SEGURTASUN ESKEMA NAZIONALA UNIBERTSITATE ADITU IKASTAROA

GAIA	Informatika, Telekomunikazio Sistemak eta Sistema Txertatuak
ECTS/ORDUAK	16 ECTS
EGUTEGIA	2022/01/17 - 2022/06/24 As-Az-Or
TOKIA	
HIZKUNTZA	Gaztelania
MODALITATEA	Online

Informazio gehiago eta izen-ematea

AURKEZPENA

Ikastaroaren helburu orokorra izango da parte-hartzaileak Segurtasun Eskema Nazionala (ENS) ezartzeko prozesua prestatzeko eta zuzentzeko gai izateko behar diren ezagutzak jasotzea Administrazio Publikoetako (AAPP) organo baten edo enpresa pribatu baten informazio-sistema batean, ziurtapen-erakunde akreditatu batek emandako adostasun-ziurtagiria lortzeko adinako bermeekin.

HELBURUAK

Ikastaroaren helburu orokorra izango da parte-hartzaileak Segurtasun Eskema Nazionala (ENS) ezartzeko prozesua prestatzeko eta zuzentzeko gai izateko behar diren ezagutzak jasotzea Administrazio Publikoetako (AAPP) organo baten edo enpresa pribatu baten informazio-sistema batean, ziurtapen-erakunde akreditatu batek emandako adostasun-ziurtagiria lortzeko adinako bermeekin.

Antolaketari, administrazioari eta legeei lotutako helburu zehatzak hauek dira:

- ENSaren xedea, izaera, egitura eta edukia eta horren oinarri den lege esparrua ezagutzea.
- Administrazio publikoen digitalizazio-prozesua arautzen duen araudia ezagutzea, bai eta administrazio horiek izan beharko lituzketen sistemak eta zerbitzuak ere, ENSari lotuta egon daitezkeen informazio-sistemak identifikatu ahal izateko.
- ENSak ezartzen dituen printzipio, betekizun eta segurtasun-neurrien egitura, izaera eta funtzioa ezagutzea.
- Aplikagarritasun-deklarazioa informazio-sistema baterako behar diren segurtasun-neurriekin zehaztu ahal izatea, sistemaren kategorizazio-prozesuen azterketan, arrisku-azterketan eta inpaktu-azterketan oinarrituta.
- Erakunde batean segurtasun-egitura bat garatzen jakitea, eta erakunde horren ezaugarrietara egokitutako beharrezko rolak eta erantzukizunak ezartzea.
- NBEri lotutako sistemen ziurtapen- eta ikuskapen-prozesua ezagutzea, eta ikuskapen-plan bat egiteko eta gauzatzeko gai izatea.
- Erakunde baten informazio sistemak ENSaren aginduak bete ditzan beharrezkoak diren jarraibide, konfigurazio eta barne arauak ezartzeko behar den dokumentazioa idazteko gai izatea.

- Administrazio publiko edo sistema jakin batzuetan Segurtasun Eskema Nazionala betetzeko berezitasunak eta egokitzapenak ezagutzea.
- Segurtasun Eskema Nazionalaren inplementazioa egokitzeko gai izatea, Datuak Babesteko Legean eta informazio-sistemen segurtasuna kudeatzeko ISO 27001 estandarrean jasotako neurriak betetzen direla bermatzeko.

Sistemaren alderdi operatiboekin lotutako berariazko helburuak hauek dira:

- ENSari lotutako informazio-sistema baten segurtasun-dimentsioak alda ditzaketen mehatxuak ezagutzea eta behar diren babes-neurriak identifikatzea.
- Hodeiko ingurune batean ENSa ezartzeko berezitasunak ezagutzea eta ingurune horretan sistemaren babesa bermatzeko beharrezko neurriak ezartzeko gai izatea.
- Informazio sistema baten babes fisikorako behar diren faktoreak aztertzeko gai izatea eta haren aplikazioa arautuko duen arau bat garatzeko gai izatea.
- Zerbitzuak kudeatzeko prozedurak eta mekanismoak ezagutzea eta prozesu hori behar bezala arautzeko araudia garatu ahal izatea.
- Sistemaren etengabeko monitorizazioko mekanismoak planifikatu eta ezartzeko gai izatea, eta sistemaren babes-egoera metrika eta adierazle egokiekin konparatzeko gai izatea.

Eta hauek dira segurtasun neurrien inplementazio teknikoarekin zerikusia duten berariazko helburuak:

- Sakoneko babesa eskatzen duen segurtasun-arkitektura baten garapen eta inplementazio teknikoari lotutako neurriak ezagutzea, baita sarbidea kontrolatzeko, perimetroa babesteko eta sarea babesteko eta host-ak babesteko neurriak ere.
- Sistemaren segurtasun-konfigurazioen inplementazio teknikoari lotutako gidak eta gomendioak ezagutzea, eta horiek bere kabuz ezartzeko gai izatea, edo kanpoko teknikari aditu bati jarraibide egokiak ematea.

