CONSEJO NACIONAL DE RECTORES

Oficina de Planificación de la Educación Superior

División Académica

DICTAMEN SOBRE LA SOLICITUD DE CREACIÓN DE LA MAESTRÍA EN CIBERSEGURIDAD DEL INSTITUTO TECNOLÓGICO DE COSTA RICA

M.Sc. Alexander Cox Alvarado

OPES; no. 55-2021

CONSEJO NACIONAL DE RECTORES

Oficina de Planificación de la Educación Superior
División Académica

DICTAMEN SOBRE LA SOLICITUD DE CREACIÓN DE LA MAESTRÍA EN CIBERSEGURIDAD DEL INSTITUTO TECNOLÓGICO DE COSTA RICA

M.Sc. Alexander Cox Alvarado

OPES; no 55-2021

378.728.6
C877d

Cox Alvarado, Alexander

Dictamen sobre la solicitud de aprobación de la maestría en ciberseguridad del Instituto Tecnológico de Costa Rica. / Alexander Cox Alvarado. – Datos electrónicos (1 archivo : 500 kb). -- San José, C.R. : CONARE - OPES, 2021.

(OPES ; no. 55-2021).

ISBN 978-9977-77-436-7

Formato pdf (38 páginas)

1. CIBERSEGURIDAD. 2. COMPUTACIÓN. 3. MAESTRÍA UNIVERSITARIA. 4. OFERTA ACADÉMICA. 5. PLAN DE ESTUDIOS. 6. PERFIL PROFESIONAL. 7. PERSONAL DOCENTE. 8. INSTITUTO TECNOLÓGICO DE COSTA RICA. I. Título. II. Serie.

EBV

PRESENTACIÓN

El estudio que se presenta en este documento (OPES; no 55-2021) se refiere al dictamen sobre la solicitud de aprobación de la Maestría en Ciberseguridad del Instituto Tecnológico de Costa Rica.

El dictamen fue realizado por el M.Sc. Alexander Cox Alvarado, investigador de la División Académica de la Oficina de Planificación de la Educación Superior (OPES) con base en el documento Maestría en Ciberseguridad, 2021, elaborado por el Instituto Tecnológico de Costa Rica. La revisión del documento estuvo a cargo de la Dra. Katalina Perera Hernández, Jefa de la División citada
.
El presente dictamen fue aprobado por el Consejo Nacional de Rectores en la sesión No. 38-2021, artículo 7, inciso b), celebrada el 2 de noviembre de 2021.

Tabla de Contenido

1. Introducción

La solicitud para crear la Maestría en Ciberseguridad en el Instituto Tecnológico de Costa Rica (TEC) fue presentada al Consejo Nacional de Rectores por el señor Rector Ing. Luis Paulino Méndez Badilla, en nota SCI-1049-2021, con el objeto de iniciar los procedimientos establecidos en el documento Lineamientos para la creación de nuevas carreras o la creación de carreras ya existentes [1]

Cuando se crean posgrados, se utiliza lo establecido en los Lineamientos mencionados, los cuales establecen los siguientes temas, que son la base del estudio que realiza la OPES para autorizar las modificaciones en los programas de posgrado que se proponen:

- Datos generales
- Justificación del posgrado.
- Desarrollo académico en el campo de estudios del posgrado.
- Autorización de la unidad académica para impartir posgrados.
- Propósitos del posgrado
- Perfil académico-profesional
- Requisitos de ingreso y de permanencia
- Requisitos de graduación
- Listado de las actividades académicas del posgrado
- Descripción de las actividades académicas del posgrado
- Correspondencia del equipo docente con las actividades académicas.

2. Datos generales

La unidad académica base de la Maestría en Ciberseguridad es la Escuela de Ingeniería en Computación. La Maestría tendrá una duración de nueve ciclos, denominados bimestres, de siete semanas (63 semanas en total). Se ofrecerá con una periodicidad de

[1] Aprobado por el Consejo Nacional de Rectores en la sesión Nº27-2013, artículo 3, inciso g) y h), celebrada el 22 de octubre de 2013.

una cohorte cada año y seis meses, y de forma indefinida. La modalidad de la maestría será profesional.

Los grados académicos y títulos que se ofrecerán serán los siguientes:

- Maestría en Ciberseguridad.
- Maestría en Ciberseguridad con énfasis en Seguridad del Software.
- Maestría en Ciberseguridad con énfasis en Defensa y Ataque de Sistemas.
- Maestría en Ciberseguridad con énfasis en Gestión de la Seguridad de la Información

3. Justificación

El Instituto Tecnológico de Costa Rica justifica de la siguiente manera la necesidad de la Maestría en Ciberseguridad:

> Objeto de estudio:
> La necesidad de ciberseguridad surgió desde que se desarrollaron las primeras computadoras mainframe. En ese momento, se implementaron múltiples niveles de seguridad para proteger estos dispositivos y las misiones a las que servían. Posteriormente, la creciente necesidad de mantener la seguridad nacional de algunos países, condujo a soluciones más complejas y tecnológicamente más sofisticadas para salvaguardar la información.
> Durante los primeros años, la ciberseguridad no se identificaba específicamente como tal, era considerado un proceso sencillo compuesto predominantemente de seguridad física y clasificación de documentos. Las principales amenazas a la seguridad giraban en torno a evitar el robo físico de equipos, el espionaje contra productos de los sistemas y el sabotaje. Sin embargo, a medida que se ha extendido la dependencia de la sociedad en la información digital y de la infraestructura computacional que la soporta, los problemas o amenazas a los que se está expuesto también se han incrementado. Dado lo anterior, la ciberseguridad ha sido un área de estudio que ha venido evolucionando cada vez más. Inicialmente, ésta era vista como un elemento tangencial en el desarrollo de sistemas computacionales, sin embargo, en vista de que el desarrollo de las soluciones digitales ha impactado más allá que solo las soluciones empresariales; se ha formalizado la necesidad estudiar este tema.
> En este sentido, en diciembre 2017, los principales referentes internacionales de la computación: la ACM [Association for Computing Machinery], la IEEE [Institute of Electrical and Electronics Engineers], la AIS [Association for Information Systems] y la IFIP [International Federation for Information Processing] destacan la ciberseguridad como el surgimiento de una disciplina. Al respecto, se indica que dada la creciente dependencia de la sociedad de la infraestructura computacional (cibernética) global, no se debe sorprender que la ciberseguridad está emergiendo como una disciplina identificable con una amplitud y profundidad de contenidos que abarcan muchos de los subcampos que forman el ecosistema informático moderno. Subyacente a esto, emerge la necesidad de preparar especialistas en una variedad de roles de trabajo para complejidades asociadas con garantizar la seguridad de las operaciones del sistema desde una

