CIBERSEGURIDAD: ¿UNA ASIGNATURA PENDIENTE EN LATINOAMÉRICA?

Delfín Sarasa Miqueli

Vicepresidente para Latinoamérica
Infotecs S.A. Rusia

Resumen

La informatización de la sociedad y la automatización en todas las esferas de la actividad humana son unas de las prioridades para el desarrollo de los países. Este aspecto positivo para la sociedad, ha traído aparejado lo que se puede denominar una nueva pandemia: la ciberdelincuencia. Para poder hacer frente a esa creciente amenaza, se necesita cubrir la brecha de especialistas en ciberseguridad, la que en América Latina se estima en 700 000 especialistas.

Hoy en día sólo los conocimientos teóricos no son suficientes para poder enfrentar de forma efectiva los ataques informáticos en constante crecimiento, por lo que es necesario incorporar al sistema de enseñanza de la especialidad el uso de herramientas como las Plataformas de Entrenamiento en Ciberseguridad.

Qué son, por qué son tan necesarias y su efectividad en la enseñanza, son los aspectos tratados en el presente trabajo.

Palabras claves

ciberseguridad, educación, conocimiento, entrenamiento, ataques, ciberdelincuencia, habilidades, plataforma virtual, simulación

Introducción

En los últimos cinco años se ha visto cómo se incrementan los ataques por la red, lo que en la actualidad se ha convertido en una industria para grupos de ciberdelincuentes con miles de millones de dólares en dividendos.

Al día de hoy, la economía y la estabilidad de las infraestructuras críticas de un país dependen de cómo está instrumentada la seguridad digital de los sistemas informáticos y las redes de comunicaciones. La clave del éxito en esa tarea está en la calificación de los especialistas en ciberseguridad.

En este trabajo se analizará el estado actual de la preparación de especialistas en seguridad informática a nivel mundial, y específicamente en América Latina. De igual modo, se propondrán algunos requerimientos para su preparación y se presentará una Plataforma para el Entrenamiento en Ciberseguridad, que es uno de los pilares imprescindible para que los centros de enseñanza puedan graduar los especialistas que requiere el mercado laboral, no solo capacitados teóricamente, sino también diestros y hábiles en el manejo de las herramientas necesarias, para

contrarrestar las amenazas por la red, que cada día evolucionan y se vuelven más complejas.

Preparación de especialistas en ciberseguridad

La ciberseguridad, según Kaspersky [1], es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica.

El Banco Interamericano de Desarrollo junto con la Organización de Estados Americanos, presentaron un estudio integral del estado de la ciberseguridad en América Latina en 2016 y 2020 respectivamente, que incluyó el estado de la Formación, Capacitación y Habilidades de Seguridad Cibernética [2].

La valoración del estado de la ciberseguridad en todos los aspectos del estudio se hizo acorde al Modelo de Madurez de la Capacidad de la Ciberseguridad (CMM) para las Naciones, elaborado por el Centro Global de Capacidad de Seguridad Cibernética (GCSCC en inglés) de la Universidad de Oxford [3], el que define cinco Niveles:

1. **Inicial:** En esta etapa no existe madurez en ciberseguridad, o bien se encuentra en un estado muy embrionario. Puede haber discusiones iniciales sobre el desarrollo de capacidades de ciberseguridad, pero no se han tomado medidas concretas. Falta evidencia observable de la capacidad de seguridad cibernética.
2. **Formativo:** Algunos aspectos han comenzado a crecer y formularse, pero pueden ser ad hoc, desorganizados, mal definidos, o simplemente nuevos. Sin embargo, se puede demostrar claramente evidencia de este aspecto.
3. **Consolidado:** Los indicadores están instalados y funcionando. Sin embargo, no se le ha dado mucha consideración a la asignación de recursos. Se han tomado pocas decisiones acerca de los beneficios con respecto a la inversión relativa en este aspecto. Pero la etapa es funcional y está definida.
4. **Estratégico:** En esta etapa se han tomado decisiones sobre qué indicadores de este aspecto son importantes y cuáles lo son menos para la organización o el Estado en particular. La etapa estratégica refleja el hecho de que estas elecciones se han realizado condicionadas por las circunstancias particulares del Estado o de las organizaciones.
5. **Dinámico:** En esta etapa existen mecanismos claros para alterar la estrategia en función de las circunstancias prevalentes, como la sofisticación tecnológica del entorno de amenaza, el conflicto global o un cambio significativo en un área de preocupación (por ejemplo, delito informático o privacidad). Las organizaciones dinámicas han desarrollado métodos para

cambiar las estrategias con calma. Sin embargo, la rápida toma de decisiones, la reasignación de recursos y la atención constante al entorno cambiante son características de esta etapa.