NORI ZUZENDUA

Informazio sistemei buruzko ezagupenak dituzten graduko tituludunentzat da ikastaroa, bai maila teknikoetako titulazioetatik datozenentzat (ingeniaritza, informatika, telekomunikazioak, etab.).), bai zibersegurtasunaren arloko graduondoko ikasketak egin dituelako, bai informazioaren segurtasunaren arloan lan egin duelako, eta gai izan behar dute ENSak alderdi administratibo, operatibo eta teknikoetan ezarritako baldintzak ulertzeko.

Aditu titulua lortzeko, baldintza hauek bete beharko dira:

– Unibertsitateko titulazioa edo

– Sektorean 3 urtetik gorako esperientzia duten goi-mailako heziketa-zikloak (lanbide-esperientzia aintzatesteko, curriculum vitaea, lan-bizitza eta elkarrizketa eskatuko dira).

PROGRAMA

Módulo 1	Estructura, contenido y requisitos del ENS
1.1.	Aspectos generales

1	Naturaleza, finalidad, alcance, estructura y medidas de seguridad en el ENS
2	Guías STIC e Instrucciones Técnicas asociadas
3	Proceso de implementación / adecuación
4	Cargos y responsabilidades en el ENS
5	Implementación medidas de seguridad organizativas y operativas
6	Implementación medidas de protección
7	Políticas, normas y procedimientos
1.2	Análisis de riesgos y categorización
1	Análisis de riesgos: metodología Magerit y Pilar
2	Metodología Margferit y Pilar-1
3	Metodología Margerit y Pilar-2
1.3.	Los sistemas de información de las AAPP
1	Legislación de los sistemas de información de las AAPP
2	Portales y servicios digitales de las AAPP
3	Declaración de aplicabilidad y perfiles de cumplimiento específicos
	Examen módulo 1/1 (1.1, 1.2, 1.3, 1.4)
1.4	Formación, seguridad física y seguridad de las personas
1	Seguridad física y control de acceso físico
2	Seguridad de personas.
3	Formación y concienciación
1.5	Gestión de servicios
1	Marco de referencia en la gestión de servicios. ITIL
2	Gestión de inventario, adquisiciones y cambios
3	Gestión de cambios y configuración
1.6	Ciberamenazas y mecanismos de protección
1	Conceptos generales sobre malware y protección anti-malware en el ENS
2	Configuración segura DNS y protección contra Denegación de Servicio

3	Configuración segura de servicios Web y correo electrónico
	Examen módulo 1/2 (1.5, 1.6, 1.7)
1.7	Monitorización de sistemas, métricas y gestión de incidentes
1	Concepto general de gestión de incidentes
2	Concepto de monitorización de sistemas de información (log,s, SIEM, IDS)
3	Herramientas de seguridad
4	Análisis forense y cadena de custodia
5	Generalidades sobre metodologías de configuración segura
6	Registro de actividad de usuarios
7	Métricas en el ENS
8	Herramientas de monitorización, gestión de incidentes y métricas en el ENS
1.8	Continuidad, respaldo y resiliencia
1	Plan de continuidad y análisis de impacto
2	Sistemas de respaldo y recuperación. Gestión y destrucción de dispositivos de almacenamiento.
1.9	Control de acceso, autenticación y criptografía
1	Generalidades sobre criptografía y pseudonimización
2	Generalidades sobre autenticación, accesos remotos y VPN
3	Criptografía, autenticación y firma digital en el ENS
	Examen módulo 1/3 (1.8, 1.9, 1.10)
1.10	Implementación técnica.
1	Conceptos generales de redes: routers, switches, cortafuegos
2	Securización de firewalls, routers, switches, cortafuegos en el ENS
3	Interconexión de sistemas en el ENS
4	Securización de redes Wi-fi y Bluetooth
5	Seguridad de dispositivos móviles
6	Conceptos generales sobre arquitectura de sistemas Windows (AD, Kerberos, etc.)
7	Seguridad de servidores Windows miembro y controlador de dominio

