mujeres y ciberseguridad en Uruguay

Experiencias, desafíos y oportunidades desde una mirada de género

nómade
comunidad consultora

Mujeres y ciberseguridad
Informe de investigación cualitativa

©2025, PNUD Uruguay

Informe a cargo de nómade.

Equipo técnico nómade:
Victoria Faroppa, Laura Rivero, Mariela Moreno, Florencia Roldán, Roberta Aller.

Diseño: nómade, comunidad consultora

Supervisión PNUD:
Sabrina Rodríguez, Magdalena Preve

En caso de citar el documento:
Programa de las Naciones Unidas para el Desarrollo Uruguay. (2025). Mujeres en ciberseguridad: Trayectorias, barreras y oportunidades desde una mirada situada. Elaborado por Nómade.

Este informe es el resultado de la consultoría de investigación cualitativa desarrollada por nómade, comunidad consultora, para el Programa de las Naciones Unidas para el Desarrollo (PNUD) en Uruguay.

Según las normas aplicadas por el PNUD en todo el mundo, los autores y autoras de estas investigaciones gozan de completa independencia editorial, y aplican criterios de objetividad e imparcialidad en sus análisis.

El análisis, los puntos de vista y las recomendaciones presentadas en este informe no reflejan necesariamente la postura oficial del PNUD. Se agradece la difusión y reproducción en cualquier medio, con indicación de la fuente.

mujeres y ciberseguridad en Uruguay

Experiencias, desafíos y oportunidades desde una mirada de género

Índice

1. Objetivo general de la consultoría **06**

1.1 Objetivos Específicos 07

2. Grupos Focales **09**

Grupos focales online 10
2.1. Segmentación 11
2.2 Estrategias de reclutamiento implementadas 11
2.3 Pautas de indagación 13
2.4 Campo 13

3. Principales Resultados de los Grupos Focales **14**

3.1 Mujeres en ciberseguridad: perfiles participantes 15
3.2 Llegada y aterrizaje en el mundo ciber 16
3.3 Algunas demandas iniciales en el sector 23
3.4 Formación en Ciberseguridad 28
3.5 Brechas invisibles y visibles: los sesgos de género en ciberseguridad 30
3.5.1 Brechas “invisibles” 35
3.5.2 Brechas “visibles” 40
3.6 Características de las personas que se dedican a la ciberseguridad 50
3.6.1 Facilitadores para la elección y permanencia en el sector 52
3.6.2 Cuadro final resumen 54

Entrevistas **56**

4.1 Ejecución de campo 57
4.2 Segmentación y perfiles 57
4.3 Estrategias de reclutamiento implementadas 59
4.4 Pauta de indagación 60

5. Principales resultados de las entrevistas **61**

5.1. Barreras y habilitadores que afectan la inserción y el desarrollo profesional de las mujeres en Ciberseguridad 63
5.2 Experiencias y buenas prácticas para la inclusión de mujeres 71
5.3 Referentes femeninas: importancia, obstáculos y visibilidad 74

6. Mapas de acción **78**

6.1 Principales conclusiones 79
6.2 Recomendaciones 83
6.3 Oportunidades estratégicas 85

Referencias Bibliográficas **88**

Anexos **91**

8.1 Diagnóstico de la ciberseguridad en Uruguay 92
8.1.1 Ámbito de la educación, formación y desarrollo de talento 101

1.

Objetivo general de la consultoría

El objetivo general de la consultoría consistió en realizar un diagnóstico en Uruguay para identificar barreras y habilitantes que enfrentan las mujeres a lo largo de su vida en su inserción y participación en el sector ciberseguridad.

El estudio analiza factores estructurales, sociales, culturales y económicos que limitan su acceso y desarrollo en este sector, así como oportunidades. Además, en el capítulo final de mapas de acción, se proponen algunas estrategias concretas para superar estas barreras y fomentar la equidad de género, contribuyendo a una mayor participación de las mujeres en el ámbito de la ciberseguridad.

1.1 Objetivos Específicos

- Comprender los caminos de acceso de las mujeres al sector de la ciberseguridad, identificando las principales motivaciones que las impulsan a ingresar en esta área.

- Indagar en sus trayectorias educativas y profesionales, analizando los procesos formativos y las decisiones laborales que han influido en su desarrollo dentro del sector.

- Investigar y analizar las barreras y facilitadores presentes en ambos procesos —educativo y profesional—, con especial atención a aquellas limitaciones que responden a estructuras sociales, simbólicas o culturales relacionadas con su condición de género.

Para alcanzar con los objetivos planteados se propuso un abordaje cualitativo a través de la implementación de entrevistas en profundidad a actores claves, y grupos focales con mujeres y varones que trabajan y tienen formación en el área.

El enfoque cualitativo se adhiere a un paradigma interpretativo, donde la interpretación de quien investiga juega un rol esencial respecto a la obtención de información acorde a las valoraciones y percepciones de los sujetos involucrados, es decir: "(...) la investigación cualitativa proporciona profundidad a los datos, dispersión, riqueza interpretativa, contextualización del ambiente o entorno, detalles y experiencias únicas. Asimismo, aporta un punto de vista fresco, natural y holístico de los fenómenos, así como flexibilidad." (Hernández Sampieri, 2014, p. 16).

Asimismo, habilita a quien investiga a comprender y desentrañar los imaginarios que permean y las valoraciones que emergen en los procesos de interacción social, a través del discurso de los y las entrevistadas.

2.

Grupos Focales

La técnica de grupos focales se centra en el abordaje de ejes temáticos a partir de la utilización de una pauta (guía) de preguntas, generalmente distribuidas por módulos, que responden a la medición de ciertas dimensiones de acuerdo con al menos uno de los objetivos específicos de la investigación (Sandoval Casilimas, 1996).

Autores como Marradi, Archenti y Piovani (2007) fundamentan que los grupos son una técnica pertinente para acceder a discursos sociales, ya que, al generarse una instancia de intercambio como producto de la comunicación sostenida entre participantes, pueden surgir temáticas que no estaban previstas. La principal riqueza de la técnica reside en la reformulación de los significados que se produce en la dinámica grupal, no persiguiendo la representatividad estadística pero sí una "representación tipológica, socio-estructural, de acuerdo con los objetivos del estudio" (Flacso, 2018).

También permiten recabar información a través de un proceso deliberativo, dinámico, flexible y no lineal, que posibilita contemplar las emergencias y contingencias propias del objeto de la investigación.

Grupos focales online

Los grupos online no solo hacen posible una participación más **inclusiva y heterogénea** al eliminar barreras de distancia y movilidad, sino que son especialmente ventajosos para **mujeres con múltiples responsabilidades de cuidado**. Esto se debe a que les permiten asistir **sin que les demande demasiado tiempo de sus otras tareas**.

Los grupos se realizaron a través de la plataforma zoom, y tuvieron una duración aproximada de 2 horas.

2.1. Segmentación

La segmentación finamente realizada de los GF fue la siguiente:

n°	Ficha técnica	
1	**Mujeres profesionales en ciberseguridad (Senior).**	Ocupando puestos de liderazgo. Con personal a cargo.
2	**Mujeres profesionales en ciberseguridad (Junior).**	Ocupando roles iniciales o intermedios. Sin personal a cargo.
3	**Estudiantes mujeres de carreras relacionadas con ciberseguridad.**	Diferentes subsistemas y niveles de formación: UTU, Universidades Públicas y Privadas.
4	**Hombres profesionales en ciberseguridad.**	Pertenecientes al ámbito público y privado.

2.2 Estrategias de reclutamiento implementadas

Con el objetivo de alcanzar perfiles relevantes y diversos para la participación en los grupos focales, se desarrollaron múltiples estrategias de captación, entre las cuales se destacan:

- **Cuestionario de relevamiento en redes sociales:** Se diseñó e implementó un breve cuestionario con el fin de identificar personas vinculadas directa o indirectamente al ámbito de la ciberseguridad.

Bajo el mensaje “¿Estás o estuviste vinculado/a a áreas conectadas con la ciberseguridad? ¡Queremos saber de vos!”, el formulario fue difundido a través de redes sociales y permaneció activo durante tres semanas. A partir de esta iniciativa se identificaron múltiples perfiles, los cuales fueron considerados para el proceso de selección.

- **Contactos provistos por la contraparte institucional:** Se recibieron y sistematizaron contactos sugeridos por la contraparte del proyecto, con la previa autorización de la persona invitada al estudio. Esta base de datos fue integrada al proceso de reclutamiento.

- **Base de datos de nómade consultora:** Se utilizó una base de contactos previamente elaborada por la consultora, con perfiles vinculados a la temática abordada.

- **Estrategia de bola de nieve:** Se aplicó esta técnica de forma dirigida, a partir de contactos calificados que facilitaron nuevas referencias dentro del universo de interés.

- **Difusión en redes especializadas:** Se promovió la convocatoria en espacios digitales estratégicos tales como LinkedIn, grupos de WhatsApp profesionales, sitios y contactos institucionales de facultades y organizaciones conectadas, entre otros canales pertinentes.

- **Asistencia a eventos vinculados** a la tecnología y ciberseguridad en busca de personas referentes.

2.3 Pautas de indagación

Las pautas de indagación desarrolladas para los grupos focales se estructuraron en función de los perfiles de las personas que participaron y sus respectivas áreas de vinculación con la ciberseguridad. Se encuentran disponibles en los siguientes links de acceso:

1. Mujeres profesionales en ciberseguridad (Senior)
2. Mujeres profesionales en ciberseguridad (Junior)
3. Estudiantes mujeres de carreras relacionadas con ciberseguridad
4. Hombres profesionales en ciberseguridad

2.4 Campo

El campo de implementación de los grupos focales se realizó entre el 26 de marzo y el 4 de abril de 2025.

3.

Principales Resultados de los Grupos Focales

3.1 Mujeres en ciberseguridad: perfiles participantes

Las participantes de los grupos provienen de una amplia y diversa gama de campos profesionales, reflejando la riqueza de trayectorias que confluyen en este ámbito. Entre ellas se encuentran ingenieras en sistemas y telecomunicaciones, analistas de sistemas, especialistas en relaciones laborales, profesionales del área jurídica, profesionales de la salud, miembros de la Armada Nacional, administradoras de empresas, economistas, matemáticas, entre las principales. Si bien la mayoría de estas mujeres provienen de formaciones disciplinarias vinculadas a las STEM, no es una condición excluyente, y este cruce de saberes enriquece profundamente las conversaciones. Algunas de las participantes han llegado a la ciberseguridad tras un giro radical en su recorrido profesional. Es el caso de quienes dejaron atrás carreras consolidadas —por ejemplo, en economía o administración de empresas— o provenían de campos disciplinarios, en principio, muy poco conectados a la ciberseguridad (como la salud) para reconvertirse y abrirse camino en un nuevo campo que las desafía e interpela desde otros lugares. Esta diversidad de orígenes demuestra que la ciberseguridad puede ser un destino compartido para quienes, desde distintos puntos de partida, deciden explorar su potencial en un sector que se visualiza como muy dinámico y en constante transformación.

Cuadro de campos disciplinarios "de origen" de las mujeres que participaron en los grupos focales

Carreras de origen	Número de participantes
STEM	13
Ciencias sociales	6
Ciencias de la salud	1
Sector público	1

3.2 Llegada y aterrizaje en el mundo ciber

Tanto las participantes mujeres como los varones entrevistados coinciden en señalar que su llegada al ámbito de la ciberseguridad ha sido, en la mayoría de los casos, resultado de decisiones fortuitas, más que de una elección plenamente consciente, planificada e informada. Varias de ellas expresan esta experiencia con frases como:

"(...) yo caí de forma fortuita en la ciberseguridad. Soy una outsider total, fui aprendiendo con mentores en la organización, hasta que me fui a hacer cursos porque fui avanzando en el área y necesitaba formarme" Mujer Junior.

“(...) yo no busqué la ciberseguridad, la ciberseguridad me buscó a mí, se me cruzó en el camino”

Mujer Senior.

"(...) yo también caí por las vueltas de la vida, soy abogada y terminé trabajando en un estudio con el tema de propiedad intelectual. Y como teníamos muchos clientes de tecnología descubrí el tema (...)" Mujer Junior.

"(...) nunca me planteé en ningún punto de mi carrera estudiar Ciberseguridad. Si me gustó siempre 'encontrar errores' y trabajé mucho en Testing. Pero a la ciberseguridad llegué como un requerimiento de mi trabajo" Mujer Senior.

"(...) yo lo viví trabajando en la industria cárnica. Llegas muchas veces por requerimiento de los trabajos, por trabajar en compañías internacionales, por ejemplo. A nosotros nos exigían desde el exterior un montón de controles entre los que estaba seguridad de los datos" Mujer Senior.

"(...) yo también llegué porque trabajaba en un laboratorio, y hacían mucha investigación y el tema de la seguridad siempre estuvo sobre la mesa, más allá de la seguridad de la información, porque tenían productos protegidos por patente" Mujer Senior.

"(...) para mí también fue muy lateral el camino, fue apareciendo el tema de la ciberseguridad, trabajaba en financiera, primero en la parte de infraestructura". Mujer Senior.

Para las personas entrevistadas, tanto varones como mujeres, la difusión en torno al campo de la ciberseguridad ha sido hasta el momento sumamente limitada. Aspectos fundamentales como los programas de formación disponibles, las características específicas del área, las funciones que desempeñan los profesionales, los entornos laborales posibles y las rutas de desarrollo profesional han carecido de visibilidad.

"(...) yo dejé en un momento de estudiar, me frustré mucho. No sabía bien por dónde seguir. Es una carrera muy nueva, que tiene muchas aristas y no sabes muchas veces para donde orientarte". Mujer Junior.

En consecuencia, su acercamiento a la disciplina ha sido mayormente intuitivo: un recorrido construido a partir de la propia exploración e interés personal, más que guiado por una hoja de ruta clara o un plan formativo previamente establecido.

"(...) es una carrera nueva, desafiante, cuesta arriba por momentos sobre todo para estas primeras generaciones" Mujer Junior.

Sin embargo todos acuerdan que esta realidad está comenzando a cambiar. En la actualidad, se observa un mayor interés y una mejor difusión, con un crecimiento notable en la oferta de cursos especializados, programas académicos, certificaciones, así como una mayor presencia de contenidos relacionados en medios digitales, redes sociales y eventos especializados. Asimismo, la relevancia creciente de la profesión ha generado una mayor demanda de profesionales en el área y una mayor concientización por parte de las empresas respecto a su importancia. Esta evolución sin dudas va a terminar contribuyendo a una elección más consciente y fundamentada de la ciberseguridad como opción profesional para generaciones venideras.

“(...) ahora hay muchísima más oferta educativa, por suerte, aunque esta área siempre tuvo y va a seguir teniendo un fuerte componente autodidacta”

Mujer Senior.

Sin embargo para las actuales profesionales en el área, el ingreso a este campo estuvo fuertemente motivado por requerimientos específicos de las organizaciones en las que trabajan o trabajaban, especialmente en sectores como el financiero o aquellos que gestionan grandes volúmenes de datos o información confidencial que requiere protección.

Se menciona, a su vez, que en ciertos casos la aproximación a la ciberseguridad se dio a raíz de **incidentes concretos**, como intentos de ciberataques o robos de información. Sin embargo, estos casos son excepcionales. De forma predominante, la incorporación al campo responde a necesidades organizacionales.

Posteriormente, y en la medida que las personas comienzan a profundizar en la temática, suelen desarrollar un fuerte interés, compromiso e incluso pasión por el área.

En otros relatos también se identificaron trayectorias de llegada marcadas por una **fuerte motivación de reconversión laboral**, donde la elección de incursionar en el ámbito de la ciberseguridad se vinculó con momentos cruciales en la vida de las participantes. En estos casos, la decisión de reorientar su carrera estuvo atravesada por cuestionamientos personales y búsquedas de nuevos rumbos que

combinaran desafíos profesionales con condiciones laborales que facilitaran la conciliación con las responsabilidades de maternidad y cuidado, tradicionalmente atribuidas a las mujeres.

Algunas mujeres relataron que su acercamiento al campo de la ciberseguridad estuvo influido por la planificación de un embarazo o la reciente asunción de responsabilidades de cuidado. En ese contexto, identificaron en este sector una oportunidad para desempeñarse profesionalmente en un entorno que, percibido como flexible o adaptable, les permitiría conciliar sus nuevos roles familiares con su desarrollo laboral.

Así, la ciberseguridad fue interpretada no sólo como un campo profesional desafiante e innovador, sino también como un espacio posible para hacer efectiva una demanda emergente: la **búsqueda de equilibrios entre vida personal, maternidad y proyección profesional.**

"(...) yo trabajé muchos años en Telecomunicaciones, en la parte de telefonía celular. Un tiempo en comercial, otra en técnico. Pero era en un momento un trabajo de muchas horas y monótono. Me aburrí. Llegué a los 40 años y quería tener un hijo. Me empecé a replantear mi carrera. Y llegué por casualidad en un trabajo que tomé, a la parte de ciberseguridad. Había muchos riesgos en ese trabajo porque manejaban mucha información biométrica, y existía una necesidad y una carencia de seguridad de los datos. Empecé a trabajar con eso, después me fui a hacer un posgrado. Y estoy super contenta con este trabajo" Mujer Junior.

“(...) yo quería una salida laboral que me permitiera estar más con mi hija, tener la posibilidad de acceder a un trabajo remoto”

Mujer estudiante de ciberseguridad.

3.3 Algunas demandas iniciales en el sector

Se menciona que el ingreso al sector de la ciberseguridad, a su vez, exige de quienes se desempeñan en esta área una serie de características personales que, posteriormente, serán tematizadas como posibles obstáculos o habilitadores para el desarrollo profesional de las mujeres en el sector. Entre los aspectos más mencionados, se destaca la **constante necesidad de formación continua**, propia de un ámbito altamente dinámico y en permanente evolución.

"(...) la formación es compleja, demanda formación continua y buena parte tenes que ser autodidacta" Mujer junior.

