1.- Información institucional

1.1.- Datos de la institución

Nombre completo:	UNIVERSIDAD TÉCNICA DE AMBATO
Código de la IES:	1010
Categoría de la IES:	B
Tipo de financiamiento:	PÚBLICA
Siglas:	UTA
Misión:	Formar profesionales líderes competentes, con visión humanista y pensamiento crítico a través de la Docencia, la Investigación y la Vinculación, que apliquen, promuevan y difundan el conocimiento respondiendo a las necesidades del país.
Visión:	La Universidad Técnica de Ambato por sus niveles de excelencia se constituirá como un centro de formación superior con liderazgo y proyección nacional e internacional.
Dirección:	Av. Colombia y Chile sector. Campus Ingahurco Av. Los Chasquis y Río Cutuchi - Ciudadela Universitaria. Campus Huachi

1.2.- Datos personales del rector o rectora

Número de documento de identificación:	1702621325		
Nombre completo:	Galo Oswaldo Naranjo López		
Correo electrónico:	utarectorado@uta.edu.ec		
Correo electrónico de referencia:	rectorado_infor@uta.edu.ec		
Teléfono institucional fijo:	032521081	**Ext:**	
Teléfono celular:	0987595618		

1.3.- Datos del director o coordinador del programa

Nombre completo:	Edgar Patricio Córdova Córdova		
Correo electrónico:	edgarpcordovac@uta.edu.ec		
Correo electrónico de referencia:	patto_cordova@hotmail.com		
Teléfono institucional fijo:	032521081	**Ext:**	
Teléfono celular:	0987595618		

2.- Datos generales del proyecto del programa

Nombre completo:	1010-1-7506181C01-21273
Nivel de formación	Maestría Profesional
Tipo de trámite:	Nuevo
Tipo de proceso:	Simplificado
Tipo de programa:	Institucional
Tipo de formación:	Maestría Profesional
Modalidad de estudios/aprendizaje:	En Línea
Descripción de la ejecución de la modalidad:	La organización del aprendizaje de organizará con los siguientes componentes. El aprendizaje en contacto con el docente está mediado por el uso de tecnologías interactivas multimedia y entornos virtuales de aprendizaje que organizan la interrelación de los actores del proceso educativo a través de la plataforma virtual institucional, estos encuentros se lo realizaran de forma planificada y garantizando la participación de los actores durante encuentros dos veces a la semana. El aprendizaje autónomo se han planificado actividades específicas, tales como: la lectura crítica de textos; la investigación documental; la escritura académica y/o científica y demás actividades en correspondencia con el modelo educativo institucional. El aprendizaje práctico-experimental, ya sean actividades individuales o grupales de aplicación de contenidos conceptuales, procedimentales, técnicos, entre otros enfocados a la resolución de problemas prácticos, comprobación, experimentación, contrastación, replicación también requerirán el uso de plataforma virtual.

Anexo 3 de la Guía Metodológica para la presentación de carreras y programas: Parámetros específicos para carreras y programas en modalidades de estudio en línea, a distancia, semipresencial e Híbrida:	1010_27514_anexo3_guia_metodologica.pdf
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
Titulación:	Magíster en Ciberseguridad

Resumen de la descripción mesocurricular

Número de períodos académicos ordinarios:	2
Número de semanas por período académico ordinario:	16
Períodos extraordinarios:	No
Total de horas del programa:	1,440
Total de horas de aprendizaje en contacto con el docente:	480.00
Total de horas del aprendizaje práctico-experimental:	40
Total de horas del aprendizaje autónomo:	920.00
Total de horas de las prácticas profesionales:	0
Total de horas de la unidad de titulación:	240
Número de cohortes:	1
Número de paralelos por cohorte:	1
Número de estudiantes por cohorte:	40
Número total de asignaturas:	10

Resolución del Órgano Colegiado Superior de aprobación del programa (OCS)

Fecha de aprobación:	06/07/2021
Número de resolución:	0612-CU-P-2021
Anexo de la resolución:	1010_27514_resolucion.pdf

Lugar(es) de ejecución del programa

Estructura institucional	Ciudad de la sede	Resolución CES/CACES para funcionamiento	Nombre del Director, Responsable o Encargado	Correo electrónico institucional	Correo electrónico de referencia	Número telefónico institucional
Sede matriz	Sede matriz , Sierra, Zona 3, Tungurahua, Ambato	1010_27514_resolucion_ceaaces_11648.pdf	Galo Oswaldo Narajo López	gnaranjo@uta.edu.ec	rectorado_infor@uta.edu.ec	032521081

Convenios

Tipo	Institución	Fecha de inicio	Fecha de culminación	Objeto	Anexo
Específico					

3.- Descripción general del programa

3.1.- Objetivos del programa

3.1.1.- Objetivo general

Formar profesionales con altas capacidades y habilidades para solucionar problemas de seguridad informática y a su vez como agentes de cambio en la transferencia de tecnología en las áreas de ciberseguridad, a través de la formación práctica basada en el uso de las técnicas y herramientas del sector de la ciberseguridad.

