinantes de los vínculos entre los efectos directos y los productos. Las pruebas, cuando las haya disponibles, deberían considerar las evaluaciones rigurosas que existan de las intervenciones en otros contextos similares (validez interna), así como información sobre la aplicabilidad de la intervención en el país en el que se haya implementado (validez externa).
9. **Análisis de pertinencia**: La pertinencia se refiere a la concordancia de los objetivos del proyecto con las necesidades del beneficiario, las prioridades y estrategias normativas o de desarrollo del país, y la estrategia de asistencia del Banco y sus objetivos institucionales. La pertinencia se evalúa teniendo en cuenta las circunstancias predominantes en el momento de la evaluación. La evaluación de la pertinencia se estructura en torno a la siguiente pregunta: ¿Han variado las condiciones que hacían que el proyecto fuera pertinente en el momento de su aprobación? La pertinencia del proyecto puede estar determinada por factores ajenos a la pertinencia de los objetivos, como la lógica de la cadena de resultados o del diseño del proyecto dadas las circunstancias locales.
10. **Análisis de sostenibilidad**: Tomando en cuenta que: (a) los resultados logrados por el proyecto; y (b) la pertinencia demostrada del proyecto, la evaluación de sostenibilidad consiste en evaluar las condiciones que podrían incidir en la continuidad de los actuales resultados logrados y en la consecución prevista de resultados futuros. La sostenibilidad está determinada por una evaluación tanto de la probabilidad como del impacto de varias amenazas sobre la continuidad de los efectos directos más allá de la terminación del proyecto (implementación del proyecto ex post), teniendo en cuenta cómo se mitigaron esas amenazas en el diseño del proyecto o durante la ejecución.
11. **Contribución a los objetivos estratégicos del Banco** (objetivos estratégicos institucionales, sectoriales, y con el país) **y del país** (enmarcados en su plan de desarrollo u otro documento oficial)
12. **Análisis de la calidad del plan de seguimiento y evaluación del proyecto y su implementación**. Esta sección resume la idoneidad del diseño y la implementación del plan de seguimiento y evaluación, así como el uso de la información.
13. **Análisis de uso de sistemas nacionales**: en qué medida el diseño y la ejecución del proyecto contribuyen a fortalecer los sistemas nacionales y su utilización. El análisis abarca los sistemas nacionales fiduciarios (gestión financiera y de adquisiciones) y no fiduciarios (planificación estratégica, seguimiento y evaluación, estadística, evaluación ambiental) que sean pertinentes al Proyecto.
14. **Una sección de conclusiones y recomendaciones** con base en la evidencia recopilada. Las recomendaciones se dirigirán tanto al país para aumentar la sostenibilidad del proyecto o fortalecer otras iniciativas parecidas, como al Banco para mejorar su desempeño con el país en otras operaciones y con otros países en operaciones parecidas.
    * 1. **Evaluación de estimación del valor económico de ciberataques en Uruguay.**
    1. Antes de la finalización del proyecto, se realizará un **análisis económico ex post**. El objetivo del mismo es verificar y actualizar los supuestos expuestos en el análisis económico ex ante, y recalcular el Valor Presente Neto, la Tasa Interna de Retorno, y la Razón Beneficio-Costo. Analizará las tres vertientes incluidas en el análisis económico ex ante: (i) disminución de costos operativos de remediación; (ii) impacto económico de ciberataques en instituciones públicas; y (iii) actividad económica generada por profesionales formados en ciberseguridad.
    2. Los supuestos clave por segmento de análisis y su propuesta fuente de verificación se detallan en la tabla a continuación.

**Cuadro 5. Supuestos clave para el análisis económico ex post**

|  |  |  |
| --- | --- | --- |
| **Variable** | **Supuesto ex ante** | **Medio de verificación** |
| *Segmento 1: Disminución de costos operativos de remediación de ciberataques* | | |
| Número de ciberataques detectados | 10.000 ataques detectados anualmente al final del proyecto | Cifras del SOC (AGESIC) |
| Proporción de ciberataques que son de alta o muy alta severidad | 1% al final del proyecto | Cifras del SOC (AGESIC) |
| *Segmento 2: Impacto económico de ciberataques en instituciones públicas* | | |
| Proporción de daño económico evitado | 30% al final del proyecto | Cifras del SOC (AGESIC)  \* Nota: El Director del SOC proveerá una estimación de esta proporción, usando el porcentaje de ataques detectados oportunamente como proxy |
| *Segmento 3: Actividad económica generada por profesionales formados en ciberseguridad* | | |
| Número de personas que han cursado 40 horas o más en ciberseguridad | 150 en año 4.280 en año 5 en adelante | AGESIC recopila cifras de instituciones que participan en los programas de formación |

