Documento del Banco Interamericano de Desarrollo

**Uruguay**

**Fortalecimiento en Ciberseguridad en Uruguay**

**(UR-L1152)**

**Análisis Económico**

Este documento ha sido preparado por: Benjamin Roseth (IFD/ICS) y Harold Villalba (SPD/SDV)

1. **Introducción**
	1. Este documento presenta el análisis económico ex ante del programa Fortalecimiento de la Ciberseguridad en Uruguay (UR-L1152), cuya ejecución se tiene prevista para el período 2019‑2023. El análisis se lleva a cabo mediante la metodología de costo‑beneficio.
	2. El análisis costo-beneficio incluye tres formas en las cuales se espera que el proyecto genere retornos monetarios: (i) la disminución de costos operativos en remediación de los daños causados por ciberataques a las instituciones públicas, a través de una disminución en la proporción de ataques que son de alta severidad; (ii) la disminución en el impacto económico causado por los ciberataques a las instituciones públicas, gracias a una mayor capacidad de prevención y respuesta; y (iii) la generación de actividad económica a través de la formación de profesionales en ciberseguridad y su subsecuente inserción al mercado laboral. Los costos serán los gastos incluidos en el Programa (cuyas actividades correspondientes se describen en el Documento de Proyecto), abarcando tanto el aporte BID como la contrapartida local. Cada segmento del análisis de beneficios cuenta con supuestos y metodología propia, que se describen a continuación. Los únicos supuestos compartidos entre ellos son el de la tasa de descuento del 12%, estándar para el Banco, y el plazo de contabilización de beneficios de 10 años.
2. **Supuestos y metodología**
	1. **Disminución de gastos operativos de remediación de ciberataques.** Cada vez que se detecta un ciberataque de severidad alta, el personal del CERT (“*Computer Emergency Readiness Team*” en inglés) de AGESIC junto con la entidad afectada forma un equipo para dar respuesta. El costo de esta respuesta depende principalmente del tiempo que toma remediar el problema causado. El Programa propiciará dos cambios en este rubro de gastos: (i) un incremento en el número total de ataques registrados, gracias a un aumento en la capacidad de detección; y (ii) una disminución en la proporción de estos ataques que son de alta severidad, gracias al mismo aumento en la capacidad de detección y fortalecidas capacidades de prevención y respuesta. La secuencia de cálculos que se realizan para estimar los beneficios por este canal, y los correspondientes supuestos, se detallan a continuación.
* Según estimaciones de la AGESIC, en promedio, el costo de remediación de un incidente de severidad alta o muy alta incluye 800 horas de trabajo a un US$60 por hora, por un total de US$48.000 por incidente. La cifra que se compara en los escenarios con proyecto versus sin proyecto es la multiplicación de este costo por incidente por el número de incidentes.
* En 2018, hubo un total de 2.046 incidentes detectados, 43 de los cuales eran de severidad alta o muy alta, equivalente al 2,10%.
* Sin proyecto, se asume que el número de incidentes detectados aumentará en un 10% por año. Este supuesto se considera conservador, ya que el crecimiento observado entre el 2017 y el 2018 fue del 21%.
* Sin proyecto, se asume que la proporción de ataques que son de severidad alta o muy alta aumentará en un 7%. Este supuesto se considera conservador, ya que el crecimiento observado entre 2017 y 2018 fue del 96%.
* Con proyecto, se asume que al final de la ejecución del proyecto (2023), se detectarán 10.000 ataques. Este supuesto se justifica por el hecho que el SOC (centro de operaciones de seguridad, o Security Operations Center en inglés), expandirá su monitoreo interno de la actividad informática de dos instituciones (Presidencia y Ministerio del Interior) a 17, además de fortalecer su capacidad en monitoreo perimetral de todas las instituciones públicas. Se asume que una vez el proyecto esté implementado, la tasa anual de crecimiento del número de ataques detectados volverá al 10% (la misma tasa de crecimiento que se asume para el escenario sin proyecto).
* Con proyecto, se asume que la proporción de los ataques que son de severidad alta o muy alta se reducirá del 2,10% al 1% al final de la ejecución (2023), y que esta proporción se mantendrá a lo largo del periodo de análisis (hasta el 2028). Este supuesto se sustenta por el mismo aumento en capacidad de detección que se señala en el punto anterior, la cual facilitará que los incidentes que tienen el potencial de volverse severos sean detectados y atendidos de forma oportuna.
	1. **Disminución del impacto económico de ciberataques a instituciones públicas**. El impacto económico real de los ciberataques se desconoce, por dos motivos: (i) no existe ninguna metodología aceptada para medirlo; y (ii) las víctimas de los ciberataques tienden a no compartir información acerca de los daños causados por el riesgo reputacional asociados o temor a invitar ataques a futuro. La estimación que se describe a continuación consiste en un escalamiento al Gobierno de Uruguay de cifras auto‑reportadas de individuos y empresas de Estados Unidos. Los beneficios por este rubro se generan a través de una mayor prevención de impactos económicos de los ciberataques a instituciones públicas uruguayas gracias a aumentadas capacidades de prevención, detección y respuesta.
