FUNDACIÓN PREVENT

Bases Nio – Febrero 2025

Formación en Ciberseguridad para los guardianes de la información y los datos en el siglo XXI

Cofinanciado por:

Financiado por la Unión Europea NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Comunidad de Madrid

Partner académico:

HUB4T

TecnoCampus

Patrocinado por:

CaixaBank

endesa

Con la colaboración de:

goodhabitz online training

serunion

FUNDACIÓN PREVENT

¿Qué es el programa Nio?

Nio es un programa diseñado para dar cabida a todas las personas con inquietudes en las nuevas tecnologías.

Su objetivo es acompañar a personas con discapacidad o trastornos de salud mental en su primer acercamiento a una profesión con muy alta demanda en el sector tecnológico y en todos los sectores digitalizados: servicios, automoción, salud, consultoría, etc. para ofrecer al mercado talento diverso y a las personas nuevas oportunidades profesionales.

Nio es un programa que combina formación técnica en ciberseguridad, desarrollo de habilidades y competencias para el empleo.

La financiación de INCIBE se enmarca en el componente 19, inversión 4 «Profesionales digitales» del Plan de Recuperación, Transformación y Resiliencia (PRTR).

Requisitos para participar:

- Grado discapacidad mínimo del 33% o informe que acredite un diagnóstico en salud mental.
- Titulación mínima de la ESO.
- Se valorará tener cursos o formaciones previas como FP Grado Medio y/o Superior o equivalente de la familia profesional de Informática y Comunicaciones.
- Conocimientos medios en informática: sistemas operativos, Microsoft Office, manejo de software (valorable uso máquinas virtuales).
- Disponer de un ordenador personal con los siguientes mínimos:
    - Tipos de procesador: Intel Core i5 o superior
    - 16 GB RAM
    - Virtualización activada a la BIOS
    - SSD 500 GB
    - Tener instalado Microsoft Office y/o Open Office
    - Buena conexión Internet

Fecha de inicio y fin:

Fecha de inicio: 17 de febrero

Fecha de fin: 30 de mayo

Modalidad:

Modalidad online en directo.

Las clases se impartirán los lunes, miércoles y viernes en dos turnos:

Cofinanciado por:

Financiado por la Unión Europea NextGenerationEU

Partner académico:

Patrocinado por:

Con la colaboración de:

- Turno de mañana: lunes, miércoles y viernes de 9:30 a 12:45 h.
- Turno de tarde: lunes, miércoles y viernes de 17:00 a 20:15 h.

Contenidos:

250 horas de formación en ciberseguridad

- 125 horas de contenidos teóricos
- 125 horas de ejercicios prácticos

MÓDULO FORMATIVO	CONTENIDOS
1. INTRODUCCIÓN A LA CIBERSEGURIDAD	a. Definición de ciberseguridad b. Importancia de la ciberseguridad en el entorno actual c. Principales amenazas y riesgos d. Historia y evolución de la ciberseguridad e. Casos famosos de ciberataques
2. INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN	a. Introducción a la seguridad de la información b. Identificación de activos c. Vulnerabilidades, Amenazas, Riesgos, Ataques d. Autenticación, Autorización, Registro (AAA) e. Confidencialidad, Integridad, Disponibilidad (CIA) f. Introducción a la criptografía
3. SISTEMAS OPERATIVOS Y REDES DE PROTOCOLOS	a. Windows - Introducción - Gestión de usuarios / Administrador - Comandos de sistema - Introducción a la Seguridad en Windows b. Linux - Introducción - Gestión de usuarios / Administrador - Comandos de sistema

	- Introducción a la Seguridad en Linux
4. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	a. Sistema de gestión de la seguridad de la información b. Análisis de riesgos c. Cadena de ataque en las infraestructuras d. Controles de la ISO 27001 e. Conceptos del Esquema Nacional de Seguridad f. Legislación en protección de datos personales (RGPD)
5. ANÁLISIS DE VULNERABILIDADES EN RED	a. TCP/IP b. Servicios básicos c. Dispositivos de interconexión d. Vulnerabilidades IP e. Vulnerabilidades TCP/UDP f. Ataques a servicios
6. SISTEMAS DE PROTECCIÓN DE LA INFORMACIÓN	a. Control de accesos b. Securización de LAN c. Securización Perimetral d. Dispositivos de securización e. Gestión de la recuperación de datos
7. GESTIÓN DE LA CIBERSEGURIDAD EN LAS ORGANIZACIONES	a. Gestión de incidentes de ciberseguridad (SOC Centro de Operaciones de Seguridad) b. Detección de anomalías en el tráfico de la red corporativa c. Indicadores de incidentes / ataques d. Automatización de procedimientos e. Gestión de un incidente

FUNDACIÓN PREVENT

Contacto:

Para cualquier consulta:

Sònia Borràs: s.borras@fundacionprevent.com o 608 82 52 58

Inés Mantilla: i.mantilla@fundacionprevent.com o 636 47 91 00

Cofinanciado por:

Financiado por la Unión Europea NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Comunidad de Madrid

Partner académico:

HUB4T

TecnoCampus

Patrocinado por:

CaixaBank

endesa

Con la colaboración de:

goodhabitz online training

serunion