

Competencia Profesional

Definir e implementar estrategias de seguridad en los sistemas de información realizando diagnósticos de ciberseguridad, identificando vulnerabilidades e implementando las medidas necesarias para mitigarlas aplicando la normativa vigente y estándares del sector, siguiendo los protocolos de calidad, de prevención de riesgos laborales y respeto ambiental.

Salidas Profesionales

- Experta o Experto en ciberseguridad.
- Auditora o Auditor de ciberseguridad.
- Consultora o Consultor de ciberseguridad.
- Hacker ético.

Salidas a la universidad

- Todos los grados.



ETHAZI

Ciclos de alto rendimiento

Titulación

TÉCNICO/A SUPERIOR CON ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS DE LAS TIC

Duración

1 curso escolar (900 horas mínimo).

Acceso directo

Ciclo Formativo de Grado Superior de la Familia Informática y Comunicaciones, Sistemas de Telecomunicaciones e Informáticos, Mantenimiento Electrónico.

Módulos

Contenidos

Fundamentos básicos (60 horas)

Integración de ordenadores y periféricos en redes cableadas e inalámbricas, evaluando su funcionamiento y prestaciones. Adopción de pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo. Administración de las funciones avanzadas de los sistemas operativos atendiendo a su funcionamiento interno, implantando políticas de seguridad centralizadas, identificando los ficheros de configuración del sistema y los procesos que se ejecutan en el mismo.

Incidentes de ciberseguridad (84 h.-9c.)

Creación de programas que utilicen elementos básicos de programación, e implementen estructuras de almacenamiento de la información en memoria externa, es decir, en archivos y bases de datos.

Hacking ético (120 h.-7c.)

Formación para desempeñar las funciones de análisis, detección y respuesta a los incidentes de ciberseguridad de la organización. La función de análisis y detección de incidentes de ciberseguridad incluye aspectos como la monitorización de los sistemas para la recopilación de evidencias que permita dar una respuesta adecuada a los incidentes detectados. Así mismo se obtendrán los conocimientos necesarios para elaborar planes de prevención y concienciación en ciberseguridad.

Normativa de ciberseguridad (48 h.-3c.)

Aplicación de técnicas de ataque y defensa en entornos de prueba de sistemas, redes, aplicaciones web y aplicaciones móviles, para detectar vulnerabilidades, obtener acceso y consolidar el acceso en sistemas de información. Elaboración de análisis de riesgos para identificar activos, amenazas, vulnerabilidades y medidas de seguridad.

Bastionado de redes y sistemas (192 h.-10c.)

Identificación de los puntos principales de aplicación para asegurar el cumplimiento normativo reconociendo funciones, responsabilidades y diseño de sistemas de cumplimiento normativo seleccionando la legislación y jurisprudencia de aplicación. Conocimiento y aplicación de la normativa vigente para el cumplimiento de la responsabilidad penal de las organizaciones y personas jurídicas con los procedimientos establecidos.

Puesta en producción segura (120 h.-7c.)

Diseño de planes de securización y redes de computadores incorporando buenas prácticas para el bastionado de sistemas y redes, configurando sistemas de control de acceso y autenticación de personas, preservando la confidencialidad y privacidad de los datos. Configuración de dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad minimizando las probabilidades de exposición a ataques.

Análisis forense informático (96 h.-7c.)

Monitorización de la actividad que acontece en los distintos sistemas de información a través de la centralización de eventos en herramientas SIEM. Diseño de la integración de la parte IT con la parte OT asegurando los dispositivos OT ante posibles ataques internos o externos a la organización.

Formación práctica en empresa

Aprendizaje de herramientas de seguridad enfocada principalmente a los sistemas de supervisión y control industriales, con el objetivo de poder anticiparse y mitigar los impactos que los ciberataques puedan producir en entornos industriales.

Realización de programas organizados en objetos y clases, aplicando características avanzadas de los fundamentos de la programación orientada a objetos. Determinación del nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados. Detección y corrección de vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web. Detección de problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos. Implantación de sistemas seguros de despliegado de software, DevSecOps, utilizando herramientas para la automatización de la construcción de sus elementos.

Prácticamente todo el alumnado realiza la formación en empresas en modalidad DUAL Intensiva. Posibilidad de realizar prácticas en empresas de otros países gracias a becas Erasmus+.

IKT Inguruneetan Zibersegurtasuneko Especializazio-Ikastaroa

Lanbide Gaitasuna

Sistemen eta aplikazioen segurtasuna bermatzea, kodea modu seguruan diseinatzeko, segurtasun aktiboko eta auzitegi-ikerketako metodologiak eta tresnak erabiliz, ahultasunak eta mehatxuak identifikatzeko eta zibersegurtasuneko plan estrategikoak definituz.

Lan Irteerak

- Zibersegurtasunean aditua.
- Zibersegurtasun-auditorea.
- Zibersegurtasuneko aholkularia.
- Hacker etikoa.

Unibertsitaterako Irteerak

- Gradu guztiak.

