Mujeres en Ciberseguridad: Perspectiva desde el ámbito laboral costarricense

Karina Rivera, Ariella Quesada
Programa de Investigación y Extensión en Tecnología de Información y Desarrollo
Escuela de Informática, Universidad Nacional de Costa Rica
Heredia, Costa Rica
karyr85@gmail.com, ariella.quesada.rosales@una.cr

***Abstract*— This paper analyzes women's participation as part of the workforce in the area of cybersecurity and the existing gender gap in that field. Through interviews with professionals and associates in the area in Costa Rica, information about the current situation of professionals in cybersecurity was gathered. The interviewees point out that they came to work in positions associated with cybersecurity without previous training, and it was the development of experiences that motivated the insertion in this area. Likewise, it is suggested that there should be greater orientation and motivation, which eliminate stereotypes that mark this type of work so that women can perform in this field.**

Keywords— ***Cybersecurity, women, Costa Rica, gender gap***

***Resumen*— Este trabajo analiza la participación de las mujeres como parte de la fuerza laboral en el área de ciberseguridad y la diferencia de género existente en dicho campo. Mediante entrevistas a profesionales y asociadas al área en Costa Rica, se recolectó información acerca de la situación actual de los profesionales en ciberseguridad. Las entrevistadas señalan que llegaron a desempeñarse en puestos asociados a la ciberseguridad sin formación previa, y fue el desarrollo de experiencias el cual motivó a la inserción en esta área. Asimismo, se sugiere que debe existir una mayor orientación y motivación a las futuras profesionaoles, que elimine estereotipos que marcan este tipo de trabajo para que las mujeres puedan desempeñarse en este campo.**

Palabras clave— ***Ciberseguridad, mujeres, Costa Rica, brecha de género***

I. INTRODUCCIÓN

La Cuarta Revolución Industrial también conocida como la Industria 4.0, fue acuñado por Klaus Schwab fundador del Foro Económico Mundial en el 2016, ha fungido como impulsora de cambios en los paradigmas de trabajo. A diferencia de las revoluciones anteriores que se caracterizaron por nuevas tecnologías emergentes, esta última se identifica por la convergencia de las tecnologías digitales, físicas y biológicas que impactan todas las disciplinas e industrias [1].

Basados en esta afirmación, se puede decir que la Cuarta Revolución Industrial viene a fusionar las tecnologías descubiertas en la Tercera Revolución Industrial brindando nuevas oportunidades de empleos que anteriormente no habían sido contempladas, esto propicia cambios en los procesos, la seguridad y genera nuevas oportunidades que conlleva a utilizar la tecnología con mayor estrategia.

En esta revolución se espera que una serie de factores tecnológicos generen un cambio radical en los paradigmas laborales. Dichos factores incluyen temas relacionados con el auge de los robots, la simulación, los sistemas de integración, el internet de las cosas, la ciberseguridad, la computación en la nube, la realidad aumentada, el manejo del Big Data y las impresiones 3D para procesos de manufactura y la hiperconectividad en general.

Sin embargo, el aspecto tecnológico por sí solo no es el único responsable de las diferencias también se han sumado los ámbitos social, económico y demográfico que presentan una serie de modificaciones las cuales favorecen el surgimiento de nuevas tendencias en cuanto a empleos se trata.

En el Informe *"The Future of Jobs"* [2] para el 2016 señala un incremento gradual de la participación de las mujeres en la fuerza laboral, este elemento se ha considerado como uno de los conductores principales de la Cuarta Revolución Industrial. Asimismo, se ha hecho evidente que conforme pasan los años, los porcentajes femeninos con altos grados académicos y en puestos de jefatura han aumentado.

Luego, el Informe *"The Future of Jobs"* [3] para el 2018 muestra la ciberseguridad como una de las áreas con mayor necesidad de profesionales para el futuro, por la creciente demanda en temas de protección de la información. Tomando en cuenta lo anterior, surge la necesidad de investigar acerca de la participación femenina en el campo profesional de la ciberseguridad, considerando que la brecha de género en carreras tecnológicas siempre ha sido muy marcada (Soto et al. [4]).

Este artículo se divide en cuatro secciones. La segunda sección está dedicada a un análisis general del área de ciberseguridad, así como algunas métricas con respecto a la participación femenina en este campo. El análisis de las

entrevistas a mujeres profesionales en el área de ciberseguridad se presenta en la tercera sección. Por último, en la cuarta sección, se presentan las conclusiones.