Con el empleo de esos indicadores, se hizo una valoración por cada país respecto a Educación, Capacitación y Habilidades en Ciberseguridad (Desarrollo del conocimiento de ciberseguridad). Los resultados de ese estudio acorde al Modelo de Madurez, para los países con mejores valoraciones fueron:

	Argentina	Brasil	Chile	Colombia	Santo Domingo	México	Uruguay
Sensibilización							
Programas de sensibilización	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■
Sensibilización Ejecutiva	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■
Marco para la Formación							
Provisión	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■
Administración	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■
Marco para la Capacitación Profesional							
Provisión	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■
Apropiación	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ ■ ■

Tabla 1

Como se observa en la Tabla 1, a pesar de que esos fueron los mejores resultados para siete países de América Latina, todavía queda bastante por mejorar, sobre todo en concientizar de que es necesario invertir en la formación de especialistas en ciberseguridad. Muy pocos de los de 32 países restantes en los que se llevó a cabo el estudio han llegado al nivel Consolidado en algunos de los parámetros valorados.

Desde el momento de realización de ese estudio a la fecha, han pasado tres años, pero hay que considerar la pandemia de Covid-19, que ralentizó el proceso de mejora de esos parámetros, además de que una cantidad significativa de especialistas pasaron a trabajar a distancia, lo que trajo como consecuencia a su vez, el aumento de las vulnerabilidades de los sistemas informáticos.

Ese estudio arrojó que existe un déficit de 600 mil especialistas en ciberseguridad en América Latina.

En 2022 se hizo otra valoración por una de las compañías líderes en el mercado de las redes informáticas Cisco, de conjunto con la Organización de los Estados Americanos (OEA) [3], que arrojó que en América Latina existe una brecha o falta de especialistas en ciberseguridad de 700 mil personas.

En el pasado año 2023, ISC2, una organización líder mundial que agrupa a profesionales de la ciberseguridad, hizo un estudio muy amplio, que abarcó 23 países y a 20 Estados dentro de los Estados Unidos [4]. Lo particular de ese estudio es que se hizo mediante un cuestionario on-line en colaboración con Forrester Research, Inc. donde se entrevistaron a 14865 especialistas responsables de la ciberseguridad en sus puestos de trabajo, distribuidos por Norteamérica, América Latina, Asia-Pacífico, Europa, África y Medio Oriente.

El estudio arrojó unos resultados muy interesantes sobre el estado actual de las habilidades en la fuerza de trabajo en la ciberseguridad, por ejemplo:

- El 63% de los encuestados expresaron que están preocupados por la capacidad del equipo de seguridad para mantener protegida a la entidad.
- A la pregunta: ¿cuáles fueron los mayores desafíos que enfrentaron los profesionales de la ciberseguridad en los últimos 12 meses? La respuesta fue: el 45% escasez de trabajadores/calificaciones en la fuerza laboral.
- El 75% de todos los encuestados expresaron que el panorama de las amenazas actual es el más desafiante que haya existido en los últimos cinco años y esto varía según la industria.
- Los entornos que presentan más incidencias de ataques cibernéticos fueron: Salud Pública (79%), Ejército (79%), Energía/servicios públicos (79%), Gobierno (78%) y las Manufacturas (77%).
- A la pregunta de qué es lo que más valoran de los candidatos potenciales a cubrir los puestos de especialistas en ciberseguridad, el resultado fue que los profesionales prefieren la experiencia a títulos de doctorado (86% frente a 14%).

Otro de los aspectos que, aunque no parezca que concierne a los estados y gobiernos, es el impacto de los recortes en ciberseguridad en las empresas:

- 35% de ellos manifestó recortes en los programas de adiestramiento en Ciberseguridad (9822 especialistas en ciberseguridad).
- 62% decrecimiento de las habilidades para enfrentar a las futuras amenazas (8907 especialistas en ciberseguridad).
- A la pregunta de: su organización tiene escasez de personal en ciberseguridad. ¿Cuál crees que es la principal causa de esa escasez? El 41% reportó que su organización no puede encontrar suficiente talento calificado, el 26% que su organización no pone suficientes recursos en capacitar al personal de TI no relacionado con la seguridad para convertirse en personal de seguridad, y el 15% que su organización no hace lo suficiente para capacitar al personal.

- Casi todas las organizaciones cuentan con brechas de habilidades en ciberseguridad. El 92% de los profesionales de la ciberseguridad dijeron que su organización sufre de brechas de habilidades en una o más áreas, y el 43% citó una o más brechas de habilidades significativas o críticas en su organización.