3.1.2.- Objetivos específicos

• Analizar controles, herramientas y procedimientos que garanticen una correcta seguridad de la información.
• Gestionar la información organizacional con técnicas de detección y prevención de riesgos y amenazas informáticas.
• Definir mecanismos criptográficos que agiliten a las técnicas de criptoanálisis.

• Diseñar políticas dirigidas a prevenir ciberdelitos y contrarrestar sus consecuencias.
• Formar profesionales altamente capacitados en ciberseguridad que cubran la demanda laboral.

3.2.- Requisitos y perfil de ingreso

3.2.1.- Perfil de ingreso

Los aspirantes al programa de Maestría en Ciberseguridad deberán poseer título de tercer nivel de grado, preferentemente dentro del campo amplio de Tecnologías de la información y la comunicación(TIC). Pueden optar profesionales de campos distintos, siempre que respalden experiencia profesional de al menos un año en el campo inherente al programa de posgrado.

3.2.1.- Requisitos de ingreso

Descripción
- Poseer un título de tercer nivel de grado debidamente registrado por el órgano rector de la política pública de Educación Superior
- En caso de que el título de grado sea obtenido en el exterior, el estudiante para inscribirse en el programa deberá presentarlo a la IES debidamente apostillado o legalizado por vía consular.
- Cumplir con el proceso de admisión establecido por la UTA

3.3.- Perfil de egreso

¿Qué resultados de aprendizaje y competencias profesionales son necesarias para el futuro desempeño profesional?

Integra las herramientas y técnicas de ciberseguridad actuales para dar solución a problemas reales en cuanto a seguridad informática, obteniendo como resultado la integridad y confidencialidad de la información en sus diferentes niveles. Genera proyectos de seguridad, en los cuales se valora la capacidad de mitigar riesgos informáticos ocasionados por fallas o deficiencias en la seguridad informática; mediante el dominio de técnicas, métodos y herramientas tecnológicas de ciberseguridad. Estructura informes de seguridad informática, basado en evidencias recopiladas, descubiertas y documentadas producto del cibercrimen.

¿Qué resultados de aprendizaje relacionados con el manejo de métodos, metodologías, modelos, protocolos, procesos y procedimientos de carácter profesional e investigativo se garantizarán en la implementación de la carrera/programa?

Analiza los aspectos fundamentales de la ciberseguridad y los aplica en proyectos informáticos para fomentar la seguridad de la información personal y empresarial. Utiliza procesos regidos en la ciberseguridad para identificar casos de riesgo y amenaza informática, con el objetivo de analizar los mismos y buscar soluciones viables enfocadas en disminuir el impacto o consecuencias. Elabora métodos de criptografía analítica con el objetivo de encriptar y descifrar información sensible y susceptible a cibercrímenes.

¿Cómo contribuirá el futuro profesional al mejoramiento de la calidad de vida, el medio ambiente, el desarrollo productivo y la preservación, difusión y enriquecimiento de las culturas y saberes?

Analiza y maneja las herramientas y métodos de ciberseguridad en el ámbito empresarial mediante pensamiento analítico sobre la criptografía informática. Aplica metodologías para la identificación de pruebas y escenarios en ciberdelitos. Fundamenta y elabora planes de acción para mejorar la ciberseguridad en la sociedad.

¿Cuáles son los valores y los principios, en el marco de un enfoque de derechos, igualdad e interculturalidad y pensamiento universal, crítico y creativo, que se promoverán en la formación profesional que ofrece el programa?

Une y recaba esfuerzos, conocimientos y experiencias técnicas para mitigar y hacer frente al cibercrimen. Elabora, coordina o participa en proyectos de ciberseguridad y criptoanálisis. Fomenta el uso de la criptografía informática en las organizaciones para proteger la información sensible.

3.4.- Requisitos de titulación

3.4.1.- Requisitos de titulación

Descripción
Requisitos Académicos: a) Aprobar la totalidad de las asignaturas del programa; b) Aprobar el trabajo escrito y la defensa de una las modalidades de titulación o graduación que el programa contemple.
Requisitos Administrativos: El estudiante previo a la defensa del trabajo de titulación deberá presentar a la Secretaría de Posgrado de su respectiva Unidad Académica, los siguientes documentos: a) Documentos personales, copia de la cédula de ciudadanía y papeleta de votación (actualizados), copia del o los títulos de tercer nivel con la impresión de registro obtenida de la página web de la SENESCYT; b) Certificado de no adeudar a ninguna dependencia de la Universidad Técnica de Ambato; c) Conforme a la modalidad de titulación entregar los documentos físicos en conjunto con las páginas preliminares debidamente firmadas para el archivo de la facultad.