visión holística. Asegurar operaciones seguras implica la creación, operación, defensa, análisis y prueba de sistemas de información seguros.
[…]
Justificación
En el contexto de transformación digital (cuarta revolución industrial), la seguridad digital y la privacidad de los datos habilitados a través de una política de seguridad cibernética sólida, es fundamental para facilitar la adopción de la tecnología. La fricción entre los sistemas de producción híper conectados presenta nuevos desafíos de seguridad de la información, los cuales deben ser direccionados para lograr que las personas continúen confiando en la tecnología. Si el conocimiento y los datos almacenados en la nube se ven comprometidos, no solo se pone en peligro las operaciones de las organizaciones, sino que también se reduce la confianza y la adopción potencial de nuevos avances e innovaciones tecnológicas digitales en el futuro (World Economic Forum, 2018). Es por ello, que la ciberseguridad ha tomado un rol crítico en la sociedad de hoy.
[…]
El progreso instituto tecnológico digital trae grandes beneficios, pero también implica severas amenazas. Cada avance que se hace para agilizar y facilitar el trabajo, automatizar procesos, intercambiar datos a mayor velocidad y proteger información valiosa o sensible; genera una contrarrespuesta de intereses y organizaciones dedicadas a violar, infiltrar o afectar tales avances y beneficiarse de ellas.
Se están presentando nuevos retos para la seguridad de la información. Indica que, para la habilitación de forma segura de las iniciativas comerciales digitales de hoy, en un mundo de ataques avanzados y dirigidos; se está forzando a los líderes de seguridad y gestión de riesgos a adoptar un enfoque de evaluación adaptativa continua y de confianza en tiempo real. Lo anterior, en vista de que la exposición digital que tenemos está alcanzando niveles nunca vistos. Esto ha implicado que la infraestructura de seguridad de los sistemas digitales esté enfrentando retos mayores que hace unos años.
Adicionalmente, los consumidores digitales están cada vez más conscientes del valor de su información personal y están más preocupados por cómo la utilizan las entidades públicas y privadas. Esto está obligando a las empresas a poner atención y direccionar problemas asociados al tema de la privacidad y la ética digital: aspectos asociados al tema de la confianza digital y la salvaguarda de los derechos digitales de los usuarios y los ciudadanos.
En ese sentido, los gobiernos cada vez más planean o aprueban regulaciones con las que las empresas deben cumplir, y los consumidores están protegiendo o eliminando cuidadosamente su información. Este nuevo escenario pone un reto adicional a las empresas las cuales deben ganar y mantener la confianza con el cliente, y también deben presentar valores internos para garantizar que los clientes los vean como confiables en el mundo digital.
La gran cantidad de relaciones digitales producidas por las tendencias como internet de las cosas (IoT), implementación de tecnología 5G, la integración de la tecnología operacional con la tecnología de la información, la inteligencia artificial, las tecnologías inmersivas, blockchain, la computación en el borde, entre otras; intersecan millones de puntos de conexión y recolección de datos. Es así como podemos encontrar vulnerabilidades de seguridad en aspectos como la integridad en la identidad de las personas (con el reconocimiento facial, el reconocimiento de voz, integridad del ADN o huellas digitales); la localización (como el GPS, rastreo de células, lectores de placas o direcciones IP); lo que hacemos (como hábitos de conducción, pulso cardiaco, presión sanguínea); y lo que pensamos (motores de búsqueda, redes sociales, super cookies, emails).
Esto ha puesto de manifiesto que la seguridad de la información ha transcendido al plano político. Según el BID, la permanente intrusión del continuo digital en todas las áreas de actividad humana, así como la innovación e interdependencia tecnológica, han hecho que sea imposible tratar la ciberseguridad de forma aislada, como un asunto técnico o un área de políticas independiente. Además, en los últimos años, la ciberseguridad ha roto la barrera de los silos técnicos y se encuentra en la intersección de múltiples disciplinas y áreas de políticas: acceso digital y conectividad, resiliencia, justicia penal, diplomacia, seguridad y defensa internacional, y economía digital y comercio. Todos estos aspectos podrían ser relevantes para mantener el orden mundial y la paz, por lo que, además de sugerir que las naciones intentan beneficiarse de

la Cuarta Revolución Industrial, la seguridad cibernética se ha ganado un lugar en el enfoque de la política global que sugieren capacidades internacionales armoniosas para garantizar espacios seguros. (Instituto Tecnológico de Costa Rica, Maestría en Ciberseguridad, 2021)

4. Desarrollo académico en el campo de estudios del posgrado

Respecto al desarrollo académico en el campo de la Ciberseguridad, la Escuela de Ingeniería en Computación envió la siguiente información:

La Escuela de Ingeniería en Computación del Instituto Tecnológico de Costa Rica tiene una gran trayectoria y a través del tiempo ha venido desarrollando acciones para contribuir con el desarrollo de la sociedad y en cumplimiento de la misión del TEC. Ella fue creada en 1976 al ofertarse la Carrera de Técnico Superior en Computación Administrativa "con el propósito de formar profesionales con capacidades y habilidades para administrar la función de los sistemas de información en las empresas y desarrollar sistemas de información administrativos" (Escuela de Ingeniería en Computación, 2014).

Debido a la calidad y el éxito en el mercado profesional de los egresados, se requirió modificar el plan de estudios de tres años con grado de Técnico Superior a un plan de estudios de cuatro años con grado de bachiller. Este cambio curricular se realizó en 1979 cuando la carrera de Técnico Superior pasa a formar Ingenieros en Computación Administrativa con grado de bachiller.

Para 1986, se realizó una modificación curricular que se fundamentó en la evolución de los sistemas de información y de otras especialidades. Se buscó desarrollar dos énfasis, a saber: Sistemas de Información e Ingeniería de Software.

En 1996, se consolida un solo plan de estudios orientado a desarrollar Ingenieros en Computación. Lo anterior con el objetivo de desarrollar y fortalecer la Maestría en Computación y permitir obtener la especialización con el postgrado.

Como una iniciativa para resolver la creciente demanda de profesionales en Computación y promover el desarrollo de la zona norte del país, en el año 1994 se inicia un programa de Técnico en Programación en la sede regional en San Carlos, el cual posteriormente se hace insuficiente para la demanda y es así como a partir del año 1999 se empieza a ofrecer también el programa de bachillerato en Ingeniería en Computación en dicha sede.

