PRESTAKUNTZA-MODULUAREN IDENTIFIKAZIO-DATUAK

PRESTAKUNTZA-MODULUA	SEGURTASUNA EKIPO INFORMATIKOETAN	Iraupena	90
Kodea	MF0486_3		
Lanbide-arloa	INFORMATIKA ETA KOMUNIKAZIOAK		
Lanbide-eremua	Sistemak eta telematika		
Profesionaltasun-ziurtagiria	Segurtasun informatikoa	Maila	3
Profesionaltasun-ziurtagiria osatzeko gainerako prestakuntza	Segurtasun informatikoko auditoretza	Iraupena	90
	Segurtasun informatikoko gorabeheren kudeaketa		90
	Datuen sarbiderako eta datu-tratamendurako sistema seguruak		60
	Sistema informatikoko zerbitzuen kudeaketa (zeharkakoa)		90
	Lanekoak ez diren lanbide-jardunbideak segurtasun informatikoan		80

A atala: **GAITASUN-ERREFERENTEA**

Prestakuntza-modulu hau bat dator gaitasun-atal honekin: UC0486_3 EKIPO INFORMATIKOAK SEGURTATZEA

B atala: **AHALMENEN ETA EDUKIEN ZEHAZTAPENA**

Ahalmenak eta ebaluazio-irizpideak

A1: Erakundearen ezarpen-planak aztertzea sistematik inplikatuta dauden elementuak eta ezarri beharreko segurtasun-mailak identifikatzearren.

EI1.1 Ezarpen-plan baten egitura identifikatzea eta atal bakoitzeko edukiak azaltzea.

EI1.2 Ezarpen-planean ager daitezkeen sistemak bereiztea eta ezartzen dituzten segurtasun-funtzionalitateak deskribatzea.

EI1.3 Ezarpen-planean agertzen diren segurtasun-mailak deskribatzea eta sartzeko baimenekin lotzea, ezarpenerako.

EI1.4 Kasu praktiko batean ezarpen-plana aztertzeko eskatzen da, baita sistemak izango dituen ondorioak ere; honako lan hauek egin behar dira:

- Ezarpen-planean inplikatutako sistemak zehaztea.
- Sistema bakoitzaren segurtasun-eskakizunak aztertzea.
- Sistema bakoitzean aplikatu beharreko segurtasun-neurriak deskribatzea.
- Izaera pertsonaleko datuak fitxategien deklarazioa egiteko formularioak betetzea.

A2: Zerbitzarietarako sarbide-mekanismo fisikoak eta logikoak aztertzea eta ezartzea, segurtasun-zehaztapenei jarraiki.

EI2.1 Sarbide fisikoa kontrolatzeko mekanismoen ezaugarriak deskribatzea eta funtzio nagusiak azaltzea.

EI2.2 Traza-mekanismoak azaltzea eta zerbitzariaren sistema eragilearekin lotzea.

EI2.3 Sarbide logikoa kontrolatzeko mekanismoak identifikatzea eta ezaugarri nagusiak azaltzea (pasahitzak, IP ataken iragazketa, besteak beste).

EI2.4 Kasu praktiko batean zerbitzari bat ezarri behar da zehaztapen jakin batzuei jarraiki; honako lan hauek egin behar dira:

- Zerbitzariaren kokaleku fisikoa zehaztea funtzionatzen duela bermatzearren.
- Sistemaren integritatea bermatuko duten segurtasun fisikoko neurriak deskribatzea eta justifikatzea.
- Zerbitzariak eskatzen duen segurtasun-maila ezartzeko modulu edo aplikazio gehigarriak identifikatzea.
- Zerbitzariak izaten dituen mehatxuak zehaztea eta zenbateko arriskua duten ebaluatzea, zerbitzariaren testuingurua kontuan izanik.
- Erabiltzaileei eta erabiltzaile-taldeei sistema erabiltzeko esleitutako baimenak zehaztea.

A3: Zerbitzarian exekutatzen ari den zerbitzu bakoitzaren funtzioa eta premia ebaluatzea, segurtasun-zehaztapenen arabera.