* El impacto económico del cibercrimen en Estados Unidos en el 2017 fue de US$1,42 mil millones de dólares, según el “*Internet Crime Report*” de *Federal Bureau of Investigation* (FBI), un informe que recopila reportes individuales de ciberataques sufridos por personas naturales y jurídicas[[1]](#footnote-1).
* Esta cifra representa solamente entre el 10-12% del impacto total real – el resto de los ataques y sus impactos no se reportan, según el Internet *Crime Complaint Center* del FBI[[2]](#footnote-2). Asumiendo que representa el 12% del total, el total real entonces sería de US$11,83 mil millones.
* Se asume que el nivel de ataques por país se mueve en función del tamaño de la economía, lo cual sería consistente con un hallazgo de *Ponemon-Accenture* sobre el nivel de ciberataques experimentado por empresas privadas[[3]](#footnote-3). Según cifras del Banco Mundial, el PIB de Uruguay es el 0,29% del PIB de Estados Unidos. Por tanto, el total impacto de los ciberataques en Uruguay sería el 0,29% del de Estados Unidos – US$34,27 millones[[4]](#footnote-4).
* Para estimar el impacto económico de los ciberataques a los cuales estaría sujeto el gobierno, se escala por la proporción del PIB que representa el gasto público. El gasto público en Uruguay representa el 30% del PIB, lo cual significa que el impacto económico de los ciberataques al gobierno en el 2017 se ascendería al 30% de US$34,27 millones, o US$10,32 millones.
* Para estimar el impacto económico de los ciberataques al gobierno en 2019, se asume que la tasa anual de crecimiento del impacto en Uruguay sería igual a la tasa de incremento observada en Estados Unidos entre 2016 y 2017, que fue del 6,76%, según cifras del FBI[[5]](#footnote-5). Por tanto el impacto económico en 2019 sería del US$11,77 millones, previo a ajustes por nivel de exposición digital y nivel de capacidad de ciberseguridad.
* El total de US$11,77 millones no considera que el gobierno de Uruguay, por ser menos digitalizado que el de Estados Unidos, está menos expuesto al cibercrimen. Para reflejar esta diferencia, se utiliza el Índice de Gobierno Electrónico de Naciones Unidas. En 2018, Estados Unidos tenía un puntaje de 0,8769; y Uruguay de 0.7858; equivalente 89,61% del puntaje de Estados Unidos. Asumiendo que el nivel de ciberataques se mueve en función del nivel de exposición digital, incorporar este ajuste arrojaría un total de impacto económico de 0,8961\*11,77 = US$10,55 millones.
* El último ajuste que se realiza para estimar el total del impacto económico sufrido por las instituciones públicas uruguayas en 2019 considera la diferencia en capacidad de ciberseguridad del gobierno de Estados Unidos versus el gobierno de Uruguay. Según informes de ciberseguridad de 2016 de OEA-BID[[6]](#footnote-6), Estados Unidos tenía un puntaje de 203 sobre 245 (déficit de 42 puntos), mientras Uruguay tenía un puntaje de 149 sobre 245 (déficit de 96 puntos). Considerando esta mayor exposición a ciberataques por menor capacidad, el impacto económico para el gobierno de Uruguay sería de US$24.1 millones. Es monto que se utiliza como la línea de base para el impacto proyectado del proyecto.
* En el escenario sin proyecto, se asume que el impacto económico de los ciberataques se incrementaría en la misma tasa anual observada en Estados Unidos entre 2016 y 2017 citada arriba del 6,7%.
* En el escenario base con proyecto, se asume que, para el final de la ejecución en 2023, se podrá evitar un 30% de los impactos económicos que se hubieran sufrido gracias al aumento en capacidad de ciberseguridad. Este supuesto se considera conservador ya que la cobertura del monitoreo cibernético interno de las instituciones públicas pasará de dos (Presidencia y Ministerio del Interior) a 17, además del fortalecimiento de la capacidad en monitoreo perimetral de todas las instituciones públicas.
* Se asume que la misma tasa de prevención del 30% se mantendrá durante todo el periodo de análisis.
	1. **Aumento en actividad económica gracias a la formación de profesionales en ciberseguridad.** Los Componentes 2 y 3 del programa se concentran en la formación de profesionales en ciberseguridad. Esta formación atenderá una demanda tanto inmediata como proyectada, tanto doméstica como internacional. El beneficio que se contabiliza es la diferencia en términos de valor de ventas que harían los profesionales capacitados con la formación en ciberseguridad versus lo que harían si vendieran servicios de programación informática.
* En lo inmediato y doméstico, según una consultoría realizada para la AGESIC por la empresa de ciberseguridad israelí Avnet, hay una necesidad de 600 profesionales en ciberseguridad en Uruguay.
