Montevideo, 1 de noviembre de 2023

Mapeo sobre iniciativas y programas de creación de capacidades en el área de las TICs

Contenido

Estado de situación

Uruguay viene desarrollando desde 2020 un programa de "Fortalecimiento de la Ciberseguridad" liderado por Agesic, mediante el apoyo del Banco Interamericano de Desarrollo.

Este programa tiene como propósito fortalecer el ecosistema nacional de ciberseguridad, ampliando las capacidades de monitoreo y detección mejorando la prevención y las capacidades de respuesta, generando comunidades de práctica en el ecosistema público y privado, incorporando nuevos componentes y servicios de Identidad y Firma Digital, implantando un marco de ciberseguridad nacional y su respectiva regulación e impulsando la cantidad y la calidad de la formación de profesionales especializados.

Este último aspecto, hace hincapié en el desarrollo de las capacidades de Uruguay en temas de ciberseguridad, abarcando el conocimiento a nivel teórico y especialmente los aspectos de la práctica.

Es de importancia destacar que se han realizado distintos estudios con respecto a las necesidades, las capacidades, la cantidad de técnicos en el país, además de focus groups específicos con personas jóvenes de entre 17 y 22 años, y personas adultas de entre 33 y 47 años con la potencialidad de reconvertirse y especializarse en ciberseguridad.

El primer estudio se realizó en 2019/2020, elaborado por Agesic y KPMG, con la colaboración de DataSec[1], donde, se daba cuenta de que el país necesita aproximadamente 600 profesionales adicionales en ciberseguridad para poder dar respuesta a las necesidades. En él se observan como casi el 70% de las empresas de ciberseguridad del país intentaron contratar profesionales sin éxito y el 44% busca activamente. Se destaca también de la escasa oferta educativa especializada, con un enfoque excesivamente teórico donde el 55% de las empresas no logran satisfacer sus demandas en capacitación.

Luego de la pandemia COVID-19, se estima que estos números mínimamente se han duplicado.[2]

Con una comprensión amplia del estado de situación se han desarrollado distintas líneas de acción bajo la estrategia de impulsar la creación de capacidad y poder así reducir significativamente la brecha que existe tanto en el ámbito público como en el privado, por la falta de perfiles formados en seguridad de la información

[1] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/datos-y-estadisticas/estadisticas/informe-2020-ciberseguridad-uruguay
[2] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/ciberseguridad-uruguay-estadisticas-tendencias

Principales líneas de acción

Dar solución a estos temas requiere un enfoque sistémico y con la mayor cobertura posible, si entendemos la capacitación como una pirámide, donde en la base están los cursos más técnicos y básicos y en la punta las maestrías y doctorados, se trabajó en simultaneo en los distintos niveles. Para ampliar y consolidar la base de la pirámide se apuntó a desarrollar formaciones rápidas y técnicas. Al mismo tiempo, se impulsaron especializaciones/posgrados, con el fin de fortalecer la punta de la pirámide. En ambos casos, se procuró que la formación sea complementada con una herramienta que permita el ejercicio de los aspectos prácticos de la disciplina.

Líneas simultaneas y confluyentes fueron:

a) La elaboración de una **currícula de nivel técnico en ciberseguridad**, elaborada por la Universidad de la República (UdelaR), facultad de ingeniería (FING), donde la capacidad técnica y docente es excelente, consagrada hace ya varios años. La currícula resultante es abierta y se encuentra disponible para todas las instituciones del país que deseen implementarla.

b) El **soporte de la especialización y posgrado existente**, y el apoyo para aquellos que estaban en pleno proceso de gestación o recién nacidos, donde este soporte fue clave. Se otorgaron becas en la UdelaR/FING, en la Universidad ORT/Facultad de Ingeniería y en la reciente especialización dictada por la UTEC a través de un convenio con la Universidad Oberta de Catalunya – España.

c) **Publicación** en el sitio de Agesic de la **Oferta Educativa en Ciberseguridad** en el país. A través del contacto con el sector académico se recopilan los datos de todos los cursos y carreras existentes en la materia, así como la cantidad total de estudiantes y el porcentaje de mujeres que cursaron cada uno de ellos.

d) **Concientización y capacitación**: Se han continuado y fortalecido las acciones de concientización y sensibilización a través de la campaña de difusión Seguro te conectás. Se han desarrollado cursos virtuales y presenciales brindados por Agesic, también se ha trabajado en la capacitación a Docentes, así como en eventos u otras actividades con el fin de crear capacidades y buenas prácticas de ciberseguridad en la población.

e) La adquisición de una **herramienta de Cyber Range**, especializada para poder brindar entrenamientos prácticos a técnicos en ciberseguridad, simulando ambientes y ataques reales.

f) **Estudios y análisis de datos.** Para atender los distintos temas de Ciberseguridad sobre los que trabaja Agesic, se realizan estudios cualitativos y cuantitativas específicos, que permitan comprender mejor la situación seguridad informática y así poder definir mejores acciones.

