¿Hacker ético? especialista explica a estudiantes de la UAA qué implica convertirse en uno

Universidad Autónoma de Aguascalientes

Departamento de Comunicación y Relaciones Públicas

Piso 3, Edificio Académico Administrativo,
Av. Universidad No. 940, Ciudad Universitaria,
C.P. 20100, Aguascalientes, Ags., México

Tel. conmutador:
449 910 74 00

uaa.mx

BOLETÍN 141

- El experto enfatizó la relevancia de este campo, no solo por las buenas perspectivas laborales, sino por el impacto positivo que los profesionales pueden tener en la sociedad al proteger los datos y sistemas digitales.

En una conferencia titulada “Mamá quiero ser hacker: La realidad laboral”, impartida recientemente en la Universidad Autónoma de Aguascalientes, Rafael Bucio, destacado hacker mexicano y director general y fundador de tpx Security, compartió su visión sobre lo que implica convertirse en un profesional de la seguridad digital y cómo navegar en este campo lleno de retos y oportunidades.

Bucio describió el hacking ético como un profesional que prueba y evalúa la seguridad de los ecosistemas digitales. "El hacker ético detecta vulnerabilidades en sistemas o aplicaciones y proporciona soluciones para corregir esas fallas. Es la persona encargada de decirte lo que está mal y darte las herramientas para remediarlo", explicó.

El ponente subrayó que, dado que el hacking ético puede ser fácilmente malinterpretado, los profesionales deben tener una clara comprensión de lo que está bien y lo que está mal. "La ética es crucial. Si una persona sabe lo que es correcto y tiene objetivos claros hacia la sociedad, puede desempeñarse con integridad en esta carrera", enfatizó. La ética, según Bucio, no solo influye en la toma de decisiones dentro del trabajo, sino que también es fundamental para que un hacker ético gane la confianza en la sociedad y en el entorno profesional.

Además de la ética, Bucio destacó las habilidades necesarias para tener éxito en este campo. Entre ellas, mencionó que la capacidad de aprender y adaptarse es esencial, ya que, en el hacking, siempre hay algo nuevo que estudiar, desde lenguajes de programación hasta nuevas vulnerabilidades. Asimismo, el especialista resaltó la importancia de habilidades en lógica de programación, redes y comunicación, que son esenciales para abordar los desafíos de seguridad.

El panorama laboral para los especialistas en ciberseguridad y hacking ético también fue un tema central. Bucio señaló que el campo está creciendo de manera exponencial, y las oportunidades laborales aumentan a medida que surgen nuevas especializaciones, además, indicó que la ciberseguridad no solo abarca la protección de aplicaciones, sino que también incluye la seguridad en infraestructuras complejas y ecosistemas de gran escala.

No obstante, también mencionó algunos de los principales desafíos que enfrenta la industria, como la falta de cultura y comprensión sobre la importancia de la seguridad digital en muchos sectores, especialmente a nivel ejecutivo. También destacó que la ciberseguridad es una disciplina costosa, tanto en términos de herramientas como de capacitación, lo que representa un obstáculo en su

implementación adecuada.

Finalmente, el hacker mexicano ofreció un consejo a los estudiantes interesados en iniciar una carrera en este campo: "No se desanimen. El mundo de la ciberseguridad tiene muchas ramificaciones, desde la protección de aplicaciones hasta la seguridad en infraestructura o incluso la seguridad humana. Cada uno tiene su especialidad y su valor dentro de este vasto campo", concluyó.

---000---

Ciudad Universitaria

07 de abril del 2025