



## LA CIBERSEGURIDAD COMO PROFESIÓN: OTRO ASPECTO QUE MERECE SER ANALIZADO

A través de las numerosas ediciones de boletines que tenemos al día de hoy, hemos abordado diferentes aspectos relativos a la ciberseguridad y las distintas tecnologías. Sin embargo, poco hemos hablado, hasta ahora, de la seguridad informática desde la perspectiva profesional.

Precisamente, ese es el enfoque que queremos darle el día de hoy: **nos interesa pensar la ciberseguridad en términos de lo que implica profesionalmente**, de cuáles son sus alcances, los desafíos que propone y las ventajas de trabajar en áreas relativas a la seguridad informática.

Con el objetivo de ahondar en dicho aspecto, nos dedicamos a investigar de qué forma las empresas y entidades educativas se posicionan frente al campo profesional de la seguridad informática y, a su vez, consultamos a varios profesionales que se desempeñan en diferentes roles dentro del área para conocer sus opiniones.

Según muchos estudios se estima que para 2022 habrá una escasez aproximada de 1.8 millones de especialistas en ciberseguridad, por lo cual considerarla como una posible carrera profesional puede ser una gran idea.

Como resultado de dicho análisis, lo primero que pudimos observar dado que aparece como punto de alerta en múltiples informes y estudios<sup>1</sup> sobre el tema es que, actualmente, los últimos pronósticos elaborados a la luz de los acontecimientos ocurridos durante el 2017, indican que **para el 2022 habrá una escasez de alrededor de 1.8 millones de trabajadores especializados en ciberseguridad**. Ello pone de manifiesto que, con vistas al prometedor futuro que proyecta el área, especializarse en ciberseguridad constituye una excelente idea.

Lo más interesante de todo es que, si bien existe la especialización y diferentes cursos y tecnicaturas en seguridad informática dentro de

las carreras relativas a Sistemas, **los amplios alcances que ha tenido la tecnología –y se propone continuar- vuelven necesario el hecho de que diferentes profesionales de diversas áreas se vean atraídos, se interioricen y puedan trabajar también en ciberseguridad.** Nos referimos, por ejemplo, a abogados, psicólogos, sociólogos, filósofos, especialistas en comunicación y egresados de carreras de Cs. Exactas, aunque la lista bien podría continuar. De hecho, de acuerdo con el informe 2017 Global Information Security Workforce Study de Frost & Sullivan<sup>2</sup>, **uno de cada cinco profesionales que actualmente trabaja en ciberseguridad proviene de sectores que no tienen relación con la tecnología** y, a su vez, el 24% de la totalidad de los profesionales no posee títulos de grado, lo cual demuestra que no se requiere de una profunda experiencia ni habilidades técnicas para iniciarse en el mundo de la ciberseguridad.

**El hecho de que muchos avances de la informática se basen en modelos provenientes de la naturaleza es un aspecto de gran atractivo para muchos profesionales del área.**

Ahora bien, con el propósito de no quedarnos sólo con datos estadísticos e impersonales, conversamos con algunos profesionales que actualmente se dedican a la Seguridad Informática en Argentina y encontramos respuestas las cuales, además de estar en sintonía con los informes disponibles, resultan por demás interesantes y motivadoras.

Por ejemplo, frente a la pregunta acerca de **cuáles consideran que son los principales atractivos que tiene el campo de la tecnología en general y el de la ciberseguridad en particular desde la perspectiva profesional**, destacaron los aspectos divertidos, interesantes e innovadores de las posibilidades que ofrece tanto la seguridad informática,

como la informática en sentido más amplio. Una de las respuestas expresaba: *“saber cómo funciona un virus y cómo la gente buscó su analogía a los virus orgánicos, desde el inicio, me pareció algo totalmente resaltante... imitar la ‘reproducción’ de nivel biológico hacia el nivel digital hace que cualquiera se emocione con ello”*. Y otro de los entrevistados expresó: *“me es muy atractivo que sea una verdadera democratización del conocimiento, a un nivel nunca antes visto en la historia de la humanidad, comparable quizás solo con la invención de la imprenta”*. A su vez, remarcaron como punto de interés el hecho de que la tecnología se haya metido en prácticamente todas las áreas de trabajo –incluso las menos relacionadas a simple vista-, lo cual vuelve crucial la necesidad de proteger y garantizar la validez de recursos e información y revela lo profundamente implicada que está la ciberseguridad en nuestra vida cotidiana. En palabras de una de las entrevistadas: *“la ingeniería social que se aplica en este campo es muy interesante, ver como las personas tienen patrones que pueden ser usados a su favor... o en su contra es una tarea súper importante”*.

El aumento vertiginoso de la tecnologización de nuestra vida cotidiana, requiere que los profesionales estén en constante capacitación.



Debido a que Internet está presente en cada vez más objetos de uso diario, se vuelve fundamental tomar acciones en pos de nuestra ciberseguridad.

Luego, les preguntamos **cuáles creen que son los desafíos más relevantes que propone el mundo de la tecnología** y todos coincidieron en que el principal desafío consiste en poder educar a los usuarios en el uso que hacen de las diferentes TICs; en que logren tomar conciencia de hasta dónde pueden quedar expuestos si no incorporan las medidas de seguridad y prevención necesarias.