* Las tendencias recientes sugieren que habrá un aumento constante en la necesidad de profesionales en ciberseguridad. Por ejemplo, el sector TIC en Uruguay ha registrado un crecimiento anual típicamente alrededor del 12% (11,55% en el periodo 2007-2017, según la Cámara Uruguaya de Tecnologías de la Información (CUTI)[[7]](#footnote-7)). En el mismo sentido, el estudio de Avnet demuestra que, a nivel Latinoamericano, el mercado de capacitación en ciberseguridad tiene una tasa de crecimiento prevista de más del 15,4% anual.
* A nivel regional, hay una brecha sustancial de profesionales en ciberseguridad: Avnet estima que hacen falta más de 20.000 profesionales en América Latina. Esto, a su vez, es indicativo de un mercado potencial de venta de servicios de ciberseguridad de empresas uruguayas a países latinoamericanos. (ISC)², una asociación profesional de ciberseguridad calcula el déficit en la combinación de la necesidad doméstica y el mercado internacional, teniendo en cuenta la falta de oferta de formación en otros países latinoamericanos, 136.000 profesionales a nivel regional[[8]](#footnote-8). Esto sugiere que el potencial de absorción en el mercado de los profesionales formados en ciberseguridad es casi ilimitado.
* Según oficiales de la Cámara Uruguaya de Tecnologías de la Información, los servicios de ciberseguridad se venden a un precio más alto que los servicios de programación – US$100 por hora versus US$80 por hora, en promedio (siendo conservadores sobre la diferencia).
* Se asume que todos los estudiantes que reciben formación en ciberseguridad, de no haberla recibido, trabajarían en programación. Según representantes de múltiples universidades uruguayas (Universidad de la República, Universidad ORT), esto es un supuesto razonable, ya que hay muchos conocimientos compartidos entre programadores y profesionales en ciberseguridad. Nótese que este es un supuesto conservador para efectos del análisis económico, puesto que su implicación es que solo se contabilizan los beneficios marginales de la formación en ciberseguridad en vez de una formación en programación – no los beneficios absolutos de recibir la formación en comparación de no haberse formado en ningún tema.
* Se asume que los profesionales formados en ciberseguridad notrabajarán tiempo completo en la ciberseguridad. Este supuesto se basa en un hallazgo de la consultoría de Avnet que descubrió que la mayoría de los profesionales en ciberseguridad existentes en Uruguay solo dedican una porción de su tiempo a la ciberseguridad. Este hallazgo se comprobó mediante entrevistas con representantes del sector privado, incluido Deloitte y el Banco de la República Oriental de Uruguay. Para efectos de este análisis, se asume que los formados en ciberseguridad venderán el equivalente de 15 semanas completas (600 horas) de servicios de ciberseguridad al año. Parte de la motivación por este supuesto es la falta de desagregación por tipo de programa de formación en el análisis económico – no se separan proyecciones para egresados de programas de licenciaturas, maestrías o tecnicaturas.
* Según representantes de dos universidades uruguayas (Universidad de la República y ORT), el costo de impartir un curso en ciberseguridad es igual que un curso en una materia de ingeniería de sistemas u otro campo parecido, con lo cual no hay ningún costo incremental que se debe contabilizar del lado de la oferta de los programas de formación. Sin embargo, se asume que las instituciones educativas que participen en el Programa tendrán que incurrir algunos costos para poder ofrecer cursos de ciberseguridad. El análisis incluye tres tipos de costos no cubiertos por el Programa: capacitación docente, que el estudio Avnet calcula en US$112.800 para la oferta completa de cursos previstos, espacio de salas y tiempo docente. Se asume que los costos de capacitación docente se incurren en el 2021, y que los costos marginales de tiempo docente y uso de salas se incurren a partir del 2022.
* Según proyecciones del programa, el número de profesionales formados irá en aumento gradualmente. En el escenario base, se asume que se empezará a generar egresados especializados en ciberseguridad en 2022, con 50 (netos[[9]](#footnote-9)) ese año y 80 todos los años de ahí en adelante. Este supuesto, por el alto grado de incertidumbre, es el que se varía en el análisis de sensibilidad abajo. Se asume que en ausencia del proyecto el sistema educativo y las empresas privadas igual produciría profesionales en ciberseguridad, pero al ritmo más lento de 20 por año.
* Los beneficios que se contabilizan por año, entonces, son el resultado de la siguiente multiplicación: (diferencia en el precio por hora de venta de servicios de ciberseguridad versus servicios de programación)\*(600 horas)\*(# de personas formadas). Los beneficios son acumulativos, al asumir que las personas formadas en años pasados siguen vendiendo servicios de ciberseguridad durante todo el periodo analizado.
1. **Resultados y análisis de sensibilidad**
	1. El análisis contempla tres escenarios: un escenario base que utiliza los supuestos descritos más arriba, y un escenario conservador y uno optimista, que contiene las variaciones en supuestos clave descritas a continuación.