EI3.1 Erakunde baten sistema informatikoan ohikoak diren zerbitzuak identifikatzea eta horien misioa edo xedea deskribatzea informatikako eta komunikazioetako azpiegituraren barruan.

EI3.2 Zerbitzari baten funtzionamendurako beharrezkoak diren zerbitzuak identifikatzea eta deskribatzea, erakundearen sistema informatikoaren barruan betetzen duen misioaren edo xedearen arabera.

EI3.3 Exekutatzen ari diren zerbitzuen mehatxuak deskribatzea eta baimen murriztaileenak aplikatzea, exekuzioa bermatu eta arriskua minimizatzeko.

EI3.4 Kasu praktiko batean zerbitzari bat ezarri behar da zerbitzu-sorta bat exekutatzen dituela eta ustiapen-plan jakin bati jarraiki; honako lan hauek egin behar dira:

- Zerbitzari horren eta erakundearen sistema informatikoaren gainerakoaren arteko erlazioak adieraztea.
- Zerbitzariari aplikatu beharreko segurtasun-eskakizunak erauztea ezarpen-planetik.
- Sistemak funtzionatzeko beharrezkoak diren gutxieneko zerbitzuak zehaztea.

A4: Zerbitzariaren suebaki bat instalatzea, konfiguratzea eta administratzea, segurtasun-zehaztapenen arabera beharrezkoak diren ezaugarriak beteta.

EI4.1 Suebaki-motak sailkatzea, sarekoak eta lokalak, hardwarea eta softwarea, paketeenak eta aplikazioa, eta horien ezaugarriak eta funtzionalitate nagusiak deskribatzea.

EI4.2 Zerbitzari-suebaki baten iragazketa-arauak deskribatzea eta parametro nagusiak azaltzea.

EI4.3 Zerbitzari-suebaki baten trazaren formatua azaltzea eta segurtasunari buruzko informazio garrantzitsua jasotzea.

EI4.4 Kasu praktiko batean zerbitzari-suebaki bat instalatu behar da sarbide lokalak eta urrunekoak dituen testuinguru batean; honako lan hauek egin behar dira:

- Zerbitzariaren segurtasun-eskakizunak zehaztea.
- Zerbitzariak sistema informatikoko gainerako ekipoekin dituen erlazioak zehaztea.
- Zerbitzarian ezarri behar diren sarbide-arauen zerrenda osatzea.
- Ezarritako suebakia probatzeko plan bat egitea.
- Proba-plana exekutatzea eta egin beharreko zuzenketak egitea, detektatutako akatsak zuzentzearren.

.

Edukiak

1. Ekipo informatikoen segurtasunari buruz oro har onartuta dauden irizpide orokorrak

- Arriskuaren kudeaketara bideratutako segurtasun-eredua, informazio-sistemen erabilerarekin loturik
- Mehatxu ohikoenen zerrenda, eragiten dituzten arriskuak eta babesgarri ohikoenak
- Babesgarri eta segurtasun-teknologia ohikoenak
- Segurtasun informatikoaren kudeaketa babesgarrien eta neurri teknologikoen osagarri

2. Negozio-inpaktuaren azterketa

- Informazio-sistemetan oinarritutako negozio-prozesuen identifikazioa
- Negozio-prozesuetako konfidentzialtasunaren, integritatearen eta erabilgarritasunaren eskakizunen balioespena
- Negozio-prozesuen oinarri diren informazio-sistemen eta horien segurtasun-eskakizunen zehaztapena

3. Arriskuen kudeaketa

- Arriskuak kudeatzeko prozesuaren aplikazioa eta alternatiba ohikoenen azalpena
- Arriskuak identifikatzeko eta aztertzeko ohiko moduan onartutako metodologiak
- Babes-neurrien eta kontrolen aplikazioa arriskua murriztearren

4. Segurtasuna ezartzeko plana

- Sistemetako segurtasun-mailaren zehaztapena negozio-prozesuetan ezinbestekoak diren segurtasun-eskakizunekin alderatuta.
- Informazio-sistemen segurtasun-eskakizunak betetzeko babes-neurrien hautaketa
- Hautatutako babesgarrien ezarpen-plana osatzeko gida.