**Metodología de estimación de impacto económico de ciberataques y aplicación piloto**

* 1. A fin de generar conocimiento acerca del impacto económico de los ciberataques y los beneficios de invertir en la capacidad de ciberseguridad – escaso en el mundo – se diseñará una metodología práctica, la cual se aplicará de manera piloto en una selección de instituciones públicas uruguayas.
  2. La metodología de estimación de impacto económico de los ciberataques considerará, como mínimo, los siguientes elementos: (i) quiénes son las víctimas del ataque; (ii) cuáles son los activos comprometidos de forma directa; (iii) cuales son las implicaciones, directas e indirectas, del compromiso de los activos para el negocio (la misión) de la institución responsable de dichos activos. Esto puede incluir, pero no estará limitado a interrupciones en la prestación de servicios, robo de información, alteración de información, y robo directo de dinero, (iv) los costos de reparación de los daños derivados de la interrupción del funcionamiento de los activos informáticos (por ejemplo, si hubo que pagar alguna compensación a una víctima individual); y (v) los costos de remediación de los sistemas informáticos.
  3. Además de orientación para la estimación del impacto económico, la metodología propondrá un sistema de clasificación de ciberataques y correspondientes respuestas que permita una comparación entre sí. Este sistema de clasificación puede incluir elementos tales como: institución y oficina afectada, tipo de activo afectado, tipo de ataque (e.g. *phishing, denial of service*, etc.), tiempo transcurrido entre el inicio del ataque y su detección, y tiempo transcurrido entre la detección del ataque y el despliegue de la respuesta, entre otros.
  4. La metodología tendrá en cuenta la dificultad que tendrán los equipos operativos de recopilar información adicional durante el proceso de respuesta a un ciberataque, y propondrá métodos alternativos que no impliquen una carga adicional a estos equipos durante momentos críticos durante la respuesta.
  5. A fin de refinar la metodología propuesta y sacar estimaciones preliminares, se llevarán a cabo 10 aplicaciones piloto de ataques de severidad alta o muy alta. La definición de la selección de los casos piloto será a discreción del Director de Seguridad de la Información de la AGESIC en consideración de aspectos tales como variedad de activos vulnerados, institución afectada, y tipo de ataque. Esta definición se deberá hacer hacia el inicio de la ejecución del Programa para que los equipos involucrados (por ejemplo, del SOC y la institución afectada) tengan claridad acerca de los requerimientos de recopilación de información
  6. Los resultados de las aplicaciones piloto serán sistematizados en un informe que esconde los nombres reales de las instituciones afectadas y activos vulnerados a fin de no exponerlos a riesgo adicional. El informe se compartirá únicamente entre la AGESIC y el BID a menos que ambas partes explícitamente acuerden realizar una difusión más amplia.