Asimismo, se subraya la importancia de contar con ciertas **cualidades personales**, como la tolerancia a la frustración y al error, la curiosidad, la capacidad de investigación, y una marcada habilidad para la autoformación. En este sentido, varias personas entrevistadas coinciden en señalar que "hay mucho de autodidacta en este rubro".

"a veces tenes que decir: 'Si yo me voy a poner a llorar cada vez que me dicen algo feo o algo que no me gusta...'. Tenés que tener una capacidad también como de indagatoria, ¿entendés? Como ir por tu cuenta y saber cómo moverte" Mujer junior.

"(...) tener claro el hacia dónde querés llegar y no dejar que comentarios te machaquen" Mujer estudiante de ciberseguridad.

Aunque algunas de estas capacidades tienden a ser relacionadas socialmente con el género femenino, la mayoría son percibidas como más afines al género masculino. Esta percepción puede incidir en la forma en que se construyen las trayectorias profesionales en el sector, así como en los obstáculos simbólicos y culturales que enfrentan las mujeres para insertarse y desarrollarse en él.

En esta línea, emergen testimonios que reproducen ciertas construcciones de género en relación con las formas de aproximación al conocimiento y al riesgo. Algunas participantes afirman, por ejemplo:

"(...) las mujeres somos muy curiosas, pero tenemos menos tolerancia al error y a la experimentación. Los hombres son más de lanzarse, más arriesgados y no tienen tanto miedo a la falla y al error. Las mujeres, como que tenemos que saber todo antes de largarnos a hacer algo; tenemos menos tolerancia a fallar y a arriesgar" Mujer junior.

Estas representaciones revelan la existencia de patrones culturales que pueden influir en la autopercepción de las mujeres frente a los desafíos del rubro y en su disposición a asumir riesgos en entornos tecnológicos aún percibidos como predominantemente masculinos.

En este sentido, se menciona en más de una ocasión el "**miedo**" que algunas sintieron al ingresar al área, especialmente por temor a fallar o a no estar a la altura de las exigencias del sector. La exposición constante a situaciones de vulnerabilidad y la necesidad de ofrecer respuestas efectivas ante éstas demanda un alto nivel de responsabilidad.

"(...) terminé al mando del mayor proyecto de seguridad de los datos que había habido en el Banco con mucho susto. No sabía si iba a ser capaz de comandarlo" Mujer Senior.

"(...) si sos una persona muy sensible que todo te afecta te va a costar adaptarte al ambiente un montón" Mujer Senior.

Además, muchas entrevistadas señalan que el entorno de trabajo en ciberseguridad implica enfrentarse constantemente a altos niveles de autoexigencia. Según ellas, esta autoexigencia es más difícil de manejar para las mujeres que para los varones, lo que puede generar más ansiedad, presión y sentimientos de insuficiencia.

Esta menor percepción de autoeficacia[1] en mujeres se vincula con normas de género tradicionales (actitudes y expectativas sobre los roles, comportamientos y responsabilidades apropiadas para hombres y mujeres) y entornos masculinizados (como el campo de las STEM), que tienden a reforzar la idea de que las mujeres tienen menor competencia en áreas técnicas. Diversos estudios muestran que, aun con desempeños similares, las mujeres tienden a subestimar sus capacidades en estos campos y tienen menores expectativas de rendimiento, lo que impacta en su interés y en sus aspiraciones educativas y laborales. Esta brecha en la autopercepción de eficacia contribuye a perpetuar la subrepresentación femenina en sectores como la tecnología y la ciberseguridad (Chan, 2022).

1. Las capacidades percibidas para aprender o desempeñarse bien en un campo específico (Chan, 2022).

"(...) las mujeres estamos formateadas para estar 100% capacitadas y seguras para enfrentarnos a desafíos. Los hombres no. Con un 40% de los que tienen que saber y de lo que saben las mujeres se tiran al agua y se creen expertos" Mujer Senior.

"(...) nos tiramos para abajo y nos autolimitamos" Mujer Senior.

Tanto mujeres como varones coincidieron en señalar que el **imaginario social en torno a la figura del profesional en ciberseguridad sigue estando fuertemente masculinizado**. Predomina la representación de un hombre altamente calificado que desempeña tareas complejas, muy difíciles y técnicas, lo cual refuerza la percepción de que se trata de un campo de difícil acceso. Este estereotipo actúa, en muchos casos, como una barrera simbólica para las mujeres, que pueden no sentirse suficientemente capacitadas o legitimadas para ingresar o desarrollarse en esta área.

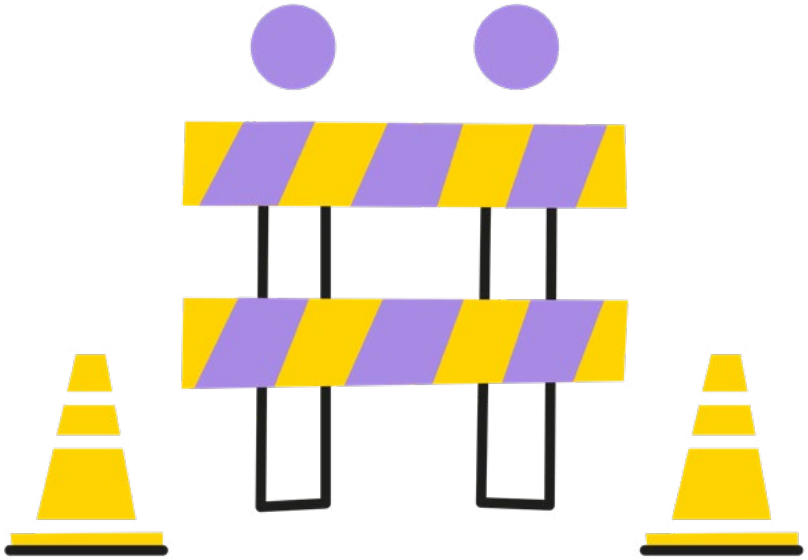
Desde el inicio del proceso de exploración de la ciberseguridad como un campo profesional posible, surgieron de manera recurrente tanto habilitadores como barreras que condicionan el acceso y la permanencia de las mujeres en este ámbito. Estas dimensiones, expresadas de forma explícita o implícita en los distintos relatos, se encuentran estrechamente vinculadas a su condición de género.

“(...) los lugares de trabajo y estudio están llenos de hombres, y si sos mujer te podés sentir intimidada o incómoda”

Mujer Junior.

A continuación, se resumen dichos aspectos en el siguiente cuadro:

Factores asociados al inicio y aterrizaje en la ciberseguridad	
Barreras	
Escaso conocimiento y difusión de la formación y el trabajo en el área	Falta información sobre funciones que desempeñan los profesionales, los entornos laborales posibles y las rutas de desarrollo profesional, áreas y lugares de estudio y formación, etc.
Exigencias de la profesión	Formación continua. Demanda tiempo.
Cualidades proyectadas a los profesionales del rubro	Tolerancia al error, y a la frustración. Autoexigencia. Motivación a la experimentación. Imaginario social: hombre, hacker, muy inteligente y capaz. Área laboral asociada a mucha complejidad: matemática, tecnología, etc.
Habilitadores	
Desarrollo profesional y/o reconversión laboral	Flexibilidad: permite una mayor conciliación entre maternidad y trabajo, favoreciendo un mejor equilibrio entre la vida personal y la proyección profesional.
Cualidades proyectadas a los profesionales del rubro	Curiosidad, motivación a la investigación teórica.



3.4 Formación en Ciberseguridad

Todas las mujeres que actualmente se desempeñan en el área de ciberseguridad cuentan con formación específica en la temática, adquirida tanto a nivel nacional como internacional. Se mencionan diversas instancias de capacitación, que incluyen cursos de especialización, posgrados, maestrías, doctorados, así como certificaciones internacionales reconocidas en el rubro. Entre las instituciones más destacadas aparecen UNIT, UTU, UTEC, Agesic, la Facultad de Ingeniería de la Universidad de la República, la Universidad ORT, la Universidad de Montevideo y la Universidad Católica del Uruguay, Fundación Telefónica, así como centros internacionales como la Universidad Europea de España y organismos de certificación como ISACA, entre otros.

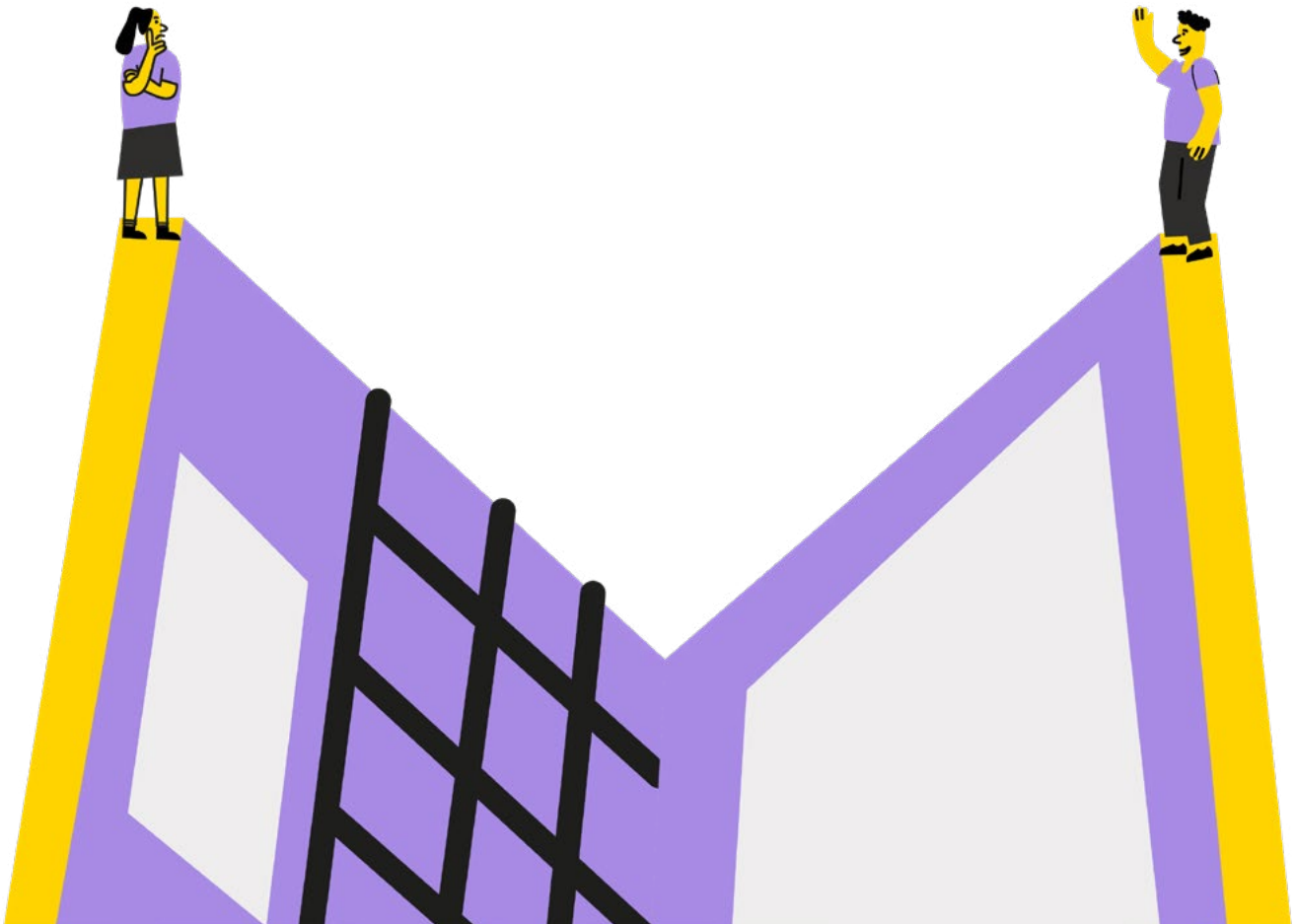
Las participantes resaltan que la oferta formativa en ciberseguridad ha experimentado un crecimiento significativo en los últimos años. En comparación con el panorama de hace una década, el cambio ha sido notorio, tanto en términos de cantidad como de diversidad de propuestas.

Actualmente, se observa que ha comenzado a ampliarse el acceso a la formación en el área de ciberseguridad, permitiendo el ingreso de profesionales provenientes de disciplinas diversas y no exclusivamente de las denominadas STEM. De esta manera, se reconoce cada vez más que las mujeres pueden incorporarse a estudios en ciberseguridad, aun cuando su formación previa no esté vinculada a los campos científico-tecnológicos.

Sin embargo, se percibe que aún existe un marcado desconocimiento respecto a las múltiples áreas y dimensiones que comprende esta temática, la cual trasciende lo meramente técnico y científico. Se remarca que es necesaria una mayor difusión sobre ámbitos de capacitación, sensibilización, comunicación, y aspectos legales, entre otros, que abren alternativas para personas provenientes de diversas disciplinas, como las comunicaciones, la abogacía, la psicología, entre otras.

"(...) creo que ahora está cambiando un poco. Hay más oferta y se estimula más a que se anoten mujeres. Por ejemplo, el curso de mujeres hackers" Mujer junior.

"(...) pero ahora ha ido evolucionando todo. Antes no había cursos de ciberseguridad. Se pensaba que solo podías llegar por la ingeniería pura, y tenías que pagar una fortuna para formarte. Ahora hay opciones, becas, ¡se está haciendo más inclusivo!" Mujer junior.



Las dificultades que persisten en torno a la comunicación y difusión de estas ofertas formativas, podrían estar incidiendo en una menor convocatoria de la esperada, sobre todo cuando la ciberseguridad queda excesivamente asociada al área de las STEM.

"(...) igualmente en los cursos y en la formación la proporción de mujeres es muy baja. Yo estoy acostumbrada a ser la única mujer en mis cursos" Mujer junior.

"(...) pero pasa en todas las STEM, a ver, esto es un embudo, llegan pocas a Ingeniería y similares y ¡muchas menos a ciberseguridad!" Mujer junior.

3.5 Brechas invisibles y visibles: los sesgos de género en ciberseguridad

"(...) un varón organizador de un evento de ciberseguridad nos dijo: ¿ustedes se dan cuenta que esto es muy difícil incluso para un hombre? Nos hizo ese comentario: ¡incluso! Ahí te das cuenta lo que son los prejuicios!" Mujer Senior.

Al introducir las diferencias de género en la elección de la profesión, todas las participantes están de acuerdo en admitir que existe un contexto cultural más amplio que atraviesa a las mujeres desde etapas muy tempranas. Tanto en ciberseguridad como en otras áreas STEM, los sesgos de elección profesional tienen su origen en la socialización

primaria. Desde el entorno familiar y social se producen y reproducen estereotipos de género que asocian lo femenino a ciertas tareas y profesiones —vinculadas al cuidado, la docencia o lo estético— mientras que lo técnico, científico y lógico-matemático se representa tradicionalmente como terreno masculino. Dichos estereotipos influyen en las expectativas, la percepción de autoeficacia y las decisiones vocacionales de niñas y adolescentes (Canclini Masserini & Fernández-Darraz, 2024; Caballero, 1998). Así, muchas niñas crecen sin imaginarse a sí mismas como futuras científicas, ingenieras o expertas en tecnología, lo que genera una desventaja estructural desde el inicio.

"(...) desde la infancia comienza esto. A las mujeres nos gustan y estimulan más los juegos de cuidado y creativas. Nos gustan las muñecas, dibujar. Ellos mientras tanto juegan con legos, desarman y arman aparatos. Y eso se estimula a su vez desde la casa y se continúa años posteriores. Desde siempre te formatean para que vayas por esos lados" Mujer Junior.

"Yo cuando era chica y decía que iba a ser ingeniería, me decían '¿Por qué no estudias algo de mujer?'" Mujer estudiante de ciberseguridad.

"(...) las barreras empiezan de niñas. Y después esto hace que si elegís esta profesión, te tenés que esforzar más. Porque ya arrancas con desventajas"

Mujer Senior.

“(...) sí a mí me hubiesen acercado herramientas como un soldador, o un lego, me hubiese sido más fácil llegar a donde llegué, fui muy cuestionada por el entorno cuando elegí ingeniería y después ciberseguridad. Me miraban como diciendo ¡estás loca! Con ingeniería me dijeron que era una carrera de varón”

Mujer Junior.

Estos mensajes se refuerzan luego en la socialización secundaria, a través de la escuela y el liceo, donde persisten representaciones que asocian ciertas disciplinas con uno u otro género. Las investigaciones muestran que el sistema educativo continúa transmitiendo expectativas diferenciadas sobre las capacidades de varones y mujeres, lo que influye tanto en la percepción de autoeficacia como en el desarrollo de intereses vocacionales. En particular, las niñas siguen siendo orientadas, explícita o implícitamente, hacia carreras feminizadas, mientras que las disciplinas técnicas y científicas se asocian a atributos tradicionalmente masculinos, como la racionalidad, el liderazgo o la competitividad (Canclini Masserini & Fernández-Darraz, 2024; Peacock & Irons, 2017; Caballero, 1998). Esta reproducción de estereotipos limita las posibilidades de exploración libre y equitativa de trayectorias profesionales desde edades tempranas. Aunque en los últimos años ha habido avances importantes —como la creación de eventos, talleres y campañas que promueven la participación de niñas y jóvenes en las ciencias—, aún falta camino por recorrer para desmantelar completamente estos estereotipos.

Una de las grandes dificultades señaladas por las entrevistadas es la ausencia de referentes visibles. La falta de modelos femeninos en el área STEM, y más específicamente en ciberseguridad, se traduce en un vacío simbólico que limita el sentido de posibilidad de las niñas y adolescentes.

"(...) yo en una charla que di sobre mi trabajo en la escuela de mi hija, se me acercó una chiquilina y me dijo: Yo si sigo esta carrera mi padre nunca me lo perdonaría". Mujer Senior.

