DOCUMENTOS
FELABAN No. 26

8 de mayo de 2019

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

¿Cuál es el impacto de la escasez de talento en ciberseguridad en la banca latinoamericana?

Recientemente los ciberataques han incrementado en cantidad, frecuencia y severidad a nivel mundial. Ello ocurre en un mundo cada vez más conectado a nivel digital, pues la cantidad de dispositivos desde los cuales se comparte información multiplica exponencialmente las fuentes de amenazas en el ciberespacio. Ello ha dinamizado significativamente la demanda de profesionales en ciberseguridad, particularmente durante la última década.

Este dinamismo es congruente con la rapidez de los avances en la tecnología y del ritmo de crecimiento en la creación y difusión de información. No obstante lo anterior, también ha evidenciado que la oferta de personal especializado en ciberseguridad no crece al mismo ritmo que su demanda.

Esto es una mala noticia para empresas, hogares y gobiernos. Desafortunadamente, estos actores también se encuentran en la frontera de la tecnología en lo relacionado con uso y acceso de la misma, lo cual explica en gran parte el creciente número de incidentes cibernéticos cuyas consecuencias negativas impactan a empresas, clientes y gobiernos indistintamente. En el sector financiero, el más reciente estudio de Morphisec Lab[1] reveló que en 2018 el 25% de los ataques empresariales fueron dirigidos al sector bancario,[2] principalmente en la forma de troyanos.

En América Latina la situación es lejana de ser la ideal para combatir dicha problemática. Cifras del Foro Económico Mundial[3] estiman que la brecha de habilidades profesionales de América Latina es la más grande de mundo, pues 50% de las empresas en nuestra región afirman no encontrar candidatos con las habilidades que requieren - superior al 36% reportado por las empresas en la OCDE. El informe afirma que esta problemática parece ser más aguda en Perú, Brasil, México y Colombia

Específicamente en materia de ciberseguridad, un estudio reciente de (ISC)², la entidad profesionales certificados en ciberseguridad más grande del mundo, estimó recientemente[4] que al cierre del 2018 dicha escasez de talento alcanzó los 2,93 millones de profesionales, de los cuales el 73% se concentró en Asia Pacífico, el 17% en Estados Unidos, y un 5% (o alrededor de 136.000 profesionales) en América Latina.

Dicha escasez de talento disminuye la capacidad de reacción y recuperación del sector bancario latinoamericano ante ciberataques. La Organización de Estados Americanos (OEA) encontró recientemente[5] que el 49% de los bancos

[1] *Morphisec Lab Threat Report 2018*. Disponible en https://engage.morphisec.com/december-2018-morphisec-labs-threat-report
[2] En informática, un *troyano* es un programa malicioso que aparenta ser legítimo y/o inofensivo, y de ser ejecutado, permite al cibercriminal tomar acceso remoto del dispositivo del usuario.
[3] *In Latin America, companies still can't find the skilled workers they need*. Disponible en https://www.weforum.org/agenda/2017/03/in-latin-america-companies-still-can-t-find-the-skilled-workers-they-need/
[4] *ISC)² Cybersecurity Workforce Study*, 2018. Disponible en https://www.isc2.org/Research/Workforce-Study
[5] *State of Cybersecurity in the Banking Sector in Latin America and the Caribbean*. Disponible en https://www.oas.org/es/sms/cicte/sectorbancarioeng.pdf

de la región no utiliza nuevas tecnologías (*big-data,* inteligencia artificial, *machine learning*) para prevenir ciberataques; 92% de los bancos han reportado algún tipo de incidente de seguridad digital; 60% de los responsables en ciberseguridad afirmaron que convencer a la junta directiva del banco de invertir en este rubro es "*moderadamente complejo*"; y que aunque el 74% de los bancos tiene algún área de ciberseguridad, el 41% de dichas áreas no reporta directamente al CEO del banco.

Las causas son variadas, y a nivel regional varían significativamente entre

- Posible desconexión entre la oferta académica de las universidades y las demandas del sector empresarial. A nivel mundial, la mayoría de profesionales en ciberseguridad tienden a ser ingenieros, pues la oferta de pregrados con énfasis en ciberseguridad es mínima. Lo anterior genera que las vacantes en dicha materia no sean adecuadamente cubiertas, y que el componente de capacitación interna sea el determinante en las áreas de ciberseguridad.

- Alta competencia por el talento. La ciberseguridad es un asunto de empresas de todos los tamaños y todos los sectores económicos, no solamente aquellas de tecnología. Ello, sumado a la baja oferta de talento, incentiva a las grandes empresas a competir en forma más intensa por el poco talento altamente cualificado disponible en el mercado laboral.