II. LAS MUJERES EN CIBERSEGURIDAD

El reporte del Foro Económico Mundial denominado "*The Future of Jobs*" [3] presenta una visión de la fuerza de trabajo mundial futura, proporciona elementos con el fin de comprender el potencial de las nuevas tecnologías para cambiar y crear empleos, además indica una lista de puestos estables para ese año junto con una lista de emergentes para el 2020.

De acuerdo con el Reporte [3] se dará el desarrollo de otros campos de la industria de las tecnologías de información y comunicación (TIC); tal es el caso de los especialistas en seguridad de la información. El Cuadro 1 muestra un listado de los puestos de trabajo relacionados con carreras TIC que jugarán un papel importante en el período 2018-2020.

CUADRO 1. LISTA DE LOS PUESTOS DE TRABAJOS RELACIONADOS CON CARRERAS TIC QUE JUGARÁN UN PAPEL IMPORTANTE EN EL PERÍODO 2018-2020

Puestos estables	**Nuevos puestos**
Desarrolladores y analistas de software y aplicaciones[a]	Analistas de datos y científicos[a]
Analistas de datos y científicos[a]	Especialistas en Inteligencia Artificial y Machine Learning
Profesionales en Bases de Datos y Redes	Especialistas en Big Data
Analistas de Seguridad de la Información[a]	Especialistas en Transformación Digital
Ingenieros en Electrotecnología	Especialistas en Nuevas Tecnologías
Especialistas en Ingenieros en Robótica[a]	Desarrolladores y analistas de software y aplicaciones[a]
	Servicios de Tecnologías de Información
	Especialistas en Automatización de Procesos
	Analistas de Seguridad de la Información[a]
	Especialistas en Ingenieros en Robótica[a]

[a]Según el Informe, las ocupaciones que se encuentran en ambas columnas permanecerán estables, pero a su vez se desarrollarán en otros campos de la industria.

Fuente: Elaboración propia a partir del Informe *The Future of Jobs* [3].

Como se puede observar, los pronósticos para los especialistas en ciberseguridad son positivos con respecto a oferta laboral en las diferentes ramas de este campo.

Dentro de las especialidades en ciberseguridad, según "*The Future of Jobs*" [3], se encuentran desde aquellas que requieren de muchos años de experiencia hasta las tareas que pueden ser realizadas por recién graduados. Algunas de las áreas más generales incluyen:

- Gobierno Corporativo, Riesgo y Cumplimiento: generalmente estos equipos se encargan de verificar el cumplimento de las buenas prácticas y estándares de las empresas para medir los riesgos y elaborar planes de contingencia y recuperación en caso de ser necesarios. Las funciones de estos especialistas suelen relacionarse con las de los auditores internos y, comúnmente, requieren de amplio conocimiento sobre las políticas de la empresa, por lo que es normal que estos puestos sean ocupados por personas con mucha experiencia.
- Respuesta a incidentes: en ciberseguridad, este tipo de rol se encarga de la detección de problemas y, mediante las acciones pertinentes según el caso, corregir dichos problemas.
- Análisis de datos forenses: estos profesionales se encargan de analizar los hallazgos de un ataque para descifrar qué hizo el atacante y cómo fue llevado a cabo el ataque. Se refiere a una especie de ingeniería inversa con el fin de encontrar los orígenes de las amenazas de seguridad.
- Pruebas de penetración: este tipo de trabajo se lleva a cabo mediante ataques planeados a los sistemas, con el fin de detectar fallos en la seguridad y su posterior corrección. Por lo general los encargados de estas funciones operan de manera anónima ya que, además de las herramientas tecnológicas, también se valen de estrategias como la ingeniería social para acceder a los objetivos.
- Desarrollo de software: dentro de los departamentos de ciberseguridad es muy común encontrar equipos de trabajo dedicados al desarrollo de software, ya sea en términos de aplicaciones específicas para la seguridad de la empresa o para mantenimiento de plataformas ya existentes. También dentro de este grupo de profesionales se encuentran aquellos que desarrollan pruebas para labores de control de calidad.
- DevOps: son los encargados de labores como la instalación, operación y configuración de software, en el caso de la seguridad, un ejemplo podría ser un firewall.
- Administración de identidades y accesos: estos son roles que requieren de un manejo muy especializado de las políticas de la empresa y todos los roles. Les corresponde la identificación, la autorización o desautorización de permisos para mantener el cumplimiento de los estándares de seguridad de la información e incluso, los estándares de seguridad de activos y controles de accesos físicos.
- Prevención de pérdida de datos: este trabajo, como su nombre lo menciona, se encargan del manejo y producción de aplicaciones que ayudan en la detección

de software malicioso en los sistemas. Algunas labores incluyen asegurar que haya una buena interacción con las nuevas aplicaciones instaladas y el constante monitoreo en las bases de datos y servidores [5].