El imaginario social sigue representando este campo bajo la figura estereotipada del "hacker", que suele encarnarse en un varón joven, encapuchado, encerrado en una habitación oscura, con habilidades

innatas, muy inteligente y una actitud desafiante. Esta imagen no solo es reduccionista, sino que contribuye a excluir simbólicamente a quienes no se ajustan a ese molde (Foley & Basu, 2024). La arraigada cultura meritocrática que domina el campo de la ciberseguridad, fuertemente asociada a ideales masculinos de autonomía, competencia técnica y desarrollo profesional lineal, opera como una barrera simbólica de género que produce dinámicas de exclusión. Tal como señalan Foley y Basu (2024), las representaciones sociales que enmarcan estas carreras —por ejemplo, la figura del "hacker solitario" altamente técnico— refuerzan un imaginario masculino que limita tanto la participación de mujeres como la redefinición del campo desde una perspectiva más inclusiva. Se espera una validación constante de las habilidades técnicas, lo que lleva a que las mujeres sientan una exigencia permanente de demostrar su competencia en lo técnico, más allá de lo que se espera de sus pares varones (Foley & Basu, 2024; Peacock & Irons, 2017).

"(...) te venden como que es algo re complejo, re difícil, muy de hacker, ¿viste? Que está con la capucha y tiene que ser un genio en las computadoras desde que nació porque si no, no lo va a aprender" Mujer estudiante de ciberseguridad.

Por tanto, la brecha de género en ciberseguridad no surge únicamente de condiciones estructurales del mercado laboral, sino que está profundamente arraigada en mecanismos culturales y sociales que operan desde edades tempranas y que condicionan la autopercepción, la motivación y la decisión de ingreso al sector. La socialización familiar y escolar reproduce estereotipos de género que limitan las aspiraciones de niñas y adolescentes en campos como la tecnología. Estos imaginarios se consolidan en etapas posteriores, generando barreras simbólicas que afectan el ingreso y la permanencia en sectores tradicionalmente masculinizados como la ciberseguridad. (Canclini Masserini & Fernández-Darraz, 2024; Foley & Basu, 2024; Peacock & Irons, 2017).

Al abordar las posibles barreras o dificultades que enfrentan las mujeres en el proceso más tardío de formación y desarrollo profesional en el sector de la ciberseguridad, van surgiendo construcciones narrativas aparentemente disímiles:

1. Algunas entrevistadas sostienen que **no han vivido discriminación directa** por su condición de género (brechas invisibles);
2. Otras **identifican experiencias claras de desigualdad** (brechas visibles).

No obstante, incluso en los relatos que niegan explícitamente la existencia de brechas, aparecen de forma implícita indicios que las evidencian: desde la necesidad de "adaptarse al ecosistema masculino" hasta la naturalización de dinámicas simbólicamente excluyentes.

3.5.1 Brechas "invisibles"

En los relatos del primer subgrupo, en un principio se niegan las brechas de género en el sector. Sin embargo, a medida que relatan sus experiencias aparecen, casi sin querer y de manera lateral, múltiples ejemplos y expresiones que confirman las brechas que se niegan de manera manifiesta: la necesidad de "adaptarse al ecosistema masculino", de ser "una más" en un entorno de hombres o asumir actitudes que permitan ser aceptadas en esa lógica, o incluso de ser rebautizada simbólicamente como varón —"me decían Carlitos"— para poder

ser incluida. Esta sobreadaptación, lejos de eliminar las barreras, las enmascara, ya que convierte en norma la capacidad de las mujeres de moldearse a una cultura que no fue diseñada para incluirlas. A su vez, los relatos de quienes lograron “encajar” pueden funcionar como legitimadores del sistema, invisibilizando tanto los esfuerzos requeridos para sostener esa adaptación como las trayectorias de quienes no lograron permanecer en el sector. Todo esto refleja un entorno que no es verdaderamente inclusivo, sino que premia a quienes logran asimilarse a la cultura dominante, en este caso la cultura masculina.

Algunas de las citas que destacamos en sus relatos y que analizamos a continuación develan esta contradicción, por ejemplo:

"No hay brechas... pero hay que ser fuerte"

- Decir que no hay brechas puede ser una forma de normalizar el entorno: “si yo lo logré, cualquiera puede”.

- El hecho de que se requiera “fortaleza, valentía y empoderamiento” sugiere que hay barreras sociales o culturales que deben superarse. Es decir, quizás no hay barreras técnicas o legales, pero sí de actitud, representación, o percepción.

“tenés que ser capaz de elevar tu voz, hacerte escuchar”; “no es para una mili pili, una mili pili se pega un corchazo”; “si sos tímida o bajo perfil no sé si llegas”

- Muchas veces, las mujeres en campos como la ciberseguridad son minoría, lo que dificulta su representación y visibilidad en el sector. Eso no implica que estas mujeres no puedan destacarse, pero sí que deben luchar más por ser escuchadas y tomadas en serio, lo cual

puede ser agotador y desmotivante para aquellas que no se destacan por estas cualidades de “fortaleza, estar siempre a la defensiva”

“a mí un jefe me dijo; así tan suavecita como sos, ¿crees que vas a poder liderar un equipo en Ciberseguridad?”

Aunque no haya una discriminación directa, puede haber microagresiones, estereotipos o actitudes sutiles que hacen que algunas mujeres sientan que deben “probar su valor” más que sus colegas hombres.

“es para mujeres con una fuerte personalidad”; “tenes que tener cierta actitud o personalidad determinada para estar en el rubro”; “tenes que adaptarte al ecosistema masculino”; “desde que ingresé a facultad supe que iba a ser así, un mundo de hombres y yo tenía que adaptarme!”; “o te adaptas o morís”

El hecho de que las mujeres mencionen la necesidad de estar empoderadas es positivo. Habla de resiliencia y de una comunidad que impulsa el cambio desde dentro. Pero también es un reflejo de un entorno que todavía no es completamente equitativo.

Estas afirmaciones que a simple vista pueden ser motivacionales y positivas, también pueden reflejar formas de exclusión indirectas: como si sólo ciertas mujeres “especiales o superpoderosas” pudieran entrar o mantenerse en el rubro.

“Tenés que ser arriesgada”

El mensaje subyacente es: “no todas encajan, y si no aguantas, no es para ti”. Eso refuerza la idea de que el entorno no cambia por inclusión, sino que es la mujer la que debe adaptarse a éste.

Todas las mujeres que participaron, y también los hombres, admiten tácitamente que el entorno está dominado por hombres, y que, para sobrevivir o progresar, la mujer debe ajustarse a algunas reglas ya establecidas, poniendo en evidencia un entorno y una cultura que no ha sido aún adaptada para incluirla. Las representaciones culturales de la ciberseguridad —como dominio técnico, masculino, autónomo, como una "industria de hombres"— construyen un entorno en el que las mujeres no solo están subrepresentadas, sino que deben adaptarse a una lógica preexistente que las excluye simbólicamente, tanto en el ingreso como en la progresión profesional (Foley & Basu, 2024; Peacock & Irons, 2017).

"(...) siempre fui la única mujer en mis clases desde el bachillerato en informática".

"(...) una como mujer es o se adapta al ecosistema este de tanta formación masculina".

"Yo trabajo casi 90% con hombres, (...) el adaptarse, el tener esa capacidad de de subir tu voz (...)".

Y como corolario se afirma:

"Yo jamás sentí ningún tipo de discriminación por ser mujer. Siempre me integré muy bien. Eran 6 varones y yo durante la carrera de ingeniería y soy uno más del grupo."

"Yo me pongo los pantalones"

- Implica integración, pero a costa de la diferencia.

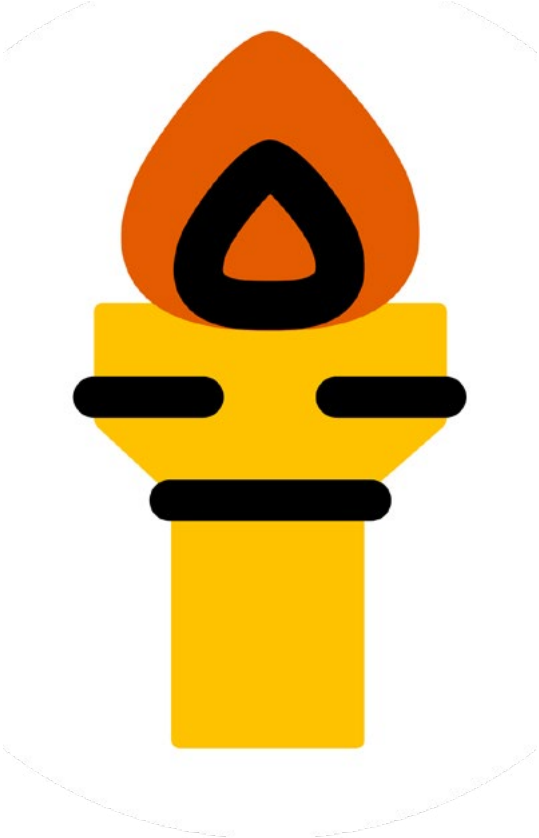
- La mujer no es aceptada como mujer, sino cuando se convierte simbólicamente en “uno de los chicos”. Rebautizarla como un hombre es una forma de suavizar o neutralizar su presencia femenina

- Esto puede generar un tipo de asimilación forzada, en la que se invisibiliza la identidad femenina para encajar. Puede ser una manera de "hacerla parte del grupo", pero bajo condiciones implícitas: solo si se masculiniza, es bienvenida. Esto muestra que el entorno no es verdaderamente inclusivo; es asimilador.

Los participantes varones en el estudio tienden a presentar una visión más técnica y lineal de su desarrollo profesional en ciberseguridad. Su foco principal se centra en los desafíos técnicos, la resolución de problemas y la adquisición de nuevas habilidades duras. A diferencia de las mujeres, los hombres generalmente no perciben el entorno laboral como hostil o exigente en función de su género. Sus relatos no suelen incluir experiencias de autoexigencia emocional o la necesidad constante de demostrar competencia debido a su identidad. Ejemplifican esta percepción al señalar que lo que importa son las habilidades y capacidades, no la identidad de género de quien las posee. Esta visión, sin embargo, a menudo desconoce cómo la identidad puede ser un factor oculto en la valoración.

“Si estás de este lado sos sos el golero, nadie quiere ser el golero”

“Históricamente en ciber nunca importó en realidad si eras mujer, si eras hombre o qué, en realidad era tu ‘nickname’ y eran 100% tus habilidades y tu capacidad de mostrar qué podías hacer, hasta dónde sí, hasta dónde no”.



3.5.2 Brechas “visibles”

En cuanto a los discursos de las mujeres que sí perciben discriminación directa por su género se destacan los siguientes ejemplos:

Ámbito laboral

Se mencionan experiencias claras de discriminación directa. Hablan de jefes que no las escuchan, que minimizan sus aportes, o que asignan menor valor a su trabajo. Algunas mujeres incluso relatan recibir salarios inferiores que sus pares varones por tareas equivalentes.

“(...) en mi trabajo anterior, me costó mucho ser escuchada y que se tomara en cuenta mi opinión. En las reuniones era la única mujer. Esto me generó formarme muchísimo carácter porque tuve que hacerlo a la fuerza. Era formarte un carácter fuerte, callarte o irte a llorar a un rincón, que también lo supe hacer. Si yo hablaba y decía algo de mi trabajo- en general algún aporte técnico- no se me escuchaba. Mi jefe miraba el celular cuando hablaba. A mis compañeros varones no les hacía eso, y muchos tenían menos formación y decían cualquier cosa sin importancia. Yo sé que era porque soy mujer”. Mujer Junior.

(...) “cuando cambié de trabajo un profesor me dijo que seguramente me tomaron a mí porque cobraba menos que los hombres” Mujer Junior.

“Yo he vivido alguna situación injusta por el hecho de ser mujer. (...) y yo me paré de punta y dije no (...)”. Mujer Senior.

Otra forma de discriminación, más sutil pero no menos significativa, es la **segmentación de las mujeres dentro del propio campo de**

la ciberseguridad. Varias entrevistadas señalaron la dificultad de acceder a roles eminentemente técnicos o relacionados con infraestructura. En estos casos, suele existir una tendencia a derivarlas hacia áreas consideradas “más adecuadas” para su perfil, como la gestión de proyectos, la normativa, la documentación o la articulación institucional. Algunos hombres coinciden con esta apreciación y reconocen esta discriminación en función de las tareas desempeñadas en el sector.

Las diferencias en la progresión de carrera y el acceso a posiciones de liderazgo también constituyen una brecha visible. Como señalan Peacock e Irons (2017), las mujeres en ciberseguridad perciben significativamente menos igualdad en las oportunidades de promoción que sus colegas varones, y deben enfrentar barreras institucionales y culturales que limitan su avance. A pesar de su esfuerzo y competencias, las mujeres pueden encontrar menos oportunidades de ascenso y una menor presencia en roles de toma de decisiones, especialmente en comparación con la visión más lineal y técnica del desarrollo profesional que suelen tener los varones (Foley & Basu, 2024). Esta situación se describe no sólo como un "techo de cristal" (glass ceiling), sino también como un "piso pegajoso" (sticky floor), donde la desigualdad salarial puede comenzar en la etapa de contratación, incluso si tienen habilidades, conocimientos y experiencia equivalentes a los hombres (Peacock & Irons, 2017).

“(...) a mi me gusta más la gestión, más pensar la estrategia que lo meramente técnico, lo de andar creando comandos, pero también es verdad que es muy difícil acceder a esos puestos siendo mujer”. Mujer Senior.

“(...) a mí también me encanta el tema, sobre todo de gestión y gobernanza de la seguridad de la información.” Mujer Senior.

“(...) a mí también me gusta la parte técnica. He ‘luchado’ para estar en ese lugar pero te convencen para ir a gestión” Mujer Senior.

“(...) las mujeres estamos mucho más orientadas a la gestión. ¿Nos fueron llevando por ahí? ¿o lo elegimos? Nos dicen que somos buenas en ese rol, que somos más ordenadas...A mí personalmente, me hubiese gustado poder desarrollarme en la parte técnica”

Mujer Senior.

"(...) sos mujer y te tiran para la parte de gestión. No se si es tan libre albedrío o te condicionan, te encasillan". Mujer Senior.

"(...) también existe una autocensura, de nosotras mismas, de elegir gestión, y no 'animarse' a la parte técnica. Miedo, tal vez, a no creerse capaz. Un poco se nos lleva, otro poco lo elegimos" Mujer Senior.

"(...) en los roles técnicos hay pocas mujeres. Hay pocas hacker éticas, pero muchas en gestión". Varón que trabaja en ciberseguridad.

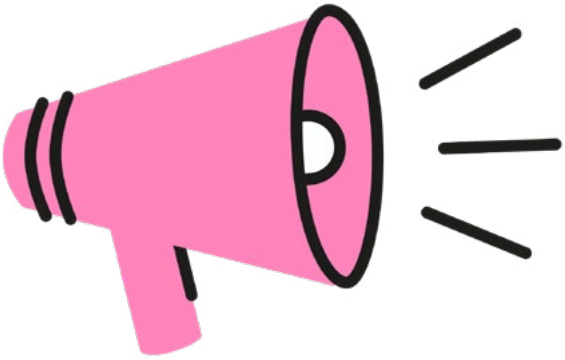
"(...) yo tengo un jefe que siempre cuando hay alguna tarea más operativa y técnica me la saca y me dice: 'esto es infra, no es para vos'. Y yo le digo: 'claro porque yo no soy ingeniera y no estudio ciberseguridad y trabajo hace tiempo en el área'. Es conectar dos cables y tirar dos comandos en una consola, ¡y él dice que es algo de hombres!" Mujer estudiante de ciberseguridad.

Esta asignación de funciones (que las tiende a excluir del área técnica), no siempre responde a los intereses o capacidades reales de las mujeres, sino a estereotipos que asocian al género femenino con habilidades como la comunicación, la empatía, la capacidad de negociación, el trabajo colaborativo o la organización. Si bien estas habilidades son valiosas y efectivamente muchas mujeres las desarrollan con excelencia, el hecho de que sean utilizadas como criterio para segmentar funciones genera una exclusión indirecta del núcleo técnico del sector.

En este sentido, se limita el acceso de las mujeres a espacios donde se toman decisiones clave sobre la infraestructura, el diseño de arquitecturas de ciberseguridad o el desarrollo de soluciones tecnológicas, ámbitos que suelen ser más valorados en términos de prestigio y proyección profesional. Esta división del trabajo —aunque no siempre explícita— contribuye a reproducir una jerarquización de roles al interior del campo, donde lo técnico sigue siendo terreno masculino y lo normativo o "blando", espacio femenino.

Más grave aún es cuando esta segmentación se impone a pesar del deseo o motivación de las propias mujeres por desarrollarse en áreas técnicas. Al imponer un recorrido profesional condicionado por su género, se les niega la posibilidad de explorar plenamente su potencial, reforzando una desigualdad estructural difícil de revertir si no se cuestionan los supuestos que la sostienen.

Aún más complejo es el caso de la discriminación ejercida por otras mujeres, especialmente desde áreas como Recursos Humanos. Algunas relatan que fueron descartadas por estar en edad fértil, o que sus pretensiones salariales fueron cuestionadas más duramente que las de sus colegas varones. Esto demuestra que el machismo estructural no depende del género de quien lo ejerce, sino de patrones culturales más amplios que todos podemos reproducir.



"(...) La única mujer que está peleando por un cargo alto y que los hombres apoyan (...) hizo comentarios a proveedores (proveedores que se sacan la bandera de apoyamos a las mujeres en ciberseguridad), pidiéndoles que que no llevaran a trabajar mujeres, explícitamente en una reunión de forma informal". Mujer Junior.

"Las propias mujeres son las que nos tocaban en las patas. Las que no te contratan porque estás por quedarte embarazada. Las que te dicen 'Ah, pero qué clavo, está embarazada, no va a poder gestionar esto, no sé qué.' O no te suben el sueldo." Mujer Junior.