- Baja inclusión de género. Las ingenierías y las ciencias exactas son estudiadas mayoritariamente por hombres, lo cual inconscientemente excluye a muchas mujeres cuyos conocimientos, experiencia e interés podrían contribuir significativamente al cierre de dicha brecha de talento.

- Presupuestos limitados o inexistentes. Debido a sus restricciones presupuestales, las PyMEs generalmente son el blanco preferido de los cibercriminales. Similarmente, no son pocas las empresas grandes, que por errores de estrategia corporativa, no abordan la gestión en ciberseguridad como prioridad estratégica.

- Automatización de procesos. Aunque en menor medida, esta causa explica cómo las empresas grandes (principalmente en el sector tecnológico) se encuentran en capacidad de automatizar los procedimientos preventivos en materia de seguridad digital sin mayores restricciones presupuestales.

- Entorno económico, social y cultural. En un informe de GSMA (entidad que agremia a los operadores de telefonía móvil a nivel mundial) titulado *Inclusión digital en América Latina y el Caribe*[6], se identifican factores de contenido (menos del 30% del contenido web se encuentra en idioma español), de asequibilidad (el alto precio de los teléfonos móviles inteligentes y de la oferta de internet de banda ancha supera la capacidad adquisitiva de muchos hogares de la región), y de brechas digitales (alrededor de 360 millones de latinoamericanos no es usuario de banda ancha móvil, a pesar de vivir en una zona con cobertura de la misma).

En definitiva, la escasez de talento altamente capacitado en ciberseguridad no se solucionará en el corto plazo. Por ello, las soluciones deben ser graduales y con un alto grado de escalabilidad, y en ese sentido, las alianzas entre empresas y la academia y la consideración de planes conjuntos en investigación y desarrollo son definitivamente un gran paso en la dirección correcta.

La política pública juega un papel clave. Normativas que penalicen severamente los delitos informáticos, la creación de sistemas nacionales de ciberseguridad (tanto en la policía, como en los ejércitos y los organismos de inteligencia y seguridad), y sistemas de intercambio de información entre empresas y jurisdicciones son alternativas que atacan la raíz de esta problemática a nivel colectivo.

En línea con lo anterior, la cooperación entre el sector privado a nivel transfronterizo es clave. El intercambio permanente de información relativo al modo de actuar de los cibercriminales es determinante para adelantar estrategias proactivas ante esta problemática. Por ello, FELABAN se encuentra en proceso de creación de un Concentrador de Fraude Regional, el cual busca mitigar el accionar de los ciberdelincuentes en lo relacionado con medios de pago físico (tarjetas crédito y débito), y del cual espera compartir novedades próximamente.

Otra alternativa adoptada por varios países (entre ellos Singapur, Israel y Nueva Zelanda) implica en incluir en el currículo académico de estudiantes de primaria fundamentos de programación, bien sea como asignatura independiente, o como componente de una asignatura tradicional (matemáticas o informática, principalmente).

Finalmente, la capacitación continua es un aspecto clave para cerrar las brechas de conocimiento en este sentido, pues permite al personal de ciberseguridad mantenerse actualizado sobre las últimas tendencias de este mundo cuya naturaleza es altamente volátil y susceptible a cambios repentinos. Al respecto, FELABAN apoya al sector bancario regional mediante programas de capacitación (Diplomado en

[6] Informe disponible en https://www.gsma.com/latinamerica/es/resources/digital-inclusion-in-latin-america-and-the-caribbean/

Riesgos Integrales de Ciberseguridad) y congresos académicos (Congreso Latinoamericano de Seguridad Bancaria), en los cuales se comparten mejores prácticas y tendencias futuras sobre la materia a los responsables de ciberseguridad y áreas afines de América Latina.

***

La 34ª versión del Congreso Latinoamericano de Seguridad Bancaria – CELAES se llevará a cabo el próximo 20 y 21 de junio de 2019 en Ciudad de Panamá, y su agenda académica generará un espacio de networking e intercambio de ideas alrededor de la seguridad en la era digital. Le invitamos a conocer más de este evento y a separar su agenda en el link http://www.celaespanama2019.com/

SECRETARÍA GENERAL DE FELABAN

SECRETARIO GENERAL
Giorgio Trettenero Castro
gtrettenero@felaban.com

DIRECTOR ECONÓMICO
Jorge Arturo Saza.
jsaza@felaban.com

DIRECTOR TÉCNICO ADJUNTO
Daniel González Vargas
dgonzalez@felaban.com

ASESOR DE COMUNICACIONES Y PRENSA
Deiby Ramírez
dramirez@felaban.com

DISEÑO Y DIAGRAMACIÓN
Katia Marcela Tovar G.
ktovar@felaban.com