1. Evaluación de impacto de la política de promoción de la oferta educativa para la mejora del ecosistema de conocimiento inclusivo en ciberseguridad.
   1. Con el objetivo de generar conocimiento sobre la efectividad de las actividades relacionadas con la promoción y generación de capital humano en ciberseguridad, se pretende llevar a cabo una **evaluación de impacto** de tipo experimental para medir la contribución del programa sobre diferentes indicadores de interés.
   2. La motivación de la evaluación se sustenta en las siguientes cifras: (i) el sector de las TIC en Uruguay ha sido el de mayor expansión en los últimos años, para 2017 el crecimiento de este sector fue de un 26% y sus ventas ascendieron a US$1.193 millones, la exportación de servicios en software lidera el mayor servicio del sector; (ii) la venta de servicios en ciberseguridad presenta múltiples desafíos para su expansión y uno de ellos es la falta de personas especializadas: en la actualidad existen 650 profesionales que trabajan en ciberseguridad y se necesita duplicar esta cifra en los próximos dos años; (iii) existe una baja oferta educativa en este tema, hoy se ofrece sólo un diplomado en la Universidad de la Republica (UDELAR) y en cifras de esta universidad en 2016 ingresaron 4 personas y se graduaron 3; y (iv) la participación de las mujeres en el sector de ciberseguridad es baja, según datos de la UDELAR en 2017 la participación femenina sobre el total de graduados fue del 0%.
   3. En síntesis, Uruguay se enfrenta a un panorama de un alto crecimiento potencial en la venta de servicios de ciberseguridad que se puede ver afectado por la falta de personas especializadas en el tema y con una participación femenina casi inexistente en este mercado. Para enfrentar este problema el componente tres del programa contempla apoyar el aumento de una oferta educativa a través del desarrollo de *currícula* de formación en ciberseguridad que pueda ser utilizada por diferentes centros académicos del país; formación de docentes en ciberseguridad; creación de una red nacional de expertos con activas vinculaciones internacionales; y actividades de difusión nacional e internacional incluyendo intercambios y eventos de difusión y comunicación.
   4. En este orden de ideas, la evaluación tiene por objetivo responder las siguientes preguntas de investigación: (i) ¿Existe una manera efectiva y costo-eficiente de aumentar la demanda por cursos de ciberseguridad? y (ii) ¿Cuál es la estrategia más efectiva y costo-eficiente para cerrar la brecha de género en ciberseguridad?
   5. Para responder las preguntas anteriores, se propone un diseño experimental en el cual se pretenden medir diferentes tipos de intervenciones contempladas en el componente tres. Dado el contenido en TIC de la ciberseguridad, esta nueva oferta de formación se puede enmarcar en el grupo de carreras STEM. De acuerdo con la literatura, la brecha de género es usual en este tipo de carreras y menciona que para aumentar la demanda por este tipo de formación las intervenciones se deben enfocar en transmitir información sobre ingresos esperados, la probabilidad de estar empleado, modelos a seguir y para el caso específico de las mujeres se debe trabajar sobre las creencias previas. A manera de ejemplo, Del Carpio y Guadalupe (2018) realizaron un experimento en Perú en el cual trabajaron en reducir el sesgo preexistente de las mujeres a creer que ellas no pueden ser exitosas en tecnología. Esta intervención duplicó la tasa de aplicación de las mujeres a programas TIC llegando a un 15% en comparación a un 7% del grupo de control
   6. En el contexto de la presente evaluación se pretende llevar a cabo las intervenciones de información a nivel de colegio y la unidad de análisis será el estudiante. Es decir, se asignarán las campañas de información de manera aleatoria a los colegios públicos de Uruguay que ofrezcan educación secundaria y se harán los análisis de impacto sobre los estudiantes, en particular, se plantean los siguientes dos grupos de tratamiento y un grupo de control:

**Cuadro 6. Conformación grupos tratamiento y control**

|  |  |  |
| --- | --- | --- |
| Grupo 1 (T1) | Grupo 2 (T2) | Grupo 3 (Control) |
| Colegios de tratamiento 1: campaña enfocada en ingresos futuros y probabilidad de empleo | Colegios de tratamiento 2: campaña que incluye la información difundida en el grupo 1 y adicionalmente se incluye información sobre modelos a seguir y creencias previas. | Colegios de control: Estos colegios no reciben ninguna campaña de información. |

* 1. Los dos grupos de tratamiento expuestos en la tabla anterior se diferencian en que el primer grupo, la intervención se enfoca en expectativas del mercado laboral, como salarios y probabilidad de estar empleado, mientras que el segundo grupo de tratamiento incluye un enfoque especifico de género, es decir, el contenido de la campaña de información incluirá un modelo a seguir mujer y contenido sobre creencias previas sobre el papel de las mujeres en carreras STEM. En este sentido, es necesario aclarar que, aunque el grupo dos tiene un enfoque para las mujeres, dicho contenido será difundido a toda la escuela, es decir, tanto hombres como mujeres recibirán dicha intervención.
  2. La medición del impacto de las intervenciones planteadas se puede expresar a través de la siguiente ecuación
  3. Donde es el resultado de interés para el estudiante i, por ejemplo, inscripción a un curso de ciberseguridad, salario esperado, asistencia a los cursos. son variables dicótomas para los indicadores de tratamiento que para T1 toma el valor de 1 si el estudiante recibió de manera aleatoria una campaña sobre ingresos futuros y probabilidad de empleo,0 de lo contrario mientras que para T2 toma el valor de 1 si el estudiante recibió la campaña descrita en el grupo, 0 de lo contrario. Por su parte, M es una variable dicótoma que toma el valor de 1 si el estudiante es mujer 0 de lo contrario, son N controles individuales incluidos para reducir la varianza residual, son efectos fijos por escuela.
  4. Los indicadores principales de resultado de la evaluación se alinean con la matriz de resultados de la operación, por ejemplo, el número de personas inscritas en cursos de ciberseguridad y porcentaje de mujeres inscritas en los cursos de ciberseguridad sobre el total de inscritos

