

# OUCH!

El Boletín Mensual de Concientización en Seguridad para ti

## Cualquiera puede empezar una carrera en ciberseguridad

### Resumen

Leemos sobre ciberseguridad en las noticias casi todos los días debido a que las organizaciones y los gobiernos de todo el mundo continúan siendo afectados por ransomware, estafas y ataques cibernéticos. Existe una gran demanda de personas capacitadas en ciberseguridad para ayudar a defender contra estas crecientes amenazas. De hecho, estudios recientes estiman que hay casi 3 millones de ofertas laborales en ciberseguridad en todo el mundo.

¿Has considerado una carrera como profesional de ciberseguridad? Es un campo de ritmo acelerado y altamente dinámico con una gran cantidad de emocionantes especialidades para elegir. Estos puestos incluyen campos como análisis forense, concientización y capacitación, seguridad endpoint, infraestructura crítica, respuesta a incidentes, programación segura y políticas. Una carrera en seguridad cibernética también te permite trabajar en casi cualquier parte del mundo, con una variedad de beneficios y la oportunidad de hacer una diferencia real.

### ¿Necesito un título en Ciencias de la Computación?

Definitivamente no. Muchos de los mejores profesionales de seguridad no tienen antecedentes técnicos. La clave es la pasión por aprender; una vez que comprendas cómo funcionan (y se vulneran) las tecnologías, podrás protegerlas mejor. La ciberseguridad es tan emocionante porque puedes comenzar a aprender a tu propio ritmo en la comodidad de tu hogar.

### ¿Cómo empiezo?

Comienza a explorar diferentes áreas para descubrir tus intereses. Puedes comenzar solo con las computadoras o dispositivos que tienes en casa.

- **Programación:** Aprende los conceptos básicos de la programación. Python, HTML o JavaScript son buenos lenguajes para comenzar. Considera un sitio de capacitación en línea o toma cualquier libro para principiantes en programación.
- **Sistemas:** Aprende los conceptos básicos de la administración de un sistema operativo, como Linux o Windows. Si realmente quieres ser un nerd, adquiere experiencia a través de la interfaz de línea de comandos y scripts.
- **Aplicaciones:** Aprende a configurar, ejecutar y mantener aplicaciones, como servidores web.

- **Redes:** Descubre cómo las computadoras y los dispositivos se comunican entre sí capturando y analizando el tráfico de la red. Esto puede ser muy divertido ya que lo más probable es que tu hogar ya esté conectado a la red con todo tipo de dispositivos conectados a este.
- **Tecnologías en la Nube:** Aprende cómo funcionan los servicios en la nube y las diferentes formas en que se pueden aprovechar.

Monta tu propio laboratorio en casa. Puedes utilizar recursos en la nube en línea, como AWS de Amazon o Azure de Microsoft, en su caso puedes crear múltiples sistemas operativos virtuales en la misma computadora física con servicios de virtualización. Si deseas trabajar directamente con hardware, compra computadoras simples y económicas como Raspberry Pi o Arduino. Una vez que tengas tus sistemas en funcionamiento, comienza a interactuar con ellos y aprende todo lo que puedas sobre cómo configurarlos y optimizarlos, o comienza a programar y crear código en estos sistemas. No hay una manera correcta o incorrecta de comenzar, solo sigue donde te lleven tus intereses.

Otra excelente manera de comenzar es conocer y trabajar con otras personas en ciberseguridad. Considera asistir a una conferencia local sobre seguridad cibernética o una conferencia virtual como Bsides o SANS New2Cyber. La parte más difícil es encontrar ese primer evento o reunión. Una vez que asistas, conéctate con otros asistentes y haz crecer tu red profesional.

Otras opciones para aprender ciberseguridad incluyen videos de YouTube, escuchar podcasts, visitar foros en línea, suscribirse a blogs de profesionales de seguridad o participar en Capture the Flag (CTF) en línea. Por último, no permitas que tu educación o antecedentes te detengan. La pasión por aprender y ayudar a los demás, así como la capacidad de "pensar fuera de lo establecido como normal" son atributos clave. Una vez que comiences a desarrollar tus habilidades técnicas y te reúnas con otros, las oportunidades llegarán.

## Editor invitado

Lodrina Cherne ([@hexplates](#)) es responsable de Defensoría en Seguridad en Cybereason, donde impulsa la innovación y el desarrollo de las mejores prácticas relacionadas con estándares y políticas de ciberseguridad. También es instructora certificada en el Instituto SANS, donde ayuda a los profesionales de seguridad de la información a avanzar en su comprensión fundamental del análisis forense digital y la respuesta a incidentes (por sus siglas en inglés DFIR).



## Recursos

Conferencias de seguridad Bsides: <http://www.securitybsides.com/>

Mujeres en ciberseguridad: <https://www.wicys.org/>

Lista de reproducción New2Cyber de YouTube: <https://youtube.com/playlist?list=PLtgaAEEemVe6BQkZiJC5nk9xx74QTGtsZ>

Ciberacademias SANS: <https://www.sans.org/scholarship-academies/>

SANS Cyber Aces (cursos gratuitos en línea): <https://www.cyberaces.org/>

Podcasts de ciberseguridad: <https://www.sans.org/blog/cybersecurity-podcast-roundup/>

**Traducido para la comunidad por:** Célica Martínez Aponte and Iván Galindo, UNAM-CERT

OUCH! Es publicado por SANS Security Awareness y distribuido bajo la licencia [Creative Commons BY-NC-ND 4.0](#). Puedes distribuir y compartir este boletín, siempre y cuando no lo vendas o modifiques. Consejo editorial: Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.