La brecha de habilidades es un área en los que los equipos de ciberseguridad carecen de trabajadores con competencia o experiencia y en particular, habilidades necesarias para funcionar eficazmente.

Otro aspecto fundamental que está ligado a la capacitación y las habilidades de los graduados, es el referido a la programación segura, que está relacionado no con los especialistas en ciberseguridad, sino que atañe además a las especialidades de Informática y Sistemas.

Debido a que una gran cantidad de graduados irán a trabajar a pequeñas y medianas empresas, donde por lo general no existirá un especialista de seguridad informática, la inclusión del tema de la ciberseguridad en los planes de estudios y la obtención de habilidades en contrarrestar amenazas por la red cada día toma un mayor peso en especialidades como las telecomunicaciones, redes de comunicación y afines.

Requerimientos de conocimientos para los especialistas en ciberseguridad

El Instituto Nacional para los Estándares y la Tecnología de los Estados Unidos (NIST en inglés) publicó en 2017 el Marco del personal para el trabajo en ciberseguridad (Iniciativa Nacional para la Educación en Seguridad Cibernética - NICE) [5].

En esa normativa se definen 7 categorías para garantizar altos niveles de funciones de ciberseguridad en la fuerza de trabajo de una compañía, además de 33 especialidades en diferentes áreas de trabajo en ciberseguridad y 52 roles que definen Grupos de Trabajo en Ciberseguridad y se definen conocimientos específicos, destrezas y habilidades para cada uno de ellos.

Ese documento fue revisado en el año 2020, y se denominó: NIST Publicación Especial 800-181 (Revisión 1) [6] Según el mismo, “en el Marco de la NICE se ofrecen un conjunto de elementos básicos para describir las tareas, los conocimientos y las habilidades que se necesitan para llevar a cabo el trabajo de seguridad cibernética realizado por individuos y equipos.” (pag. 9).

Además, se hizo una clasificación detallada del lenguaje usado para describir los aspectos que tienen que ver con la preparación de los especialistas en ciberseguridad, haciendo un énfasis especial en la habilidad de los especialistas: “una habilidad se define como la capacidad de realizar una acción observable.” (2.3 Descripción de habilidades pág.16)

Otro término importante que se define es: Competencia - “mecanismo de las organizaciones para evaluar a los alumnos” (3.3 Competencias pág. 19). Con ello, el documento crea un marco para que los especialistas sean evaluados según sus habilidades, acorde a los requisitos de las competencias del empleador en una organización.

Todo esto está relacionado con las Funciones Laborales, que también se definen: “las funciones laborales son una forma de describir un conjunto de trabajos del cual alguien está encargado o por el cual alguien es responsable” (3.4 Funciones laborales pág.24).

En esa normativa se definen otros conceptos como el trabajo en Equipo, para solucionar colectivamente trabajos complejos dentro de la seguridad informática. Este documento es de gran utilidad para las entidades educacionales que estén interesadas en preparar especialistas en ciberseguridad preparados para el mercado laboral.

¿Cómo lograr preparar especialistas competentes en ciberseguridad?

La única forma que existe para que los estudiantes de los cursos de ciberseguridad aparte de los conocimientos teóricos que reciben puedan enfrentar los incidentes de seguridad con los que tendrán que enfrentarse en su vida laboral de forma efectiva, son las prácticas o entrenamientos, que les permitan detectar y eliminar ataques reales en un medio donde no exista el riesgo de que esos ataques afecten la infraestructura o la información real de una entidad.

Para ello se han creado las Plataformas para el Entrenamiento en Ciberseguridad, las que permiten a los equipos entrenarse en un entorno hiperrealista simulado y desarrollar experiencia práctica para responder a ataques del mundo real. Esa herramienta funciona como un sistema aislado virtual autónomo, dentro del que se generan ataques reales que pueden ser repetidos tantas veces como sea necesario, hasta que los estudiantes adquieran la experiencia correspondiente.

El uso de esas plataformas hace posible que se obtengan las habilidades necesarias en el uso de herramientas para detectar y evitar ataques, cómo trabajar en equipo, entrenarse en lo que se denomina *forensis*, o la investigación de los incidentes de seguridad y determinar y erradicar las vulnerabilidades de los sistemas y computadoras y otras muchas cosas que no se pueden realizar sin el uso de esas plataformas.

Plataforma para el entrenamiento en Ciberseguridad.

La Plataforma para el entrenamiento en Ciberseguridad o Cyber Range Platform [7] es un sistema de simulación compuesto de 4 módulos fundamentales:

1. Un módulo para generar una red compuesta por máquinas virtuales, que tienen diferentes vulnerabilidades y que pueden corresponder a diferentes

estructuras funcionales, como puede ser una red empresarial, una red de una compañía de telecomunicaciones, una red bancaria o una red de una planta industrial.