También, como parte de la consolidación y madurez que ha caracterizado a la Escuela, se debe destacar que posteriormente, con el fin de procurar más la satisfacción de las demandas nacionales, en el transcurso de la vida de la Escuela, se ha realizado la apertura de nuevas ofertas académicas:

- En 1986, se apertura el programa de Maestría en Computación. Este programa se impartió inicialmente en el Campus Instituto Tecnológico Central para luego ofrecerlo en forma ordinaria en el Campus Instituto Tecnológico Local de San José. Sin embargo, también fue ofertado en empresas que han solicitado se imparta en sus propias instalaciones. También se ha impartido en otras universidades del área centroamericana. Ello ha contribuido a la internacionalización del programa.
- En 2007, se abre la carrera de Licenciatura en Administración en Tecnologías de Información. Esta carrera se abre en conjunto con la Escuela de Administración de Empresas. Su gobierno está dado por la formalización del área académica del mismo nombre.
- En 2006, la Escuela es parte del área académica de Maestría en Gerencia de Proyectos. Este programa fue abierto en colaboración con las escuelas de Administración y Construcción. Su gobierno está dado por la formalización del área académica del mismo nombre.
- En 2008, se abre la carrera de Licenciatura en Ingeniería en Computadores. Esta carrera se abre en conjunto con la Escuela de Electrónica. Su gobierno está dado por la formalización del área académica del mismo nombre.

- En 2012, se abre la carrera de Ingeniería en Computación en el Centro Académico de Alajuela.
- En 2013, se abre la carrera de Ingeniería en Computación en el Centro Académico de San José.
- La última apertura de oferta académica se llevó a cabo en el 2014 en el Centro Académico de Limón.
- En el año 2014, la Escuela forma parte del diseño del Doctorado en Ingeniería que es desarrollado en forma conjunta entre el TEC y la UCR, el cual tiene como fin primordial la formación de investigadores en el área de la ingeniería.
- Más recientemente en agosto 2016, la Escuela es parte del área académica del Doctorado en Ciencias Naturales para el Desarrollo. En este caso la Escuela es representada por la unidad desconcentrada de San Carlos.

Como se puede distinguir, de la narrativa expuesta, la Escuela tiene una trayectoria importante en el ofrecimiento de ofertas académicas para suplir las necesidades de la sociedad. Con ello se puede justificar el nivel de madurez que esta Escuela tiene para ofrecer una nueva maestría en campo de la ciberseguridad.

[…]

Un antecedente importante en el contexto de Costa Rica es la iniciativa que dirige PROCOMER al establecer un Clúster de Ciberseguridad para el país (julio 2019). Este clúster convoca a diversos sectores para trabajar en conjunto con el fin de habilitar y crear capacidades para el ejercicio profesional de la ciberseguridad para y desde Costa Rica (teniendo presente una perspectiva de servicios para el mundo). El TEC ha sido convocado a participar de esta agrupación con la intención de que pueda ofrecer programas de formación y/o capacitación en el tema.

En el desarrollo de las reuniones del clúster de Ciberseguridad, las empresas participantes han indicado claramente la necesidad de desarrollar ofertas de educación a diferentes niveles. Primero relacionado con la alfabetización de la población con el fin de que conozcan los peligros derivados de la digitalización y cómo esto les puede afectar en el día a día. Se considera que los ciudadanos deben conocer las dimensiones de sus acciones en el mundo digital. Segundo, desarrollo de planes de estudios para los colegios técnicos (secundaria); y tercero, programas de formación en la educación universitaria.

Para tal fin, el clúster, por medio de la colaboración entre sus participantes académicos, organizaciones de la sociedad civil (que velan por los derechos digitales) y las empresas de la industria (que actualmente representan a las principales organizaciones que emplean y dan servicios de ciberseguridad en el país); desarrolló un trabajo conjunto para determinar los tópicos que deben ser ofrecidos por las diferentes entidades formadoras de talento humano. Ello con el fin de solventar la demanda que se requiere actualmente en el país para aumentar la oferta de servicios hacia otros países.

El resultado de este estudio fue planteado en términos de perfiles de formación en ciberseguridad, donde las empresas empleadoras de personal capacitado en este tema (IBM, HP, CISCO, Hewlett Packard Enterprise, Access Now, Microsoft, Akamai y Procomer) indicaron los tópicos de formación que consideraban debían formarse por perfil. Los perfiles consultados fueron los siguientes:

- Fundamentos: Asociado con el conocimiento básico que puede ser adquirido en la secundaria.
- Operaciones: Asociado a la persona que puede realizar acciones operativas definidas en ciberseguridad. Principalmente porque sabe utilizar una tecnología ya desarrollada. Está asociado a la obtención de certificaciones o diplomados.
- Profesionalización: Asociada al estudio de carreras universitarias o certificaciones avanzadas.
- Especialización: Relativa a estudios formales en especializaciones profesionales o maestrías profesionales.
- Investigación: Asociado a un perfil de investigador formal. Generalmente para desarrollar nuevo conocimiento producto de la investigación formal. Se ve asociado al estudio de

> doctorados académicos. (Instituto Tecnológico de Costa Rica, Maestría en Ciberseguridad, 2021)

5. Autorización de la unidad académica para impartir posgrados

La actual Escuela en Ingeniería de Computación fue autorizada a impartir posgrados por el CONARE el 22 de enero de 1985, sesión 2-1985, cuando se autorizó la creación de la Maestría en Computación.

6. Objetivo general del posgrado

El objetivo general del posgrado es el siguiente:

Promover la profesionalización de la ciberseguridad mediante la especialización en el tratamiento seguro de la información personal, organizacional y de la sociedad, considerando la investigación práctica aplicada tanto como mecanismo de generación de conocimiento como de identificación de las mejores prácticas que permitan impulsar estadios más avanzados en cuanto a seguridad y privacidad de la información en el contexto de la sociedad digital.

7. Perfil académico-profesional

El Instituto Tecnológico de Costa Rica envió la siguiente información sobre el perfil profesional, establecido por competencias:

> Reconocer la necesidad del desarrollo profesional continuo:
> El graduado debe estar consciente que el dominio de la ciberseguridad es muy cambiante, y por lo tanto debe entender que es una necesidad seguir desarrollando su conocimiento a lo largo de toda su vida profesional. La naturaleza de la disciplina de ciberseguridad implica el tratar constantemente con nuevas amenazas y el establecimiento de nuevas estrategias de defensa con el fin alcanzar el máximo estado posible seguro de la información. Por otro lado, desde la perspectiva de la privacidad, igualmente se debe vigilar que las tecnologías emergentes no invadan derechos de las personas y de la sociedad.
>
> Trabajo en Equipo y Liderazgo:
> Los graduados ejecutarán su profesión mediante equipos de trabajo, por esto deben tener la habilidad de participar activamente como miembros o líderes de un equipo. Esto incluye la capacidad de trabajar en equipos remotos y virtuales; locales e internacionales.
>
> Competencia Multicultural:
> Se refiere a la necesidad actual de la hiperconectividad donde el egresado tenga la capacidad de entender y trabajar con otras culturas distinta a la suya y así poder resolver los retos que esto conlleva. La seguridad y privacidad de la información es un problema global y no se puede tratar como

problemas aislados de una organización, país o región. Así por ejemplo una amenaza como un virus no afecta a solamente un país y su impacto tiene diferentes naturalezas (financiera, política, social, reputacional). Todos los contextos derivados de ello deben ser comprendidos y gestionados. Sin embargo, esto ocurre en coordinación con muchos lugares del planeta lo que implica necesariamente tener habilidades de trabajo en ambientes multiculturales.