Opciones de aprobación de la unidad de titulación

3.4.2.- Trabajos de titulación

Artículos profesionales de alto nivel

Proyecto de titulación con componentes de investigación aplicada y/o de desarrollo

3.3.- Breve descripción de las opciones de la unidad de integración curricular (¿qué?, ¿cómo? y duración)

1) Proyecto de titulación con componentes de investigación aplicada y/o de desarrollo: buscan lograr soluciones creativas y prácticas a problemas de la realidad, atienden necesidades puntuales o permiten aprovechar oportunidades para crear o mejorar productos, procesos o servicios. 2)Artículos profesionales de alto nivel: tiene la finalidad de comunicar los resultados de las investigaciones, ideas y debates de una manera clara, precisa y objetiva, acorde a la epistemología del campo del conocimiento al que pertenece el programa. Está sujeto a la crítica de revisores que fungen como pares académicos, previo a su aceptación para publicarse en una revista científica periódica. El artículo científico, debe corresponderse con las líneas de investigación del programa, y el proyecto de investigación en el que se enmarca el tema del anteproyecto que de preferencia respondan a las líneas de investigación institucional aprobadas. Para que el artículo científico sea tomado en cuenta, debe estar enviado y aceptado (certificado de aceptación para publicación por el editor o director de la revista) o

publicada en una revista científica periódica, arbitrada, indizada al menos en base de datos Scopus u otras de mayor reconocimiento o cobertura. En cualquiera de las formas seleccionada la Unidad de Titulación tendrá una duración de 240 horas.

4.- Pertinencia

4.- Pertinencia

Síntesis de la pertinencia:

La Maestría en Ciberseguridad fundamenta su pertinencia en la Ley Orgánica de Educación Superior, que dice: "Art. 107.- Principio de pertinencia.- El principio de pertinencia consisten en que la educación superior responda a las expectativas y necesidades de la sociedad, a la planificación nacional, y al régimen de desarrollo, a la prospectiva de desarrollo científico, humanístico y tecnológico mundial, y a la diversidad cultural. Para ello, las IES articularán su oferta a la demanda académica, a las necesidades de desarrollo local, regional y nacional, a la innovación y diversificación de profesiones y grados académicos, a las tendencias del mercado ocupacional local, regional y nacional, alas tendencias demográficas locales, provinciales y regionales; a la vinculación con la estructura productiva actual y potencial de la provincia y la región, y a las políticas nacionales de ciencia y tecnología.". Considerando los aspectos que se detallan en el artículo, relacionado con las formas como la Educación Superior debe responder a las expectativas y necesidades de la sociedad, concretamente a la demanda académica y en forma específica de profesionales en Ciberseguridad; esta Maestría a través de su currículo aportará a la formación de profesionales especializados, con conciencia ética y solidaria, capaces de producir soluciones a los problemas de seguridad de la información mediante el fortalecimiento de técnicas informáticas. La alta dependencia de las personas a la tecnología viene asociada a una mayor vulnerabilidad, la cual es necesario ser mitigada con la ayuda de la CIBERSEGURIDAD. En este contexto surge la necesidad de formar expertos en esta rama con las competencias profesionales necesarias para: indagar, determinar y definir riesgos y vulnerabilidades a los que informáticamente se encuentra expuesta la sociedad; además de la aplicación de buenas prácticas y métodos de ciberseguridad en la implementación de modelos de gestión efectiva de información, buscando contribuir a la concientización de la ciudadanía y de las organizaciones en la prevención de riesgos asociados a la tecnología y la información digital.

Anexo de la pertinencia: 1010_27514_analisis_pertinencia.pdf

Anexo del estudio de demanda y empleabilidad: 1010_27514_estudio_demanda.pdf

5.- Planificación curricular

5.1.- Objetivos de estudio

Objeto de estudio del proyecto:

La formación del maestrante en Ciberseguridad, tiene como objetivo de estudio investigar cómo reducir los factores de riesgo del ciberespacio al que se expone la sociedad y las organizaciones de todo nivel, mediante la investigación, recolección y análisis de los aspectos teórico, prácticos y metodológicos que involucran a la Ciberseguridad. En la actualidad los problemas y casos de ciberdelincuencia aumentan constantemente y pese a que la información o conocimientos por medio del internet es cada vez más pública y accesible, se sigue careciendo de profesionales que ayuden hacer frente a los problemas del Ciberespacio. siendo este una problemática que se busca dar solución mediante los procesos de investigación de la Universidad Técnica de Ambato

5.2.- Metodologías y ambientes de aprendizaje

Metodologías y ambientes de aprendizaje:

La impartición de las clases se lo realizará en línea, por medio de una plataforma virtual amigable y de calidad que responde principalmente a la formación del maestrante de Ciberseguridad y su desarrollo como un ente dinámico e interactivo que fomenta los procesos de aprendizaje autónomo y colaborativo; esta modalidad está pensado en el maestrante como ser que cubre y responde a las necesidades de una nueva sociedad, que evoluciona vertiginosamente y a la que se debe adaptar ágilmente para sumir los retos de cambio que propone la nueva era digital; en la que , la transformación digital ha dado nacimiento a lo que hoy se conoce como Ciberespacio. La Universidad Técnica de Ambato cuenta en su estructura interna con una plataforma educativa oficial como herramienta de apoyo para el aprendizaje. Cada asignatura contara con un aula virtual en la cual, bajo la organización del docente, los estudiantes compartan dinámica e interactivamente contenidos multimedia para complementar la formación; construyendo el conocimiento por medio del colectivismo. En estos espacios se promueve la participación en entornos virtuales para foros, chats, wikis, software adicional, que son evaluados durante todo el proceso. Finalidad y Objetivos y Naturaleza de la Dirección de Educación a Distancia y Virtual Artículo 2. Finalidad. La Dirección de Educación a Distancia y Virtual tiene como finalidad formar, capacitar y especializar a docentes, estudiantes, personal administrativo, trabajadores y público en general con acceso a estudios orientados a la realización personal, ciudadana, para toda la vida, con significación social en los niveles de grado, postgrado y educación continua, en las diversas modalidades: presencial, a distancia, virtual y B-learning, con la utilización de ayudas dialécticas, recursos tecnológicos y metodológicos que faciliten los procesos académicos, de investigación y vinculación con la colectividad, bajo los principios de calidad, equidad, pertinencia y sostenibilidad y mediante el establecimiento de un sistema de educación continua.

5.3.- Descripción microcurricular del programa

Justificación de la estructura curricular:

En el proyecto se contempla los componentes de aprendizaje divididos en: aprendizaje en contacto con el docente 520 horas y aprendizaje autónomo 920 horas.
Las unidades de organización Curricular en la maestría en Ciberseguridad incluyen asignaturas como:

Unidad de Investigación [480 horas]:
• Aspectos legales de la seguridad informática y los delitos informáticos
• Seguridad en redes empresariales y sistemas operativos
• Análisis forense digital
Unidad de Formación Disciplinar Avanzada [720 horas]:
• Gestión de la seguridad informática
• Criptografía y mecanismos de seguridad
• Análisis de vulnerabilidades
• Auditoría de la seguridad informática
• Seguridad en el software
Unidad de Titulación [240 horas]
• Metodología y diseño de la Investigación
• Desarrollo del trabajo de titulación

Anexo justificación de la estructura curricular: 1010_27514_justificacion_estructura_curricular.pdf

Anexo malla curricular: 1010_27514_malla_curricular.pdf

Anexo plan de rotación:

Descripción microcurricular

Nombre de la asignatura	Periodo académico ordinario	Unidad de organización curricular	Resultados de Aprendizaje	Contenidos mínimos	Aprendizaje en contacto con el docente	Aprendizaje autónomo	Aprendizaje práctico/experimental	Prácticas profesionales	Total
Análisis forense digital	1	Unidad de investigación	Diseñar estrategias para la detección de evidencias en ataques cibernéticos y adoptar medidas precisas para mantener la cadena de custodia de dichas evidencias	• Introducción al Análisis forense digital • Metodologías y normas internacionales de AFD • Etapas del afd • Obtención de las evidencias • Evaluación de pruebas para el análisis de evidencias • Análisis de las evidencias • Resultados	50	100	0	0	150

Nombre de la asignatura	Periodo académico ordinario	Unidad de organización curricular	Resultados de Aprendizaje	Contenidos mínimos	Aprendizaje en contacto con el docente	Aprendizaje autónomo	Aprendizaje práctico/experimental	Prácticas profesionales	Total
Aspectos legales de la seguridad informática y los delitos informáticos	1	Unidad de investigación	Identificar los principales aspectos legales de la seguridad y los delitos informáticos, sus consecuencias y delimitaciones.	• Protección de datos y privacidad de la información personal • Derechos de propiedad intelectual • COIP • Situación actual • Protección del canal de información y telecomunicación • Protección de comercio electrónico, firmas digitales y mensajes de datos. • Introducción a la delincuencia informática • Sujetos del delito informático • Bienes jurídicos protegidos del delito informático • Tipos de delitos informáticos • Situación internacional • Convenios de cibercriminalidad • Delito informático y su realidad procesal • Problemas de persecución. • Cibercrimen y delitos informáticos	60	120	0	0	180
Gestión de la seguridad informática	1	Unidad de formación disciplinar avanzada	Aplicar medidas de seguridad en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.	• Proceso de planificación del GSI • Estructuración de políticas de GSI • Medidas y procesos para la GSI • Indicadores de gestión del proceso de gestión de seguridad informática • Normas internacionales de SGSI	40	80	0	0	120

