CRITERIOS DE SELECCIÓN DE ESTUDIANTES

RESUMEN DEL PROGRAMA

El programa "Creación de una Trayectoria Profesional en Seguridad Digital", coordinado conjuntamente por el Programa de Ciberseguridad de la Organización de los Estados Americanos (OEA) y el Trust of the Américas, busca capacitar a jóvenes de hogares de bajos ingresos y fomentar su preparación profesional en cuatro países de América Latina y el Caribe: Colombia, Perú, República Dominicana y Costa Rica. Específicamente, este programa proporcionará capacitación en seguridad digital a 160 jóvenes de edades comprendidas entre los 17 y 25 años (40 jóvenes en cada país).

Los mejores 20 estudiantes del programa tendrán acceso a una incubadora de emprendimiento que tendrá lugar en León, España, como preámbulo del Summer Bootcamp al que también podrán asistir con gastos pagados. Además, otros 20 estudiantes y posiblemente alguno más, recibirán una pasantía en el sector privado en sus respectivos países.

El plan de estudios consistirá de aproximadamente 48 horas de teoría técnica sobre ciberseguridad (examen incluido) y aproximadamente 16 horas sobre preparación laboral y emprendimiento durante un periodo de 8 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 17 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, estudiantes y recién graduados, o aquellas personas que tengan pasión por el tema pero que aún no se han embarcado en una carrera. 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
- Acceso a la incubadora de emprendimiento diseñada para este programa
- Acceso al Summer Bootcamp con gastos pagados
- Acceso a pasantías en el sector privado

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.

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)
- Exigencias de trabajo o familia durante el estudio

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. Estos atributos también serán evaluados durante la entrevista.

TEMARIO TECNICO DEL CURSO

Fundamentos básicos de Ciberseguridad (1 jornada de unas 8 horas)

- **Ciberseguridad: A qué nos enfrentamos**
  - Vulnerabilidad y amenaza
  - Ciberdelitos y ciberciminalidad: incidentes de seguridad
  - Criptografia/cifrado
  - Sistemas de anonimización: VPN, Deep Web, red TOR y similares
  - Delitos tradicionales potenciados por sistemas de información
  - Principales actores en la detección, prevención, respuesta y recuperación frente a ciberataques

- Problemática de la investigación en internet desde una perspectiva técnica

- **Introducción a la ciberseguridad: tecnologías**
  - Evolución y contexto tecnológico actual
  - Redes y sistemas operativos
  - Virtualización
  - Cloud pública y privada

<u>Gestión de Incidentes</u> (1,5 jornadas de unas 8 horas)

- **Gestión de incidentes:**
  - Conceptos
  - Objetivos de la gestión de incidentes
  - Gestión de incidentes vs. respuesta a incidentes
  - Metodologías
  - Herramientas
  - Ciclo de vida de un incidente
- **Incidentes críticos:**
  - Valoración de la criticidad
  - Niveles
- **Avisos de seguridad:**
  - Servicios reactivos: alertas y advertencias
  - Servicios proactivos: Comunicados y anuncios
  - Otros
  - Procesos asociados
- **Fuentes de información:**
  - Avisos de seguridad
  - Otras fuentes: logs, registros, eventos
- **Role-Play:**
  - Utilidad
  - Toma de decisiones

<u>Análisis de Amenazas</u> (1,5 jornadas de unas 8 horas)

- **Introducción a los tipos de amenazas y vectores de infección**
- **Diferencias entre análisis estático y dinámico**
- **Preparación del entorno de trabajo:**
  - Herramientas necesarias
  - Anti-análisis y ocultación de máquinas virtuales
  - Aislamiento
- **Introducción al análisis de malware:**
  - Identificación de una máquina afectada
  - Recolección de indicadores de compromiso (IOCs)
  - Clasificación de malware en memoria
  - Análisis de tráfico de red

<u>Introducción al análisis forense</u> (1,5 jornadas de unas 8 horas)

- **Sistema Operativo:**
  - Diferencias entre Windows 7, Windows 8 y Windows 10.
  - Arquitectura de Linux
- **Kits de respuesta ante incidentes:**
  - Basados en agente
  - Sin agente
- **Extracción de evidencias:**
  - Navegación
  - Conexiones de Red
  - Aplicaciones
  - Sistema de ficheros
  - Módulos
- **Nuevos artifacts en Windows 10:**
  - Asistente personal CORTANA
  - Introducción
  - Integración en Windows 10

- Captura y análisis de información
- Integración de aplicaciones
- Centro de notificaciones
- Geo-localización en Windows 10

- **Análisis de línea temporal:**
  - Cuándo un sistema ha sido actualizado, arrancado, parado, etc
  - Análisis de creación/modificación de ficheros (malware)
  - Ocultación y ex-filtración de datos
  - Relación de procesos, puertos y conexiones realizadas

Examen basado en una caso práctico (0,5 jornadas de unas 8 horas)