Análisis ético:
Los graduados deben poder demostrar actitudes y prioridades que honren, protejan y mejoren la estatura ética de sus acciones en el campo de la ciberseguridad.

Profesionalismo:
Se necesita que los profesionales comprendan asuntos de la profesión, legales, de seguridad, políticos, humanistas, ambientales, culturales y éticos. Además, deben comprender los efectos de sus intervenciones profesionales sobre los individuos, organizaciones y la sociedad.

Entendimiento técnico claro en Ciberseguridad:
El graduado debe tener claro conocimiento en las bases computacionales de la ciberseguridad y su relación con otras disciplinas.

Apreciación de la relación entre teoría y práctica:
En general, el graduado debe poder entender cómo interactúan la teoría y la práctica; y cómo se influencian la una a la otra.

Entendimiento de prácticas y estándares:
Esto incluye la implementación eficaz de las herramientas generalmente utilizadas para el aseguramiento de la información, con especial énfasis en la comprensión de todo el proceso de uso de estándares para resolver problemas prácticos de ciberseguridad.

Diseño, implementación y evaluación de la seguridad y privacidad de sistemas de información:
El graduado debe poder identificar, evaluar, diseñar e implementar soluciones seguras a problemas en los sistemas de información, considerando las restricciones de privacidad derivadas.

Conocimiento y puesta en práctica de fundamentos matemáticos:
Los graduados deben poder aplicar su conocimiento matemático para poner en práctica soluciones de seguridad a problemas complejos.

Experiencia en empresas y proyectos reales:
Se debe exponer al egresado a experiencias prácticas tanto de investigación como de desarrollo, que le permitan desarrollar los conceptos teóricos en la práctica.

Conciencia del contexto socioeconómico, cultural y ambiental:
El egresado debe poder experimentar cómo las soluciones computacionales desde una perspectiva de ciberseguridad que se crean, diseñan e implementan, afectan la economía, cultura y ambiente.

Prácticas técnicas modernas de diseño y construcción de software seguro:
El graduado debe poder experimentar en práctica el uso de teorías actuales, modelos y técnicas que proporcionan la base para la identificación de problemas, análisis, diseño, desarrollo, construcción, ejecución, verificación y validación de software desde una perspectiva de seguridad de la información.

Pensamiento analítico y crítico:
El graduado debe poder analizar y hacer críticas sobre problemas y soluciones complejas del campo de la ciberseguridad.

Creatividad:
El graduado debe mostrar la capacidad de proponer soluciones novedosas que se salgan de los esquemas convencionales y sociales.

Habilidad para identificar, comprender y resolver problemas en el campo de la Ciberseguridad:
Debe mostrar la capacidad de identificar, comprender, analizar, investigar, experimentar, diseñar e implementar soluciones para poder extraer conclusiones.

Transdisciplinariedad:
El graduado debe tener conciencia de las diversas aplicaciones de la ciberseguridad en todos los campos, y aprender de estos, sin limitarse a su disciplina específica.

Identificar y comprender los riesgos inherentes derivados de las innovaciones tecnológicas:
Al terminar su carrera el egresado debe poder identificar los riesgos derivados de las tendencias tecnológicas, de acuerdo con su entorno económico, social y cultural.

Perfil académico profesional por énfasis

En esta sección se presenta la diferenciación del perfil profesional por titulación. Para tal fin, se da una especificación de las competencias que hacen la diferencia entre cada énfasis.

Énfasis en Seguridad del Software

Entendimiento claro en Ciberseguridad:
Para este énfasis el área de conocimiento se centra en el desarrollo y uso del software considerando la preservación confiable de las propiedades de seguridad de la información y los sistemas que protege. La seguridad del software depende de qué tan bien los requisitos de seguridad coinciden con las necesidades que el software debe abordar, qué tan bien se diseña, implementa, prueba, libera y mantiene.

Diseño, implementación y evaluación de la seguridad y privacidad de sistemas de información:
En el Área de Seguridad del Software la seguridad por diseño es incluida durante todo el ciclo de desarrollo de software, desde la toma de requerimientos hasta su implementación.

Prácticas técnicas modernas de diseño y construcción de software seguro:
El graduado de este énfasis podrá desarrollar software seguro en diferentes arquitecturas actuales, por ejemplo, aplicaciones nativas de la nube, Internet de las cosas, Internet del valor, entre otros.

Habilidad para identificar, comprender y resolver problemas en el campo de la Ciberseguridad:
Debe mostrar la capacidad de identificar, comprender, analizar, investigar, experimentar, diseñar e implementar soluciones desde una perspectiva de software seguro desde el diseño; considerando la problemática asociada a la complejidad, extensibilidad y conectividad del software.

Énfasis en Defensa y Ataque de Sistemas

Entendimiento claro en Ciberseguridad:
El egresado conocerá los elementos asociados al desarrollo de software seguro y seguridad en las redes, siendo estos los insumos para dominar y asimilar las principales técnicas de defensa y ataque de sistemas. Adicionalmente conocerá las principales técnicas de ingeniería inversa como mecanismo para establecer estrategias de la solución de problemas derivados de las pruebas de penetración en sistemas informáticos.

Apreciación de la relación entre teoría y práctica:
Dada la naturaleza práctica de este énfasis, el graduado debe aplicar la teoría durante los ejercicios de ataque de sistemas; por otro lado, también debe de utilizar sus conocimientos prácticos para crear mecanismos de defensa, que eviten ataques futuros.

Habilidad para identificar, comprender y resolver problemas en el campo de la Ciberseguridad:
Debe mostrar la capacidad de identificar, comprender, analizar, investigar, experimentar, diseñar e implementar soluciones desde una perspectiva de defensa y ataque; considerando una problemática asociada la ejecución de pruebas de penetración y los otros mecanismos que permitan la respuesta anticipada o preventiva ante un ataque.

Énfasis en Gestión de la Seguridad de la Información.

Entendimiento claro en Ciberseguridad:
Para este énfasis el área de conocimiento se centra en la administración segura de datos, la gestión de la respuesta ante los incidentes, teniendo en cuenta ataques de nivel humano y velar por la correcta aplicación de estándares y frameworks se seguridad como mecanismo para establecer estrategias de la solución de problemas derivados de correcta gestión y mayordomía de los sistemas computacionales.

Entendimiento de prácticas y estándares:
Esto incluye la implementación eficaz de las herramientas generalmente utilizadas para el aseguramiento de la información, con especial énfasis en la comprensión de todo el proceso de uso de estándares y marcos de trabajo para resolver problemas prácticos de ciberseguridad.