Nombre de la asignatura	Periodo académico ordinario	Unidad de organización curricular	Resultados de Aprendizaje	Contenidos mínimos	Aprendizaje en contacto con el docente	Aprendizaje autónomo	Aprendizaje práctico/experimental	Prácticas profesionales	Total
Metodología y diseño de la investigación	1	Unidad de titulación	Conocer niveles, métodos, teorías y técnicas de la investigación que facilitan la interpretación del contexto en Ciberseguridad.	• Fundamentos introductorios a la investigación • Enfoques cualitativos y cuantitativos • Planteamiento y desarrollo del problema • Definición y delimitación del tema de investigación • Perspectiva teórica del proyecto de investigación • Construcción del objeto de estudio • Propósitos, objetivos y metas de la investigación. • Tipos e identificación de variables.	60	60	0	0	120
Seguridad en redes empresariales y sistemas operativos	1	Unidad de investigación	Reconocer y evaluar las técnicas para proteger redes empresariales y sistemas operativos frente a ataques y software malintencionado.	• Importancia de la seguridad en redes empresariales • Soluciones de seguridad en redes empresariales • Sistemas confiables • Hardering • Políticas de seguridad de los sistemas operativos • Seguridad en sistemas Windows • Seguridad en sistemas Linux	40	100	10	0	150
Análisis de vulnerabilidades	2	Unidad de formación disciplinar avanzada	Analizar las herramientas y métodos utilizados por los delincuentes informáticos para recopilar información sobre el objeto al cual se va a realizar un ataque informático.	• Introducción a la vulnerabilidad informática • Análisis de vulnerabilidades • Metodologías de análisis de vulnerabilidades. • Fases del análisis de vulnerabilidades	30	80	10	0	120
Auditoria de la seguridad informática	2	Unidad de formación disciplinar avanzada	Comprender tipos y técnicas para realizar auditorías en sistemas de información	• Conceptos generales de auditoría informática • Auditoría de políticas de seguridad • Auditoría de la gestión de activos informáticos • Auditoría de la seguridad relacionada con el personal. • Auditoría del acceso	50	100	0	0	150

Nombre de la asignatura	Periodo académico ordinario	Unidad de organización curricular	Resultados de Aprendizaje	Contenidos mínimos	Aprendizaje en contacto con el docente	Aprendizaje autónomo	Aprendizaje práctico/experimental	Prácticas profesionales	Total
Criptografía y mecanismos de seguridad	2	Unidad de formación disciplinar avanzada	Comprender las técnicas básicas sobre los procedimientos de difusión de la información mediante cifrado utilizando algoritmos de secreto compartido y cifrado público.	• Introducción a la criptografía informática • Usos de la criptografía • Clasificación de la criptografía • Protocolos criptográficos • Aplicación de criptografía en redes seguras	50	120	10	0	180
Desarrollo del trabajo de titulación	2	Unidad de titulación	Elaborar el proyecto de investigación, con base en fundamentos de investigación relacionados a la Ciberseguridad	• Introducción justificación y objetivos del trabajo de titulación • Marco teórico • Metodología • Resultados y análisis de resultados	60	60	0	0	120
Seguridad en el software	2	Unidad de formación disciplinar avanzada	Establecer mecanismos de seguridad activa, describir características y relacionarlas con las necesidades del uso del software.	• Características del software y la seguridad • Amenazas al software • Mecanismos de seguridad • Criterios de evaluación del software y la seguridad • Metodologías de criterios de evaluación del software y seguridad • Análisis de código seguro • Buenas prácticas en la codificación	40	100	10	0	150
					480	920	40	0	1440

Tabla resumen

Total de asignaturas:	10
Total de horas de aprendizaje en contacto con el docente:	480
Total de horas de aprendizaje autónomo	920
Total de horas de aprendizaje práctico/experimental:	40
Unidad de titulación:	240
Total de horas de prácticas profesionales	0
Duración del programa:	1,440

5.4.- Investigación

Investigación:

El modo de organización de la investigación del programa de posgrado: Maestría en Ciberseguridad, está en concordancia con los componentes de investigación en la profesionalización del encargado de resguardar los recursos informáticos y la información digital. La formación investigativa del maestrante en ciberseguridad responde a la dialéctica: teoría – práctica, objetividad – subjetividad, gestión – innovación. (Manzini, 2014). Las líneas de investigación de la Maestría en Ciberseguridad se basen en los dominios y líneas de investigación de la Universidad Técnica de Ambato, específicamente al dominio de Optimización de los sistemas productivos, técnicos - tecnológicos y

desarrollo urbanístico y sus líneas Tecnología de la información y sistemas de control. En cuanto a las políticas de investigación, el programa de Maestría en Ciberseguridad busca potenciar el talento humano con una filosofía de mejora continua en los procesos para el desarrollo de investigación tecnológica y seguridad de la información, con el firme propósito de mejorar los servicios a la comunidad.

Modelo de investigación (de acuerdo al nivel de formación): 1010_27514_plan_investigacion.pdf

5.5.- Componentes de vinculación con la sociedad

Describir el componente de vinculación con la sociedad: El proyecto de Ciberseguridad se basa en la asimilación de contenidos de los módulos de Seguridad de redes empresariales y sistemas operativos y el de Gestión de la seguridad informática para enfocarlos a desarrollar proyectos de prevención y vinculación con la sociedad; cuyo objetivo general es analizar y generar planes para resguardar la información personal y empresarial. Durante el transcurso del programa de maestría los estudiantes generaran planes y proyectos englobados en el concepto de vinculación que se define como el aporte de la Universidad para resolver problemas que afectan a la sociedad. El Reglamento del Régimen Académico del CES, manifiesta en su artículo 50 que - La vinculación con la sociedad hace referencia a la planificación, ejecución y difusión de actividades que garantizan la participación efectiva en la sociedad y la responsabilidad social de las instituciones del Sistema de Educación Superior con el fin de contribuir a la satisfacción de necesidades y la solución de problemáticas del entorno, desde el ámbito académico e investigativo.", articulándose al resto de funciones sustantivas, oferta académica, dominios académicos, investigación, formación y extensión de las IES en cumplimiento del principio de pertinencia. De igual forma la Universidad Técnica de Ambato, en su Modelo Educativo, señala sobre la Vinculación: Educación-Sociedad-trabajo: "Las instituciones formadoras de profesionales deben actuar conjuntamente con la colectividad a la que sirven y en particular con el ámbito correspondiente de trabajo para que los egresados puedan desempeñar de acuerdo con un proyecto ético de vida personal y de nación, a través del ejercicio idóneo de la profesión con visión local y planetaria. "El Programa de Maestría de Ciberseguridad que propone la Facultad de Ingeniería en Sistemas Electrónica e Industrial, a tono con la necesidad del vínculo de los programas de posgrado y en particular los de profesionalización; propone un enfoque integral en la formación del maestrante expresado en la organización y dirección de sistema de influencias educativas a partir de las exigencias que demanda la práctica profesional, lo que implica la necesidad de formar maestrantes en vínculo directo con sus contextos de actuación. La aplicación de este enfoque permite trabajar simultáneamente y de forma gradual en sus intereses, conocimientos, habilidades y valores, así como en la formación de la autovaloración del maestrante en su aplicación de dichos conocimientos y habilidades a la solución de los problemas de la práctica social. Generando proyectos de seguridad, en los cuales se valora la capacidad de mitigar riesgos informáticos ocasionados por fallas o deficiencias en la seguridad informática; mediante el dominio de técnicas, métodos y herramientas tecnológicas de ciberseguridad. Se planifica de mejor manera la vinculación en el documento adjunto en Documentos Complementarios.

5.6.- Modelo de prácticas profesionales del programa

Modelo de prácticas profesionales del programa: No aplica

6.- Infraestructura y equipamiento

Describa la plataforma tecnológica integral de infraestructura e infoestructura: Según el Reglamento de Educación a Distancia y Virtual de la UTA, la Finalidad y Objetivos y Naturaleza de la Dirección de Educación a Distancia y Virtual Artículo 2. Finalidad. La Dirección de Educación a Distancia y Virtual tiene como finalidad formar, capacitar y especializar a docentes, estudiantes, personal administrativo, trabajadores y público en general con acceso a estudios orientados a la realización personal, ciudadana, para toda la vida, con significación social en los niveles de grado, postgrado y educación continua, en las diversas modalidades: presencial, a distancia, virtual y B-LEARNING, con la utilización de ayudas dialécticas, recursos tecnológicos y metodológicos que faciliten los procesos académicos, de investigación y vinculación con la colectividad, bajo los principios de calidad, equidad, pertinencia y sostenibilidad y mediante el establecimiento de un sistema de educación continua. Se hará uso de la plataforma virtual MOODLE. En cuanto a la infraestructura de la plataforma se puede indicar que se la utiliza como un recurso adicional por parte de cada docente, en donde se muestra herramientas tecnológicas, contenidos y uso de estrategias que juegan un papel primordial en el aprendizaje significativo de los contenidos a desarrollar en modalidad B-LEARNING, es decir, que los estudiantes podrán subir tareas y revisar materiales para su aprendizaje autónomo. Normalmente se encuentra un tema por semana de clases, lo que incluye una sección de exposición de contenidos, una sección de retroalimentación y una sección de construcción y una de evaluación que se alinea a la metodología conocida como PACIE.

Laboratorios y/o talleres

Estructura institucional	Nombre del laboratorio	Equipamiento	Metros cuadrados	Puestos de trabajo
Sede matriz , Sierra, Zona 3, Tungurahua, Ambato	Laboratorio 1	20 Computadoras Procesador Core i7 11 generación. 16GB de RAM	52.5	40

Estructura institucional	Nombre del laboratorio	Equipamiento	Metros cuadrados	Puestos de trabajo
Sede matriz , Sierra, Zona 3, Tungurahua, Ambato	Laboratorio 2	20 Computadoras Procesador Core i7 9 generación. 17GB de RAM	53.46	40

Anexo de laboratorios y/o talleres: 1010_27514_laboratorios_talleres.pdf

Bibliotecas específicaspor estructura institucional

Sede	Número de titulos	Titulos	Número de volúmene	Volúmenes	Número de base de datos	Base de datos	Número de suscripciones	Suscripciones a revistas

Sede	Número de titulos	Titulos	Número de volúmene	Volúmenes	Número de base de datos	Base de datos	Número de suscripciones	Suscripciones a revistas
Sede matriz , Sierra, Zona 3, Tungurahua, Ambato	76	Los libros contienen información sobre temas relacionados a Ciberseguridad, y se encuentran en la Biblioteca de la Facultad de Ingeniería en Sistemas Electrónica e Industrial en la Sede Matriz. Para mayor detalle Ver anexo de libros por estructura institucional.	89	Los libros contienen información sobre temas relacionados a Ciberseguridad, y se encuentran en la Biblioteca de la Facultad de Ingeniería en Sistemas Electrónica e Industrial en la Sede Matriz. Para mayor detalle Ver anexo de libros por estructura institucional.	4	Las Bases de datos con múltiples colecciones catalogadas, actualizadas y ordenadas son: 1. IEEE: Es una base de datos especializada en las áreas de ingeniería eléctrica,computación y electrónica. Permite acceder al texto completo de las publicacionescientíficas y técnicas elaboradas por el Institute of Electrical and Electronics Engineers (IEEE) y sus socios editoriales. 2. e-libro.Net: Contiene más de 110.000 libros . En las áreas de: Ciencias sociales, Arquitectura, Ciencias Económicas Administrativas, Ciencias de la Salud, Psicología, Ciencias Exactas y Naturales, Ciencias Biológicas, Veterinarias, Ingeniería y Tecnología, Informática, Comunicación y Telecomunicaciones, Ciencias de la Información. 3. ProQuest Ebook Central: Contiene 198.200 libros títulos de libros, en las áreas de salud, medicina, negocios, ciencias sociales, artes y humanidades, noticias, ciencia y tecnología. 4. Springer: Permite acceder a 6752 ebooks con temáticas en computación, biomedicina, ingeniería civil, electrónica, ingeniería industrial, ingeniería mecánica, física aplicada, energía y 1561 journals en las áreas de tecnología,	201	En el anexo se incluye el detalle de los journals a los que tiene acceso la IES

Sede	Número de titulos	Titulos	Número de volúmene	Volúmenes	Número de base de datos	Base de datos	Número de suscripciones	Suscripciones a revistas
						medicina, matemáticas, computación, ciencias sociales y estadística. En el anexo se incluye el detalle de los journals relacionados al programa a los que tiene acceso la IES.		

Inventario de bibliotecas por estructura institucional: 1010_27514_fondo_bibliografico.pdf

Aulas por estructura institucional

Estructura Institucional	Número de aulas	Puestos de trabajo
Sede matriz , Sierra, Zona 3, Tungurahua, Ambato	20	30

Infraestructura y equipamiento obligatorio para las modalidades "A distancia, en línea y semipresencial o convergencia de medios": El laboratorio es el lugar donde se prestan servicios de cómputo a los miembros de la comunidad universitaria. En el contexto educativo, los laboratorios se ubican en la estructura institucional: Sede Matriz, y tiene como objetivo proporcionar a los estudiantes de pregrado y posgrado el servicio de uso de equipos de cómputo, para la enseñanza o el aprendizaje.
En el proyecto se contempla el uso de los laboratorios que la Facultad de Ingeniería en Sistemas, Electrónica e Industrial y la Universidad Técnica de Ambato, tienen disponible para los estudiantes de la Maestría en Ciberseguridad.

7.- Información financiera

Costos

Valor de la matrícula: 450.00

Valor del arancel: 4,550.00

Información financiera

Presupuesto total que garantice la culminación de la primera cohorte					
Desglose	**Provisión de educación superior**	**Fomento y desarrollo científico y tecnológico**	**Vinculación con la sociedad**	**Otros**	**Total**
Gastos corrientes					
Gastos en personal administrativo	35,028.94	0	0	0	35,028.94
Gastos en personal académico	69,072	0	0	0	69,072
Bienes y servicios de consumo	50,000	0	0	0	50,000
Becas y ayudas financieras	4,550	0	0	0	4,550
Otros	0	0	0	0	0
				Subtotal	158,650.94
Inversión					
Infraestructura	0	0	0	0	0
Equipamiento	41,349.06	0	0	0	41,349.06
Bibliotecas	0	0	0	0	0
				Subtotal	41,349.06
Total	200,000	0	0	0	200,000

Anexo de información financiera/justificación 1010_informacion_financiera.pdf

Anexo estudio técnico para la fijación de aranceles: 1010_estudio_tecnico.pdf

8.- Personal

8.1.- Director/a o Coordinador/a

Estructura institucional	Perfil profesional	Cargo / función	Horas de dedicación a la semana a la IES	Tipo de relación laboral o vinculación a la IES
Matriz Ambato	Poseer título de cuarto nivel en sistemas informáticos o en el campo específico de tecnologías de la información y comunicación. Justificar un mínimo de 120 horas de capacitación en formación específica en educación en línea y a distancia.	Director Académico Administrativo	40	Contrato sin relación de dependencia

