

Curs 22-23
Admissió del
19 fins 29 de
Maig

Torn Vesprada

CE Ciberseguretat en Entorns TIC



IES Jaume II el Just
Tavernes de la Vallidigna

IES Jaume II El Just

Tavernes de la Vallidigna

Índex

CE Ciberseguretat en Entorns TIC	3
Duració.....	3
Requisit d'accés	3
Què vaig a aprendre i fer?.....	3
Eixides professionals	4
Mòduls Professionals.....	4
Organització del Curs d'Especialització.....	6
Horari	6

IES Jaume II El Just

Av de la Dula 31

Codi Postal : 46760

Telèfons : 962829995

FAX : 962829996

Correos :46008340@gva.es46008340.secret@gva.es**Página WEB :**<https://portal.edu.gva.es/iesjaumeeljust/><http://moodle.ieseljust.com>

CE Ciberseguretat en Entorns TIC

El “Curs d’Especialització en Ciberseguretat en Entorns de les Tecnologies de la Informació” capacita per a definir i implementar estratègies de seguretat en els sistemes d’informació realitzant diagnòstics de ciberseguretat, identificant vulnerabilitats i implementant les mesures necessàries per a mitigar-les aplicant la normativa vigent i estàndards del sector, seguint els protocols de qualitat, de prevenció de riscos laborals i respecte ambiental.

Duració

Aquests estudis tenen una durada de 720h, organitzats en un curs acadèmic.

Requisit d’accés

- Tècnic Superior en Administració de Sistemes Informàtics en Xarxa
- Tècnic Superior en Desenvolupament d’Aplicacions Multiplataforma
- Tècnic Superior en Desenvolupament d’Aplicacions Web
- Tècnic Superior en Sistemes de Telecomunicacions i Informàtics
- Tècnic Superior en Manteniment Electrònic

Què vaig a aprendre i fer?

- Elaborar i implementar plans de prevenció i conscienciació en ciberseguretat en l’organització, aplicant la normativa vigent.
- Detectar i investigar incidents de ciberseguretat, documentant i incloent-los en els plans de securització de l’organització.
- Dissenyar plans de securització contemplant les millors pràctiques per al enduriment de sistemes i xarxes.
- Configura sistemes de control d’accés i autenticació en sistemes informàtics, complint els requisits de seguretat i minimitzant les possibilitats d’exposició a atacs.
- Dissenyar i administrar sistemes informàtics en xarxa i aplicar les polítiques de seguretat establertes, garantint la funcionalitat requerida amb un nivell de risc controlat.
- Analitzar el nivell de seguretat requerit per les aplicacions i els vectors d’atac més habituals, evitant incidents de ciberseguretat.
- Implantar sistemes segurs de desplegat de programari amb l’adequada coordinació entre els desenvolupadors i els responsables de l’operació de programari.
- Realitzar anàlisis forenses informàtics analitzant i registrant la informació rellevant relacionada.
- Detectar vulnerabilitats en sistemes, xarxes i aplicacions, avaluant els riscos associats.

- Definir i aplicar procediments per al compliment normatiu en matèria de ciberseguretat i de protecció de dades personals, implementant tant internament com en relació amb tercers.
- Elaborar documentació tècnica i administrativa complint amb la legislació vigent, responent als requisits establerts.

Eixides professionals

- Expert en ciberseguretat.
- Auditor de ciberseguretat.
- Consultor de ciberseguretat.
- Hacker ètic.

Mòduls Professionals

- Incidents de ciberseguretat (120h, 4h/setmana) [IC]
 - Desenvolupament de plans de prevenció i conscienciació en ciberseguretat
 - Auditoria d'incidents de ciberseguretat
 - Investigació dels incidents de ciberseguretat
 - Implementació de mesures de ciberseguretat
 - Detecció i documentació d'incidents de ciberseguretat
- Bastionat de xarxes i sistemes (210h, 7h/setmana) [BXS]
 - Disseny de plans de securització
 - Configuració de sistemes de control d'accés i autenticació de persones
 - Administració de credencials d'accés a sistemes informàtics
 - Disseny de xarxes de computadors segures
 - Configuració de dispositius i sistemes informàtics
 - Configuració de dispositius per a la instal·lació de sistemes informàtics
 - Configuració dels sistemes informàtics
- Posada en producció segura (150h, 5h/setmana) [PPS]
 - Prova d'aplicacions web i per a dispositius mòbils
 - Determinació de l'nivell de seguretat requerit per aplicacions
 - Detecció i correcció de vulnerabilitats d'aplicacions web
 - Detecció de problemes de seguretat en aplicacions per a dispositius mòbils
 - Implantació de sistemes segurs de desplegament de programari
- Anàlisi forense informàtic (120h, 4h/setmana) [AFI]
 - Aplicació de metodologies d'anàlisi forenses
 - Realització d'anàlisis forenses en dispositius mòbils
 - Realització d'anàlisis forenses en Cloud

- Realització d'anàlisis forenses en Iot
- Documentació i elaboració d'informes d'anàlisis forenses. Apartats dels que es compon l'informe
- Hacking ètic (120h, 4h/setmana) [HE]
 - Determinació de les eines de monitorització per detectar vulnerabilitats
 - Atac i defensa en entorn de proves, de les comunicacions sense fil
 - Atac i defensa en entorn de proves, de xarxes i sistemes per accedir a sistemes de tercers
 - Consolidació i utilització de sistemes compromesos
 - Atac i defensa en entorn de proves, a aplicacions web
- Normativa de ciberseguretat (30h, 1h/setmana) [NC]
 - Punts principals d'aplicació per a un correcte compliment normatiu
 - Disseny de sistemes de compliment normatiu
 - Legislació per al compliment de la responsabilitat penal
 - Legislació i jurisprudència en matèria de protecció de dades
 - Normativa vigent de ciberseguretat d'àmbit nacional i internacional
 - Esquema Nacional de Seguretat (ENS).
 - Llei PIC (Protecció d'infraestructures crítiques).

Organització del Curs d'Especialització

Es tracta d'uns estudis presencials amb una duració de 720h que s'impartiran en horari de vesprada a raó de 25 hores per setmana.

Equip Educatiu

Mòduls	
IC	- Incidents de Ciberseguretat
BXS	- Bastionat de xarxes i sistemes
PPS	- Posta en producció segura
AFI	- Anàlisi Forense informàtic
HE	- Hacking ètic
NC	- Normativa Ciberseguretat

Horari Orientatiu basat al curs 21-22

Hora	Dilluns	Dimarts	Dimecres	Dijous	Divendres
15:30-16:25					
16:25-17:20	PPS	HE	BXS	HE	IC
17:20-18:15	PPS	HE	BXS	HE	IC
18:15-18:45					
18:45-19:40	AFI	BXS	PPS	NC	IC
19:40-20:35	AFI	BXS	PPS	AFI	BXS
20:35-21:30	IC	BXS	PPS	AFI	BXS