Habilidad para identificar, comprender y resolver problemas en el campo de la Ciberseguridad:
Debe mostrar la capacidad de identificar, comprender, analizar, investigar, experimentar, diseñar e implementar soluciones desde una perspectiva de gestión de sistemas de computación; considerando una problemática asociada la correcta implementación de estándares y frameworks en una organización, con el objetivo de garantizar la privacidad de datos y el uso de las mejores prácticas para la gestión de incidentes de seguridad. (Instituto Tecnológico de Costa Rica, Maestría en Ciberseguridad, 2021.)

8. Requisitos de ingreso

Según el Instituto Tecnológico de Costa Rica, los requisitos de ingreso son los siguientes:

- Bachillerato universitario en Ingeniería en Computación o informática cuyo objeto de estudio sea ciencias de la computación o ingeniería del software; licenciatura en Ingeniería en Computadores; licenciatura en Administración de Tecnologías de Información; u otras áreas afines al objeto de estudio, según criterio de la comisión evaluadora que se designe para el proceso de admisión de estudiantes.

- Dominio instrumental del idioma inglés: Se refiere a la capacidad del estudiante para la comprensión de un texto escrito y conversación oral. El manejo instrumental mínimo requerido para el programa es el nivel B2, según el Marco Común Europeo de Referencia para las Lenguas (MCERL), o su equivalente en otros marcos de

referencia según criterio de la Comisión evaluadora que se designe para el proceso de admisión de estudiantes.

Se debe cumplir con los demás requisitos administrativos que establezca el Instituto Tecnológico de Costa Rica

9. Requisitos de permanencia y de graduación

La permanencia en la Maestría está determinada por el Reglamento del Sistema de Estudios de Posgrado del TEC.

Se establece como requisito de graduación lo siguiente:

- Aprobación de todos los cursos y las actividades del plan de estudios.

Adicionalmente, el estudiante debe cumplir con los demás requisitos financieros y administrativos del Instituto Tecnológico de Costa Rica.

10. Listado de las actividades académicas del posgrado

El plan de estudios de la Maestría, presentado en el Anexo A, consta de 60 créditos y tiene una duración de nueve bimestres de siete semanas. El énfasis consta de dieciséis créditos (el 26,7% del posgrado). Para graduarse en un énfasis, hay que aprobar todos los cursos del énfasis (dieciséis créditos); si el estudiante lleva asignaturas de varios énfasis, puede graduarse de la Maestría sin énfasis, siempre que lleve al menos dieciséis créditos en otras asignaturas y cumpla así con los 60 créditos del posgrado.

La malla curricular cumple con la normativa respecto al grado de maestría, a la modalidad profesional de la maestría y a los énfasis.

11. Programas de las actividades académicas del posgrado

Los programas de los cursos se muestran en el Anexo B.

12. Correspondencia del equipo docente con las actividades académicas

El requerimiento mínimo para el personal docente que participa en una Maestría es poseer un posgrado. En el Anexo C, se indica el título y grado del diploma respectivo de cada uno de los docentes de la Maestría en Ciberseguridad.

Todas las normativas vigentes respecto a los docentes se cumplen.

13. Conclusiones

La propuesta cumple con la normativa aprobada por el CONARE en el Convenio para crear una nomenclatura de grados y títulos de la Educación Superior Estatal[2], en el Convenio para unificar la definición de crédito en la Educación Superior[3] y con los procedimientos establecidos por el documento Lineamientos para la creación de nuevas carreras o la creación de carreras ya existentes.

14. Recomendaciones

Con base en las conclusiones del presente estudio, se recomienda lo siguiente:

- Que se autorice al Instituto Tecnológico de Costa Rica la creación de la Maestría en Ciberseguridad con sus objetivos, perfiles, malla curricular y contenidos de acuerdo con los términos expresados en este dictamen.
- Que el Instituto Tecnológico de Costa Rica realice evaluaciones internas durante el desarrollo del posgrado.

[2] Aprobada por el CONARE en la sesión del 10 de noviembre de 1976.
[3] Aprobado por el CONARE en la sesión 19-03, artículo 2, inciso c), del 17 de junio de 2003.

ANEXO A

PLAN DE ESTUDIOS DE LA MAESTRÍA EN CIBERSEGURIDAD DEL INSTITUTO TECNOLÓGICO DE COSTA RICA

ANEXO A

PLAN DE ESTUDIOS DE LA MAESTRÍA EN CIBERSEGURIDAD DEL INSTITUTO TECNOLÓGICO DE COSTA RICA

CICLO Y NOMBRE DEL CURSO	CRÉDITOS
Primer bimestre	8
Asignatura del tronco común	4
Taller de investigación práctica aplicada	4
Segundo bimestre	8
Asignatura del tronco común	4
Investigación práctica aplicada I	4
Tercer bimestre	4
Asignatura del tronco común	4
Cuarto bimestre	8
Asignatura del tronco común	4
Investigación práctica aplicada II	4
Quinto bimestre	4
Asignatura de tópicos electivos en tendencia	4
Sexto bimestre	7
Asignatura de tópicos electivos profesionalizantes	4
Investigación práctica aplicada avanzada I	3
Sétimo bimestre	7
Asignatura de tópicos electivos profesionalizantes	4
Investigación práctica aplicada avanzada II	3
Octavo bimestre	7
Asignatura de tópicos electivos profesionalizantes	4
Investigación práctica aplicada avanzada III	3

CICLO Y NOMBRE DEL CURSO	CRÉDITOS
Noveno bimestre	7
Asignatura de tópicos electivos profesionalizantes	4
Presentación de Proyecto de Investigación práctica aplicada avanzada	3
Total de créditos	60

Asignaturas del tronco común (eventualmente se podrán ofrecer otras):

Análisis de Datos en Ciberseguridad
Seguridad y Criptografía
Principios de Seguridad en Sistemas Operativos
Políticas y Gobernanza de la Ciberseguridad

Asignaturas de tópicos electivos en tendencia (eventualmente se podrán ofrecer otras):

Blockchain y Ledger Distribuidos
Seguridad en Sistemas Ciberfísicos

Asignaturas de tópicos electivos profesionalizantes (énfasis en Seguridad del Software):

Seguridad de Software Avanzado
Tecnologías para Mejorar la Privacidad
Seguridad e Internet de las Cosas
Seguridad en la Nube

Asignaturas de tópicos electivos profesionalizantes (énfasis en Defensa y Ataque de Sistemas):

Seguridad de Software Avanzado
Seguridad de Redes Avanzadas
Defensa y Ataque de Sistemas
Ingeniería Inversa

Asignaturas de tópicos electivos profesionalizantes (énfasis en Gestión de la Seguridad de la Información):