Currícula y Carrera Técnica

En 2022 la agencia impulsó la primera curricula técnica en ciberseguridad del país, desarrollada con la Facultad de Ingeniería (Instituto de Computación) a través de la Fundación Julio Ricaldoni, con el apoyo del Banco Interamericano de Desarrollo (BID). La currícula es de acceso libre y flexible para que cualquier institución educativa del país pueda implementarla y complementarla, de acuerdo con su propuesta académica y la evolución de las necesidades del mercado. Asimismo, el enfoque de formación fue elaborado para posibilitar la continuidad en estudios de grado y posgrado.

La propuesta académica impulsada por Agesic y la Facultad de Ingeniería permite formarse o reconvertirse técnicamente en Ciberseguridad a las personas interesadas que hayan culminado segundo grado de enseñanza secundaria. El plan de estudios tiene una duración de 2 años para obtener el título de "*Técnico en Ciberseguridad*", con la posibilidad de cursar un tercer año de especialización con materias electivas para adquirir el título de "*Analista Técnico en Ciberseguridad*". La currícula es de acceso libre y flexible para que cualquier institución educativa del país pueda implementarla y complementarla de acuerdo con su propuesta académica y la evolución de las necesidades del mercado. Asimismo, el enfoque de formación fue elaborado para posibilitar la continuidad en estudios de grado y posgrado.

A principios del 2022 se realizó un estudio cualitativo de forma de comprender y caracterizar la demanda potencial para la formación en Ciberseguridad, este fue dirigido a jóvenes: para comprender el proceso de toma de decisiones, identificar barreras y facilitadores para la elección y a adultos para comprender los factores que intervienen en el proceso de elección de las distintas opciones de formación y su vínculo con el mercado laboral. Estos estudios se realizaron con mujeres y varones residentes de la capital de Uruguay, así como en otros departamentos del país, con edades comprendidas entre los 17 y 22 años y entre los 33 y 47 años. En ambos casos, se exploraron las representaciones simbólicas en torno a la ciberseguridad y se realizó un FODA con los elementos encontrados.

Análisis FODA comparado

También se llevaron a cabo instancias de trabajo con el sector académico y el de la industria de TI de país, para relevar las necesidades de ambos sectores.[3]

Con esa información sistematizada, se elaboró la Curricula técnica en Ciberseguridad[4].

KCS Challenge 23/24 Cybersecurity Skills

En colaboración con la Universidad Tecnológica de Uruguay (UTEC) y a partir del interés compartido y las necesidades en el territorio, Agesic está impulsando un proyecto para llevar adelante desafíos que buscan promover el desarrollo de habilidades digitales avanzadas en ciberseguridad a estudiantes universitarios, y soluciones digitales para desarrollar habilidades digitales básicas en ciberseguridad a estudiantes de educación media y básica.

Este desafío busca la sinergia entre instituciones públicas educativas, universidad, sector productivo y sector digital, es que este desafío KCS (Servicio centrado en los conocimientos) tiene como objetivos:

- Promover la experiencia y el aprendizaje práctico, brindando a los estudiantes la oportunidad de aplicar sus conocimientos y habilidades digitales en ciberseguridad en proyectos concretos que colaboren a solucionar problemas reales.

- Fomentar la colaboración entre estudiantes, instituciones educativas, el sector digital y el sector productivo, con el fin de fortalecer y expandir la comunidad digital en el país.

[3] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/proposito-fortalecer-curricula-ciberseguridad

[4] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/se-lanzo-primera-curricula-tecnica-ciberseguridad-del-pais

Especialización y Posgrados en Ciberseguridad (becas)

Asimismo, en 2022 se implementó el Programa de Becas de Especialización en Ciberseguridad una iniciativa impulsada por Agesic a través de la Fundación Julio Ricaldoni (FJR), con el fin de promover la formación y el desarrollo de capacidades locales en temas de ciberseguridad. Estas se orientaron a todas aquellas personas que tengan interés en formarse o perfeccionarse en esta disciplina. Este programa también se lleva adelante con el apoyo del Banco Interamericano de Desarrollo (BID), en el marco del Proyecto de Fortalecimiento de la Ciberseguridad en Uruguay.[5]

Se otorgaron hasta 38 becas en total, en dos ediciones 2022/2023, en ofertas de cursos y posgrados en temas de Ciberseguridad que dictan la Facultad de Ingeniería de la Universidad de la República (FING-Udelar) y la Facultad de Ingeniería de la Universidad ORT Uruguay, y se espera continuar en el 2024, las postulaciones son evaluadas por un comité integrado por profesionales de cada organización.