8.2.- Personal académico de la carrera

Perfil docente	Período académico	Asignatura	Estructura institucional	Horas de dedicación a la IES	Horas de dedicación semanal al programa	Tiempo de dedicación al programa	Tipo de personal académico/Categoría del docente	Observaciones
Poseer título de cuarto nivel de Magister en sistemas informáticos o en el campo específico de tecnologías de la información y comunicación afín a la asignatura. Justificar mínimo 120 horas de capacitación en formación específica en educación en línea y a distancia. Experiencia profesional comprobable en derecho informático de preferencia que trabaje en el campo legal.	1	Aspectos legales de la seguridad informática y los delitos informáticos	Matriz Ambato	15	15	Tiempo parcial	No Titular Invitado	
Poseer título de cuarto nivel de Magister en sistemas informáticos o en el campo específico de tecnologías de la información y comunicación afín a la asignatura. Justificar mínimo 120 horas de capacitación en formación específica en educación en línea y a distancia. Auditor Líder ISO27001, CISM y/o CRISC	1	Gestión de la seguridad informática	Matriz Ambato	15	15	Tiempo parcial	No Titular Invitado	
Poseer título de cuarto nivel de Magister en sistemas informáticos o en el campo específico de tecnologías de la información y comunicación afín a la asignatura. Justificar mínimo 120 horas de capacitación en formación específica en educación en línea y a distancia. Certificaciones: Linux LPT, COMPTIA, CCNP Security Certification.	1	Seguridad en redes empresariales y sistemas operativos	Matriz Ambato	15	15	Tiempo parcial	No Titular Invitado	

Poseer título de cuarto nivel de Magister en sistemas informáticos o en el campo específico de tecnologías de la información y comunicación afín a la asignatura. Justificar mínimo 120 horas de capacitación en formación específica en educación en línea y a distancia. De preferencia poseer certificaciones: ECSA, CHFI, Autopsy Certification	1	Análisis forense digital	Matriz Ambato	15	15	Tiempo parcial	No Titular Invitado	
Poseer título de cuarto nivel de Doctor equivalente a cuarto nivel (PHD) en el campo amplio de tecnologías de la información y comunicación, ingeniería o educación. Justificar mínimo 120 horas de capacitación en formación específica en educación en línea y a distancia.	1	Metodología y diseño de la investigación	Matriz Ambato	15	15	Tiempo parcial	No Titular Invitado	
Poseer título de cuarto nivel de Magister en sistemas informáticos o en el campo específico de tecnologías de la información y comunicación afín a la asignatura. Justificar mínimo 120 horas de capacitación en formación específica en educación en línea y a distancia. De preferencia poseer certificaciones CEH, Security+	2	Criptografía y mecanismos de seguridad	Matriz Ambato	15	15	Tiempo parcial	No Titular Invitado	
Poseer título de cuarto nivel de Magister en sistemas informáticos o en el campo específico de tecnologías de la información y comunicación afín a la asignatura. Justificar mínimo 120 horas de capacitación en formación específica en educación en línea y a distancia. De preferencia poseer certificaciones CEH, OSCP, eWPT, OSWE	2	Análisis de vulnerabilidades	Matriz Ambato	15	15	Tiempo parcial	No Titular Invitado	
Poseer título de cuarto nivel de Magister en sistemas informáticos o en el campo específico de tecnologías de la información y comunicación afín a la asignatura. Justificar mínimo 120 horas de capacitación en formación específica en educación en línea y a distancia. De preferencia certificaciones Auditor Lider ISO27001, CISM, CISA	2	Auditoria de la seguridad informática	Matriz Ambato	15	15	Tiempo parcial	No Titular Invitado	

Poseer título de cuarto nivel de Magister en sistemas informáticos o en el campo específico de tecnologías de la información y comunicación afín a la asignatura. Justificar mínimo 120 horas de capacitación en formación específica en educación en línea y a distancia. De preferencia certificaciones CSSLP, CCSP	2	Seguridad en el software	Matriz Ambato	15	15	Tiempo parcial	No Titular Invitado	
Poseer título de cuarto nivel de Doctor equivalente a cuarto nivel (PHD) en el campo amplio de tecnologías de la información y comunicación, ingeniería o educación. Justificar mínimo 120 horas de capacitación en formación específica en educación en línea y a distancia.	2	Desarrollo del trabajo de titulación	Matriz Ambato	15	15	Tiempo parcial	No Titular Invitado	

Anexo de la justificación de los perfiles propuestos

Anexo de la justificación de los perfiles propuestos

9.- Peritaje/Informe académico

Anexo de peritaje académico: 1010_27514_peritaje_informe_27514.pdf

Documentos complementarios

Documentos complementarios: 1010_27514_graficos_tablas.pdf

FIRMA DIGITALIZADA

Dr. M.Sc. Galo Naranjo López
RECTOR
UNIVERSIDAD TÉCNICA DE AMBATO

Galo Oswaldo Naranjo López