"Cuando tuve la oportunidad de ascender [al nivel dos], y estaba embarazadísima, me dijeron '¿No quieres ascender al nivel uno? Porque el nivel dos... vas a tener una bebé chiquita. Capaz que es demasiado'" Mujer Senior.

A veces, las exigencias en el ámbito laboral son mayores con las mujeres, deben estar más formadas, ser más capaces que sus pares los varones, demostrar más sapiencia y solvencia, para llegar a cargos de relevancia en el sector o ser consideradas como “iguales en capacidades” por el segmento masculino con el que trabajan.

“(...) siendo mujer tienes que ser mejor, demostrar más capacidades. Estar dispuesta a estudiar más. Mis compañeros no están ni la mitad de formados que yo”. Mujer Senior.

“(...) yo tuve jefas mujeres y compañeras mujeres, y la verdad que eran muchísimo más capaces que yo y el resto de los varones del grupo. Siempre destacaron” Varón que trabaja en ciberseguridad.

Ámbito de formación

En el ámbito académico y profesional también aparecen micromachismos, como preguntas sobre quién cuida la casa mientras ellas estudian o comentarios que sugieren que están descuidando su rol doméstico. Estos discursos refuerzan estereotipos de género profundamente arraigados y limitan simbólicamente la participación femenina, al cuestionar su presencia y dedicación.

“(...) yo tenía un profesor que me preguntaba cómo hacía para llegar tan tarde a mi casa después de clase. O quién atendía mi casa si yo llegaba tan tarde!”. Mujer Junior.

Relatan que, con frecuencia, tanto compañeros como docentes hombres no esperan ni reconocen que las mujeres puedan sobresalir académicamente por encima de ellos. Por ello, cuando obtienen calificaciones destacadas, muchas mujeres deben enfrentar expresiones de asombro e incredulidad que, lejos de ser halagos, reflejan actitudes y comentarios discriminatorios sobre sus capacidades.

"(...) '¿cómo vas a ser mujer y te vas a sacar más nota que nosotros?', ese tipo de comentarios tenes que escuchar a veces". Mujer estudiante de ciberseguridad.

""(...) recuerdo haber hecho un curso técnico sencillo, no fue nada del otro mundo. Y que vengan compañeros y me dijeran asombrados "Ay, pero te sacaste el máximo!" ¡Más que Menganito! ¡Sorpresa de que vos, como mujer lo hayas logrado mejor!" Mujer estudiante de ciberseguridad.

Asimismo, señalan que muchas de las invitaciones laborales para participar en cursos de ciberseguridad presentan sesgos de género, ya que suelen estar orientadas a que las mujeres profundicen en temáticas vinculadas con la gestión y las tareas administrativas, en lugar de fomentar su participación en áreas técnicas o estratégicas

"(...) o las convocatorias que te arriman son más que nada de gestión. Como que no te invitan a participar de un curso técnico. Si es infraestructura no es para mujeres. Mujer: ¡vaya a documentar o a administrar!". Mujer estudiante de ciberseguridad.

Una barrera específica que se señala en relación con los cursos de esta temática es la escasa oferta de modalidades a distancia. Esta limitación afecta particularmente a las mujeres con hijos y responsabilidades de cuidado que no pueden delegar, restringiendo su posibilidad de participar en estas instancias de formación, especialmente si residen fuera de Montevideo.

"(...) yo como barrera adicional señalo la centralidad de Montevideo y que no hay muchos cursos que se puedan hacer a distancia son todos presenciales y son barreras fuertes para las mujeres con familia". Mujer estudiante de ciberseguridad.

"(...) yo veo que la oferta a veces no es muy adecuada a las mujeres que tenemos otras responsabilidades, hijos, trabajos... faltan cursos más cortos en el medio o

más vinculados a temáticas concretas por ejemplo ciberseguridad y IA, que no te demanden tanta presencialidad. Yo prefiero hacer certificaciones a distancia Internacionales que me ofrecen estas facilidades" Mujer que abandonó curso de ciberseguridad en Uruguay.

Las estudiantes de ciberseguridad mencionan que los abandonos que han presenciado durante sus cursos están estrechamente relacionados con las múltiples limitaciones que enfrentan las mujeres, más que con una falta de interés o capacidad. Esta situación refuerza la idea de que, para mantenerse en el sector, las mujeres deben contar con una resiliencia y fortaleza excepcionales, capaces de sostenerlas frente a obstáculos significativos que no afectan de igual manera a sus pares varones.

"(...) yo tenía dos compañeras que siempre las animaba a seguir. Les decía ustedes pueden no dejen pero terminaron dejando, para mi es un tema de personalidad y falta de autoestima. Como que no tenían mucha confianza en sí mismas y por todo lo que tenes que pasar, terminan dejando" Mujer estudiante de ciberseguridad.

Una dimensión relevante que emerge de los relatos de las entrevistadas es que la percepción de las brechas de género está más influenciada por la generación a la que pertenecen que por su nivel de cualificación o el rol que desempeñan en la organización. En este sentido, la edad se configura como un factor más determinante que la posición jerárquica, ya sea en niveles senior o junior.

En general, las mujeres más jóvenes parecen tener una mayor conciencia de los sesgos y estereotipos que aún permean el sector de la ciberseguridad. De hecho, muchas de ellas identifican estos obstáculos con mayor claridad y los denuncian de manera más directa. Por otro lado, las mujeres de generaciones más adultas tienden a visualizar estas dinámicas de manera más difusa o, en algunos casos,

incluso minimizarlas. **En muchos relatos, se observa una tendencia a internalizar los sesgos de género como parte del entorno laboral, lo que genera una visión más resignada o naturalizada de las brechas**. Este fenómeno, como se mencionó anteriormente, puede explicarse por la socialización y los roles de género internalizados a lo largo de los años, donde el entorno tecnológico y de ciberseguridad era predominantemente masculino y las mujeres se adaptaban a esa realidad, a veces sin cuestionarla.

"(...) claramente todo va cambiando, pero es gracias justamente a las mujeres que se animan y que van derribando fronteras. Y que las animan, ¿entendés? Desde las familias que confían en ellas, que les muestran otros modelos" Mujer Junior.

"(...) yo misma creía que no podía hacerlo porque siempre, en mi generación, la ingeniería la estudiaban los hombres y listo" Mujer estudiante de ciberseguridad.

Sin embargo, las mujeres más jóvenes, que han crecido en un contexto de mayor conciencia sobre la igualdad de género, están más dispuestas a desafiar estos estereotipos y actuar en consecuencia. Este cambio generacional se refleja, por ejemplo, en el esfuerzo consciente de los jóvenes, tanto hombres como mujeres, por evitar reproducir conductas discriminatorias o sesgos de género. Esta actitud más proactiva hacia la inclusión es una señal positiva de transformación dentro del sector, pero aún queda trabajo por hacer para consolidar estos cambios y garantizar una verdadera equidad.

"yo voy muy de frente y eso molesta. (...) el hecho de que vayas, encares la situación y digas, 'Mira, me está pasando esto, capaz estoy malinterpretando'. Siempre bien, ¿no? Siempre con respeto, nunca levantando la voz ni nada de eso, pero explicándote y siendo abierta". Mujer estudiante de ciberseguridad.

"(...) el grupo humano que tengo como compañeros es excelente. Si bien somos 3 mujeres y 20 y pico de varones en total, la verdad es excelente. Los chiquilines no tienen problema de explicarte 50 veces las cosas y la verdad es que me siento como como en casa" Mujer Junior.

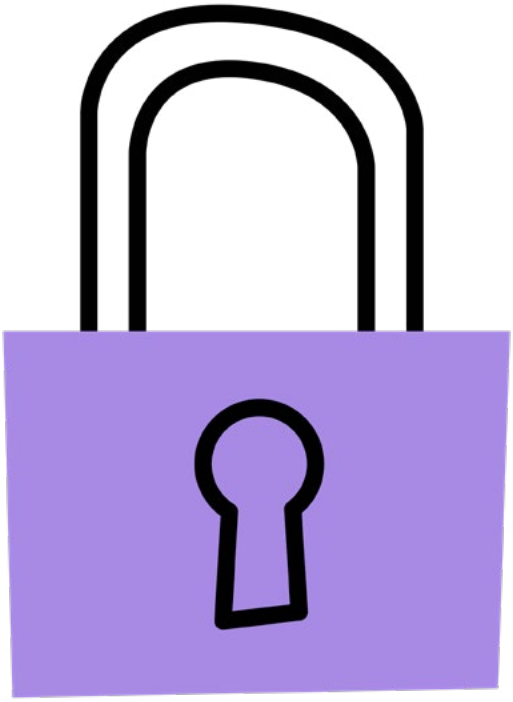
“(...) también es una falta de costumbre porque somos tan pocas. Hay gente [hombres] que hace años que está trabajando y capaz que nunca trabajó con una mujer en el área de informática, ¿no? Siempre trabajó con hombres. Entonces quizás hay gente que se adecúa lo más bien (...) y hay gente como que sí ve diferencias en ese sentido”

Mujer estudiante de ciberseguridad.

3.6 Características de las personas que se dedican a la ciberseguridad

A la hora de elaborar un estereotipo de las personas que se dedican a esta profesión se mencionan las siguientes características necesarias para el sector:

Capacidades duras y blandas que se perciben como necesarias y deseables en una persona dedicada al sector	• Que sepa de arquitectura y de infraestructura • Autorregulación emocional: capacidad para tolerar la frustración, gestionar el estrés y mantener la calma ante situaciones adversas. "No ponerse a llorar cuando algo no sale"
"Una característica que tenemos las mujeres que nos dedicamos a esto, es una ADAPTABILIDAD enorme. Hay mujeres que pueden sentirse intimidadas. Capaz que esas mujeres desisten" Mujer Senior.	• Animarse a la experimentación, a probar. Tolerancia al fallo, al error y al fracaso. Saber gestionar la autoexigencia sin perder la autoestima. • Saber poner límites, ser fuerte, tolerar la crítica, hacerse escuchar y respetar • No ser "demasiado sensible". • Disponibilidad horaria amplia– algunos cargos demandan estar a "disposición". Y para formación continua. • Arriesgada, mandada, no temerosa. • Adaptabilidad al mundo masculino si sos mujer. • Ser competitivo/a. • Creatividad, curiosidad. Que piense "fuera de la caja" • Sistematicidad, orden, capacidad de organización, detallista • Confidencialidad, persona reservada, responsable y confiable. • Saber trabajar en equipo, saber comunicarse. • Hacker bueno, con la capacidad de pensar "mal", *"tenés que poder pensar en las vulnerabilidades del sistema, ¿quién y cómo puede hacerle daño a esto?"*.



En estas características y en términos generales, las mujeres se perciben muy adecuadas en algunas (creatividad, organización, curiosidad, trabajo colaborativo, responsabilidad, detallismo, conocimientos técnicos) pero con mayores dificultades que los varones en las restantes capacidades.

Estas creencias también imponen sesgos y restricciones importantes a las mujeres que muchas veces se auto perciben y son percibidas por el entorno con características insuficiente para adecuarse a una carrera y a un cargo en esta área.

Las mujeres que logran superar las barreras e insertarse en el sector manifiestan un alto grado de conformidad con su trabajo, sintiéndose frecuentemente apasionadas por los desafíos que implica su rol. No obstante, también mencionan experimentar cierta sensación de soledad en un entorno predominantemente masculino, donde la camaradería más sólida suele darse entre los varones. Esto las hace sentirse excluidas de algunas instancias de socialización, como asados o salidas extralaborales, lo que a su vez las lleva, en muchos casos, a buscar vínculos laborales por fuera de su propia sección de trabajo.

"(...) la camaradería más fuerte es entre ellos, a veces pasas mucha soledad también en el trabajo. Son ambientes de trabajo más formales. Los vínculos más fuertes los tenes que buscar afuera" Mujer Junior.

3.6.1 Facilitadores para la elección y permanencia en el sector

Finalmente, los facilitadores identificados como claves tanto para la elección de la ciberseguridad como para la permanencia en la carrera y en el ámbito laboral se relacionan con los siguientes aspectos:

- La percepción de la ciberseguridad como un **área desafiante, estimulante, creativa** y en permanente evolución, lo que la convierte en un **ámbito laboral dinámico y alejado de la monotonía**.

- La **diversidad de áreas** dentro del sector, como la **gestión de riesgos, la legislación y normativa, la capacitación y la sensibilización**, etc., permite el **desarrollo de múltiples aptitudes y facilita la incorporación de perfiles con enfoques y habilidades variadas.**

- La **alta empleabilidad** caracteriza al sector, lo cual representa una **fuente laboral estable** y con **amplias oportunidades de inserción profesional**.

- La **flexibilidad laboral asociada al sector** —aunque no siempre se materializa en la práctica—, ya que se lo vincula comúnmente con **modalidades de trabajo remoto y horarios flexibles**, lo que facilita la **conciliación entre la vida profesional y personal**, la esfera pública y privada de la vida. Si bien algunas participantes consideran que la profesión puede ofrecer cierta flexibilidad y ser compatible con sus roles de cuidado, otras -en mayor número- señalan que la exigencia de estudio continuo y la rápida evolución del sector demandan una dedicación que entra en conflicto con las responsabilidades familiares, creando una tensión constante. Esta polaridad en las percepciones pone de relieve la necesidad de matizar el discurso sobre las condiciones laborales en el ámbito.

"(...) yo madre quiero ser y lo veo un trabajo compatible con el cuidado de bebés, si tenes flexibilidad y un trabajo remoto más aún" Mujer estudiante de ciberseguridad.

- La posibilidad de **contribuir al cuidado y la protección de datos e información**, tanto a nivel individual como institucional, lo cual otorga a la carrera un **sentido de utilidad social** que puede alinearse con los mandatos tradicionales de género vinculados al cuidado y la ayuda a los demás.

"(...) no solo la plata. La parte de contribuir, ayudar a las personas y las organizaciones, ayudar a resolver problemas es muy importante". Mujer estudiante de ciberseguridad.

- La **oportunidad de aplicar los conocimientos teóricos en contextos reales**, evitando una aproximación puramente técnica y favoreciendo la **búsqueda de soluciones prácticas**, lo que refuerza el carácter aplicado de la carrera.

- La existencia de **niveles salariales competitivos y adecuados**, que no solo permiten alcanzar una **buena calidad de vida**, sino también **desarrollar proyectos personales con mayor autonomía e independencia**.

- La presencia de **iniciativas y programas** orientados a **fomentar la inclusión de las mujeres** en el sector, lo cual contribuye a reducir brechas de género y a generar entornos más equitativos y diversos.

"(...) hay algunas iniciativas por ejemplo, a través del fondo Telefónica, la UM mujeres Hackers. Que fomentan la inclusión de las mujeres en el sector". Mujer Senior.

3.6.2 Cuadro final resumen

Facilitadores e inhibidores para estudiar y trabajar en ciberseguridad

	Facilitadores	Inhibidores u obstáculos
Factores previos a la elección de Ciberseguridad como ámbito futuro de formación y/o trabajo	**STEM en general** **Referentes femeninos** en roles no tradicionalmente asignados a las mujeres: ingenieras en la familia pero no exclusivamente, en otros roles no tradicionales o cuestionadores del statu quo: “yo siempre tuve una madre que me fomento hacer lo que quiera” “mi abuela estudió medicina, en su casa le dijeron si perdes un examen te vas a cocinar y ella entonces jamás perdió uno y fue una médica destacada. Me crié con eso.” **Ciberseguridad** – cualidades proyectadas y datos a priori conocidos de este sector: • Profesión que permite cierta flexibilidad y la posibilidad de trabajar remoto. • Adecuada a una mayor conciliación trabajo-maternidad y cuidado. • Permite la reconversión laboral. • Buen salario. • Alta empleabilidad del sector. • Cualidades asociadas significadas como “más femeninas”: detallismo, sistematicidad, creatividad, curiosidad.	**STEM en general.** **Socialización primaria:** mensajes desde lo familiar a las niñas/os: juguetes que se regalan, roles que se muestran y fomentan. Por ejemplo cuidar y tareas domésticas a las mujeres/ armar, analizar a los varones. **Socialización secundaria:** mensajes y fomento desde los centros educativos a los alumnos/as. Orientaciones científicas y matemáticas elegidas por varones fundamentalmente. **Ciberseguridad:** estereotipo asociado a los masculino – **hacker hombre**- y a determinadas características de personalidad que se consideran menos presentes en el género femenino: tolerancia al error, autoexigencia, etc. **Campo disciplinario asociado exclusivamente a formaciones vinculadas a las STEM**. Menor conocimiento del desarrollo de la ciberseguridad en **otras áreas y desde otros enfoques**: normativa-legal, social, psicológica, de sensibilización y capacitación.

Formación	**Difusión y existencia** de cada vez más cursos, certificaciones, posgrados, etc. **Promoción de cursos y formación específica para mujeres.** Becas, formación gratuita.	**Insuficiente promoción** aún focalizada en las mujeres. **Pocos cursos a distancia u online**, con contenidos acotados, no permite conciliar trabajo y cuidados con la obligatoriedad de presencialidad y carga horaria. **Faltan hojas de ruta** que puedan orientar la formación o carrera en el sector. **Formación continua:** para algunas mujeres dificulta la conciliación con la vida privada. **Profesores varones** con cierta misoginia que emiten mensajes contraproducentes al segmento. **Formación demasiado asociada** aún a las orientaciones proveniente de las STEM.
Vida laboral	**Alta empleabilidad** **Salarios** **Desafío constante**/ **Creatividad** **Documentar y gestión: muy acorde a las habilidades significadas como "típicamente" femeninas: habilidades blandas** de comunicación, detallismo, prolijidad, sistematicidad, etc. **Trabajo remoto y flexible** Compatibilizar vida privada y trabajo. **Bajar a tierra, poner en práctica saberes teóricos**. Ayudar a las personas y empresas a proteger sus datos y cuidar la información. **Posibilidad de trabajar en múltiples roles**, distintos enfoques: gestión del riesgo, sensibilización, documentación, normativa, etc.	**Rasgos de personalidad exigidos a las mujeres de ciber:** fortaleza, adaptabilidad al mundo masculino, empoderamiento, capacidad de plantarse y ser escuchada. Inhibe a mujeres que no se identifican con estos rasgos. Obliga a la **adaptabilidad**, asimilarse al mundo masculino. **Segmentación de los roles:** dificultad de acceso a roles técnicos y de infraestructura **Trabajo técnico "demandante"** y sin horario. **Discriminación directa** aún presente en algunos roles y lugares: salarios más bajos que hombre con igual rol y función, malos tratos, etc.