**Cuadro 7. Indicadores de resultado de la evaluación**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Indicador** | **Unidad de medida** | **Línea de base** | | **Objetivo** | | **Frecuencia** | **Fuente** | **Metodología de evaluación** |
| **valor** | **año** | **valor** | **año** |  |  |  |
| Número de personas que han tomado al menos 40 horas de capacitación en ciberseguridad anual. | Número de personas | 10 | 2018 | 150 | 2024 | Anual | Cifras UDELAR | Experimento controlado |
| Porcentaje de mujeres que han tomado al menos 40 horas de capacitación en ciberseguridad anual | % | 0 | 2018 | 15 | 2024 | Anual | Cifras UDELAR | Experimento controlado. |

* 1. Una vez explicado el experimento, se incluyen los cálculos de poder para determinar el tamaño de muestra. La tabla 2 presenta el efecto mínimo detectable calculado para cada varios tamaños de muestra expresado en número de escuelas, se asumen los siguientes parámetros: (i) poder (1-beta): 90%; (ii) significancia (1 menos alfa) – 95%; (iii) la distribución de los grupos tiene la misma proporción, es decir de la muestra total, un tercio será del grupo de tratamiento uno, un segundo tercio será el grupo tratamiento dos y otro tercio será del grupo de control; (iv) se asume una correlación intracluster de 0,5, es decir que los estudiantes dentro de una escuela no son completamente iguales; y (v) el número promedio de estudiantes por escuela es de cuarenta.

**Cuadro 8. Tamaño de muestra y efecto mínimo detectable**

| **Tamaño de muestra (T&C)** | **Efecto mínimo detectable** |
| --- | --- |
| 90 | 0,9 |
| 120 | 0,51 |
| 150 | 0,46 |
| 180 | 0,42 |
| 210 | 0,39 |