Administración Segura de Datos
Respuesta ante incidentes, riesgo y continuidad
Cibercrimen
Frameworks y estándares de Seguridad

ANEXO B

PROGRAMAS DE LOS CURSOS DE LA MAESTRÍA EN CIBERSEGURIDAD DEL INSTITUTO TECNOLÓGICO DE COSTA RICA

ANEXO B

PROGRAMAS DE LOS CURSOS DE LA MAESTRÍA EN CIBERSEGURIDAD DEL INSTITUTO TECNOLÓGICO DE COSTA RICA

Curso: Análisis de Datos en Ciberseguridad

Créditos: 4

Descripción del curso:

Este curso provee un conjunto de conceptos teóricos y prácticos para la aplicación de análisis de datos en el campo de la ciberseguridad. El análisis de ciberdatos es un campo amplio con gran diversidad de técnicas y aplicaciones. El presente curso se centra en estudiar las técnicas más utilizadas en la detección de anomalías, perfilación de comportamiento de personas y software, minería de datos en tiempo real (data stream mining), procesamiento de datos distribuidos, ingeniería inversa automatizada y minería de datos para la privacidad.

Objetivo general:

El estudiante al finalizar el curso está en la capacidad de desarrollar soluciones para detección de anomalías, descubrimiento de conocimiento, análisis de amenazas y diagnóstico de software en ciberseguridad; mediante herramientas de software orientadas al análisis de datos.

Temática:

- Repaso de Conceptos de Estadística y Cálculo para el Análisis de Datos
- Técnicas para identificación anomalías y detección de fraude
- Técnicas de minería de Datos en Tiempo Real (Stream Mining)
- Técnicas para el procesamiento de datos distribuidos
- Técnicas de ingeniería inversa automatizada
- Función de conocimiento.

Curso: Seguridad y Criptografía

Créditos: 4

Descripción del curso:

En este curso se estudian las tecnologías de criptografía y la teoría matemática, utilizadas diariamente en el Internet y las tecnologías de la información en general, como medio para asegurar la confidencialidad, autenticidad y la integridad de las comunicaciones y los datos. Además, se estudiará en particular la matemática detrás de los cifrados simétricos y asimétricos, además de tópicos avanzados como el sellado de tiempo, Advanced Encryption Standard (AES), ataques diferenciales y lineales, Stream Ciphers, el protocolo Diffie-Hellman, Curvas Elípticas, entre otros.

Objetivo general:

El estudiante al finalizar el curso está en la capacidad de justificar soluciones de criptografía aplicada, mediante el análisis del estado del arte de los protocolos y algoritmos criptográficos para la seguridad y privacidad.

Temática:

- Historia del cifrado.
- Cifrado Simétrico.
- Cifrado Asimétrico.
- Tópicos Avanzados.

Curso: Principios de Seguridad en Sistemas Operativos

Créditos: 4

Descripción del curso:

En este curso se estudiará la caracterización general de las arquitecturas de sistemas comúnmente utilizadas en entornos de Tecnologías de la Información actual, con el objetivo de conocer e identificar contextos para posibles vectores de ataque, como medio para diseñar estrategias de defensa sobre las arquitecturas en los sistemas de control industrial, Internet de las Cosas, sistemas empotrados, sistemas móviles, sistemas autónomos, virtualización y sistemas de propósito general.

Objetivo general:

El estudiante al finalizar el curso está en la capacidad de deconstruir las arquitecturas de sistemas, para la identificación de vectores de ataque presentes en ellas, mediante casos de estudio y la revisión de la teoría básica que lo sustenta.

Temática:

- Procesos, hilos e interbloqueos.
- Administración de memoria.
- Sistemas de archivos y entrada-salida.
- Sistemas de múltiples procesadores.
- Seguridad en sistemas operativos.
- Seguridad en internet.

Curso: Políticas y Gobernanza de la Ciberseguridad

Créditos: 4

Descripción del curso:

En este curso se estudian las técnicas actuales asociadas a la aplicación de políticas y gobernanza en un entorno organizacional, tanto internas como externas, como medio para ejercer un gobierno responsable y efectivo en la implementación de un planeamiento estratégico, análisis de riesgo y cumplimiento regulatorio, a través de la creación de políticas, planes y programas de aseguramiento de la organización. Además, se estudiarán en particular tópicos relacionados al análisis del contexto,

privacidad de datos, estado actual de la legislación nacional e internacional, cumplimiento de estándares, comunicación a nivel ejecutivo en la organización y presentación de la información.

Objetivo general:

El estudiante al finalizar el curso está en la capacidad de establecer estrategias de gestión en ciberseguridad para la protección de una organización mediante la definición de políticas o acciones para los diferentes procesos involucrados en la gestión de la seguridad de la información y la privacidad.

Temática:

- Gobernanza y Políticas en Ciberseguridad.
- Diagnóstico y Evaluación en Ciberseguridad.
- Aprovisionamiento de Soluciones Seguras.
- Operación y Mantenimiento.
- Monitoreo y Mejora continua.
- Planeamiento Estratégico en Ciberseguridad.

Curso: Blockchain y Ledger Distribuidos

Créditos: 4

Descripción del curso:

En este curso se estudiará el diseño e implementación de sistemas complejos basados en Blockchain, a través del análisis de las tecnologías de modelos de consenso, contratos inteligentes, mercados financieros, mecanismos de distribución, sistemas de paso de mensajes y la relación con los sistemas de base de datos existentes.

Objetivo general:

El estudiante al finalizar el curso está en la capacidad de construir soluciones basadas en Blockchain, mediante la programación contratos inteligentes e implementación de ledgers distribuidos para implementar sistemas de confianza en contextos que por su naturaleza no confiables entre sí.

Temática:

- Introducción.
- Plataformas existentes de Blockchain.
- Arquitectura de Blockchain.
- Arquitectura de Software de Blockchain.
- Patrones de Blockchain. Casos de estudio.

Curso: Seguridad en Sistemas Ciberfísicos

Créditos: 4

Descripción del curso:

Los Sistemas Ciberfísicos (SCFs) abarcan una variedad de aplicaciones en las que sistemas computacionales interactúan con aspectos físicos del mundo real. Estos sistemas incluyen, sistemas de control industrial, edificios inteligentes, dispositivos médicos, vehículos autocontrolados, y muchos otros más. Su capacidad de influenciar el entorno físico combinado con la accesibilidad a distancia que proveen redes locales o remotas, hacen de los SCFs objetivos estratégicos para ciber-criminales. En este curso se analizarán problemas y soluciones de seguridad en sistemas ciberfísicos. Quienes atiendan el curso conocerán los principales aspectos a tomar en cuenta para asegurar SCFs en desarrollo, así como criterios para evaluar la seguridad en SCFs ya desarrollados.

Objetivo general:

Quienes atiendan al curso estarán en capacidad de aplicar las mejores prácticas, herramientas y procesos en la solución de problemas de seguridad en sistemas ciberfísicos, mediante el estudio de casos comunes en este contexto; evaluando proyectos de creación de soluciones de esta naturaleza.

Temática:

- Introducción a los SCFs.
- Seguridad en redes de SCFs.
- Prevención de intrusiones en SCFs.
- Detección de intrusiones en SCFs.
- Manejo de ataques en SCFs.
- Administración de riesgo en SCFs

Curso: Seguridad de Software Avanzado

Créditos: 4

Descripción del curso:

El curso presenta un estudio de la seguridad del software. Se considerarán vulnerabilidades y vectores de ataque, desde una perspectiva avanzada, que pueden servir para violentar el software creado. Entre ellos: Buffer Overflows, SQL Injection, robo de sesiones, entre otros. Además, también se considerarán defensas para prevenir o mitigar estos ataques incluyendo técnicas de programación, modelado de vulnerabilidades y algunas técnicas avanzadas de pruebas.

Objetivo general:

Al finalizar el curso, el estudiante estará en capacidad de diseñar soluciones de Software Seguro a través de mecanismos conocidos como Seguridad desde el Diseño; con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de los datos en las aplicaciones.

Temática:

- La importancia de la Seguridad en el Software
- Administración de Riesgo Aplicado a la Seguridad del Software
- Vulnerabilidades comunes en Seguridad de Software
- Principios de Programación Segura
- Seguridad basada en el Lenguaje de programación
- Técnicas de Análisis Estático de código
- Consideraciones para la seguridad del software
- Base de Conocimiento en Seguridad del Software.

Curso: Tecnologías para el Mejoramiento de la Privacidad

Créditos: 4

Descripción del curso:

El presente curso buscar responder la incógnita de proteger la privacidad de los usuarios participantes mientras a su vez se habilitan mecanismos para compartir y utilizar los datos de forma distribuida. Se estudiarán algunas tecnologías para mejorar la privacidad de los datos de usuario y de la organización, a través de técnicas, algoritmos y estándares para su transmisión, re-identificación, de-identificación y publicación de datos que garanticen la privacidad de la información. Además, se plantean soluciones de almacenamiento y mayordomía de los datos desde una perspectiva de privacidad en cumplimiento con la legislación nacional (Ley de Protección de Datos de los Habitantes) e internacional (GDPR, entre otros), que promueven la transparencia, responsabilidad social e integridad de la información.

Objetivo general:

Al finalizar el curso, el estudiante estará en capacidad de aplicar técnicas para el mejoramiento de la privacidad en la transmisión y almacenamiento de datos, y en la administración de la identidad; para el diseño de soluciones que garanticen la privacidad.

Temática:

- Introducción
- Mecanismos de comunicación anónima
- Privacidad en la administración de identidad
- Privacidad en bases de datos
- Procesamiento privado de datos

Curso: Seguridad en Internet de las Cosas

Créditos: 4

Descripción del curso:

En este curso se estudiarán algunas arquitecturas de sistemas comunes relacionadas con el Internet de las cosas que involucra sensores, refrigeradores, sistemas empotrados y sistemas de control industrial; y mecanismos para asegurar estos dispositivos, utilizando módulos de seguridad de hardware (HSM), técnicas de comunicación segura de máquina a máquina (M2M),

administración de llaves de confianza (trusted key manager), políticas de actualización de dispositivos; con el objetivo de garantizar la integridad, disponibilidad y confidencialidad de los datos y equipos dentro de un entorno de IoT.

Objetivo general:

Al finalizar el curso, el estudiante estará en capacidad de diseñar soluciones seguras en IoT, mediante el entendimiento de la confianza, privacidad y seguridad desde el diseño en este tipo de soluciones, en vista del impacto que las soluciones de IoT están generando en la sociedad.

Temática:

- Revisión de conceptos y aplicaciones de IoT
- Diseño de IoT
- Confianza desde el diseño
- Arquitecturas para el aseguramiento de IoT
- Mecanismos de autenticación
- Defensa de IoT

Curso: Seguridad en la Nube

Créditos: 4

Descripción del curso:

En este curso el estudiante debe comprender y aplicar los conceptos y modelos seguros asociados a las tecnologías de computación en la nube; mediante la evaluación, diseño, implementación y prueba de arquitecturas de sistemas en la nube, por ejemplo: máquinas virtuales, contenedores, clústeres, microservicios, serverless computing, trusted computing, entre otros. Todas ellas comúnmente utilizadas en prácticas actuales de desarrollo de software; con el objetivo asegurar cada uno de los componentes del sistema de acuerdo con las amenazas y vulnerabilidades encontradas.

Objetivo general:

Al finalizar el curso, el estudiante estará en capacidad de diseñar soluciones seguras que involucran computación en la nube por medio del estudio de arquitecturas seguras y mejores prácticas en ese contexto; esto como complemento necesario para el desarrollo de software nativo para plataformas de la nube.

Temática:

- Fundamentos de Computación en la Nube
- Arquitecturas de computación en la nube
- Software seguro utilizando computación en la nube
- Riesgos de computación en la nube
- Problemas comunes de seguridad en computación en la nube
- Arquitectura de seguridad en computación en la nube
- Administración de vulnerabilidades

Curso: Seguridad de Redes Avanzadas

Créditos: 4

Descripción del curso:

Los sistemas de comunicación y de red son actualmente fundamentales para la sociedad. En este curso se estudiará cómo asegurar las redes avanzadas de computadoras, mediante una comprensión profunda en la manera que las redes y sus servicios son diseñados y la interconexión de distintos componentes, utilizando el análisis de tráfico de red en las capas del modelo OSI como mecanismo para alcanzar un aseguramiento integral del equipo de red.

Objetivo general:

Al finalizar el curso, el estudiante estará en capacidad de aplicar las mejores prácticas para asegurar los servicios de comunicación en las diferentes capas de red, para el diseño de estrategias de mejoramiento de la seguridad de los sistemas de computadores y comunicaciones.

Temática:

- Seguridad en capa física
- Seguridad en capa de enlace
- Seguridad en capa de red
- Seguridad en capa de transporte
- Seguridad en capa de aplicación

Curso: Defensa y Ataque de Sistemas

Créditos: 4

Descripción del curso:

En este curso se estudiarán técnicas de hacking ético comúnmente conocidas, que le permitan al estudiante evaluar los mejores mecanismos para atacar un sistema computacional a través de técnicas de hacking y explotación de vulnerabilidades de sistemas, además de determinar las mejores prácticas para defender un sistema computacional a través de mecanismos que potencien la protección de la confidencialidad, integridad y disponibilidad de los datos.

Objetivo general:

Al finalizar el curso el estudiante será capaz de analizar medidas efectivas para proteger sistemas informáticos a través de la investigación, identificación y explotación de vulnerabilidades en sistemas de prueba.