8	Seguridad de cliente Windows 10 aislado y en dominio
9	Seguridad de otros servidores Windows: impresoras, servidor ficheros
10	Empleo de herramienta auditoría Windows CLARA
11	Conceptos generales arquitectura sistemas Linux
12	Seguridad en un sistema servidor Linux
13	Generalidades sobre la nube
14	Perfil de cumplimiento sistemas en la nube privados
15	Sistemas MS Azure. Teoría.
16	Configuración de seguridad Azure. Aplicación.
17	Perfil de cumplimiento SAAS: Office 365.
18	Conceptos básicos de virtualización y contenedores
19	Seguridad de la virtualización en el ENS
	Examen módulo 1/4 (1.11)
Módulo 2	**Auditoría y certificación en el ENS**
2.1.	La auditoría-1
2.1	La auditoría del ENS
2.2.	La certificación del ENS, certificación de productos y personas
	Examen módulo 2
Módulo 3	**ENS y gestión empresarial**
3.1.	La Seguridad Nacional. Derecho de la ciberseguridad
3.2	ENS - ISO 27001
3.3	ENS - RGPD
3.4	Protección de instalaciones críticas. Legislación
3.5	Protección de instalaciones críticas. Sistemas de información
	Examen módulo 3

METODOLOGIA

Saio sinkronoak astelehen, asteazken eta ostiraletan eginen dira, 16:00etatik 19:00etara.

Eskola presentzialak (teleprestakuntza) hiru orduko saioetan emanen dira, bi eduki motarekin:

1. Azalpen saioak. Irakasleak edukiak modu argi, atsegin eta egituratuan azalduko ditu, ikasleak haiek asimilatu, ulertu eta aplikatzeko gai izan dadin.
2. Froga saioak. Irakasleak konfigurazio teknikoa ezarriko du edo agiri bat idatziko du urratsez urrats, ikasleak prozesua xehetasunez ezagutu, ulertu eta, beharrezkoa denean, bere kabuz egiteko gai izan dadin.
3. Saio presentzialek 175 ordu iraunen dute guztira.

Eskola presentzialez gain, ikastaroa gainditu eta diploma eta ENSeko aditu-ziurtagiria lortzeko, ikasleak kasu praktiko bat ebatzi behar du, jasotako ezagutzak bereganatu dituela eta Segurtasun Eskema Nazionala behar bezala ezartzeko behar den dokumentazioa bere kabuz garatzeko gai dela egiaztatzeko. Parte-hartzaileak agertoki adierazgarri bati lotutako prestakuntza-dokumentazioa jasoko du. Agertoki horren gainean, parte-hartzaileak gai izan beharko du, gutxienez, dokumentu hauek egoki idazteko:

- Erakundearen segurtasun-politika, segurtasun-egitura barne.
- Aplikatu beharreko segurtasun neurriei lotutako segurtasun prozedurak eta arauak.
- Arriskuen analisiaren prozesua eta horren emaitza.
  Sistema kategorizatzeko prozesua eta horren emaitza.
- Eraginaren azterketa eta eskuragarritasunari buruzko emaitzak.
- Aplikagarritasunaren deklarazioa.
- Erakundea egokitzeko plana.
- Sistemaren ikuskapen-plana.
- Kasu praktikoa ebazteko, gutxi gorabehera 80 eskola ordu beharko dira.

Kasu praktikoa irakasleek ebaluatuko dute. Ikastaroaren amaierako ziurtagiria lortzeko, 8/10eko puntuazioa lortu beharko da.

Gainera, Segurtasun Eskema Nazionalean Aditu Ikastaroa lortzeko, ikasturtean sei azterketa eta azken azterketa gainditu behar dira.

Erantzun anitzeko galderak izanen dira azterketen formatua. Azterketa igortzeko, osatzeko eta garaiz igortzeko mekanismoa ikasturtean zehar erabilitako teleprestakuntza sistemaren ezaugarrietara egokituko da.

KOORDINAZIOA

Hauek zuzentzen eta koordinatzen dute ikastaroa:

Jose Salvador.

Erreserbako Lurreko armada koronela. CISA, Cybersecurity Auditor, 20 urtetik gorako esperientzia informazio-sistemetan.

Jesus Lizarraga

Mondragon Unibertsitateko irakaslea eta Ingeniaritza Fakultateko Telematika eta Zibersegurtasun arloko koordinatzailea.

Irakasle-taldea ENSa ezartzen eta hura betetzen dela ikuskatzen esperientzia handia duten profesionalek osatzen dute.

ERAKUNDEA

Ikastaro hau IVAC Ziurtapen Institutuarekin elkarlanean antolatu da.

JASOKO DEN TITULAZIOA

Unibertsitateko aditu-titulua Segurtasun Eskema Nazionalean, Mondragon Unibertsitatean.

Unibertsitateko aditu titulua lortzeko baldintzak betetzen ez dituztenek, ikastaroa egin izana egiaztatzen duen diploma jasoko dute.

https://www.mondragon.edu/cursos/eu/segurtasun-eskema-nazionala