

Bases Nio – Febrer 2025

Formació en Ciberseguretat per als guardians de la informació i les dades al segle XXI

Cofinanciado por:



Partner académico:



Patrocinado por:



Con la colaboración de:



Què és el programa Nio?

Nio és un programa dissenyat per donar cabuda a totes les persones amb inquietuds en les noves tecnologies.

El seu objectiu és acompanyar persones amb discapacitat o trastorns de salut mental en el seu primer acostament a una professió amb molt alta demanda en el sector tecnològic i en tots els sectors digitalitzats: serveis, automoció, salut, consultoria, etc. per oferir al mercat talent divers i a les persones noves oportunitats professionals.

Nio és un programa que combina formació tècnica en ciberseguretat, desenvolupament d'habilitats i competències per a l'ocupació.

El finançament d'INCIBE s'emmarca en el component 19, inversió 4 «Professionals digitals» del Pla de Recuperació, Transformació i Resiliència (PRTR).

Requisits per participar-hi:

- Grau discapacitat mínim del 33% o informe que acrediti un diagnòstic en salut mental.
- Titulació mínima: ESO.
- Es valorarà tenir cursos o formacions prèvies com FP Grau Mitjà i/o Superior o equivalent de la família professional d'Informàtica i Comunicacions.
- Coneixements mitjans en informàtica: sistemes operatius, Microsoft Office, maneig de programari (valorable ús de màquines virtuals).
- Disposar d'un ordinador personal amb els següents mínims:
 - Tipus de processador: Intel Core i5 o superior
 - 16 GB RAM
 - Virtualització activada a la BIOS
 - SSD 500 GB
 - Tenir instal·lat Microsoft Office i/o Open Office
 - Bona connexió a Internet

Data d'inici i fi:

Data d'inici: 17 de febrer

Data de fi: 30 de maig

Modalitat:

Modalitat online en directe.

Les classes s'impartiran els dilluns, dimecres i divendres en dos torns:

Cofinanciat per:



Partner acadèmic:



Patrocinat per:



Con la col·laboració de:



- Torn de matí: dilluns, dimecres i divendres de 9:30 a 12:45 h.
- Torn de tarda: dilluns, dimecres i divendres de 17:00 a 20:15 h.

Continguts:

250 hores de formació en ciberseguretat

- 125 hores de continguts teòrics
- 125 hores d'exercicis pràctics

| MÒDUL FORMATIU | CONTINGUTS |
|--|--|
| 1. INTRODUCCIÓ A LA CIBERSEGURETAT | <ul style="list-style-type: none"> a. Definició de ciberseguretat b. Importància de la ciberseguretat en l'entorn actual c. Principals amenaces i riscos d. Història i evolució de la ciberseguretat e. Casos famosos de ciberatacs |
| 2. INTRODUCCIÓ A LA SEGURETAT DE LA INFORMACIÓ | <ul style="list-style-type: none"> a. Introducció a la seguretat de la informació b. Identificació d'actius c. Vulnerabilitats, Amenaces, Riscos, Atacs d. Autenticació, Autorització, Registre (AAA) e. Confidencialitat, Integritat, Disponibilitat (CIA) f. Introducció a la criptografia |
| 3. SISTEMES OPERATIUS I XARXES DE PROTOCOLS | <ul style="list-style-type: none"> a. Windows <ul style="list-style-type: none"> - Introducció - Gestió d'usuaris / Administrador - Ordres del sistema - Introducció a la Seguretat a Windows b. Linux <ul style="list-style-type: none"> - Introducció - Gestió d'usuaris / Administrador - Ordres del sistema |

Cofinanciado por:



Partner acadèmic:



Patrocinado por:



Con la colaboración de:



| | |
|--|--|
| | - Introducció a la Seguretat a Linux |
| 4. GESTIÓ DE LA SEGURETAT DE LA INFORMACIÓ | <ul style="list-style-type: none"> a. Sistema de gestió de la seguretat de la informació b. Anàlisi de riscos c. Cadena d'atac a les infraestructures d. Controls de la ISO 27001 e. Conceptes de l'Esquema Nacional de Seguretat f. Legislació en protecció de dades personals (RGPD) |
| 5. ANÀLISI DE VULNERABILITATS EN XARXA | <ul style="list-style-type: none"> a. TCP/IP b. Serveis bàsics c. Dispositius d'interconnexió d. Vulnerabilitats IP e. Vulnerabilitats TCP/UDP f. Atacs a serveis |
| 6. SISTEMES DE PROTECCIÓ DE LA INFORMACIÓ | <ul style="list-style-type: none"> a. Control d'accessos b. Securització de LAN c. Securització Perimetral d. Dispositius de securització e. Gestió de la recuperació de dades |
| 7. GESTIÓ DE LA CIBERSEGURETAT EN LES ORGANITZACIONS | <ul style="list-style-type: none"> a. Gestió d'incidents de ciberseguretat (SOC Centre d'Operacions de Seguretat) b. Detecció d'anomalies en el trànsit de la xarxa corporativa c. Indicadors d'incidents / atacs d. Automatització de procediments e. Gestió d'un incident |

Cofinanciado por:



Partner académico:



Patrocinado por:



Con la colaboración de:



Contacte:

Per qualsevol 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:



Partner académico:



Patrocinado por:



Con la colaboración de:

