

**Oferta vigente del Sistema de Educación Superior del Ecuador:**

Impresión realizada el: 06-05-2021

**Detalle del programa**

IES: UNIVERSIDAD PARTICULAR INTERNACIONAL SEK
Siglas: UISEK
Código sniese: 1036
Tipo de financiamiento: PARTICULAR AUTOFINANCIADA
Sitio web: <https://www.uisek.edu.ec/>
Tipo de IES: UNIVERSIDADES Y ESCUELAS POLITÉCNICAS

Estado del programa: VIGENTE
Tipo de programa: MAESTRÍA ACADÉMICA (MA) CON TRAYECTORIA PROFESIONAL (TP)
Campo amplio: TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC)
Campo específico: TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC)
Campo detallado: SISTEMAS DE INFORMACIÓN
Programa: CIBERSEGURIDAD
Título que otorga: MAGÍSTER EN CIBERSEGURIDAD
Codificación: 1036-7506181C01-S-1701
Lugar de ejecución: SEDE MATRIZ
Provincia: PICHINCHA
Cantón: DISTRITO METROPOLITANO DE QUITO
Ciudad: QUITO
Duración: 2 PERIODOS
Periodo académico: ORDINARIO
Modalidad: SEMIPRESENCIAL
Valor de la matrícula: \$ 0,00
Valor del arancel: \$ 8.409,00
N° de resolución del CES: RPC-SO-04-NO.086-2020
Estado actual: APROBADO POR EL CES
Fecha de aprobación: 2019-06-13
Año de aprobación: 2019
Años de vigencia: 6 años.
Vigente hasta: 2025-06-13
N° de cohortes: 2 POR AÑO
Convenio con otras entidades: NO APLICA
N° de horas: 1.440 Horas.

**Oferta vigente del Sistema de Educación Superior del Ecuador:**

Impresión realizada el: 06-05-2021



Detalle del programa

Requisitos de ingreso:

- TENER TÍTULO DE TERCER NIVEL DEBIDAMENTE REGISTRADO EN LA SENESCYT.
- COPIA DE CÉDULA DE IDENTIDAD O PASAPORTE.
- SUFICIENCIA EN EL IDIOMA INGLÉS EQUIVALENTE AL NIVEL A1 SEGÚN EL MARCO COMÚN EUROPEO.
- APROBAR EL EXAMEN DE ADMISIÓN DEL PROGRAMA.

Objetivo general:

FORMAR TALENTO HUMANO EN COMPETENCIAS PROFESIONALES EN CIBERSEGURIDAD, MEDIANTE UN PROCESO FORMATIVO QUE FAVORECE EL APRENDIZAJE TEÓRICO-PRÁCTICO DE HERRAMIENTAS DE SEGURIDAD DE ENTORNOS TECNOLÓGICOS ASOCIADOS A LA ECONOMÍA DIGITAL, PARA CONTRIBUIR A LA IMPLEMENTACIÓN DE UNA SEGURIDAD ESPECIALIZADA EN EL CIBERESPACIO, TANTO DEL GOBIERNO, DE LAS PERSONAS, COMO DE LAS EMPRESAS EN EL SECTOR PÚBLICO Y PRIVADO.

Perfil de ingreso:

EL PROGRAMA DE MAESTRÍA EN CIBERSEGURIDAD, ESTÁ DIRIGIDO A PROFESIONALES CON TÍTULO DE TERCER NIVEL REGISTRADO EN LA SISTEMA NACIONAL DE LA INFORMACIÓN DEL SISTEMA DE EDUCACIÓN SUPERIOR DEL ECUADOR PREFERENTEMENTE EN CAMPOS DETALLADOS DEL CONOCIMIENTO DE: TÉCNICAS AUDIOVISUALES Y PRODUCCIÓN PARA MEDIOS DE COMUNICACIÓN, CIENCIAS COMPUTACIONALES DISEÑO Y ADMINISTRACIÓN DE REDES Y BASE DE DATOS, DESARROLLO DE ANÁLISIS Y SOFTWARE Y APLICACIONES, SISTEMAS DE INFORMACIÓN, ELECTRÓNICA, AUTOMATIZACIÓN Y SONIDO, MECÁNICA Y METALISTERÍA, DISEÑO Y CONSTRUCCIÓN DE VEHÍCULOS, BARCOS Y AERONAVES MOTORIZADAS, MECATRÓNICA, TELECOMUNICACIONES, NANOTECNOLOGÍA, EDUCACIÓN POLICIAL, MILITAR Y DEFENSA, SEGURIDAD CIUDADANA, GESTIÓN DEL TRANSPORTE, FORMACIÓN PARA DOCENTES CON ASIGNATURAS DE ESPECIALIZACIÓN (LICENCIADO EN PEDAGOGÍA DE LA INFORMACIÓN).

Perfil de egreso:

- PROPONER HERRAMIENTAS DE GESTIÓN DE PROYECTOS TECNOLÓGICOS A PARTIR DE LOS FUNDAMENTOS DE GESTIÓN DE PROYECTOS RECONOCIDOS COMO LAS MEJORES PRÁCTICAS PARA EL GERENCIAMIENTO DE PROYECTOS.
- EVALUAR LA GESTIÓN DE LAS OPERACIONES DE TI DESDE LOS FUNDAMENTOS DE LAS MEJORES PRÁCTICAS DE CIBERSEGURIDAD.
- DEBATIR LA NORMATIVA LEGAL VIGENTE SOBRE DELITOS INFORMÁTICOS, SU IMPLICACIÓN JURÍDICA, LA PROBLEMÁTICA QUE GENERA LA CONTRATACIÓN ELECTRÓNICA, LA FIRMA ELECTRÓNICA Y SU IMPORTANCIA EN EL MUNDO GLOBALIZADO.
- APLICAR LAS PRINCIPALES METODOLOGÍAS Y TÉCNICAS DE SEGURIDAD EN EL DESARROLLO DE SOFTWARE PARA LA CREACIÓN DE APLICACIONES COMPUTACIONALES CONFIABLES Y SEGURAS A LOS CIBERATAQUES.
- APLICAR NORMAS INTERNACIONALES Y NACIONALES EN EL CAMPO DE LA CIBERSEGURIDAD PARA IDENTIFICAR RIESGOS DE SEGURIDAD DESDE FUERA DE LA ORGANIZACIÓN.
- IMPLEMENTAR REGLAS DE SEGURIDAD BASADAS EN NORMAS, PROTOCOLOS Y ALGORITMOS DE ENCRIPCIÓN DE INFORMACIÓN PARA LA PROTECCIÓN DE LOS DATOS DE LA ORGANIZACIÓN.
- APLICAR TÉCNICAS Y PROCEDIMIENTOS DE INVESTIGACIÓN FORENSE PARA LA OBTENCIÓN DE INFORMACIÓN QUE PERMITA RECONSTRUIR HECHOS DELICTIVOS DEL CIBERCRIMEN.
- APLICAR MÉTODOS Y TÉCNICAS DE CIBERSEGURIDAD EN LA PROTECCIÓN DE INFORMACIÓN Y DE LA PLATAFORMA TECNOLÓGICA, EN LO CONCERNIENTE A: EQUIPOS INFORMÁTICOS; REDES DE COMUNICACIONES; BASES DE DATOS; PROGRAMAS Y SERVICIOS TECNOLÓGICOS.
- APLICAR TÉCNICAS DE MITIGACIÓN DE RIESGOS PARA PROCEDER REACTIVA Y PROACTIVAMENTE ANTE LAS VULNERABILIDADES A LAS QUE ESTÁN EXPUESTOS LOS SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN.

- PREDECIR EL COMPORTAMIENTO ESPERADO DEL CIBERCRIMEN SEGÚN EL AVANCE Y DEPENDENCIA DE LA TECNOLOGÍA.
- ORIENTAR A LOS ACTORES DIGITALES (GOBIERNO, EMPRESA PÚBLICA, EMPRESA PRIVADA Y USUARIOS) ANTE LOS FUTUROS RIESGOS DEL CIBERENTORNO Y LA EFECTIVA MITIGACIÓN DE SUS PERJUICIOS.
- APLICAR MÉTODOS DE INVESTIGACIÓN EXPLORATORIO, DIAGNÓSTICO, EN EL DESARROLLO DE PROYECTOS TECNOLÓGICOS QUE RESUELVAN PROBLEMAS DE CIBERSEGURIDAD DE ENTORNOS TECNOLÓGICOS INTERCONECTADOS EN RED.
- IDENTIFICAR ESTRATEGIAS DE REDUCCIÓN DE VULNERABILIDADES PARA MINIMIZAR LOS RIESGOS QUE CONLLEVA LA DIGITALIZACIÓN EMPRESARIAL.
- VALORAR LOS CRITERIOS ÉTICOS Y DEONTOLÓGICOS DE LA PROFESIÓN EN EL DISEÑO DE LAS SOLUCIONES TÉCNICAS DE CIBERSEGURIDAD.
- ARGUMENTAR LA RELACIÓN QUE CARACTERIZA LA FORMACIÓN PROFESIONAL CON LOS PRINCIPIOS Y NORMAS MORALES QUE DEMANDA EL EJERCICIO DE LA PROFESIÓN.

Objeto de estudio:

EL MÁSTER EN CIBERSEGURIDAD ESTUDIA LOS RIESGOS ASOCIADOS A LA VULNERABILIDAD QUE REPRESENTA EL CIBERESPACIO, QUE POR LA CRECIENTE DEPENDENCIA DE LAS TECNOLOGÍAS DIGITALES EMERGERÁN NUEVAS FORMAS Y MEDIOS PARA LA MANIPULACIÓN DELICTIVA DE LOS ENTORNOS TECNOLÓGICOS INTERCONECTADOS EN RED, DESDE UNA VISIÓN FORMATIVA QUE FAVORECE EL APRENDIZAJE TEÓRICO Y PRÁCTICO DE UN CONJUNTO DE HERRAMIENTAS DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE LOS DIFERENTES SECTORES Y ACTORES DE LAS RELACIONES SOCIALES, HUMANAS, LABORALES, FINANCIERAS, DE GOBIERNO, DADAS EN EL CIBERENTORNO, MEDIANTE LA APLICACIÓN DE UN CONJUNTO DE PROTOCOLOS, MÉTODOS, APLICACIONES Y MEJORES PRÁCTICAS DE CIBERSEGURIDAD.

Modalidad titulación:

- PROPUESTAS METODOLÓGICAS Y TECNOLÓGICAS AVANZADAS
- EXAMEN COMPLEXIVO