4.

Entrevistas

4.1 Ejecución de campo

Se llevaron a cabo doce entrevistas en profundidad, realizadas entre los meses de marzo y abril de 2025. Las entrevistas se desarrollaron en modalidad online o presencial, según la preferencia de cada persona entrevistada. Cada encuentro tuvo una duración aproximada de una hora.

4.2 Segmentación y perfiles

La segmentación realizada para las entrevistas fue la siguiente:

n°	Segmentos	Consideraciones
1	**Líderes y responsables de recursos humanos en el sector público y privado**	Pertenecientes al sector financiero, tecnologías de la información, emprendedores, instituciones educativas.
2	**Mujeres profesionales en ciberseguridad**	Pertenecientes al sector jurídico, militar.
3	**Expertos en género y tecnología**	Consultores, emprendedores, académicos.
4	**Mujeres vinculadas a la ejecución o generación de acciones o políticas públicas**	Sector público, organismos internacionales.

En base a la anterior segmentación se entrevistaron los siguientes perfiles:

n°	Sector o rol	Perfil
1	**Referente de Recursos Humanos**	Experta en Recursos Humanos y transformación digital
2	**Referente en el sector público**	Experta Senior en ciberseguridad
3	**Referente en el sector privado**	Gerente de operaciones y Consultor experto senior en ciberseguridad
4	**Referente en el ámbito multilateral**	Sector público, organismos internacionales.
5	**Referente sector académico**	Especialista Ciberseguridad y Profesor en Universidad
6	**Referente del sector privado**	Directora de laboratorio de IA
7	**Referente sector académico**	Ingeniero en Computación UDELAR
8	**Referente sector emprendedor**	Directora de emprendimiento vinculado
9	**Referente del sector bancario**	Gerenta general
10	**Referente del sector jurídico**	Abogada, especializada en Derecho Informático y Nuevas Tecnologías
11	**Referente del sector público**	Oficina pública unidad de ciberseguridad
12	**Referente del sector público**	Senadora - Calidad de Software

4.3 Estrategias de reclutamiento implementadas

Con el fin de obtener perfiles relevantes y variados para participar en las entrevistas, se sumaron las siguientes estrategias específicas a las ya desarrolladas para reclutar a las participantes de grupos:

- **Participación y difusión en reuniones especializadas:** nómade realizó una fuerte apuesta de sondeo de eventos estratégicos en las temáticas tecnológicas, de ciberseguridad, de emprendedores, en sectores empresariales o estatales durante los meses de marzo y abril. El objetivo de estas acciones fue ganar mayor conocimiento e información acerca del sector de la tecnología y la ciberseguridad en ámbitos específicos para mujeres, pero también de dar a conocer el proyecto y atraer el interés de mujeres especializadas en este sector. De esta manera, las acciones de reclutamiento se vieron enriquecidas por la participación de los siguientes eventos:

- **El 25 de marzo: Woman's day, organizado por "Mujeres al cubo":** Se trató de un evento concebido para inspirar, fortalecer y promover el liderazgo de las mujeres en el ecosistema tecnológico y emprendedor. El encuentro buscó generar un espacio de diálogo en torno a la inclusión, la equidad y el empoderamiento femenino en los ámbitos empresarial y tecnológico. Se centró en visibilizar el talento femenino y promover la igualdad de oportunidades en el sector tecnológico.

- **El 2 de abril: Foro IAméricas, organizado por Cubo Itaú e IAméricas**, en colaboración con BID Lab. Reunió a actores clave del ecosistema de innovación e IA: startups, empresas, inversionistas y

sector público. El evento tuvo como dentro de su temas centrales la inteligencia artificial responsable, con atención a la inclusión y equidad en el uso de esta herramienta.

4.4 Pauta de indagación

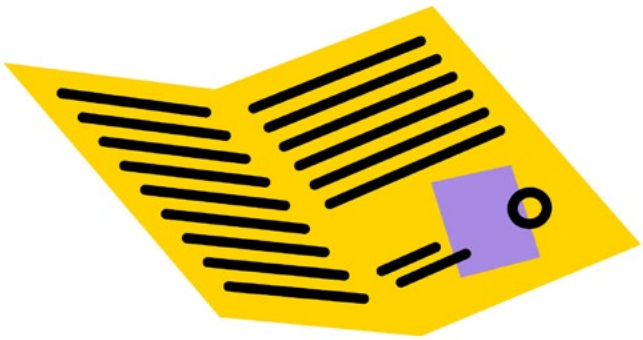
La pauta de entrevista, adaptada a cada perfil, se encuentra disponible en el siguiente link: **Pauta Ciberseguridad entrevistas**

5.

Principales resultados de las entrevistas

Las personas entrevistadas provienen de una **amplia y diversa variedad de campos profesionales**, lo que evidencia la riqueza de trayectorias que convergen en este ámbito. Provienen del campo **militar, diplomático, del sector jurídico, técnico (vinculados a disciplinas de licenciatura y/o ingeniería en sistemas, computación, software, operaciones, transformación digital), político, docente, bancario, entre otras**.

Como se mencionó para el caso de los grupos focales, algunas de las personas entrevistadas también han llegado al campo de la ciberseguridad tras realizar especializaciones que les permitieron direccionar su rumbo profesional hacia ese sector. El aterrizaje en este campo también significó la combinación de dos vocaciones, de sectores que, en un principio, podrían parecer distantes como la jurídica y la ciberseguridad, por ejemplo.

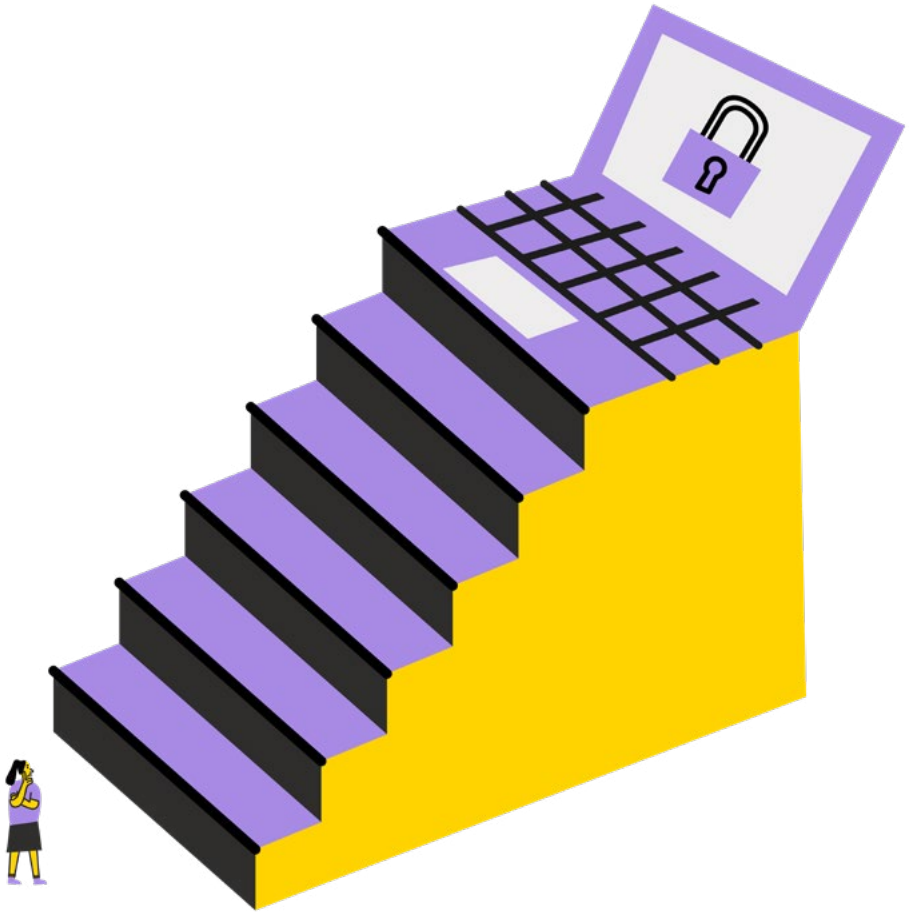


Así, aunque muchas de las personas entrevistadas tienen formaciones vinculadas a disciplinas STEM, esta no fue una condición excluyente en la investigación.

Esta diversidad de trayectorias demuestra que la ciberseguridad puede ser un punto de encuentro para quienes, desde distintas disciplinas y recorridos, deciden explorar su potencial en un entorno altamente dinámico y en constante evolución.

5.1. Barreras y habilitadores que afectan la inserción y el desarrollo profesional de las mujeres en Ciberseguridad

La participación de las mujeres en el sector tecnológico en general, y en ciberseguridad en particular, es baja en Uruguay, lo que refleja una problemática similar a otros sectores tradicionalmente masculinizados.



Las cifras indican una baja presencia de mujeres. Referentes de organismos internacionales mencionan datos que muestran que

2. Cita el informe: "Mujeres e industria TI" CUTI (2025): "las mujeres ocupan solamente el 24% de los cargos en el área de tecnologías de la información"

"24%[2] de las mujeres ocupan cargos en el sector de tecnologías de la información en Uruguay, pero obviamente eso es el en general, me imagino que en ciberseguridad debe ser aún menos".

Los mismos datos son compartidos por referente del sector privado, quien sugiere que la composición de género en ciberseguridad es una de las peores en el sector tecnológico.

"En computación el porcentaje ronda el 70/30 entre hombres y mujeres, pero en cursos específicos de ciberseguridad es de 90/10 u 85/15".

Consideran que esto se relaciona con *"la formalidad del área, la percepción de poca inserción laboral específica en ciberseguridad, la histórica asociación del ambiente con lo masculino" y 'cuestiones culturales históricas' ('la mujer dentro de la ciencia')".*

En el sector bancario, si bien no se presentan datos específicos para el área de ciberseguridad, referente del sector percibe una **superación de estereotipos de género a nivel general**, donde *"cualquier rol puede ser desempeñado por hombres o mujeres"*. Aunque reconoce que la industria financiera y el banco tuvieron una historia tradicionalmente machista, y que en el pasado hubo cierta resistencia a que las mujeres ocuparan determinados puestos aunque considera que eso hoy está *"absolutamente superado"* a nivel interno:

"Hace más de 40 años que estoy trabajando en el (sector bancario). Entré muy jovencita a trabajar en el banco, y cuando yo entré éramos un puñado de mujeres. Éramos un porcentaje bajísimo (...), es decir, había un porcentaje superior al 90% de hombres cuando yo ingresé".

Entre los factores que contribuyen a la **brecha** de presencia de mujeres en el sector de la ciberseguridad se identificaron los siguientes:

1 **Estereotipos sociales y culturales:** La percepción de que estas carreras son masculinas es una barrera significativa. Referente de organismos multilaterales menciona *"el estereotipo de carreras que son masculinas, más hombres"*. Referente del sector privado describe el sector como *"masculinizado, hiper, hiper masculinizado. Es como de las cosas más masculinas porque además tiene que ver también con cómo es la percepción popular respecto a lo militar"*. Algunos entrevistados que trabajan en el sector tecnológico señalan que los estereotipos sobre cómo son los profesionales en ciberseguridad no se ajustan a la realidad. Específicamente se menciona que *"piensan que somos estos de la capucha, estamos con la capucha, (...) así tapados y estamos con la computadora, o sea, como que ellos también son conscientes de esos estereotipos y que nada que ver. No es así"*. En esta línea, otro experto agrega que *"hay que*

sacar el misticismo de que la seguridad informal es para gente de capucha que está metida en los curros y haciendo cosas malas”.

2 **Falta de conocimiento acerca de referentes femeninas:** La ausencia de modelos a seguir dificulta que las mujeres jóvenes se vean en este campo. Referente de organismos multilaterales menciona *"la falta de referentes femeninos, el poder animarse, ¿no?, a que hay otra gente, otras mujeres que han podido lograr eso".* Experta senior en ciberseguridad también destaca que *"faltan o no se conocen, no sé si faltan, no se conocen, hay muchos más hombres, entonces como que te copan el discurso y el aspecto público de lo que se hace".*

3 **Percepción de dificultad con el área de estudio:** Existe la creencia de que las carreras tecnológicas y de ciberseguridad son excesivamente complicadas, especialmente en relación con las matemáticas. Experta senior en ciberseguridad señala que las personas *"no ven la carrera ni siquiera la de tecnología y menos la de ciberseguridad, no la ven como una posible salida laboral. No la ven, la ven como algo super complicado"*. También se menciona el *"miedo a la matemática"*.

4 **Responsabilidades en las tareas de cuidados:** Las responsabilidades de cuidado recaen mayoritariamente en las mujeres (**feminización del cuidado**), lo que puede limitar su tiempo para la formación y el desarrollo profesional. Referente de organismos multilaterales indica que *"la realidad es que la mayoría de las mujeres, como se comprobaron estudios que se han hecho en la en la pandemia, las que nos encargamos de los cuidados y el trabajo de la casa son mayor mayoritariamente mujeres"*. Esta barrera es un aspecto transversal constante en los entornos de trabajo, especialmente en un sector que demanda alta disponibilidad y estudio continuo. Aunque algunas entrevistadas señalaron una aparente flexibilidad en la profesión, que podría compatibilizar con las responsabilidades de cuidado, el hallazgo más generalizado apunta a

que la exigencia de estudio y actualización es tan alta que dificulta enormemente la gestión de los roles de cuidado tradicionalmente asignados a las mujeres. Esta tensión entre la dedicación profesional y las responsabilidades familiares emerge como un obstáculo significativo y poco reconocido.

5 **Falta de empoderamiento y networking:** Las mujeres tienden a ser más cautelosas al postularse a oportunidades y tienen menos redes de contacto informales (*"networking"*) que los varones. Referente del sector privado observa que *"las mujeres estamos muy mal con el tema networking, mucho peor que los varones"* y *"falta un montón con respecto a autohabilitarse a a postular a cosas y hablar"*. La exclusión también se manifiesta en formas sutiles, pero determinantes para el acceso a redes y oportunidades. Ejemplos de esto son las *"decisiones que se toman con una cerveza a las 3 AM"*, es decir, la relevancia de las interacciones informales y extra-laborales que a menudo quedan fuera del alcance de las mujeres, impactando en ascensos y toma de decisiones clave. Esto refuerza la idea de que la autoestima y la resiliencia son clave para sostenerse en un entorno masculinizado, donde la adaptación de comportamientos masculinos a veces se percibe como necesaria para integrarse o evitar discriminación.

6 **Desconocimiento de oportunidades:** La falta de difusión y visibilidad de las carreras en tecnología y ciberseguridad contribuye a que las mujeres no las consideren. Experta senior en ciberseguridad cree que el problema *"no se ve, hay un problema previo educativo donde no se ve esto con las carreras de tecnología y ni que hablar ciberseguridad como una salida, como una profesión en sí y una salida laboral"*.

7 **Diseño de los requisitos en llamados laborales:** Un punto recurrente es el posible desajuste generado por los reclutadores al crear llamadas con largas listas de requisitos. Esto parece afectar desproporcionadamente a las mujeres, quienes tienden a no postularse si

no cumplen todos los requisitos, a diferencia de los varones que se animan si cumplen solo algunos. Se sugiere que la forma de comunicación de los puestos, especialmente para niveles de entrada, podría necesitar ser diferente para alentar a las mujeres a postularse. A modo de ejemplo, una experta en ciberseguridad reflexiona:

"O sea, que en el medio el filtro que sería recursos humanos (...) es quien quizás está generando capaz esta desconexión y puede ser que (...) las mujeres también que son las que tratan de pasar toda la lista de chequeo no se presenten (...) Eso también es de conocimiento de quienes plantean esos posteos y quienes piden esos jobs, de los cuales también somos toda la industria responsables de permitir también que eso pase".

Sin embargo se identifican **oportunidades** que contribuyen a la presencia de mujeres en el sector de la ciberseguridad:

1 **Modalidad de trabajo:** La posibilidad de trabajar de forma remota es una oportunidad significativa para las mujeres que tienen responsabilidades de cuidado. Referentes de organismos internacionales destacan que *"ahora tenemos mucho más oportunidad porque se las mujeres una mujer que tengan responsabilidad de cuidar a a sus padres ancianos o tenga hijos, puede darse el tiempo"*. La naturaleza remota de muchos trabajos en ciberseguridad también se presenta como una ventaja: *"la ventaja de la ciberseguridad es que se puede hacer todo remoto a distancia"*.
No obstante, si bien el teletrabajo puede facilitar la conciliación entre la vida laboral y familiar, también puede reforzar la sobrecarga de las mujeres, al superponer en un mismo espacio físico y temporal el trabajo remunerado y las tareas de cuidado. La imbricación de la vida privada y doméstica con la vida pública y profesional se destaca como uno de los límites más fuertes para el éxito profesional de las mujeres (Caballero, 1998). En contextos donde las responsabilidades domésticas recaen desproporcionadamente sobre ellas, la modalidad remota corre el riesgo de profundizar la doble jornada, dificultando el descanso y la desconexión (Batthyány, Katzkowicz &

Scavino, 2022; Fang, Kang & Kaplan, 2022; Giuzio & Cancela, 2021; Paris, 2011). Esta tensión evidencia la necesidad de acompañar estas oportunidades con políticas de corresponsabilidad y límites claros entre los ámbitos personal y laboral.