5. Izaera pertsonaleko datuen babesa

- Izaera pertsonaleko datuak babesteko printzipio orokorrak
- Izaera pertsonaleko datuak babesteari dagokionez, indarreko legedian bildutako arau-hausteak eta zehapenak
- Erakundeak erabiltzen dituen eta izaera pertsonaleko datuak dituzten fitxategien identifikazioa eta erregistroa
- Izaera pertsonaleko datuak babesteari dagokionez, indarreko legedian eskatzen den segurtasun-dokumentuaren lanketa

6. Sistemen segurtasun fisikoa eta industriala. Sistemen segurtasun logikoa

- Segurtasun fisikoko perimetroen zehaztapena
- Erakundearen instalazioetarako eta sistema informatikoak kokatuta dauden eremuetarako sarbide fisikoa kontrolatzeko sistema ohikoenak
- Sistema informatikoen kokaleku fisikoa hautatzeko segurtasun-irizpideak
- Sistema informatikoei elektrizitate-horniduraren kalitatea eta jarraitutasuna bermatzeko elementu ohikoenen azalpena
- Sistema informatikoei aplikatu beharreko suteen aurkako babeserako eta klimatizaziorako eskakizunak
- Erakundearen segurtasun fisikoari eta industrialari buruzko araudiaren lanketa
- Gehien erabiltzen diren fitxategi-sistemak
- Sistema informatikoek erakundearen komunikazio-sarerako duten sarbide-kontrolaren ezarpena
- Erabiltzaileen direktorioaren direktiben eta politiken konfigurazioa
- Fitxategietarako sarbide-kontroleko zerrenden (ACLak) ezarpena
- Erabiltzaileen alten, bajen eta aldaketen kudeaketa, baita esleituta dituzten pribilegioena ere
- Erabiltzaileak autentifikatzeko sistema ahulak, sendoak eta biometrikoak
- Sarbide-kontrola gainbegiratzeko eta monitorizatzeko beharrezkoak diren sistema eragilearen auditoretza-erregistroen zerrenda
- Sistema informatikoetarako sarbide-kontrolari buruzko araudiaren lanketa

7. Zerbitzuen identifikazioa

- Informazio-sistemek erabiltzen dituzten protokoloen, zerbitzuen eta ataken identifikazioa
- Irekitako zerbitzuen eta ataken azterketa egiteko erreminten erabilera, beharrezkoak ez direnak zehaztearren

- Komunikazioen trafikoa aztertzeko erreminten erabilera, informazio-sistemek protokoloak, zerbitzuak eta atakak egiaz nola erabiltzen dituzten zehazteko

8. Sistemen gotortzea
- Informazio-sistema guztietako erabiltzaile eta pasahitz lehenetsien aldaketa
- Erabiltzaileen direktorioan pribilegioak eta pasahitzak kudeatzeko direktiben konfigurazioa
- Behar-beharrezkoak ez diren erreminten, utilitateen, zerbitzuen eta ataken itxiera eta ezabaketa
- Informazio-sistemen konfigurazioa ahal denean protokolo seguruak erabil ditzaten
- Sistema informatikoen segurtasun-adabakien eguneratzea
- Informazio-sistemen babesa kode gaiztoen aurrean
- Komunikazioen, karpeta partekatuen, inprimagailuen eta sistemaren bestelako baliabide partekatuen kudeaketa segurua
- Informazio-sistemen erabilera egokiaren eta segurtasunaren monitorizazioa

9. Suebakiaren ezarpena eta konfigurazioa
- Suebaki-mota guztien zerrenda, kokalekuaren eta funtzionalitatearen arabera
- Zona Desmilitarizatuen (DMZ) bitartez suebakian sareak bereizteko segurtasun-irizpideak
- Sare Pribatu Birtualen (VPN) erabilera komunikazioetako kanal seguruak ezartzeko
- Suebakietako ebaketa-arauen definizioa
- Segurtasun-gertaerak eta behar bezala funtzionatzen dutela gainbegiratzeko eta monitorizatzeko beharrezkoak diren suebakiaren auditoretza-erregistroen zerrenda
- Suebakiaren proben eta monitorizazioaren ezarpena

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