Para su evaluación se están realizando encuestas anónimas y estudios cualitativos a los becarios del programa para:

- Comprender el proceso de toma de decisiones en la elección de la formación en ciberseguridad
- Comprender representaciones simbólicas del mercado laboral
- Indagar acercade la relación entre la formación y empleo
- Aplicabilidad de los conocimientos de la formación en el empleo actual
- Identificar posibles diferencias de género percibidas en la universidad y en el empleo

Reciente se otorgaron, también, becas para la especialización/posgrado dictado por la UTEC a través de un convenio con la Universidad Oberta de Catalunya – España.

[5] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/2a-edicion-del-programa-becas-especializacion-ciberseguridad

Oferta educativa en Ciberseguridad en el país.

Uno de los mayores desafíos que se enfrentan a nivel mundial es la falta de profesionales y personal técnico calificados en ciberseguridad. En el marco del 10º objetivo de la Agenda Digital Uruguay 2025, Agesic trabaja con distintos actores del ecosistema con la finalidad de apoyar el desarrollo de la ciberseguridad en los diferentes centros educativos del país, así como también promover el desarrollo de una red de especialistas a nivel nacional que incorpore a todos las personas involucradas.

Desde el año 2021 se pública en el sitio de Agesic un desglose genérico de la oferta educativa de nuestro país en materia de ciberseguridad, incluyendo instituciones educativas públicas y privadas, con los enlaces de acceso a cada institución/curso. Esta información disponible en un único punto facilita sustancialmente la toma de decisión por quienes se interesan en formarse en la materia.

La evolución anual de participación por institución educativa es muy prometedora y enriquecedora, permitiendo monitorear distintas aristas como lo son; ingresos vs egresos, participación por edad, género, a modo de ejemplo, y definir acciones en base a estas.

Esto nos ha permitido observar un descenso de estudiantes durante la pandemia COVID-19, con un fuerte repunte tras ella y trabajar sobre ofertas ajustadas a las necesidades de la industria y la academia. Como ya se mencionó en este informe, la implementación de la currícula de ciberseguridad en la Universidad Técnica del Uruguay ha marcado un hito en la formación en Ciberseguridad, con más de 700 inscripciones viables para esta primera edición, la cual al igual que la Especialización/posgrado en la UTEC con la Universidad Oberta de Catalunya, se proyecta que siga impulsando el ecosistema en los siguientes años.

Concientización, cursos, capacitaciones y eventos brindados por Agesic

Con el objetivo de fortalecer las habilidades necesarias para el uso seguro de la tecnología y el ecosistema nacional de ciberseguridad, desde Agesic se han organizado y apoyado diversas actividades de capacitación y difusión sobre temáticas de ciberseguridad.

Seguro te conectás

Seguro te conectás es una campaña de difusión creada en 2014, con el objetivo de sensibilizar sobre el uso responsable de internet, mediante recomendaciones y buenas prácticas, así como educar acerca de los riesgos existentes y brindar la información necesaria para la adopción de comportamientos seguros en el uso de la tecnología.
La campaña Seguro te conectas está basada en la propuesta "***Stop think connect***". Con foco inicialmente en la población, utiliza mensajes positivos, lenguaje simple, común, sin estigmatizaciones.

Digitalización segura

En la misma línea de Seguro te Conectás, se promueve la digitalización segura de la ciudadanía, realizando distintas acciones de sensibilización y comunicación para fortalecer el uso seguro y responsable de la tecnología por parte de las personas realizando contenidos y charlas de buenas prácticas y vídeos como ¿Qué es la Ciberseguridad? y ¿Por qué estudiar y trabajar en Ciberseguridad? ambos disponibles en el canal de Agesic en YouTube.

Por otra parte, desde Agesic se colabora con otras instituciones y organizaciones para que más personas se interesen por las disciplinas Ciencias, Tecnología, Ingeniería y Matemáticas (STEM, por su sigla en inglés).