2 **Programas y talleres específicos:** Se considera que los programas y talleres dirigidos específicamente a mujeres pueden ayudar a fomentar su interés y participación desde edades tempranas. Referentes de organismos internacionales sugieren que *"deberían haber programas dirigidos solo para mujeres, para promover (...) sobre todo en la adolescencia, tal vez cursos solamente donde haya para mujeres"*.

3 **Mentorías y redes de apoyo:** Las redes de apoyo y mentorías son cruciales para guiar y motivar a las mujeres en este campo. Referente de organismos multilaterales cree que *"en el tema también de oportunidades y tendencias lo que ayuda mucho es esto de las mentorías y redes de apoyo"*.

4 **Diversificación de perfiles:** La evolución de la ciberseguridad y la tecnología permite la inserción de profesionales de diversas áreas, no solo de ingeniería o informática tradicional. Referente de empresas tecnológicas menciona que en inteligencia artificial *"pueden entrar estadísticos, pueden entrar economistas... biólogos, químicos, otro tipo de científicos, ¿no? De matemáticos que tienen otra inclinación, por ejemplo, química. Es una formación hiper feminizada"*. Referente del sector jurídico señala que *"la ciberseguridad justamente no es solamente el código, sino que es todo el ecosistema también que la rodea"*.

5 **Necesidad de ambientes inclusivos:** Es fundamental crear entornos laborales donde las mujeres se sientan cómodas. Referente de organismos multilaterales habla de la importancia de la *"creación de ambientes inclusivos (...) donde las mujeres se sientan que eso que*

no que no son las únicas y que no se encuentren con no se intimiden de llegar a un lugar y que que sólo haya hombres".

6 **El rol de quienes reclutan:** Se reconoce la importancia de que los reclutadores sean conscientes de los sesgos de género y fomenten la postulación de mujeres. Referente de empresas tecnológicas destaca *"qué importante es el rol de los de los y las reclutadores"*.

7 **El desarrollo de una industria nacional de ciberseguridad aprovechando la industria de software existente**. Referentes de organismos internacionales menciona que la Estrategia Nacional de Ciberseguridad[3] *"propone posicionar una industria nacional de ciberseguridad sólida, y eso aprovechando la industria de software que tiene ya Uruguay"*.

3. Estrategia Nacional de Ciberseguridad: "La Estrategia Nacional de Ciberseguridad (ENC) 2024 - 2030 tiene como objetivo consolidar un ciberespacio seguro, abierto, resiliente y confiable. La iniciativa impulsa el desarrollo sostenible y protege los derechos y las libertades de las personas".

Los hallazgos obtenidos en los grupos focales y entrevistas permiten construir una **mirada integral sobre las barreras y habilitadores** que afectan la inserción y el desarrollo profesional de las mujeres en ciberseguridad. Mientras que los grupos focales ponen el acento en vivencias subjetivas y trayectorias personales —revelando tensiones en torno a la **autoexigencia**, la **segmentación de roles** y la necesidad de **adaptarse** a entornos masculinizados— las entrevistas con actores institucionales complementan esa mirada con una lectura estructural: subrayan la **persistencia de estereotipos de género**, la **falta de referentes visibles** y el diseño de **procesos de selección poco sensibles a la desigualdad**. Ambas fuentes convergen en un diagnóstico común: la baja participación de mujeres en ciberseguridad **no responde a una sola causa**, sino a un entramado de **condicionamientos culturales, institucionales y simbólicos** que se refuerzan mutuamente desde etapas tempranas de socialización hasta la vida laboral. A la vez, coinciden en señalar que ciertos habilitadores como la **flexibilidad, la diversidad de perfiles posibles y las oportunidades de reconversión** pueden representar puertas de entrada para revertir esta tendencia si se acompañan de políticas activas de equidad

5.2 Experiencias y buenas prácticas para la inclusión de mujeres

Con respecto a iniciativas o programas dirigidos a fomentar la inclusión de mujeres en tecnología y ciberseguridad, desde el ámbito público se mencionan propuestas como:

- Promover políticas de formación en ciberseguridad desde edades tempranas, **aprovechando herramientas existentes como el Plan Ceibal**.
- Establecer **políticas de soberanía digital** que definan claramente los roles requeridos, lo que implicaría mayor capacitación y demanda de perfiles técnicos diversos.
- Diseñar **becas diferenciadas y mecanismos de incentivo para mujeres** en programas de formación técnica.
- Apoyar **iniciativas de mentoría y reconversión laboral con perspectiva de género** desde organismos públicos. Estos espacios brindan un sentido de comunidad, la oportunidad de compartir experiencias, resolver dudas y recibir orientación de quienes ya transitaron caminos similares. La presencia de modelos a seguir y el respaldo de pares contribuyen significativamente a la confianza y la permanencia en el sector.

- Establecer **mecanismos de auditoría para garantizar que las mujeres** están efectivamente incluidas en los procesos de formación pública vinculados a esta área, lo que contribuiría a generar condiciones de acceso más equitativas.

En este sentido se relevaron múltiples iniciativas ya existentes que apuntan a fomentar la participación de mujeres en tecnología y ciberseguridad:

- En la Escuela Militar, orientados a fomentar la participación femenina, como la eliminación del cupo fijo por género, con el objetivo explícito de promover la inclusión de mujeres en este campo tradicionalmente masculinizado.

- Referente en el ámbito de los Recursos Humanos destacó el valor de generar becas diferenciadas para mujeres en universidades privadas como mecanismo de incentivo. Además, mencionó el programa Herpath de Herlabs[4], emprendimientos especialmente diseñados para mujeres interesadas en reconvertirse o comenzar su camino profesional en ciberseguridad, que incluye mentorías y formación práctica.

- Desde la academia se mencionó la iniciativa "Techy por el Día"[5] de CUTI y ANEP. Este programa organiza que niñas visiten empresas de tecnología para que mujeres que trabajan allí les cuenten su trayectoria y cómo llegaron a estudiar tecnología. De esta manera, estas mujeres profesionales en las áreas de tecnología sirven de referentes directos y cercanos.

- Expertos senior del área de ciberseguridad, agregan programas como “Mujeres hackers” de INEFOP y la Fundación Telefónica Movistar[6], bootcamps de empresas como Globant, “She Secures” de la OEA[7] y Girls in Tech (GIT)[8].

4. Herpath, Herlabs

5. Techy por el Día, CUTI y ANEP

6. Mujeres Hackers, INEFOP y Fundación Telefónica Movistar

7. She Secures, OEA

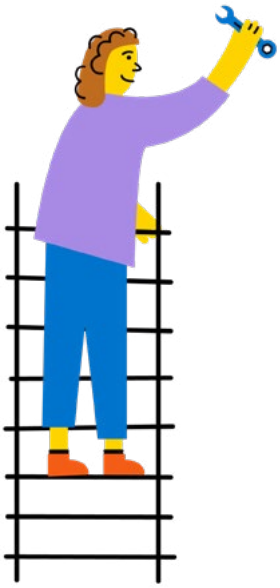
8. Girls in Tech

- Una referente del ámbito público también destacó experiencias lúdicas y educativas realizadas en eventos como los del Antel Arena, así como el potencial de Agesic para impulsar mecanismos de auditoría que generen demanda de profesionales capacitados en ciberseguridad.

Al respecto, las personas entrevistadas consideran que, si bien el impacto no es inmediato, estas acciones contribuyen a modificar percepciones y referencias a mediano plazo. Sin embargo, también señalan que estas iniciativas necesitan un mayor alcance y coordinación: *"el alcance que tienen esas cosas no es tanto"*.

Referentes de organismos multilaterales comparten que internamente *"se promueve la inclusión de mujeres en todos los proyectos y existen cuotas de género que rara vez se cumplen"*. También que, en otro organismo, existe una política general de *"paridad de género en puestos de mando a todo nivel"*. Sin embargo, especifica que esta política *"no es específica para las áreas de tecnología"*.

Desde el sector bancario, se comparten iniciativas para blindarse contra ciberataques, pero no específicamente sobre políticas internas de apoyo a las mujeres en las áreas de ciberseguridad. Por ejemplo, se comparte información sobre la inversión significativa que se realiza en ciberseguridad, incluyendo formación continua del personal. La estrategia incluye asumir que un ataque ocurrirá y trabajar en la capacidad de recuperación rápida y ordenada.



El análisis conjunto de grupos focales y entrevistas evidencia que las buenas prácticas para promover la inclusión de mujeres en ciberseguridad requieren una **acción articulada en múltiples niveles**. Las voces recogidas desde la experiencia directa de mujeres insertas en el sector destacan el impacto positivo de **programas de becas, mentorías y acciones afirmativas**, pero también advierten sobre su **alcance limitado** si no se acompañan de transformaciones culturales y organizacionales. En esta línea, las entrevistas aportan una

perspectiva estratégica sobre el rol de las políticas públicas, la importancia de auditar la implementación de medidas de equidad y la necesidad de **repensar los procesos formativos** desde una lógica más inclusiva. La intersección entre ambas fuentes revela que no basta con sumar mujeres al sector: es imprescindible modificar las condiciones que definen su participación, desde las **formas de reclutamiento hasta los modelos de liderazgo, reconociendo el valor de la diversidad como componente estructural y no como una meta simbólica.**

5.3 Referentes femeninas: importancia, obstáculos y visibilidad

Las personas entrevistadas destacan consistentemente la importancia de contar con referentes femeninas para fomentar la participación de las mujeres en la tecnología y la ciberseguridad. Se considera que la visibilidad de mujeres que ya trabajan y han tenido éxito en estos campos es crucial para inspirar a nuevas generaciones y contrarrestar los estereotipos existentes.

En este marco, se mencionaron distintos perfiles que, para algunas personas entrevistadas, representan trayectorias destacadas en áreas vinculadas a la ciberseguridad, la tecnología, la innovación digital o la producción de datos. Entre los nombres señalados se encuentran mujeres que ocupan roles de liderazgo, investigación, desarrollo o activismo en estos campos, así como también quienes se destacan por su conocimiento sobre la participación de mujeres

en programas tecnológicos. Se mencionaron, por ejemplo, mujeres que impulsaron el desarrollo temprano de infraestructura digital en el país, fundadoras de espacios vinculados a la ciberseguridad y la economía digital, impulsoras de estudios sobre género y tecnología, líderes en el sector legal y educativo vinculado a la transformación digital, y referentes en industrias creativas y de videojuegos con enfoque inclusivo.

Otras voces, comparten su experiencia en actuales empleos y trayectorias educativas y profesionales, sin mencionar mujeres referente en particular. Desde el sector privado una referente indica: *"Mujeres que trabajan en ciber que visibilicen su trabajo. Yo no conozco ninguna. Ese role model"*.

Una experta en el ámbito de la ciberseguridad menciona que aunque la participación de mujeres en ciberseguridad en Uruguay es menor que en tecnología en general, sí existen mujeres referentes, aunque quizás no sean tan visibles. En su propia experiencia, tuvo una docente mujer en la universidad que la inspiró en el área de auditoría y seguridad; ella fue una referente importante en su camino profesional.

“yo creo que solamente conozco a una referente femenina, a una a una este a una persona vinculada a las a la ciberseguridad del del sexo femenino”.

“No, no tengo así que yo diga, escucha, por ella es que yo estoy acá. Porque en realidad ni en la carrera militar. También soy de las primeras generaciones de mujeres en la carrera militar Así que ni en la carrera militar ni en la parte de tecnología me fue una mujer que me dijo, "Vamos a estudiar esto, vamos a hacer esto." O que yo la haya tenido muy cerca” .

Se comparte que la creación de redes y espacios de encuentro solo para mujeres también se ve como una forma crucial de generar apoyo mutuo y potenciar la visibilidad. Referente en el área de Recursos Humanos comparte que hay muchas mujeres destacadas en la comunidad de mujeres en tecnología y que es clave visibilizar sus trayectorias para inspirar a otras.

Referente del sector jurídico coincide, y comparte experiencias en este sentido:

“lo que he visto que generalmente ayuda un poco más a generar un sentido capaz que hasta de identidad y de apoyo son mucho los grupos comunitarios, en el sentido de por decir algo, no sé, en determinados países se arma grupos de mujeres, por ejemplo, en determinada tecnología, por ejemplo, mujeres en inteligencia artificial, mujeres en blockchain, mujeres en ciberseguridad. Eso muchas veces ayuda también a generar esos vínculos y esos vínculos empiezan a intentar abrir otros y

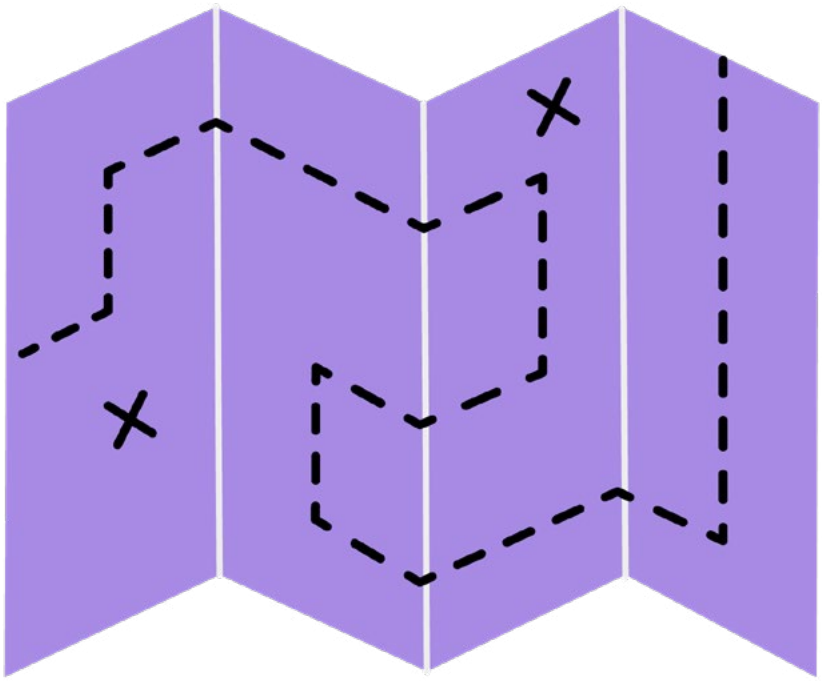
se generan eventos, iniciativas y bueno, eso a veces también ayuda mucho como a generar un poco un dinamismo a nivel grupo"

En definitiva, la escasa visibilidad de referentes femeninas en ciberseguridad no solo **limita la proyección de nuevas generaciones hacia el sector**, sino que también **reproduce imaginarios que refuerzan su masculinización**. La investigación muestra que, si bien existen mujeres con trayectorias destacadas, su **reconocimiento es fragmentado** y muchas veces confinado a círculos especializados. La intersección entre los relatos personales recogidos en los grupos focales y las percepciones institucionales relevadas en las entrevistas revela una necesidad urgente: **construir una narrativa colectiva que visibilice, legitime y multiplique la presencia de mujeres en distintos niveles del ecosistema ciber**. Generar espacios de visibilidad, redes de apoyo y comunidad no es solo una estrategia de empoderamiento individual, sino una condición estructural para transformar el sentido de posibilidad que niñas, jóvenes y mujeres proyectan sobre su lugar en el sector.

6.

Mapas de acción

6.1 Principales conclusiones



- **La llegada al sector de ciberseguridad para las mujeres ha sido mayormente fortuita y no planificada**, resultado de necesidades organizacionales o reconversiones laborales, más que de una elección consciente e informada. Esto se relaciona directamente con lo novedoso de la temática y el escaso **conocimiento y difusión** que ha habido sobre las múltiples facetas del área, sus rutas formativas y oportunidades laborales.

- Una de las principales vías de entrada, y un facilitador clave, es el **interés genuino en el conocimiento y una curiosidad autodidacta**. Muchas entrevistadas destacan una inclinación natural hacia el aprendizaje constante y la exploración de nuevas áreas de la tecnología, lo que les permite adentrarse en la ciberseguridad incluso sin una formación formal previa específica.

- Asimismo, las **trayectorias híbridas y la reconversión profesional** emergen como un facilitador fundamental. La posibilidad de ingresar al campo desde otras disciplinas –ya sean técnicas, humanísticas o de salud, como se observó en el perfil de algunas participantes– demuestra que la ciberseguridad es un campo permeable que valora la diversidad de pensamiento y enfoques. Esta apertura permite que mujeres con distintas bases de conocimiento encuentren su lugar.

- Existe un **fuerte imaginario social masculinizado** del profesional en ciberseguridad Este estereotipo de un hombre técnico y muy capaz actúa como una **barrera simbólica** que dificulta el acceso de las mujeres, haciéndolas percibir el campo como ajeno o de difícil entrada.

- A su vez, se identifican **cualidades personales percibidas como necesarias y deseables** en el rubro (como tolerancia al error y al fracaso, experimentación, osadía) que son asociadas socialmente de forma más acentuada al **género masculino**. Esta percepción puede **incidir negativamente en la autopercepción de las mujeres**, generando dudas sobre su capacidad o disposición para afrontar los desafíos del sector.

- Se destaca que las **barreras para el acceso y la participación femenina en el sector comienzan en la socialización primaria y secundaria**. Desde la infancia, los estereotipos de género asocian lo técnico a lo masculino, y esta tendencia se refuerza en los centros. **La falta de referentes femeninos visibles** en STEM y ciberseguridad agrava esta situación, dificultando que niñas y adolescentes se imaginen a sí mismas en estos campos.

- Una vez integradas al sector, las mujeres dan cuenta de **brechas de género tanto "invisibles" como "visibles"** en los ámbitos de formación y trabajo.

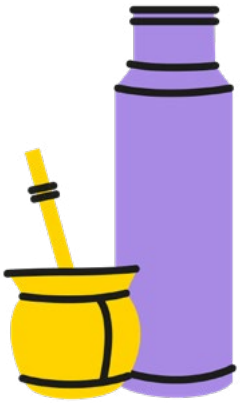
- Las **"invisibles"** incluyen la necesidad de **"adaptarse al ecosistema masculino"**, naturalizando entornos no inclusivos y micromachismos

para ser aceptadas profesionalmente. Esto a menudo implica la necesidad de desarrollar una **personalidad "fuerte"** y **"hacerse escuchar"** en entornos predominantemente masculinos.

