PRESTAKUNTZA-MODULUAREN IDENTIFIKAZIO-DATUAK

PRESTAKUNTZA-MODULUA	DATUEN SARBIDERAKO ETA DATU-TRATAMENDURAKO SISTEMA SEGURUAK	Iraupena	60
Kodea	MF0489_3		
Lanbide-arloa	INFORMATIKA ETA KOMUNIKAZIOAK		
Lanbide-eremua	Sistemak eta telematika		
Profesionaltasun-ziurtagiria	Segurtasun informatikoa	Maila	3
Profesionaltasun-ziurtagiria osatzeko gainerako prestakuntza	Segurtasuna ekipo informatikoetan	Iraupena	90
	Segurtasun informatikoko auditoretza		90
	Segurtasun informatikoko gorabeheren kudeaketa		90
	Sistema informatikoko zerbitzuen kudeaketa (zeharkakoa)		90
	Lanekoak ez diren lanbide-jardunbideak Segurtasun informatikoan		80

A atala: **GAITASUN-ERREFERENTEA**

Prestakuntza-modulu hau bat dator UC0489_3 DATUEN SARBIDERAKO ETA DATU-TRANSMISIORAKO SISTEMA SEGURUAK DISEINATZEA ETA EZARTZEA gaitasun-atalarekin

B atala: **AHALMENEN ETA EDUKIEN ZEHAZTAPENA**

Ahalmenak eta ebaluazio-irizpideak

A1: Enkriptatze-teknikak ebaluatzea, bete beharreko segurtasun-eskakizunen arabera egokiena hautatzeko.

EI1.1 Gako pribatudun eta gako publikodun enkriptatze-algoritmoen arteko aldeak deskribatzea eta horien erabilerak adieraztea.

EI1.2 Enkriptatze-modu guztiak identifikatzea eta ezaugarri nagusiak deskribatzea.

EI1.3 Gako pribatudun algoritmoak sailkatzea eta exekuzio-faseak deskribatzea.

EI1.4 Gako publikodun algoritmoak sailkatzea eta exekuzio-faseak deskribatzea.

EI1.5 Gakoak elkartrukatzeko protokoloak identifikatzea eta horien funtzionamendua deskribatzea.

A2: Enkriptazioko teknikak eta zerbitzuak ezartzea behar den zerbitzuetan, segurtasun informatikoko zehaztapenen arabera.

EI2.1 Sistema informatikoen arteko komunikazioetan enkriptatze-teknikak erabiltzeko premia justifikatzea, erabiltzen diren kanalen arabera.

EI2.2 Bi sare modu seguruan konektatzeko enkriptatze-teknikak definitzea eta beharrezkoak diren betekizunak eta funtzionalitateak deskribatzea.

EI2.3 Bi ekipo modu seguruan konektatzeko teknikak (SSL eta SSH tunelak) definitzea eta beharrezkoak diren eskakizunak eta funtzionalitateak deskribatzea.

EI2.4 Kasu praktiko batean komunikazio segurua ezarri nahi da bi sistema informatikoen artean; honako lan hauek egin behar dira:

- Proposatutako komunikazio-arkitekturaren segurtasun-eskakizunak aztertzea.
- Konponbide egokiena adieraztea eta hori hautatzeko arrazoia justifikatzea.
- Sareak konektatzeko VPN eta IPSec zerbitzuak instalatzea.
- Urruneko ekipoak konektatzeko SSL edo SSH tunelen zerbitzuak instalatzea.

A3: Ziurtagiri digitalen sistemak erabiltzea konfidentzialtasuna eta integritatea eskatzen duten komunikazioetan, segurtasun-zehaztapenen arabera.

EI3.1 Ziurtagiri digitaletan zerbitzarirako erabili diren atributuak identifikatzea eta horien balioak eta funtzioa deskribatzea.

EI3.2 Ziurtagiri digitalen erabilera-moduak deskribatzea eta segurtasun-zehaztapenekin lotzea: konfidentzialtasuna, integritatea eta irisgarritasuna.

EI3.3 Zigilatze-sistema digital baten egitura deskribatzea eta egitura osatzen duten elementuen funtzioak adieraztea.

A4: Ziurtapen digitaleko zerbitzuak diseinatzea eta ezartzea ustiapeneko eta segurtasun informatikoko premien arabera.

EI4.1 Gako publikodun azpiegituraren egitura deskribatzea eta egitura osatzen duten elementuen funtzioak adieraztea.

EI4.2 Ziurtapen-agintaritzaren betebeharrak eta zerbitzuak deskribatzea eta ziurtapen-jardunbideen deklarazioarekin eta ziurtapen-politikarekin lotzea.