Cursos técnicos de Ciberseguridad

Se dictaron cursos técnicos de ciberseguridad, que se entendían necesarios para la comunidad gobierno del país:

Curso	Carga horaria	Participantes	Mujeres
Desarrollo Seguro de Software (2)	40	60	13
Evaluación de Seguridad (1)	30	24	8
Análisis Forense Digital (1)	40	28	8

Se impulsó la capacitación para docentes de UTU y de esa forma lograr poner en funcionamiento la primera implementación de la currícula Técnica de Ciberseguridad, apoyando con especializaciones/posgrados de la UdelaR/FING y en la UTEC, así

como con los cursos dictados por AGESIC, alcanzando en el 2023 un total de 20 docentes capacitados.

Capacitaciones

Durante el 2022[6] se dictaron 10 instancias de capacitación, 8 fueron de cursos de concientización sobre seguridad de la información y las mejores prácticas que se pueden adoptar en el ámbito laboral y personal. Además, se incorporaron capacitaciones en la plataforma Educantel de Antel, con alcance a toda la ciudadanía

También se dictaron charlas informativas destinadas a organismos públicos y a la ciudadanía en general, sobre buenas prácticas en seguridad de la información, identificación digital, firma digital y sobre el Marco de Ciberseguridad en las que participaron 1880 personas.

Eventos

Agesic apoyó en 2021 y 2022 la iniciativa del OEA Cyberwomen Challenge, desafío que busca disminuir la disparidad de género en la industria tecnológica, particularmente en el área de ciberseguridad. Este año la iniciativa organizada por la Organización de Estados Americanos (OEA) y el Comité Interamericano Contra el Terrorismo (CICTE), con el apoyo de Agesic y el Estado Mayor de la Defensa (ESMADE), será bajo el nombre SheSecures, con el fin de brindar a las mujeres una forma divertida y práctica de fortalecer sus habilidades técnicas a través de ejercicios virtuales de ciberseguridad.

[6]Los datos de capacitaciones presentados corresponden a año 2022, y serán actualizados a diciembre de este año. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/iniciativas-ciberseguridad-impulsadas-durante-2022

Cyber Range

Este año se realizó el primer entrenamiento de ciberseguridad que consiste en una simulación de ataque cibernético para la detección y respuesta a un incidente en tiempo real. El mismo se realizó en la plataforma Cyber Range de Agesic en la Facultad de Ingeniería de ORT y fue dictado por OWASP UY. Esta iniciativa se enmarca en el fortalecimiento del ecosistema de conocimiento en ciberseguridad,con el objetivo de potenciar el uso de tecnología avanzada en la formación académica.

La actividad fue abierta y convocada por OWASP UY donde participaron personas técnicas interesadas en temas de ciberseguridad, simulando escenarios reales y controlados, que habiliten su preparación ante ataques reales. También se realizaron entrenamientos internos para integrantes del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) y para distintas comunidades de especialistas técnicos de la comunidad de ciberseguridad del país.

Se planean se dictarán otros entrenamientos abiertos, dirigidos a personas con conocimientos en Tecnologías de la Información y las Comunicaciones (TIC) que deseen entrenar sus habilidades en ciberseguridad, lo que totalizara cerca de 100 especialistas técnicos entrenados durante el 2023.

Estudio y análisis de datos

Conocer cómo se comporta el mercado permite potenciar y brindar apoyo a la industria de las Tecnologías de la Información -en pleno crecimiento económico- logrando transformar al país no solo en un centro de referencia sino también en un ejemplo de la colaboración público - privada en la materia.

Informe 2020: Ciberseguridad en Uruguay

El objetivo de este estudio fue de analizar la situación del desarrollo de la seguridad de la información en Uruguay, fundamentalmente el mercado laboral, la demanda de servicios, las tendencias y los principales desafíos que enfrenta el sector. Asimismo, este estudio incluyo grandes esfuerzos en investigación con el objetivo de comparar los hallazgos encontrados con los análisis de otros estudios locales, regionales y globales reconocidos en búsqueda de las principales tendencias en la temática

Informe Ciberseguridad: empresas y sector público 2021

Desde Agesic se ha definido trabajar en una medición de línea base sobre la situación de la ciberseguridad en Uruguay que permita a mediano plazo analizar en profundidad algunos datos que hoy son presentados de forma descriptiva. El estudio sobre “Ciberseguridad: empresas y sector público" se realizó durante el 2021 y releva información de empresas, instituciones de salud y sector público.

Estudio Cualitativo: Caracterización de la demanda de formación en Ciberseguridad

Este estudio se enfocó en comprender y caracterizar la demanda potencial para la formación en Ciberseguridad.