El tema de las opciones de especialidades en seguridad, como se puede ver es muy vasto. En contraste con las opciones de trayectoria profesional, la diversidad de género en estos campos se queda estancada.

La participación femenina en las tecnologías de información representa el 20% del total (Soto et al. [4]). Este porcentaje se disminuye todavía más si se toma en consideración la cantidad de mujeres que se desempeñan en el área de la ciberseguridad. Estudios realizados por Frost y Sullivan [6] señalan que Norteamérica es la región con el índice más alto de mujeres que laboran en ciberseguridad, con un 14%. A nivel mundial, solamente el 11% de la fuerza laboral de ciberseguridad corresponde a mujeres.

Adicionalmente, existe una brecha salarial ligada al género, donde las mujeres en ciberseguridad ganan considerablemente menos que los hombres. Esta situación se torna más difícil de explicar si se toma en cuenta que las mujeres, en este campo, tienen un 6% de grados académicos más altos que los obtenidos por los hombres [7].

Otros estudios señalan que la ausencia de participación femenina en este ámbito se debe a la falta de información (Soto et al. [4]) y de orientación acerca de cómo pueden encaminar sus intereses (no necesariamente informáticos) a la ciberseguridad [8], así como estereotipos que marcan las carreras tecnológicas como terreno no apto para las mujeres.

En una industria cuya mayor representación es masculina, es necesario aprender a retener el talento femenino. Sin embargo, Frost y Sullivan [6] encontraron que la mayoría de las mujeres no sienten que su labor cuenta con la mentoría apropiada ni con el respaldo que les gustaría para desarrollar el máximo potencial de su carrera. Por lo tanto, el factor motivacional juega en contra a la hora de promover el interés femenino por permanecer en ciberseguridad.

Según Terwoerds y Naidoo [9], una razón adicional para el estancamiento de los porcentajes femeninos en ciberseguridad es que no hay un verdadero progreso de las mujeres en roles de liderazgo optando finalmente por apartarse. La existencia de programas apropiados de capacitación, mentorías especializadas y un correcto apadrinamiento por parte de los superiores son factores que marcan la diferencia entre una mujer que siente que su rol es importante y valorado y una que no. Aunado a ello, la motivación puede traducirse en sentido de pertenencia.

Se estima que para el 2022, el déficit de profesionales en ciberseguridad ascenderá a 1.8 millones aproximadamente (Frost y Sullivan [6]). Sin embargo, el porcentaje de mujeres ha estado estancado durante años, por lo cual el panorama se muestra un poco nublado con respecto a la disminución de la brecha de género.

Efectivamente, una mayor participación femenina podría ayudar a reducir considerablemente la diferencia entre cantidad de hombres y mujeres que se desempeñan profesionalmente en ciberseguridad, sin embargo, los números no han variado lo suficiente en los últimos años. Según, Joyce Brocaglia (2017), la principal herramienta en la lucha por una industria más equitativa es un cambio de cultura que comienza desde el proceso de reclutamiento [10].

La inclusión de mujeres en los análisis de candidatos y entrevistas es fundamental para que aumente la cifra de contrataciones, debido a que existe una tendencia en el ser humano a reclutar a aquellos candidatos con quienes se siente identificado, por lo que tener mujeres en las comisiones de reclutamiento puede ser favorable para que más candidatas sean seleccionadas [10].

El incentivar a las mujeres desde que son estudiantes puede generar una mayor participación en el área al momento de aplicar a un puesto de trabajo. En "*The 2017 Global Information Security Workforce Study: Women in Cybersecurity*" [6] se hace un análisis relacionado a la preparación académica que tienen las mujeres que se desempeñan como profesionales de ciberseguridad en puestos de dirección o superiores, a nivel mundial. Un dato interesante es que, si bien la mayoría cuenta con una carrera en el área de Ciencia, Tecnología, Ingeniería y Matemáticas (CTIM o STEM, por sus siglas en inglés), este porcentaje es menos de la mitad, como se muestra en el Cuadro 2.

CUADRO 2. PORCENTAJES DE ESPECIALIDADES DE MUJERES EN CIBERSEGURIDAD CON PUESTOS DE DIRECCIÓN O SUPERIORES, POR ÁREA ACADÉMICA

Área	Porcentaje
Ciencia, Tecnología, Ingeniería y Matemáticas	40%
Comercio y Finanzas	18%
Ciencias Sociales y Humanidades	17%
Educación	2%
Arte	1%

Fuente: Elaboración propia con información de "The 2017 Global Information Security Workforce Study: Women in Cybersecurity" [6].