**Tabla 1. Parámetros del análisis de sensibilidad**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Beneficio** | **Supuesto** | **Escenario base** | **Escenario conservador** | **Escenario optimista** |
| Costos de remediación | % de los ataques que son de severidad alta o muy alta al final de la ejecución del proyecto | 1% | 1,5% | 0,5% |
| Impacto económico de los ciberataques | % del impacto económico evitado al final de la ejecución del proyecto | 30% | 20% | 40% |
| Actividad económica por formación de profesionales | # 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 |

El detalle de los cálculos de los resultados se encuentra en el archivo excel que acompaña este documento. El resumen por escenario se encuentra a continuación.

**Tabla 2. Resultados del análisis económico**

|  |  |  |  |
| --- | --- | --- | --- |
| **Escenario** | **Valor presente neto (US$)** | **Tasa interna de retorno** | **Razón beneficio-costo** |
| Base | 40.334.603.75  | 96% |  7,07  |
| Conservador  | 14.446.785.34  | 45% |  3,18  |
| Optimista | 72.818.040.28  | 165% |  11,96  |

1. **Conclusiones**

Puede afirmarse que el programa posee una alta rentabilidad económica. Aun en el escenario más conservador, se mantiene la rentabilidad, observando una razón beneficio-costo de 3,18 dólares por cada dólar invertido, con una TIR del 45% superior a la tasa del 12% establecida como estándar del Banco. Estos resultados reflejan la gran brecha en materia de ciberseguridad que el programa apunta reducir.

1. [Internet Crime Report](https://www.fbi.gov/news/stories/2017-internet-crime-report-released-050718). [↑](#footnote-ref-1)
2. [Crime Complaint Center](https://www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html). [↑](#footnote-ref-2)
3. [2017 *Cost of Cyber Crime Study*](https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017). [↑](#footnote-ref-3)
4. Esta cifra es conservadora considerando que una extrapolación de una estimación de CSIS y *McAfee* daría que el impacto total para Uruguay es de entre US$75-150 millones. Ver [página 7](https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf). Para esta extrapolación, se asume que Uruguay ocupa el 0,5% del PIB regional. [↑](#footnote-ref-4)
5. Ver [*Internet Crime Report 2016*](https://www.fbi.gov/news/stories/ic3-releases-2016-internet-crime-report) y [2017](https://www.fbi.gov/news/stories/2017-internet-crime-report-released-050718). [↑](#footnote-ref-5)
6. [*Cybersecurity: Are We Ready in Latin America and the Caribbean*?](https://publications.iadb.org/en/publication/17071/cybersecurity-are-we-ready-latin-america-and-caribbean); Ver [*Advanced Experiences in Cybersecurity Policies and Practices*](https://publications.iadb.org/publications/english/document/Advanced-Experiences-in-Cybersecurity-Policies-and-Practices-An-Overview-of-Estonia-Israel-South-Korea-and-the-United-States.pdf)*.* [↑](#footnote-ref-6)
7. [CUTI](http://www.cuti.org.uy). [↑](#footnote-ref-7)
8. [*Cybersecurity workforce study*, 2018](https://www.isc2.org/Research/Workforce-Study). [↑](#footnote-ref-8)
9. “Netos” se refiere al hecho que probablemente habrá personas que deserten la profesión de la ciberseguridad. Las cifras utilizadas, entonces, representan las personas formadas menos las personas que desertan. [↑](#footnote-ref-9)