EI4.3 Ziurtagiri digital baten nahitaezko eta aukerako atributuak identifikatzea eta atributu horien ohiko erabilera deskribatzea.

EI4.4 Pribilegioak kudeatzeko azpiegituraren egitura deskribatzea eta egitura osatzen duten elementuen funtzioak adieraztea.

EI4.5 Atributuen ziurtagirien esparruak zehaztea, eta horien ohiko erabilera eta ziurtagiri digitalekin duten lotura deskribatzea.

EI4.6 Kasu praktiko batean ziurtapen-sistema bat ezarri nahi da sistema informatiko baterako; honako lan hauek egin behar dira:

- Gako publikodun azpiegitura bat diseinatzea, zehaztapenen arabera.
- Diseinatu den ziurtapen-agintaritzen hierarkia justifikatzea.

- Ziurtagiriak ematea; horretarako, Ziurtapen-Jardunbideen Deklarazioan adierazitako prozedurak bete behar dira.

Edukiak

1. Kriptografia

- Kriptografiaren ikuspegi historikoa eta helburuak
- Informazioaren teoria
- Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía: confidencialidad, integridad, autenticidad, no repudio, imputabilidad y sellado de tiempos konfidentzialtasuna, integritatea, autentikotasuna, ez gaitzestea, egozgarritasuna eta denboren zigilatzea
- Gako pribatudun eta gako publikodun kriptografiaren funtsezko elementuak
- Ziurtagiri digitalen ezaugarriak eta atributuak
- Gehien erabiltzen diren gako-elkartrukeko protokoloen funtzionamenduaren identifikazioa eta deskribapena
- Gehien erabiltzen diren algoritmo kriptografikoak
- Ziurtagiri digitalen elementuak, ohiko moduan onartuta dauden formatuak eta horien erabilera
- Laburpen-funtzioen funtsezko elementuak eta horiek erabiltzeko irizpideak
- Sinadura elektronikoari buruzko abenduaren 19ko 59/2003 Legean bildutako lege-eskakizunak
- Sinadura digitalaren funtsezko elementuak, sinadura-motak eta horiek erabiltzeko irizpideak
- Fluxuko eta blokeko enkriptatze-teknikak erabiltzeko irizpideak
- Gakoak elkartrukatzeko protokoloak
- Enkriptatze-erreminten erabilera, hala nola PGP, GPG edo CryptoLoop

2. Gako publikodun azpiegitura baten (PKI) aplikazioa

- PKI baten osagaien eta erlazio-ereduaren identifikazioa
- Ziurtapen-agintaritza eta dagozkion elementuak
- Ziurtapen-politika eta ziurtapen-jardunbideen deklarazioa (CPS)
- Ezeztatutako ziurtagirien zerrenda (CRL)
- Ziurtagirien sinadura-eskaeren funtzionamendua (CSR)
- Pribilegioak kudeatzeko azpiegitura (PMI)
- Atributuen ziurtagirien esparruak, ohiko erabileren deskribapena eta ziurtagiri digitalekin duten lotura deskribatuta
- PKI bat izatean oinarritzen diren aplikazioak

3. Komunikazio seguruak

- Sare pribatu birtualen definizioa, xedea eta funtzionalitatea
- IPSec protokoloa
- SSL eta SSH protokoloak
- SSL VPN sistemak
- Enkriptatutako tunelak
- VPN teknologia ezartzeko aukera guztien abantailak eta eragozpenak.

C atala: **ESKAKIZUNAK ETA BALDINTZAK**

Baldintza hauetakoren bat bete behar da:

– Batxilergoko titulua izatea.
– 3. mailako profesionaltasun-ziurtagiriren bat edukitzea.
– Lanbide-arlo eta -eremu bereko 2. mailako profesionaltasun-ziurtagiriren bat edukitzea.
– Goi-mailako heziketa-zikloetan sartzeko baldintza akademikoak betetzea edo goi-mailako zikloetara sartzeko dagozkion probak gainditu izana.
– 25 urte baino gehiagokoentzako eta/edo 45 urtetik gorakoentzako unibertsitatera sartzeko proba gainditu izana.
– Prestakuntzari behar adinako probetxua ateratzeko behar diren prestakuntza- edo lanbide-ezagupenak izatea, ezartzen den araudiaren arabera.

Prestatzaileen, instalazioen eta ekipamenduen arloko eskakizunei dagokienez, profesionaltasun-ziurtagiri honetarako ezarritako eskakizunak hartuko dira kontuan: Segurtasun informatikoa