Finalmente, quisimos conocer su opinión acerca de **hasta dónde creen que tienen influencia las temáticas relativas a la seguridad informática desde una perspectiva cotidiana, pensándolo en términos de alcance**. Respecto de ello, comentaron que, a causa de la creciente incorporación de la tecnología en las actividades de todos los días (herramientas bancarias online, auriculares conectados por bluetooth, smartwatches, etc.) la ciberseguridad tiene influencia en prácticamente todos los aspectos de nuestra vida cotidiana. Sin embargo, en una de las respuestas destacaban que dichas temáticas *“deberían tener muy poca influencia, deberíamos armar los sistemas de manera tal que con pocos cuidados los usuarios sepan que están en un ‘área protegida’*. *Nuevamente la clave sería la educación, si se naturalizan algunos conceptos y se generaliza cierta información básica, la seguridad informática estaría en la cabeza de todos, pero de una manera no invasiva”*.

A los fines de completar el panorama de los diferentes puntos de vista desde los cuales se puede analizar la seguridad informática, le pedimos su opinión a Sebastián Stranieri (CEO de VU Security) quien lleva varios años desarrollándose en el área y cuenta con vasta experiencia sobre el tema. Así se expresó.

*“Desde sus orígenes en la década del 80, la ciberseguridad en sí no era una profesión. Los especialistas en seguridad informática provenían de otras disciplinas, principalmente ingeniería y tecnología, y también matemática, psicología y administración. Sin embargo, hoy la realidad es distinta. La demanda por ciberseguridad, en aumento por la cantidad de ataques y amenazas, ahora necesita profesionales capacitados y especializados. En el mundo en que vivimos, la ciberseguridad ya es una carrera en sí misma, y no como parte de los estudios de IT. De hecho, según el último estudio de Cisco, para este 2018 se estima que estarían faltando alrededor de 500.000 especialistas de seguridad.*

*Cuando uno empieza a trabajar en ciberseguridad se compromete full life. No es un trabajo del que uno pueda conectarse y desconectarse a su voluntad porque las amenazas están latentes en todo momento y, por lo tanto, también tenemos que estar alertas a tiempo completo, ya que nunca se sabe en qué momento se puede dar una brecha de seguridad o un robo de identidad. Las amenazas no se toman descansos. A su vez, es una profesión en la que uno siempre debe estar aprendiendo. De hecho, esa es una de las cosas más emocionantes de trabajar en ciberseguridad. Es imposible aburrirse. Todo cambia y es necesario evolucionar y mejorar constantemente. Los atacantes innovan y desarrollan nuevos tipos de*

***“Hoy en día, vivimos en una especie de Gran Hermano constante en la que cualquier persona con acceso a la tecnología tiene la posibilidad de publicar información sobre sí misma o los demás.”***

- Sebastián Stranieri



No debemos olvidar que así como Internet constituye una gran herramienta con múltiples utilidades, si no se toman las precauciones necesarias puede transformarse en una amenaza a nuestra privacidad.

*ataques; para estar protegidos, debemos innovar de forma permanente nosotros también para tener el contraataque listo.*

*El proceso continúa fuera del trabajo, en nuestras vidas cotidianas. La irrupción de Internet ha dado origen a nuevas formas de comunicación, acelerando las relaciones interpersonales y comerciales. La transformación digital nos permite conectarnos desde cualquier lugar, en cualquier momento y a través de cualquier dispositivo. Frente a este cambio, los fraudes, extorsiones y secuestros virtuales han adoptado también nuevas formas, por lo que la ciberseguridad está pasando a ser protagonista en nuestro día a día.*

*Tenemos que estar atentos cuando posteamos en las redes sociales o incluso elegir cuidadosamente desde qué lugar realizamos procesos de onboarding o autenticación, ya que algunos de esos procesos no son 100% digitales y a veces requieren intervención de personas que tienen acceso a las fotos que se utilizan para llevarlos adelante. Por ejemplo, es más conveniente realizar una autenticación con biometría facial desde la cocina que desde el baño, aunque se sorprenderían de saber cuánta gente se loguea con poca ropa en un lugar tan íntimo!*

*Hoy en día, vivimos en una especie de Gran Hermano constante en la que cualquier persona con acceso a la tecnología tiene la posibilidad de publicar información, fotos y videos sobre nosotros en la calle, en un restaurante, en un aeropuerto o cualquier otro lugar.*

*Como profesionales de la ciberseguridad, esto nos obliga a que seamos también capacitadores para ayudar a que las personas tomen conciencia porque, en definitiva, la seguridad comienza por uno mismo: es necesario pensar cuidadosamente qué información decidimos hacer pública y con qué frecuencia.”*

Como vemos, existe un consenso general respecto de que el campo de la seguridad informática es altamente prometedor y ofrece múltiples alternativas que pueden ajustarse a los distintos intereses. Desde **BA-CSIRT**, creemos que resulta sumamente importante, pensando sobre todo en el bienestar de las personas y el futuro de nuestro país, que cada día más hombres y mujeres se interesen y se acerquen a la tecnología con ésta perspectiva. Este último, de hecho, constituye uno de los principales objetivos de nuestro trabajo ya que, para impulsar la responsabilidad digital en los usuarios, necesitamos profesionales apasionados y comprometidos con lo que hacen. ■

<sup>1</sup> <https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf>

<sup>2</sup> Íb.