- Las **"visibles"** abarcan **discriminación directa** (no ser escuchadas, salarios inferiores, la minimización de aportes) y **segmentación de roles** hacia áreas no técnicas ("blandas"), como gestión o normativa, limitando su acceso a funciones que pueden ser socialmente más valoradas y/o técnicas.

- No obstante estos obstáculos y dificultades, el sector de ciberseguridad ofrece **facilitadores importantes** que motivan la elección y permanencia de las mujeres. Estos incluyen la **alta empleabilidad**, los **buenos salarios**, la **naturaleza desafiante y creativa** del trabajo, y la **percepción de posible flexibilidad laboral** que puede ayudar a conciliar la vida privada y profesional (aunque esta conciliación no siempre se logra fácilmente en la práctica), la posibilidad de **impactar positivamente** (protección de datos y derechos) y la **existencia de múltiples roles y enfoques** que se le puede brindar al sector, entre las más destacadas.

- Un aspecto vital para el sostenimiento de las mujeres en este ámbito es el **capital simbólico familiar y las redes de apoyo en el hogar**. El respaldo emocional, la comprensión de la exigencia de la profesión y, en muchos casos, la colaboración en las tareas de cuidado, permiten a las mujeres gestionar de mejor manera las demandas de una carrera en ciberseguridad. La posibilidad de contar con una estructura de apoyo sólida en el entorno familiar libera tiempo y energía, permitiéndoles dedicarse a la formación continua y al desarrollo profesional que este campo exige.



- Es fundamental problematizar la ciberseguridad más allá de sus componentes puramente técnicos y tecnológicos. Este estudio subraya la necesidad de **reconocer cómo la ciberseguridad impacta directamente en los cuerpos y las vidas de las personas**, lo que

implica una ineludible dimensión social y ética. En este sentido, la ciberseguridad es también un problema social e interdisciplinario, moldeado por los comportamientos humanos, regulaciones y las políticas públicas, y no únicamente una cuestión de tecnología (Foley & Basu, 2024). Desde esta perspectiva, la ciberseguridad debe entenderse como un derecho a una ciudadanía digital segura e inclusiva, con un énfasis particular en la protección y empoderamiento de mujeres, niñas y poblaciones vulnerables. Esto es crucial porque las mujeres son con frecuencia sujetos de abusos habilitados por la tecnología, como el ciberacoso, la ciberhostigamiento y el abuso basado en imágenes. Estos abusos rara vez son considerados por los controles de ciberseguridad comunes. Cerrar la brecha de género no implica solo aumentar la proporción de mujeres trabajando en el sector, sino también abordar los sesgos de género en que se conceptualizan la ciberseguridad y el ciberriesgo (Foley & Basu, 2024).

Integrar esta visión (inspirada en la perspectiva propuesta desde el sector emprendedor) es crucial para diseñar políticas y programas que no solo protejan sistemas, sino que también promuevan equidad y bienestar en el espacio digital.

6.2 Recomendaciones

- **Mejorar la difusión y el conocimiento del área:** Informar sobre las múltiples facetas de la ciberseguridad (no solo técnicas) y las rutas formativas y profesionales disponibles. **Diseñar rutas formativas claras y accesibles.**

- **Abordar estereotipos de género desde la infancia:** Contrarrestar la socialización primaria y secundaria que asocia lo técnico y científico a lo masculino. **Fortalecer la difusión temprana de la ciberseguridad entre niñas y adolescentes.**

- **Profundizar programas educativos y campañas que desmitifican el perfil del profesional de ciberseguridad** y acerquen a las niñas a las tecnologías desde edades tempranas. Es fundamental fomentar el interés en STEM desde la niñez, mostrándola como un área accesible y con diversidad de roles más allá de lo puramente técnico.

- **Visibilizar referentes femeninos en ciberseguridad:** Ofrecer modelos a seguir para niñas y adolescentes en STEM y ciberseguridad. Promover historias de mujeres líderes y profesionales en el área para inspirar y dar legitimidad al ingreso de más mujeres en el sector.

- **Adaptar la formación:** Promover activamente la participación femenina en cursos, ofrecer modalidades más flexibles (online) para facilitar la conciliación, y abordar posibles actitudes misóginas en el ámbito académico. Se necesitan opciones de formación más cortas y accesibles, como tecnicaturas, y profundizar la oferta de becas o apoyos financieros para eliminar barreras.

- **Promover entornos laborales más inclusivos**: Impulsar cambios en las culturas organizacionales para que las mujeres no tengan que

“adaptarse” al modelo masculino, sino que se fomente activamente la diversidad de estilos y liderazgos. Combatir la discriminación directa (salarios, minimización de aportes) y la segmentación de roles hacia áreas no técnicas

- **Impulsar políticas de equidad en la asignación de roles técnicos:** Evitar la segmentación de tareas basada en estereotipos de género y garantizar oportunidades de acceso a posiciones técnicas de alta responsabilidad.

- **Ajustar los procesos de reclutamiento:** revisar la redacción, vías y formas de comunicación de los puestos laborales, principalmente evitar largas listas de requisitos que puedan disuadir a las mujeres. La implementación de políticas de igualdad de oportunidades a la interna de las organizaciones. Ofrecer flexibilidad en las modalidades de trabajo es un factor importante para facilitar la conciliación de la vida laboral y personal. Se sugiere considerar perfiles diversos (no solo técnicos) para roles en ciberseguridad. Se reportan algunas experiencias donde la valoración de las habilidades de las mujeres no se basó únicamente en su competencia técnica, sino que estuvo permeada por prejuicios de género. Esto puede manifestarse en preguntas inapropiadas, una subestimación de sus logros o la preferencia implícita por perfiles masculinos.

- Realizar capacitaciones y **promover entornos laborales que prevengan la discriminación directa por género, y que valoren la diversidad de estilos de comunicación, trayectorias e identidades**. Es fundamental generar culturas organizacionales en las que las mujeres no se vean forzadas a adoptar comportamientos percibidos como “masculinos” ni a silenciar aspectos de su vida personal para ser aceptadas o tomadas en serio.

- **Combatir micromachismos:** Erradicar comentarios y actitudes que cuestionan la dedicación de las mujeres por sus roles de género.

- **Fomentar cualidades percibidas como "masculinas":** Apoyar a las mujeres en el desarrollo de características como la tolerancia al error o la autoexigencia, o redefinir cómo se perciben estas cualidades sin sesgos de género.

- **Generación de comunidad y redes de apoyo:** Fomentar y apoyar la creación de grupos comunitarios y redes de mujeres en tecnología y ciberseguridad desde todas las disciplinas participantes en el sector puede generar un espacio de apoyo, networking y mentoring.

6.3 Oportunidades estratégicas

- **Potenciar sectores con mayores avances institucionales en inclusión y seguridad:** El sector bancario, especialmente a través de sus estrategias de formación continua, inducción institucional y profesionalización del área de ciberseguridad, representa un modelo a considerar. Sin embargo, estas buenas prácticas no siempre se diseñan ni evalúan con enfoque de género. Integrar esta dimensión podría contribuir a ampliar la participación de mujeres en áreas técnicas y de liderazgo dentro de sectores tradicionalmente masculinizados.

- **Incorporar de forma estructural la dimensión jurídica con perspectiva de género:** Varias personas entrevistadas señalaron una ausencia crítica de formación en derecho digital en ámbitos clave como la Facultad de Derecho. Esta carencia impacta negativamente

en la posibilidad de que mujeres provenientes de disciplinas jurídicas encuentren una vía legítima de entrada al campo de la ciberseguridad, contribuyendo así a mantener su carácter excluyente y sobrerrepresentado por perfiles técnicos masculinos.

- **Intervenir sobre los procesos de decisión estratégica con enfoque inclusivo:** La falta de sensibilización sobre género en los niveles jerárquicos y de dirección empresarial fue señalada como una barrera estructural. La resistencia o indiferencia de la alta dirección frente a los desafíos de paridad e inclusión impide transformar los entornos laborales desde sus estructuras de poder. Capacitar a líderes y reclutadores en sesgos inconscientes y liderazgo inclusivo aparece como una línea de acción prioritaria.

- **Reconocer que la inequidad de género se reproduce en un ecosistema aún inmaduro:** La limitada madurez del campo de la ciberseguridad en Uruguay —diagnosticada por múltiples actores— configura un doble desafío. Por un lado, impide generar trayectorias estables y accesibles para todas las personas. Por otro, agrava las desigualdades de género, al dejar en manos de estrategias informales o individuales (como el networking, el autodidactismo o la exposición constante) las oportunidades de inserción. Incorporar la perspectiva de género desde el diseño mismo de este ecosistema en construcción representa una oportunidad clave para revertir esta tendencia.

7.

Referencias Bibliográficas

Batthyány, K., Katzkowicz, S., & Scavino Solari, S. (2022). *Género y teletrabajo: El caso de las trabajadoras del programa Uruguay Crece Contigo.* Psicoperspectivas, 21(3). https://dx.doi.org/10.5027/psicoperspectivas-vol21-issue3-fulltext-2600

Caballero, Z. (1998). Clio & Asociados (3), pp. 79-87. En Memoria Académica. http://www.memoria.fahce.unlp.edu.ar/art_revistas/pr.10223/pr.10223.pdf

Canclini Masserini, M. & Fernández-Darraz M. C. (2024). *Elecciones vocacionales de mujeres jóvenes: factores familiares, sexismo y motivaciones académicas.* CALIDAD EN EDUCACIÓN, 60, pp. 5-28. https://doi.org/10.31619/caledu.n60.1438

Chan, R.C.H. (2022). *A social cognitive perspective on gender disparities in self-eficacy, interest, and aspirations in science, technology, engineering, and mathematics (STEM): the influence of cultural and gender norms.* International Journal of STEM Education, 9 (37). https://doi.org/10.1186/s40594-022-00352-0

Fang, D.; Kang, S. K. & Kaplan, S. (2022). *We need to make sure telecommuting does not exacerbate gender disparity.* The Lancet, 400(10355), pp. 795 - 797.

Flacso, 2018

Foley, M. & Basu, S. (2024). Decoding the gendered imaginary of cybersecurity careers: a social shaping of technology perspective. Information, Communication & Society, 28(8), 1425–1441. https://doi.org/10.1080/1369118X.2024.2391818

Giuzio, G. & Cancela, M. (2021). *Teletrabajo e inequidades de género*. Revista Internacional y Comparada de RELACIONES LABORALES Y DERECHO DEL EMPLEO, 9(1), pp.

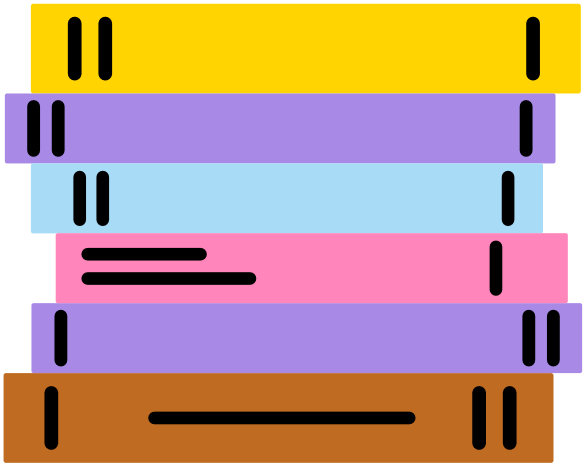
Hernández Sampieri, 2014

Marradi, Archenti y Piovani (2007)

Paris, L. (2011). *Teletrabajo y género: perspectivas de los teletrabajadores acerca de la conciliación familia - trabajo.* III Congreso Internacional de Investigación y Práctica Profesional en Psicología XVIII Jornadas de Investigación Séptimo Encuentro de Investigadores en Psicología del MERCOSUR. Facultad de Psicología - Universidad de Buenos Aires, Buenos Aires.

Peacock, D. & Irons, A. (2017). *Gender Inequalities in Cybersecurity: Exploring the Gender Gap in Opportunities and Progression.* International Journal of Gender, Science and Technology, 9(1)

Sandoval Casilimas, 1996



8.

Anexos

8.1 Elementos de contexto adicionales sobre la agenda de ciberseguridad

A continuación, se presentan hallazgos colaterales identificados durante la implementación de la presente investigación. Si bien no responden directamente a la pregunta principal del estudio, aportan insumos valiosos para comprender el contexto estructural en el que se inserta el campo de la ciberseguridad en Uruguay. Estos elementos resultan especialmente relevantes para el diseño e implementación de políticas públicas orientadas al fortalecimiento del sector.

Se observa un consenso amplio entre las personas entrevistadas sobre la creciente relevancia y la necesidad urgente de fortalecer la ciberseguridad en Uruguay. Si bien se reconocen avances en la agenda pública y el desarrollo de estrategias, la situación actual presenta desafíos significativos.

En particular, durante las semanas en que se realizaron las entrevistas, la ciberseguridad ha ganado un lugar importante en la agenda pública, especialmente a raíz de incidentes recientes en oficinas públicas y empresas privadas.

Referentes de organismos internacionales recuerdan *“acá en Uruguay hemos visto en las últimas dos semanas amenazas de bomba, ciberataques también donde publicaron la foto y el número de celular del presidente (...) Así que creo que en ese sentido en Uruguay ocupa un punto importante de la agenda"*. Un experto senior en ciberseguridad concuerda, indicando que los recientes ataques tuvieron *“una impronta claramente política”*. *"(...) Justo en estos días que ha habido una serie de ciberataques (...) lo que he visto son*

cosas muy básicas, pero que han tenido un impacto a nivel mediático (...) Es algo que de alguna manera está en boga y ayuda mucho a crear conciencia, lamentablemente".

Si bien el tema de la ciberseguridad está cada vez más presente en la sociedad, en gran parte impulsado por los mencionados ataques que lo han vuelto más próximo y visible, no se le da la relevancia que realmente debería tener. **Persiste una falta generalizada de concientización en amplios sectores de la población y organizaciones, viéndose a menudo como algo minimizado o lejano**. Desde la academia se lo describe como hacer ***"ciberseguridad por esperanza"***, esperando que no suceda nada, mientras que desde los profesionales se lo asocia a la alfabetización digital en ciertos grupos etarios:

"esto es un es una percepción, no es algo que pueda tener con datos concretos, pero sí a partir de la percepción que me da los diferentes ataques o puntualmente estafas que se vienen repitiendo en el último tiempo, creo que un grupo que va entre los 45, 50 años hacia arriba de edad, y sin distinción de formación educativa, creo que es un grupo que está bastante vulnerable en ese sentido, más allá de las diferentes campañas que se han hecho para generar conciencia al respecto".

Las percepciones de las personas entrevistadas sobre la ciberseguridad a nivel estatal son disímiles: por un lado, se considera que a pesar de tener lineamientos del sector político, **el sector público muestra una gran fragilidad y una respuesta lenta a los problemas actuales**. Por otro lado, se comparte una percepción de estancamiento en los últimos años. Por último, se percibe que el tema **no estuvo en la agenda de las últimas elecciones nacionales, y que no es un tema prioritario.**

"El sector público claramente sigue los lineamientos del sector político (...) Uruguay tenía un rol de líder en la región. Hoy ese rol se está perdiendo porque hubo 5 años años que no pasó nada"

(Experto senior en ciberseguridad).

Desde la política uruguaya se atribuye esto a una idiosincrasia de "bajísima percepción del riesgo" (*"acá nos conocemos todos"*, *"inocencia institucional"*). Se considera que hay una baja percepción de "cuánto es mucho", ya que las cantidades de transacciones en Uruguay a menudo no desafían los sistemas como lo harían en mercados más grandes. **Esto provoca que la seguridad digital no sea tenida en cuenta aún como un componente más de la seguridad nacional.**

"Tenemos una idiosincrasia de una bajísima percepción del riesgo. Es eso. ¿Cómo vos me podés decir, 'Yo gasto millones de dólares en el guardián para proteger las pruebas de mi sistema criminal o del sistema que me permite investigar casos criminales y tengo esa inocencia institucional que permite que alguien entre con una cuadernola a copiar la información de la pantalla? (...) Ese concepto de que la seguridad digital sea un componente más de la seguridad nacional es todo un tema y hay que empezar a ponerlo sobre la mesa porque eso te genera roles, y te genera cierta conciencia" (Referente del sector público).

Referente del sector jurídico considera que el tema continúa en la agenda: *"hay un claro interés a nivel del Estado y del gobierno de intentar avanzar, o sea, es una temática que generalmente está sobre la mesa"*.

Desde la academia se comparte que *"Dentro de los planes prioritarios no está la ciberseguridad y hoy en día tienen un problema gigante en sus manos porque estamos viviendo ataques permanentemente en el sector público"*.

En definitiva, los ataques recientes han expuesto una gran fragilidad en este sector, y **las personas entrevistadas coinciden que es un problema grave que no tiene una solución inmediata**

La falta de formación y precaución a nivel institucional y personal es un problema recurrente. Referente del sector privado señala: *"Uruguay necesita trabajar un montón más en ciberseguridad de lo que está trabajando... a nivel institucional, pero también a nivel de formación personal, gente que de repente sube documentos propios a un Drive de Google"*. La sofisticación creciente de los ciberataques, como el phishing requiere respuestas más avanzadas. Desde el sector privado se agrega que *"cada vez son más sofisticadas las técnicas de phishing[11], cada vez son más sofisticados los hackers y por lo tanto cada vez deben ser más sofisticadas las técnicas de firewalls"*.

La conciencia sobre la **responsabilidad individual en la ciberseguridad es limitada**.