SISTEMA 

ETHAZI

Etekin Handiko Zikloak

Titulazioa

IKT INGURUNEETAN ZIBERSEGURTASUNEAN ESPEZIALIZATUTAKO GOI-MAILAKO TEKNIKARIA

Iraupena

Ikasturte bat (900 ordu gutxienez).

Sarbide zuzena

Informatika eta Komunikazioak Familiako edozein Goi Mailako Heziketa Zikloa, Telekomunikazio- eta Informatika-Sistemak, Mantentze-Lan Elektronikoa.

Moduluak Edukiak

Oinarrizko oinarriak (60 ordu)

Ordenagailuak eta periferikoak sare kableatuetan eta haririk gabeko saretan integratzea, eta horien funtzionamendua eta prestazioak ebaluatzea. Informazioa segurtasunez tratatzeko jarraibideak eta praktikak hartzea, sistema informatiko baten ahultasunak ezagutzeko eta hau ziurtatzeko beharra. Sistema eragileen funtzio aurreratuak administratzea hauen barne-funtzionamendua kontuan hartuta, segurtasun-politika zentralizatuak ezarri, eta sistemako konfigurazio-fitxategiak eta exekutatzeko diren prozesuak identifikatu. Programazioko oinarrizko elementuak erabiltzen dituzten programak sortzea, eta informazioa kanpoko memorian biltegitratzeko egiturak inplementatzea, hau da, artxiboetan eta datu-baseetan.

Zibersegurtasun- intzidenteak (84 o.-9k.)

Erakundearen zibersegurtasun-intzidenteak aztertze, detektatzeko eta horiei erantzuteko eginkizunak betetzeko prestakuntza. Zibersegurtasun-intzidenteak aztertze eta detektatzeko eginkizunak hainbat alderdi barne hartzen ditu, hala nola ebidentziak biltzeko sistemen monitorizazioa antzemandako gertakarietara erantzun egokia eman ahal izateko. Era berean, zibersegurtasunaren arloko prebentzio- eta kontzientziazio-planak egiteko beharrezkoak diren ezagutzak lortuko dira.

Hacking etikoa (120 o.-7k.)

Eraso- eta defentsa-teknikak ezartzea sistemen, sareen, web-aplikazioen eta aplikazio mugikorren proba-inguruneetan ahultasunak detektatzeko, sarbidea lortzeko eta informazio-sistemetan sarbidea sendotzeko. Arriskuen analisia egitea aktiboak, mehatxuak, ahultasunak eta segurtasun-neurriak identifikatzeko.

Zibersegurtasun- araudia (48 o.-3k.)

Araugintza betetzea bermatzeko aplikazio-puntu nagusiak identifikatzea funtzioak, erantzukizunak eta araudia betetzeko sistemen diseinua aitortuz eta aplikagarria den legeria eta jurisprudentzia hautatuz. Ezarritako prozedurak dituzten erakundearen eta pertsona juridikoen erantzukizun penala betetzeko indarrean dagoen araudia ezagutzea eta aplikatzea.

Sareen eta sistemen bastionatzea (192 o.-10k.)

Sekurizazio-planak eta ordenagailu-sareak diseinatzea, sistemak eta sareak bastionatzeko praktika egokiak txertatuta, pertsonen sarbidea eta autentifikazioa kontrolatzeko sistemak konfiguratuta, eta datuen konfidentialtasuna eta pribatasuna zainduta. Segurtasun-eskakizunak betetzen dituzten gailu eta sistema informatikoak konfiguratzea erasoekiko esposizio-probabilitateak minimizatuta.

Ekoizpen seguruan jartzea (120 o.-7k.)

Objektuetan eta klaseetan antolatutako programak egitea, objektuei orientatutako programazioaren oinarrien ezaugarri aurreratuak aplikatuta. Aplikazioek eskatzen duten segurtasun-maila zehaztea, eta ohiko eraso-bektoreak eta horiei lotutako arriskuak identifikatzea. Web aplikazioen ahultasunak hautematea eta zuzentzea, hauen iturburu-kodea aztertuta eta web zerbitzariak konfiguratuta. Gailu mugikorretarako aplikazioetan segurtasun-arazoak hautematea, hauen gauzatzea monitorizatuta eta fitxategiak eta datuak aztertuta. Softwarea zabaltzeko sistema seguruak ezartzea, DevSecOps, bere elementuen eraikuntza automatizatzea tresnak erabiliz.

Auzitegi- analisi informatikoa (96 o.-7k.)

Ordenagailu pertsonaletan, gailu mugikorretan, hodeian eta IoT-en auzitegi-analisiaren metodologia finkatuak, eguneratuak eta aitortuak aplikatzea, kontserbazio, eskuratzeko, analisi eta dokumentazio faseak ezaugarrituz.

Prestakuntza praktikoa enpresan

Lan praktikak inguruko enpresetan egin. Ikasle bakoitzak tutore bat izango du ikastetxean eta instruktore bat enpresan. Hauek ikaslearen praktikaren jarraipen zehatza eramango dute.

Ia ikasle guztiek DUAL Intentsiboa modalitatean egiten dute prestakuntza enpresetan, beken bidez. Lan praktikak atzerriko enpresetan egiteko aukera Erasmus+ bekei esker.

Espezializazio-Ikastaroa