



PERFIL OCUPACIONAL DEL PROGRAMA PROFESIONAL:

ESPECIALISTA EN CIBERSEGURIDAD

El programa de capacitación profesional para especialista en ciberseguridad prepara a los adultos para ayudar a mantener segura la tecnología de una empresa, desde las cuentas de usuario y los dispositivos hasta las redes y los sistemas en la nube. Los alumnos aprenden a supervisar las alertas de seguridad, investigar posibles amenazas y seguir los procedimientos de respuesta establecidos bajo supervisión. Al trabajar junto a los equipos de TI y de negocios, ayudan a proteger los sistemas y los datos de la empresa al detectar vulnerabilidades, documentar problemas y apoyar las mejoras continuas de las prácticas de seguridad.

Esta ocupación es ideal para personas a las que:

- Les gusta investigar problemas y descubrir qué salió mal.
- Están orientadas a los detalles y les gusta seguir procesos estructurados para encontrar respuestas.
- Se ven a sí mismos en un rol que combina el análisis técnico, la comunicación clara y el trabajo práctico de seguridad.

¿Los alumnos pagan una tarifa para participar?

No, los alumnos no están obligados a pagar nada por participar.

¿Cuánto ganan los alumnos mientras completan el programa?

Si bien la remuneración varía según el sector, el tamaño de la organización y el alcance completo del puesto, los alumnos pueden esperar un salario en el rango de **\$17 a \$25 por hora** durante el programa. Los alumnos son empleados y están sujetos a las políticas de su empleador en cuanto a tiempo libre remunerado, beneficios, evaluaciones de desempeño y aumentos salariales.

¿Qué hacen los alumnos como especialistas en ciberseguridad?

- **Monitoreo y clasificación de alertas:** monitorear, clasificar y documentar las alertas de seguridad mediante flujos de trabajo estandarizados y criterios de decisión; priorizar el trabajo en función de la gravedad, la confianza y el impacto en el negocio.
- **Investigación:** realizar investigaciones iniciales al correlacionar evidencias de identidad, de puntos finales y de red en cronogramas; identificar amenazas comunes y patrones de ataque como phishing, malware y robo de credenciales.
- **Respuesta y contención:** ejecutar acciones de respuesta aprobadas (contener, bloquear, restablecer, aislar, revocar) siguiendo los manuales de procedimientos y las reglas de escalamiento.
- **Vulnerabilidad y corrección:** respaldar el seguimiento de la corrección de vulnerabilidades y la validación de las soluciones en colaboración con los equipos de TI; documentar las excepciones y la aceptación de riesgos.
- **Documentación, informes y seguridad:** mantener tickets precisos, evidencias y resúmenes concisos para el escalamiento y la presentación de informes; contribuir a los manuales de procedimientos, las recomendaciones de ajuste de la detección y las mejoras de los procesos; seguir las mejores prácticas de seguridad, incluidos los controles de acceso, el manejo de datos y el uso seguro de herramientas de IA.

Todo el trabajo se realiza bajo supervisión, con una independencia cada vez mayor a medida que pasa el tiempo.

HORARIO HABITUAL

Duración del programa de capacitación

Dos años de aprendizaje remunerado a tiempo completo, divididos entre la experiencia en el lugar de trabajo con un empleador y la instrucción especializada en un centro de formación interempresarial.

Semana típica

Meses 1–3:

Fundamentos y exposición segura

- 3 días por semana en el centro de formación (laboratorios y simulaciones)
- 2 días por semana en las instalaciones del empleador (observación y tareas controladas)

Meses 4–6:

Responsabilidad supervisada de las tareas cotidianas

- 2 días por semana en el centro de formación
- 3 días por semana en las instalaciones del empleador

Meses 7–12:

Rendimiento productivo y aprendizaje aplicado

- 1 día por semana en el centro de formación
- 4 días por semana en las instalaciones del empleador

Meses 13–18:

Investigaciones más exhaustivas e impacto

- Medio día por semana en el centro de formación
- 4.5 días por semana en las instalaciones del empleador

Meses 19–24:

Trabajo de nivel asociado y portafolio final

- Todo el tiempo en las instalaciones del empleador, a excepción de 1 día al mes en el centro de formación

¿Cuáles son algunas de las habilidades que los alumnos adquieren en el puesto de trabajo?

- Fundamentos de seguridad y comunicación
- Protección de identidad, de puntos finales y de acceso
- Seguridad de redes, nube y datos
- Monitoreo, respuesta y mejora continua
- IA aplicada para la detección, la clasificación y la generación de informes

¿Qué educación o experiencia deben tener los alumnos antes de comenzar el programa?

Aunque no es obligatorio, existen varias oportunidades de formación preparatoria y de transición que ofrecen una base sólida para el éxito. Antes de su programa de capacitación o en paralelo a este, se recomienda a los adultos que realicen cursos en línea a su propio ritmo sobre fundamentos de TI y conceptos básicos de ciberseguridad para acelerar su preparación.

Por ejemplo:

- Cursos básicos
 - Fundamentos de tecnología de la información
 - Aplicaciones digitales y responsabilidad
 - Fundamentos de redes
- Cursos básicos de soporte de TI
 - Soporte de TI
 - Hardware informático y sistemas operativos
 - Fundamentos de TI/operaciones de soporte técnico
- Cursos avanzados/relacionados
 - Fundamentos de ciberseguridad
 - Conceptos de la nube y la virtualización
 - Gestión de proyectos

¿Qué credencial recibe un alumno al completar el programa?

Los alumnos obtienen una credencial de INCAP que será reconocida por TechIndiana y las empresas relacionadas con la tecnología de todo Indiana reconocen como equivalente a un título académico de asociado en un programa de grado relacionado con la TI o la tecnología. También pueden recibir créditos universitarios para obtener un programa de grado relacionado.

También existen oportunidades para obtener certificaciones de la industria acumulables durante el programa, como ISC2 Certified in Cybersecurity (CC), CompTIA Security+ y Microsoft Security, Compliance, and Identity Fundamentals (SC-900).

¿Qué oportunidades profesionales están disponibles después de completar el programa?

Este programa prepara al alumno para ocupar puestos de nivel inicial que apoyan las operaciones de seguridad y la infraestructura de TI, entre ellos:

- | | |
|---|-----------------------------------|
| • Analista de seguridad | • Administrador de redes |
| • Especialista en respuesta a incidentes | • Administrador de sistemas |
| • Centro de Operaciones de Seguridad (SOC) | • Administrador de bases de datos |
| • Hunter de amenazas | • Gerente de proyectos de TI |
| • Analista de vulnerabilidades | • Ingeniero de la nube |
| • Analista de gobernanza, riesgo y cumplimiento (GRC) | • Ingeniero de DevOps |
| • Especialista en seguridad en la nube | |

¿A quién debo contactar para obtener más información?

TechIndiana administra los programas profesionales de INCAP para Tecnología/TI. Puede obtener más información en [TechIndiana.org](https://www.techindiana.org).