III. PERSPECTIVA DE LA PARTICIPACIÓN DE MUJERES COSTARRICENSES EN CIBERSEGURIDAD

Con el propósito de conocer la perspectiva de la participación de mujeres en ciberseguridad en el plano laboral costarricense, se realizó una entrevista a ocho mujeres profesionales que se desempeñan en esta área o asociada a la misma en diferentes empresas. Cabe mencionar que la búsqueda de las participantes fue extensa, sin embargo, se encontraron pocas mujeres asociadas a este campo laboral.

El instrumento utilizado fue una entrevista semiestructurada dividida en tres apartados: aspectos generales, desempeño profesional y brecha profesional. Cada una de las entrevistas tenía una duración entre 30 y 45 minutos.

En el apartado de aspectos generales se consultó acerca del grado académico, experiencia profesional y formación académica en ciberseguridad. En cuanto al desempeño profesional, se orientó a las razones que motivaron participación, así como su experiencia en esta área. Por último, se solicitó indicar los factores para reducir la brecha de género y elementos que motiven la participación femenina en ciberseguridad. Los resultados se presentan a continuación.

A. Aspectos generales

Todas las mujeres entrevistadas se desempeñan en empresas transnacionales. En su formación académica, cuentan con un título de bachillerato universitario como máximo grado académico, para efectos de esa investigación no se tomó en cuenta si actualmente se encuentran cursando algún posgrado.

Luego se les hace la consulta de que antes de desempeñarse en el área de ciberseguridad, ¿contaba con formación académica en esta área? o si ha realizado alguna especialización en ciberseguridad, las entrevistadas afirman no contar con una formación académica previa asociada al área. Sin embargo, su interés las ha llevado a capacitarse de manera autodidacta en temas de ciberseguridad aunado con el desarrollo y desafío de sus tareas laborales.

Cabe señalar que a nivel país se han hecho esfuerzos por la capacitación en temas de seguridad, la Organización de los Estados Americanos (OEA) y Trend Micro Incorporated, (líder mundial en soluciones de ciberseguridad), con el apoyo del Ministerio de Ciencia, Tecnología y Telecomunicaciones durante la primera edición del *OEA Cyberwomen Challenge* capacitaron a alrededor de 60 mujeres en ciberseguridad a finales del 2018 [11]. Por lo tanto, se pueden ver una de las primeras iniciativas a nivel país que busca promover la inclusión de las mujeres en los temas de ciberseguridad.

En cuanto a la experiencia profesional de las entrevistas, las participantes indican que tienen entre los 7 meses y 4 años de laborar en el área de ciberseguridad. Por lo tanto, brindan su opinión a partir de lo que ha sido hasta ahora su experiencia en este campo.

B. Desempeño profesional

Para la parte del desempeño profesional se les consulto acerca de las razones que motivaron su interés en el área de ciberseguridad, donde las respuestas varían entre la marcada tendencia de crecimiento que se experimenta en este campo, las oportunidades laborales, así como algún interés personal más allá de lo tecnológico, la mezcla de los desafíos personales y laborales, y aquella que indica ninguna razón en específico.

En la parte del principal aporte de las mujeres que trabajan en ciberseguridad, todas las entrevistadas coinciden en que el apoyo mutuo entre mujeres en un área que es mayormente dominada por hombres es la contribución más importante. Este apoyo e inclusión se traduce en diversidad en las empresas, debido que se obtienen perspectivas distintas para análisis y resolución de problemas, que son un aporte clave para el éxito empresarial. También indican que son muy detallistas en sus proyectos lo que suma a la fuerza para ser constantes y lograr todo aquello que se proponen.

C. Brecha profesional

A raíz de los bajos niveles de presencia de mujeres en carreras tecnológicas, para lo cual la brecha de género sea acentúa en el campo de seguridad informática donde sólo el 11% de las profesionales son mujeres que trabajan en este campo en todo el mundo, se pregunto acerca de los factores que las mujeres consideran importantes para reducir la brecha de género en ciberseguridad.

En cuanto a los factores que se consideran esenciales para reducir la brecha de género en ciberseguridad, las entrevistadas tienen distintas opiniones acerca del momento propicio durante el proceso de enseñanza-aprendizaje en el que se debería incentivar la participación femenina en ciberseguridad. Sin embargo, todas coinciden en que la información acerca del área es fundamental. Hacerles saber a las mujeres que este campo existe, que pueden ser parte de él y cómo pueden ser parte él.