11. Siguiendo a Agesic "El phishing es un tipo de ataque informático. Consiste en un conjunto de técnicas que persiguen el engaño de una persona, imitando la identidad de un tercero de confianza, como podría ser un banco, una institución pública, empresa o red social, con el fin de manipularla y lograr que brinde información sensible (por ejemplo, usuarios y contraseñas, datos personales, entre otros)." Enlace aquí

"Si tú le preguntas a la mayoría de la gente, dice, 'Sí, ciberseguridad, entre políticas o avance tecnológico o el firewall, pero es cada uno, o sea, cada persona es responsable de la ciberseguridad porque así es como los hackers entran a un sistema, ¿no?'" (Referente de organismos multilaterales).

Desde las personas emprendedoras se percibe una distancia muy grande entre lo que la sociedad está pudiendo procesar en términos de ciberseguridad y hacia dónde va la situación. Sienten que, a pesar de los recientes acontecimientos en Uruguay que han puesto el tema en la agenda (como ciberataques, filtración de información, amenazas de bomba), **"venimos tarde" en percibir y entender la magnitud del cambio**. Se argumenta que **la naturaleza del "ciberentorno" genera una falsa sensación de anonimato en el que las niñeces son particularmente vulnerables**. Finalmente agregan que **la comprensión pública de la ciberseguridad es mínima**, las soluciones actuales son insuficientes, y la solución pasa por una educación masiva y urgente desde la infancia, junto con una regulación estatal robusta hacia las grandes empresas tecnológicas.

Las reflexiones de referentes del sector bancario comparten que es un sector que ha ido creciendo y madurando en ciberseguridad, reconociendo su importancia fundamental para su supervivencia y actividad diaria. La estructura del área de ciberseguridad también evolucionó: inicialmente integrada con seguridad física, luego dentro de tecnología, y finalmente se creó un área independiente dentro del área de riesgo. Este último movimiento se debió a la necesidad de oposición de intereses entre quienes emiten políticas y controles y quienes ejecutan acciones, como se trabaja con otros riesgos (crediticios, de mercado, operativos). Hasta el momento de la entrevista, desde el sector bancario no habían tenido ningún evento de seguridad "relevante" como brechas o robo de información:

"tanto para lo digital como para lo presencial, nosotros hemos tenido que ir evolucionando en cuanto a lo que es toda nuestra protección de nuestro ecosistema digital en todo lo que tiene que ver con aspecto de ciberseguridad, es decir, ir avanzando en todo el tema de Firewall, en (...) tratar de generar un perímetro seguro que nos permita tanto, porque hoy la banca tanto para lo digital como para lo presencial depende exclusivamente de la tecnología. Es decir, la tecnología es el soporte básico de todo lo que es la actividad financiera".

Con respecto al sector jurídico, el marco regulatorio y sancionatorio, referentes comparten que **si bien se han dado pasos en la regulación, como la ley de ciberdelitos, falta madurez en su aplicación y el régimen sancionatorio es percibido como insuficiente.** Desde el sector jurídico comentan que "*la realidad es que no son significativas [las sanciones] en comparación con lo que pasa en otros lugares del mundo*". También se menciona la falta de adhesión al Convenio de Budapest[12] como una limitación para la cooperación internacional.

12. Es el único tratado internacional en la actualidad que tiene por objetivo central el abordaje integral de la problemática de la ciberdelincuencia: Enlace aquí

A nivel de empresas tecnológicas, las personas expertas en el sector entrevistadas coinciden en que existe una barrera importante en la falta de concientización y entendimiento por parte de la alta dirección de las empresas, lo que dificulta la implementación de medidas de seguridad.

Expertos senior en ciberseguridad analizan que *“el problema es que a nivel organizacional si la cúpula la dirección, los dueños, la alta dirección, como lo quiera llamar, dependiendo de qué tipo de empresa estemos hablando, no está concientizada y no decanta hacia abajo, es un problema este implantar esto”*.

Otra persona experta coincide, puntualizando que las dificultades se encuentran a nivel de los roles de *"tomadores de decisiones de ciberseguridad"*, que a menudo son cubiertos por personas no especialistas, lo que lleva a *"políticas que son pobres"*.

Agregan la dificultad de comunicación entre los perfiles técnicos en ciberseguridad y la dirección, debido a la falta de habilidades blandas para transmitir información compleja. Por último, a nivel general de los sectores empresariales, aún no han realizado ni siquiera diagnósticos básicos de seguridad.

Referentes del sector privado perciben que la ciberseguridad es un tema *"todavía a trabajar"* en Uruguay, a pesar de la creciente atención mediática. Menciona la falta de datos oficiales actualizados sobre el estado de la ciberseguridad a nivel general de las empresas, aunque existen informes de empresas privadas.

Se identifica una necesidad urgente de profesionales con especialización en ciberseguridad.

"No solamente en ciberseguridad, pero en Uruguay y creo que también pasa en otros países es el tema de la gente con habilidades computacionales o digitales" (Referente del ámbito multilateral).

"Muchísimo menos (profesionales de ciberseguridad) de lo que se necesita". En ciberseguridad falta de todo. O sea, no es solo un tema de que falten mujeres, no hay nada, hay poca gente en en ciber, ese es el problema" (Experto senior en ciberseguridad).

"[Antes de pensar en las mujeres] primero tienes que generar el proceso. El tema es que hay una inmadurez del tema en Uruguay" (Referente del sector público).

"Nosotros ahora estamos trabajando en nuestros equipos (...), asumamos que en algún momento del tiempo, será ahora, será dentro de X periodo de tiempo, vamos a tener un ataque. Asumamos que vamos a tener un ataque. Ahora estamos trabajando nuestra capacidad de salir de ese ataque en la forma más rápida y ordenada posible"

(Referente del sector bancario).

Referente en el ámbito multilateral subraya *"crear culturas de ciberseguridad"* dentro de las organizaciones. Esto implica que cada persona, cada empleado, entienda la importancia de acciones básicas como saber si abrir o no un correo electrónico.

"Cuando las personas ingresan al banco(...) hacemos un proceso de inducción que dura una semana (...) Hay una charla específica del equipo de ciberseguridad donde de alguna forma les muestra las alertas o los cuidados que hay que tener para este desde el momento que vamos a tener un usuario del banco y desde el momento que nos convertimos en empleado del banco, nos convertimos en una potencial puerta de ingreso de de ataques" (Referente del sector bancario).

En la misma línea, referentes del sector bancario consideran que hay un componente bien importante que es la educación de la organización para no ser el eslabón más débil, ya que cualquiera dentro de la institución puede ser la puerta de entrada a un ataque. Deben tener una organización preparada, alerta y atenta. Para lograr esto, el área de seguridad de la información emite comunicaciones periódicas y se incluye una charla específica de ciberseguridad en el proceso de inducción para nuevos empleados.

8.1.1 Ámbito de la educación, formación y desarrollo de talento

Diversas personas entrevistadas coincidieron en señalar que Uruguay cuenta con una amplia oferta educativa en el área de tecnología y ciberseguridad, aunque con desafíos importantes en términos de accesibilidad, enfoque y adecuación a distintos perfiles.

La oferta educativa y formativa relevada da cuenta de que:

- Existen carreras universitarias como Ingeniería en Informática o similar (UDELAR, Universidad Católica, UTEC, Universidad de la Empresa, Universidad de Montevideo. Por parte de personas expertas en ciberseguridad se reconoce que éstas históricamente, y en gran medida aún hoy, están muy enfocadas al desarrollo de software.

- Hay licenciaturas que son un poco más cortas (un año menos) que la ingeniería, y a veces están más enfocadas a la gestión.

- Existen cursos de analista y cursos de ciberseguridad en empresas privadas.

Se valoró especialmente la tecnicatura en ciberseguridad de UTU[13] y se mencionó una nueva propuesta de tecnicatura en ciberdefensa impulsada desde el Ejército, orientada al funcionariado público, aunque se reconoció que aún en proceso de obtención de recursos. **Finalmente, se considera que las principales barreras no son estructurales, sino que responden más bien a la percepción de dificultad de la disciplina y a la falta de interés.**

13. https://eduterciaria.utu.edu.uy/2024/06/22/tecnologo-en-ciberseguridad/

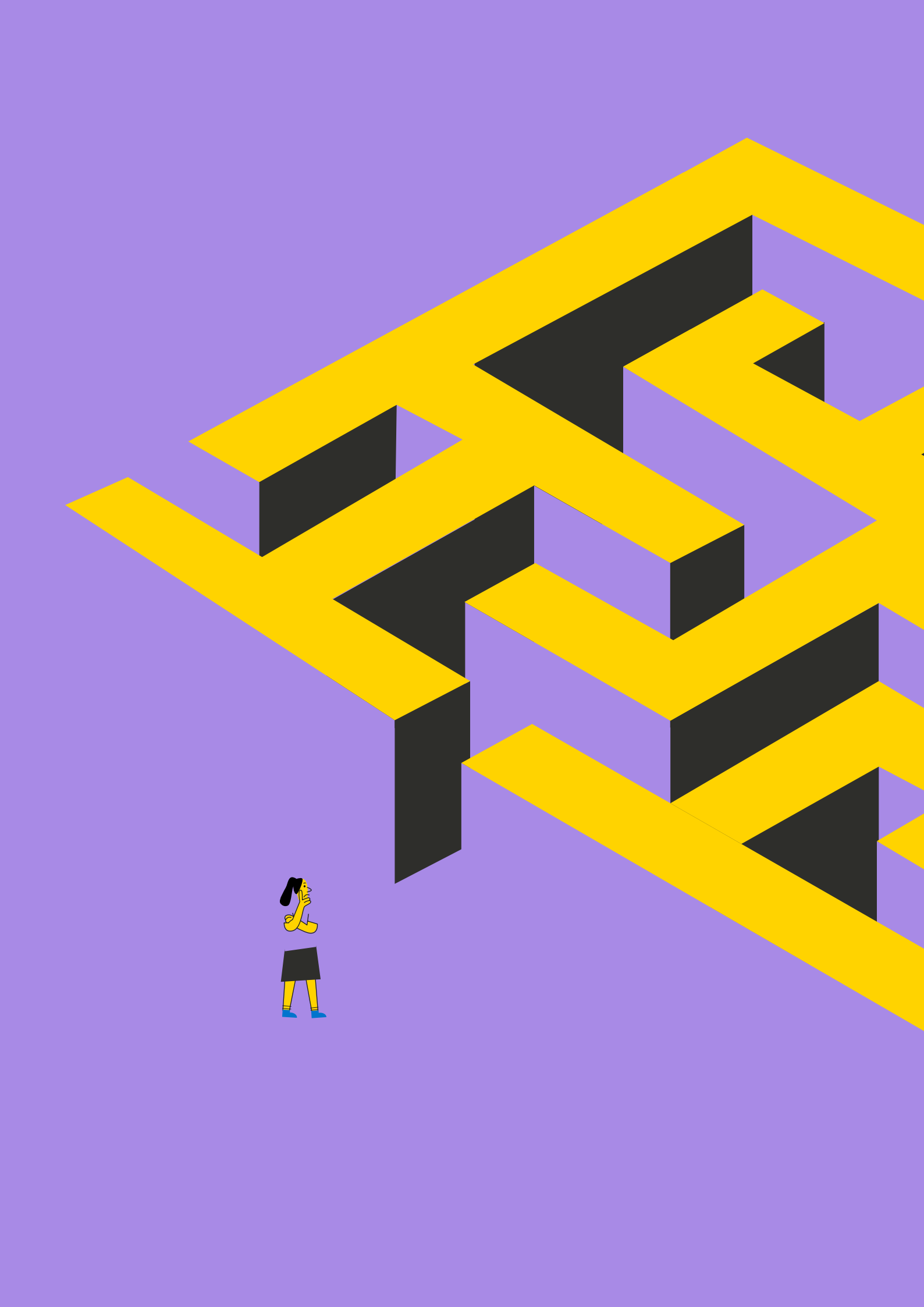
"A veces es difícil que [la ciberseguridad] sea algo que nos llame la atención y que también sintamos que podemos participar y que podemos ser útiles. A veces es normal en nosotras entender que ciertos temas muy técnicos no son nuestros." (Referente del sector público).

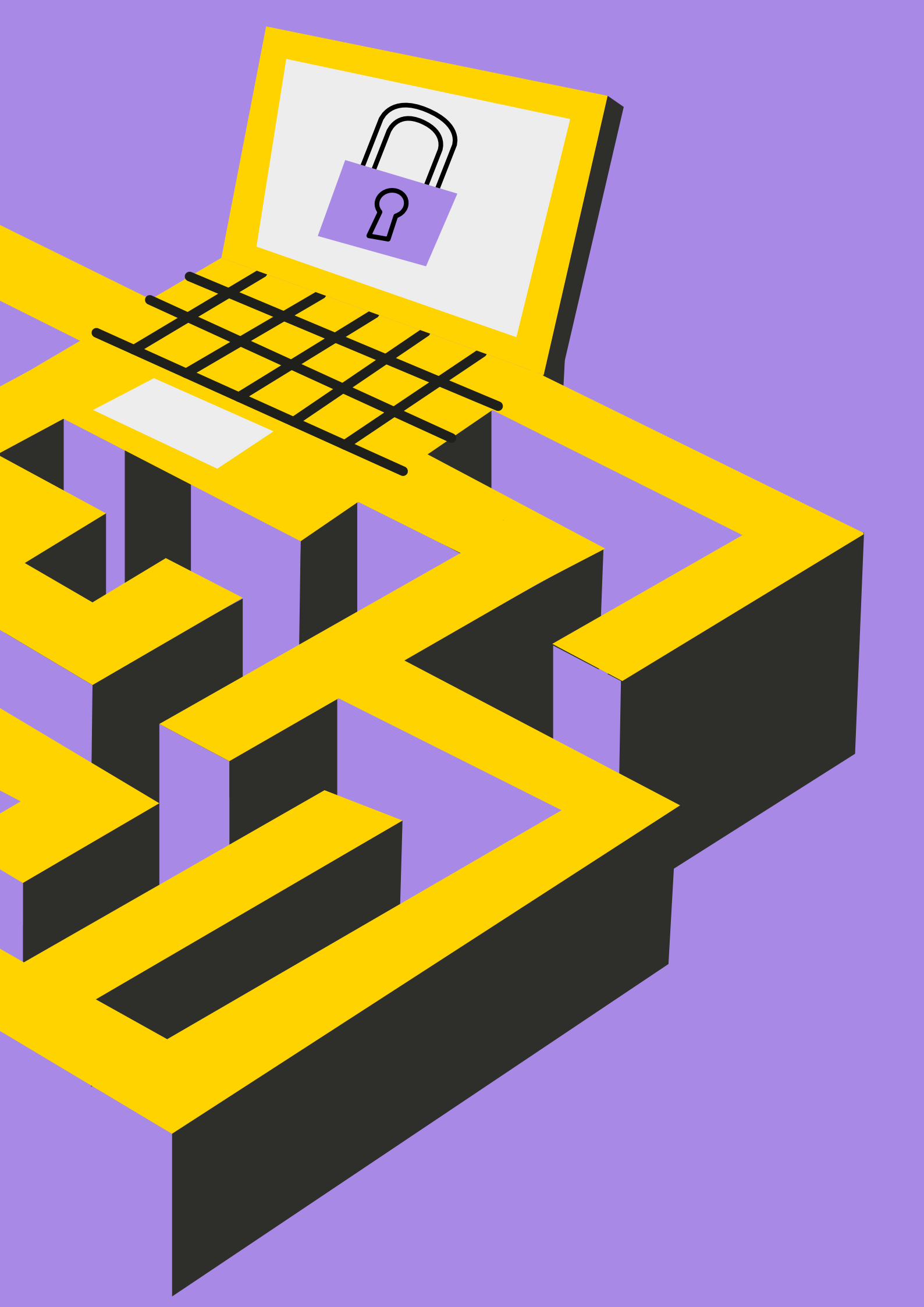
Desde una mirada institucional, se señaló que en la Facultad de Ingeniería de la Udelar los cursos de ciberseguridad requieren un avance considerable en la carrera, lo que limita su accesibilidad. En contraste, se destacaron los programas de UTU e ITS como una oportunidad democratizadora, al no requerir formación previa de grado y permitir el acceso a públicos más amplios. **Esta perspectiva es compartida desde una mirada política, donde se subrayó el potencial del Plan Ceibal para introducir contenidos vinculados a la ciberseguridad desde edades tempranas, y valoró también el papel de UTU, INEFOP y la Licenciatura de Sistemas de UTEC en ofrecer opciones formativas con alcance territorial y flexibilidad.**

En cuanto a los desafíos pendientes, desde los referentes en recursos humanos se advierte que, si bien hay múltiples oportunidades de formación inicial, persiste una brecha entre esa oferta y las opciones de especialización, que muchas veces están por encima del nivel inicial y tienen un costo elevado, configurando una barrera económica importante. Los docentes, por su parte, subrayan la necesidad de fortalecer la formación en habilidades técnicas avanzadas, comparando la escasa disponibilidad actual con la amplitud de la formación pública en otras áreas como la medicina. **Finalmente, expertos alertan sobre una carencia crítica en el sistema educativo: la ausencia de formación específica en derecho digital en la Facultad de Derecho, algo que se considera inaceptable en el contexto actual.**

“Se habla un montón de las habilidades blandas blandas. Yo sé que es muy importante hacer un montón de cosas anexas. [Pero] Las habilidades duras en esta práctica tienen que estar mucho más disponibles para la gente. Como esto necesita mucho esfuerzo, mucha dedicación, ¿no? Necesitamos tener todas estas habilidades mucho más disponibles, más capacitaciones de calidad. ¿Para qué? Para captar más gente. Te lo pongo de otra manera. ¿Cuántos cirujanos existirían en Uruguay si la Universidad de la República no fuera pública?”

(Academia)





Programa de las Naciones Unidas para el Desarrollo en Uruguay(PNUD)
Paraguay 1470, piso 5
CP 11100
Tel: (598) 2909 38 06

Montevideo, Uruguay

www.uy.undp.org

PNUDUruguay

PNUD Uruguay

PNUD_Uruguay

PNUD Uruguay