03/05/2025

Cómo la inteligencia artificial moldea el nuevo perfil profesional en ciberseguridad

El puesto de Analista de Seguridad de la Información, con gran demanda en el mundo laboral, requiere de nuevas aptitudes vinculadas a la aplicación de la Inteligencia Artificial.

La Inteligencia Artificial llegó para revolucionarlo todo, y la ciberseguridad no es la excepción. Aunque esto puede representar desafíos en el área, también ofrece una oportunidad para profesionales de este ámbito.

Actualmente, existe una brecha laboral en el campo de la ciberseguridad de casi 5 millones de profesionales. Según un estudio realizado por ISC2, el 54% de los encuestados observó un aumento sustancial en las ciberamenazas hacia finales de 2024 y, de ese 54%, un 13% atribuyó este crecimiento a las amenazas generadas por la propia IA.

Por otro lado, la Inteligencia Artificial también es considerada una tecnología muy valiosa por su contribución a tareas vinculadas a la seguridad de la información. El 82% de las personas que participaron del estudio coincide en que la IA mejorará la eficiencia laboral de los profesionales de la ciberseguridad.

A continuación, compartiremos un análisis que permita dimensionar el impacto de la Inteligencia Artificial en los profesionales del área, cómo puede ser clave en el desarrollo de amenazas y cuánto influyen las habilidades vinculadas a la IA en los perfiles de profesionales de la ciberseguridad para cubrir las crecientes necesidades del mercado laboral actual.

El riesgo: el uso de IA para fines maliciosos

Una de las aristas que es interesante analizar es aquella que vincula la utilización de la Inteligencia Artificial para crear nuevas amenazas o potenciar las existentes.

En reiteradas ocasiones hemos compartido desde WeLiveSecurity ataques en donde el uso malicioso de la Inteligencia Artificial por parte de los ciberatacantes cumple un papel fundamental. Desde cómo ChatGPT puede ser utilizado para optimizar ataques de phishing, hasta la creación de falsas imágenes y videos para sextorsión.

Entre las preocupaciones de los profesionales de ciberseguridad, relevadas en el estudio de ICS2, se encuentran las deepfakes (76%), las campañas de desinformación (70%) y la ingeniería social (64%), como principales. A su vez, 75% de los encuestados expresaron su preocupación respecto de que la IA sea utilizada como medio para lanzar ciberataques y otros actos delictivos maliciosos.

La realidad termina por dar crédito a esta sensación. La Inteligencia Artificial está facilitando los fraudes de identidad mediante la creación de videos y audios falsos, que hasta llegan a engañar a las personas más cercanas a la víctima.

La oportunidad: la IA como aliada de la ciberseguridad

Este panorama abre un gran interrogante: ¿estamos preparados para este escenario en donde las amenazas informáticas están en crecimiento, y en el que la IA puede ser utilizada a su favor por el cibercrimen? El 67% de las empresas reconoce que existe escasez de personal. En números concretos, se traduce a una brecha laboral de 4.763.963 puestos sin cubrir.

La primera conclusión entonces es que la ciberseguridad es un área de trabajo fértil, llena de oportunidades, para insertarse en el mercado laboral y desarrollar una carrera. Así lo confirma también el análisis realizado por el Foro Económico Mundial, que ubica al Analista de Seguridad de la Información dentro de los 10 empleos con mayor proyección de cara al 2027.

Ahora bien, ¿puede ser la Inteligencia Artificial la gran respuesta a esta demanda no cubierta? No, porque es poco probable que la IA logre avances sensibles para reducir la brecha que existe hoy entre la oferta y la demanda.

Pero sí podrá ser clave en permitir a los profesionales del área enfocarse más específicamente en tareas más complejas y de alto valor. Eso sí: cualquier aporte de la IA será en vano sin el criterio humano que la supervise, motivo por el cual es erróneo pensar que la Inteligencia Artificial dejará sin puestos de trabajos a las personas, sino todo lo contrario.

Es más, se espera que en un futuro cercano, el 75% de empresas adopten IA, lo cual no hace más que remarcar la demanda que existirá de expertos en seguridad. De hecho, la Oficina de Estadísticas Laborales de Estados Unidos proyecta un 32% en crecimiento de empleos de ciberseguridad entre 2022 y 2032, cifra superlativamente superior al 3% que se espera para el resto de los trabajos. Pero claro, para eso habrá que estar capacitado…

El nuevo perfil

Entre el aprovechamiento de las herramientas de IA por parte del cibercrimen y la demanda cada vez mayor de perfiles especializados, es casi obligatorio para quienes deseen desarrollar su carrera en el campo de la ciberseguridad, actualizarse con las nuevas habilidades que requiere el puesto. Y allí emergen las nuevas skills vinculadas a la Inteligencia Artificial.

Para dimensionar el impacto que la Inteligencia Artificial ya está teniendo en los perfiles profesionales de ciberseguridad, nada mejor que la opinión de la propia fuerza laboral: 88% lo ve reflejado en sus roles existentes. No solo eso: el 82 % coincide en que la IA mejorará su eficiencia laboral, mientras que más de la mitad (56%) siente que hará que algunas partes de su trabajo queden obsoletas.

Llevado a las tareas del día a día, estos son algunos de los beneficios que la IA puede ofrecer al campo de la ciberseguridad:

- Mejora del análisis de amenazas en tiempo real.
- Reducción de errores de configuración.
- Automatización de respuestas.
- Facilidad en el análisis de malware.
- Aumento de la productividad de los Centros de Operaciones de Seguridad.

El principal eje de este cambio es que los profesionales de la ciberseguridad podrán valerse de la IA para aquellas acciones que requieren mucho tiempo y son de menor valor (automatizar tareas repetitivas), como en la implementación de nuevas herramientas de detección. De allí nace la necesidad de adquirir nuevas habilidades y aptitudes mucho menos técnicas, como el pensamiento crítico, la adaptación y la ética digital.

Las nuevas skills

¿Y cómo ponerse al día para este nuevo panorama laboral? Actualmente, hay diversos cursos online gratuitos basados en la Inteligencia Artificial aplicada a la ciberseguridad: desde aquellos que incluyen contenidos más introductorios a los que requieren cierto nivel de experiencia para poder inscribirse.

Allí, se ponen en juego ciertas habilidades no tan técnicas, pero sí fundamentales para adaptarse a un escenario en constante evolución, como:

- Pensamiento crítico: cuestionar las decisiones de la IA, validando fuentes e interpretando sus resultados.
- Curiosidad y aprendizaje: dado que la IA evoluciona constantemente, es necesario actualizarse con las últimas tendencias.
- Ética: conocer los límites de cuándo y cómo usar IA sin comprometer la privacidad.

Sí, el futuro de la ciberseguridad estará muy vinculado a la aplicación de la Inteligencia Artificial, con el desarrollo de habilidades más soft y no tan técnicas.

Así lo confirma ISC2, indicando, por un lado, que la Inteligencia Artificial será una de las principales habilidades que se requerirán para ocupar puestos vinculados a la ciberseguridad. Y por otro, que aptitudes como la resolución de problemas y la comunicación están consideradas “por encima de habilidades técnicas como la seguridad en la nube o el análisis de riesgos”.

Por ello, la invitación es buscar las mejores herramientas y contenidos que se adapten a tus intereses. Seguramente, la oferta de cursos disponible seguirá creciendo, con opciones para todos los gustos. Adquirir estos skills podrá marcar la diferencia para tener un desarrollo prominente en uno de los empleos del futuro.

Fuente: https://www.welivesecurity.com/

LINK DE LA NOTICIA