En la parte de brecha de género, la mayoría de las entrevistadas opina que es una problemática a nivel mundial que no hay diferencia mayor entre Latinoamérica con en el resto del mundo.

Las razones principales por las que las mujeres no suelen desempeñarse en ciberseguridad pueden resumirse en falta de información precisa según las entrevistadas. A la vez mencionan aspectos sociales, educativos hasta la falta de apoyo y motivación.

Después de considerar las oportunidades que brinda el área de ciberseguridad se les consulto acerca de los instrumentos que utilizaría para motivar la presencia femenina en ciberseguridad. Las entrevistadas citan que el principal medio para motivar la presencia femenina en ciberseguridad es la información a través de actividades de sensibilización como talleres, foros y charlas que permiten a las mujeres “novatas” y expertas compartir conocimientos, casos de éxito a nivel nacional e internacional. Es importante visibilizar y reconocer la experiencia profesional y los logros para que cada vez más mujeres se animen a desarrollarse en el campo. Con ello, las interesadas se puedan construir un perfil acorde a las oportunidades que brinda el área de ciberseguridad para el crecimiento profesional.

Otros aportes de las entrevistas señalan que se deben desarrollar nuevos pensamientos y conceptos inclusivos para una eficiente integración de las mujeres en el área de ciberseguridad.

Asimismo, las entrevistadas coinciden con que una mayor diversidad e inclusión (al tener panoramas distintos) aporta grandes beneficios al éxito de las empresas y, que las mujeres brindan ese valor agregado de manera natural.

IV. CONCLUSIONES

Los puestos de trabajo en ciberseguridad continuarán creciendo en los próximos años, a tal punto de generar un déficit de profesionales. Pero, no hay una política clara de cómo reducir tal déficit.

La poca representación femenina en las carreras ligadas a las TIC es una problemática mundial que se agudiza cuando se inspeccionan las métricas en el campo de la ciberseguridad. Existe una brecha de género muy marcada, incluso en términos salariales. Y, esta brecha no parece estar ligada a aspectos de formación académica sino a factores motivacionales y de apoyo.

Una correcta orientación de los intereses puede despertar la atracción de más mujeres para involucrarse en este campo. Estudios demuestran que no es estrictamente necesario tener una especialización en seguridad para tener un rol activo en este campo. Por lo que, a la hora de que una mujer decida enfocarse en ciberseguridad, los aspectos académicos no son tan relevantes como una correcta motivación y mentoría.

La perspectiva de las mujeres entrevistadas corresponde con los datos de falta de información, falta de motivación y estereotipos como piedras de tropiezo para la disminución de la brecha de género y falta de interés.

REFERENCIAS

[1] Schwab, K. (2016). *The fourth industrial revolution.* New York: Crown Business.

[2] WEF, "The Future of Jobs", Colonia/Geneva, Suiza: Foro Económico Mundial (WEF), 2016.

[3] WEF, "The Future of Jobs", Colonia/Geneva, Suiza: Foro Económico Mundial (WEF), 2018.

[4] Soto, M., Corey, R. & Kolmus, P. (2015). Debate: Why is there a lack of women in IT security?. *SC Magazine: For IT Security Professionals.* (Julio-Agosto), 17.

[5] Buster, D., "8 Specializations that Define Successful Cybersecurity Organizations", 23 de agosto de 2018. Disponible en https://www.globalknowledge.com/blog/2018/08/23/8-specializations-that-define-successful-cybersecurity-organizations/

[6] Frost & Sullivan, "The 2017 Global Information Security Workforce Study: Women in Cybersecurity", California, Estados Unidos: Centro Para Ciberseguridad y Educación & Foro de Mujeres Ejecutivas Sobre Seguridad de la Información, Gestión de Riesgos y Privacidad (EWF), 2017.

[7] WEF, "The Global Gender Gap Report 2018", Colonia/Geneva, Suiza: Foro Económico Mundial (WEF), 2018.

[8] Nelson, B. (2014). Women in IT security: *Carpe Diem. SC Magazine: For IT Security Professionals.* (Julio-Agosto), 34.

[9] Terwoerds, L. & Naidoo, S. (2017). Widening The Field. *SC Magazine: For IT Security Professionals.* (Julio-Agosto), 32-34.

[10] Brocaglia, J. (2017). Cyber women on the Hill. *SC Magazine: For IT Security Professionals.* (Julio-Agosto), 49.

[11] El Mundo. (10 diciembre 2018). Capacitan a 60 mujeres costarricenses en temas de ciberseguridad. Disponible en https://www.elmundo.cr/costa-rica/capacitan-a-60-mujeres-costarricenses-en-temas-de-ciberseguridad/