* 1. La tabla anterior señala que, bajo un experimento controlado para una muestra de 210 escuelas, se necesita que el mínimo efecto detectable de la intervención de 0.39 desviaciones estándar, es decir, que, para poder observar un efecto estadísticamente significativo, los estudiantes de las escuelas de tratamiento deben aumentar la inscripción a cursos de ciberseguridad en 0,39 desviaciones estándar por encima de los estudiantes de las escuelas control. Asimismo, es importante señalar que el Universo de la intervención son todas las 853 escuelas públicas que ofrecen educación secundaria en Uruguay.
  2. Los pasos para la ejecución de la evaluación de impacto son los siguientes:
  3. Contratación de Investigador Principal (PI) por la UEP para dirigir la investigación: El PI debe ser un experto en evaluación de impacto con experiencia en experimentos aleatorios controlados, esta persona debe proveer guía técnica en la definición de la muestra, grupo de tratamiento, diseño de encuestas, términos de referencia para contratar una firma encuestadora y debe apoyar la producción el análisis estadístico del reporte final de evaluación
  4. Confirmación del universo y marco muestral: Una vez sea aprobado el documento de préstamo, en el tiempo entre aprobación y ejecución de la evaluación, se debe reconfirmar con las autoridades respectivas el universo muestral de la investigación. De manera específica, la AGESIC en coordinación con el Ministerio de Educación deben confirmar el marco muestral (base de datos de escuelas públicas que ofrecen secundaria con información de contacto) a los investigadores
  5. Levantamiento encuesta de línea de base: El investigador principal debe diseñar y discutir con la AGESIC el cuestionario final y el protocolo de aplicación para ser aplicado a los estudiantes de la muestra, se debe asegurar que el cuestionario sea piloteado y contenga todos los indicadores de resultado de interés, una vez aprobado y piloteado el cuestionario, una firma encuestadora deberá levantar la información de línea de base para toda la muestra de la evaluación. Esta encuesta toma especial relevancia, porque a pesar de saber la tasa de inscripción a cursos de ciberseguridad, es fundamental indagar por otro tipo de variables de interés, tales como: Expectativas de salarios, predisposición a escoger una carrera STEM, conocimientos previos sobre ciberseguridad y su relevancia, entre otras.
  6. Selección Aleatoria de escuelas: Basado en los acuerdos con la AGESIC sobre el marco muestral, tamaño de la muestra e implementación de las campañas de información, los investigadores procederán a asignar los grupos de tratamiento y control de manera aleatoria y con base en la información de línea de base procederán a verificar que ambos grupos se encuentran balanceados y por tanto la asignación aleatoria fue exitosa
  7. Aplicación encuesta de seguimiento: Una vez el grupo de tratamiento es intervenido, se debe contar con un tiempo de exposición de aproximadamente un año para poder ver efectos sobre las variables de resultado, luego de este tiempo de exposición, la firma encuestadora deberá recolectar una encuesta de seguimiento sobre toda la muestra de la evaluación. Si bien, se contará con recolección de data administrativa de las Universidades, es importante indagar que carreras tomaron todos los estudiantes de la muestra y no sólo observar la inscripción neta en cursos de ciberseguridad, así como el cambio en expectativas de ingreso y otros aspectos relacionados con la formación tecnica o profesional de los estudiantes.
  8. Análisis de resultados: Con base en la información de línea de base y de seguimiento, el investigador principal procederá a realizar el análisis estadístico de los resultados de impacto y proveerá información sobre la efectividad de la implementación de las HIS sobre el desempeño de los hospitales y diferentes indicadores de salud publica
  9. Productos de la evaluación. Esta investigación generará tres productos: (i) un conjunto de instrumentos de línea de base que capture los diferentes indicadores que responden las preguntas de investigación; (ii) un reporte de línea de base que muestre la calidad del proceso de aleatorización, es decir que las características de los estudiantes estén balanceadas entre los grupos de tratamiento y control, por ejemplo, el porcentaje de estudiantes que quieren escoger una carrera en ciberseguridad este balanceada entre grupos; y (iii) un reporte final de evaluación con los resultados y análisis estadísticos sobre el impacto de las campañas de información sobre la inscripción en los cursos de ciberseguridad.

# CUADRO 9: Programación y Presupuesto de Actividades de Evaluación

| **Actividades evaluación** | **Año 1** | | | **Año 2** | | **Año 3** | | **Año 4** | | **Responsable** | **Presupuesto** | **Fuente** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1** | | **2** | **1** | **2** | **1** | **2** | **1** | **2** |  |  |  |
| Evaluación intermedia |  | |  |  |  | X |  |  |  | Consultoría supervisada por el especialista del M&E | U$8.000 | UR-L1152 |
| Análisis económico expost y Evaluación final |  | |  |  |  |  |  |  | X | Consultoría supervisada por el especialista del M&E | U$12.000 | UR- L1152 |
| Levantamiento línea de base de evaluación de impacto y asignación aleatoria de centros educativos de tratamiento |  | | X |  |  |  |  |  |  | Firma encuestadora con coordinación de PI y AGESIC | U$30.000 | UR-L1152 |
| Estimación de impacto económico de ciberataques: metodología y aplicaciones piloto |  | |  |  | X | X | X |  |  | Consultoría supervisada por el Especialista del M&E | U$25.000 | UR-L1152 |
| Costo anual |  | | | U$10.000 | | U$30.000 | | U$25.000 | |  |  |  |
| **Costo total** | | **U$75.000** | | | | | | | |

# Cuadro 10: Costos totales PME

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Año 1** | **Año 2** | **Año 3** | **Año 4** | **Total** |
| **Monitoreo** | U$15.000 | U$15.000 | U$15.000 | U$15.000 | U$60.000 |
| **Evaluación** |  | U$30.000 | U$25.000 | U$20.000 | U$75.000 |
| **Total** | U$15.000 | U$45.000 | U$40.000 | U$50.000 | U$135.000 |