2. Una máquina de generación automática de ataques informáticos, capaz de generar ataques reales actualizados.
3. Un módulo capaz de generar diferentes tipos de escenarios de ataques con diferente complejidad, que van desde sencillos, hasta altamente complejos y que permite simular en ese entorno virtual todos los pasos que hace un ciberdelincuente en la vida real al atacar una red de computación de una entidad hasta llegar a su objetivo.
4. Un módulo que es el denominado *Security Operation Centre (SOC)*, donde existen las herramientas capaces de detectar los ataques generados por el sistema y que permiten a los estudiantes, durante el entrenamiento, determinar qué ocurre en la red, definir si es un evento de seguridad o un ataque y realizar las acciones necesarias para erradicar las vulnerabilidades que está utilizando el atacante y detenerlo.

El uso de la plataforma para el entrenamiento en ciberseguridad permite además de entrenar a los estudiantes en el uso de las herramientas que posteriormente van a utilizar en su vida laboral, poder familiarizarse con las formas de trabajo de los ciberdelincuentes, trabajar en equipo para erradicar los ataques y las vulnerabilidades, aplicar en la práctica los conocimientos teóricos recibidos y elevar su nivel de preparación acorde a los requerimientos del mercado, lo que le abrirá el camino en su futura vida laboral.

En la Plataforma de Entrenamiento en Ciberseguridad están agrupados los conocimientos de especialistas de muy alta calificación, que periódicamente van actualizando las vulnerabilidades y los ataques que se generan y que replican exactamente lo que hace un ciberdelincuente en la vida real. Para generar los escenarios de los ataques se utilizan las mismas herramientas que ellos utilizan.

Es necesario destacar, que el uso de estas plataformas requiere tener a su vez profesores con una alta preparación, capaces de explotar todas las posibilidades del sistema en el proceso de enseñanza.

La compañía Infotecs, cuenta con una experiencia de más de 32 años desarrollando productos para la ciberseguridad y también ha desarrollado la Plataforma para el Entrenamiento en Ciberseguridad, que agrupa en una solución la experiencia de especialistas en ciberseguridad de muy alta calificación. La plataforma es utilizada en 20 universidades y Centros de Adiestramiento, está en continua actualización y cumple con los requerimientos de NICE Framework.

Conclusiones

En este trabajo se ha tratado de prestar atención a la problemática existente en los sistemas de enseñanza actuales, y los requerimientos del mercado laboral en especialistas en ciberseguridad.

El análisis muestra que aparte de que la preparación de ingenieros o licenciados en ciberseguridad está un poco lejos de lo requerido, hay que prestar además mucha atención a qué tipo de preparación tendrán los especialistas que se gradúen en el sistema de enseñanza.

Según los estudios realizados, la habilidad y la experiencia del especialista en ciberseguridad en contrarrestar los incidentes de seguridad prevalece sobre su preparación teórica. Hay que tener en cuenta además, que los ataques por la red cada día se hacen más complejos y difíciles de detectar y a pesar de todos los medios existentes para ello, la toma de decisión siempre recae en la persona.

Otro aspecto que se menciona en el trabajo, es la necesidad del apoyo financiero de los Gobiernos a los Centros de Educación en adquirir los medios necesarios para elevar el nivel de habilidades de los estudiantes de ciberseguridad, apoyar al sistema educativo a elevar la matrícula en esa especialidad a nivel de estado y no pasar el problema a las empresas y corporaciones.

En realidad, aunque parezca algo no evidente, la inversión en la graduación y capacitación de los especialistas en ciberseguridad se revierte en la protección de las infraestructuras críticas y el avance de la economía de las naciones.

Referencias Bibliográficas

1. Karsperky ¿Qué es la ciberseguridad?.Resource Center

<https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>

2. Banco Interamericano de Desarrollo & Organización de Estados Americanos.

2020.Reporte Ciberseguridad. Riesgos avances y el camino a seguir en América Latina y el Caribe. Banco Interamericano de Desarrollo.

<https://observatoriociberseguridad.org/>

3. Organización de los Estados Americanos & Cisco Systems. 2022. Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades. OEA.

https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-069/22

4. ISC2. 2023. Cybersecurity Workforce Study.

<https://www.isc2.org/research>

5. National Institute of Standards and Technology. 2017. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. USA

<https://csrc.nist.gov/pubs/sp/800/181/final>

6. National Institute of Standards and Technology. 2020. Special Publication 800-181 Revision 1 Workforce Framework for Cybersecurity (NICE Framework). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework USA.

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>

7. Advanced Monitoring. 2024. Cyber Range Platform.

<https://amonitoring.ru/product/empire/>