

CRITERIOS DE SELECCIÓN DE ESTUDIANTES

RESUMEN DEL PROGRAMA

El programa "Creando una Trayectoria Profesional en Ciberseguridad", coordinado por el Programa de Ciberseguridad de la Organización de los Estados Americanos (OEA) y financiado por la Fundación Citi, busca capacitar a jóvenes de hogares de bajos ingresos y fomentar su preparación profesional en cinco países de América Latina y el Caribe: Argentina, Colombia, Costa Rica, Perú, y República Dominicana. Específicamente, este programa proporcionará capacitación en seguridad digital a 200 jóvenes de edades comprendidas entre los 18 y 25 años (40 jóvenes en cada país).

Los mejores 30 estudiantes del programa tendrán acceso a oportunidades adicionales de formación personal y profesional, incluyendo acceso a una capacitación de emprendimiento digital y una licencia anual de Platzi, una escuela online de formación profesional en tecnología, entre otras.

El plan de estudios consistirá de aproximadamente 44 horas de teoría técnica sobre ciberseguridad (examen incluido) y aproximadamente 4 horas sobre preparación laboral y desarrollo personal durante un periodo de 6 días. Este programa permitirá que los estudiantes adquieran los conocimientos básicos necesarios para acceder a puestos de nivel de entrada en el ámbito de seguridad digital, y abarcará temas de fundamentos básicos de ciberseguridad, gestión de incidentes, análisis de amenazas y análisis forense. Este plan de estudios también proporcionará a los estudiantes la oportunidad de tomar un examen al final del entrenamiento y recibir un certificado, que servirá como confirmación de los conocimientos y habilidades adquiridas.

QUIENES DEBERÍAN APLICAR

Personas de 18 a 25 años de edad (hombres y mujeres), provenientes de una comunidad de bajos ingresos y que posean conocimientos prácticos y conceptuales sobre la estructura de terminales computacionales (CPU, memoria, y puertos periféricos). Efectivamente, esto significa individuos con 0-3 años de experiencia en seguridad digital, y/o estudiantes que tengan pasión por el tema pero que aún no se han embarcado en una carrera en seguridad digital. Los estudiantes que estén cursando una licenciatura en Ciencias de la Computación o Ingeniería Informática pueden tener una ventaja.

BENEFICIOS DEL ENTRENAMIENTO CERTIFICADO

Abarca varias áreas temáticas, incluyendo: fundamentos básicos de ciberseguridad, gestión de incidentes, análisis de amenazas y análisis forense.

Este certificado basado en el conocimiento permitirá al candidato:

- Demostrar su comprensión sobre los principios que enmarcan y definen la seguridad digital y el papel integral de los profesionales de la seguridad digital en la protección de datos empresariales
- Añadir una credencial a su currículum vitae y acceso a pasantías
- Acceso a oportunidades adicionales de formación personal y profesional

PROCESO DE SELECCIÓN

El Programa seleccionará candidatos que: 1) tengan una alta probabilidad de completar con éxito el programa, 2) posean las cualidades consideradas valiosas en una carrera de seguridad digital, y 3) tengan un deseo e interés en el área de seguridad digital. Es imperativo ser un joven de hogares de bajos ingresos y tener entre 18 y 25 años.

1. Conocimiento

- **Requerido**
 - Perfil técnico (informática, telecomunicaciones, industriales o similar)
 - Conocimiento de Programación Básica fundamental
 - Seguridad bajo Modelo OSI (Redes, Seguridad Perimetral, BBDD, Sistemas Operativos y Aplicaciones)
 - Conocimientos básicos de ciberseguridad (se hará un breve repaso de los mismos durante la primera sesión, pero es interesante que los alumnos tengan ya unas nociones)
- **Deseable**
 - Shell scripting
 - HTML, PHP, JavaScript, Python, Perl
 - Entendimiento básico de los servidores y servicios de Windows y Unix/Linux

2. Probabilidad de éxito académico en el programa de seguridad digital

El historial académico del candidato será cuidadosamente evaluado con el objetivo de responder a la pregunta, "¿El anterior desempeño académico del candidato y la evidencia de motivación generan confianza en su habilidad para tener éxito en el currículo de seguridad digital?" Para responder a esta pregunta, se tendrán en cuenta los siguientes factores:

- Curriculum vitae
- Carta de Motivación e Interés (250 palabras)
- Desempeño académico

3. Demostración de cualidades consideradas valiosas en un profesional de seguridad digital

La OEA seleccionará candidatos que puedan demostrar las siguientes cualidades en sus futuras carreras de seguridad digital:

- Habilidades interpersonales
- Habilidades de comunicación
- Integridad
- Motivación
- Capacidad de tomar instrucciones con eficacia

Para seleccionar candidatos que puedan tener estas cualidades, la OEA revisará y evaluará el perfil del aspirante tomando en cuenta su Carta de Motivación e Interés. En caso de requerir mayor información los candidatos podrían ser entrevistados.