Temática:

- Introducción a la seguridad de la información
- Reconocimiento
- Enumeración y escaneo
- Explotación de vulnerabilidades
- Mantenimiento de acceso
- Anonimato y cubrimiento de rastros

- Contramedidas
- Pruebas de penetración

Curso: Ingeniería Inversa

Créditos: 4

Descripción del curso:

En este curso se estudiarán técnicas para realizar ingeniería inversa en el software y también mecanismos para evitarla, a través de la comprensión del software de “bajo nivel” y utilizando herramientas para la inversión, con el objetivo de deconstruir el software y permitir el auditaje de binarios de programas.

Objetivo general:

Al finalizar el curso, el estudiante estará en capacidad de aplicar técnicas de ingeniería inversa para la deconstrucción del software, con el fin de identificar vulnerabilidades en el mismo.

Temática:

- Introducción a la ingeniería inversa
- Software de bajo nivel
- Revisión de implementación de sistemas operativos de industria
- Herramientas de inversión
- Inversión de malware
- Decompilación
- Técnicas de anti-inversión

Curso: Administración Segura de Datos

Créditos: 4

Descripción del curso:

En este curso se estudiarán técnicas para el aseguramiento de los datos en ambientes informáticos, como medio para garantizar la privacidad, confidencialidad e integridad de la información de los usuarios de un sistema informático. Ello con el objetivo de implementar mejores prácticas, algoritmos y estándares para mejorar la transparencia, almacenamiento y custodia (stewardship) de los datos.

Objetivo general:

El estudiante al finalizar el curso está en la capacidad definir las estrategias tecnológicas para la administración segura de datos, a través del cifrado de datos, la gestión de datos privados, la gestión de datos abiertos y estándares relacionados; con el fin de aumentar la privacidad y la confidencialidad de los datos, al mismo tiempo que se mejora la confianza dentro de la sociedad digital.

Temática:

- Administración de datos abiertos

- Protección de datos
- Control de acceso
- Administración de cloud data

Curso: Respuesta ante incidentes, riesgo y continuidad

Créditos: 4

Descripción del curso:

En este curso se estudiarán las acciones y arquitecturas que debe tener una organización ante la respuesta a los incidentes de seguridad como medio para asegurar la continuidad del negocio, valorando los riesgos de seguridad de la información. Esto con el objetivo de diseñar estrategias para la mitigación de los ciberataques y conocer mejores prácticas para la implementación de grupos de respuesta ante incidentes de seguridad en computación (CSIRT, por sus siglas en inglés) o Centros de Operaciones en Seguridad (SOC, por sus siglas en inglés).

Objetivo general:

El estudiante al finalizar el curso estará en la capacidad diseñar procesos de gestión de crisis mediante la implementación de grupos de respuesta ante incidentes de seguridad, manejo del riesgo y aseguramiento de la continuidad del negocio; para salvaguardar la operación de la organización.

Temática:

- Respuesta ante incidentes
- Gestión de riesgos
- Continuidad del negocio

Curso: Frameworks y estándares de Seguridad

Créditos: 4

Descripción del curso:

Un gerente de seguridad de la información (Chief Information Security Officer por sus siglas en inglés) como parte de sus responsabilidades debe implementar los procesos de gestión de la seguridad. Para ello debe conocer las prácticas más reconocidas basadas en marcos de trabajo y estándares internacionales en la gestión de la ciberseguridad que permitan coadyuvar en los procesos de aprovisionamiento de servicios de la tecnología de la información, su operación, mantenimiento y monitoreo. Considerando siempre la perspectiva de la privacidad de la información. El presente curso hace una correspondencia entre estándares usualmente aplicados en la industria en la gestión de TI (por ejemplo, COBIT) y los marcos de trabajo relacionados con la seguridad de la información correspondientes.

Objetivo general:

El estudiante al finalizar el curso está en la capacidad de evaluar en los dominios de gobierno de TI, los estándares y marcos de trabajo más representativos en ciberseguridad; como insumo para la definición de las políticas organizacionales que correspondan.

Temática:

- Procesos de gestión de la Tecnología de la Información
- Aprovisionamiento seguro de servicios y productos
- Operación y mantenimiento segura de servicios
- Monitoreo para la seguridad de los servicios
- Investigación forense de incidentes

Otros cursos:

Curso: Cibercrimen

Créditos: 4

Descripción del curso:

En este curso el estudiante conocerá las principales acciones utilizadas por el cibercrimen para obtener información confidencial mediante la manipulación de usuarios legítimos, a través del uso de herramientas de espionaje, investigación y de recopilación de información; con el objetivo de proteger sistemas evaluando distintos escenarios de phising, vishing, espionaje industrial, entre otros.

Objetivo general:

El estudiante al finalizar el curso estará en la capacidad valorar la naturaleza de las acciones de individuos involucrados en actos de cibercrimen mediante el estudio de diferentes motivadores sociales y perspectivas legales, con el fin de potenciar la identificación de amenazas y su naturaleza.

Temática:

- Métodos de investigación de las Ciencias Sociales
- Cibercrimen Ingeniería social
- La ciencia del crimen
- Prevención del crimen en situación

Cursos de investigación práctica aplicada

Curso: Taller de Investigación Práctica Aplicada

Créditos: 4

Descripción del curso:

El presente curso taller ejercita los principales aspectos metodológicos requeridos para el desarrollo de las investigaciones prácticas aplicadas que los estudiantes deben desarrollar a lo largo del programa.

Objetivo general:

Al finalizar el curso el estudiante tendrá la capacidad de desarrollar formalmente un planteamiento de investigación práctica aplicada usando de base una situación hipotética.

Temática:

- Características y fines de los tipos de investigación práctica aplicada
- Metodología de la investigación práctica aplicada
- Comunicación de resultados de una investigación práctica aplicada

Cursos: Investigación Práctica Aplicada I y II

Créditos: 4

Descripción del curso:

En estos cursos, el estudiante desarrolla una investigación práctica aplicada (IPA) completa, pero de baja complejidad, sobre un contexto real utilizando los conceptos que a la fecha ha estudiado en el estudiante en el programa de la maestría. Esta IPA puede ser desarrollada en grupos de hasta por dos personas. Los estudiantes deberán utilizar los conceptos aprendidos en el curso de Taller práctica aplicada y desarrollar por su cuenta la investigación de alguna temática asociada a la ciberseguridad. En el curso no se imparten lecciones; sin embargo, tendrá asignado un profesor que facilitará la orientación de los estudiantes mediante el mecanismo de tutoría semanal.

Objetivo general:

Al finalizar el curso el estudiante tendrá la capacidad de desarrollar una investigación práctica aplicada de baja complejidad en un contexto real y significativo.

Temática:

- Identificación de la situación problemática
- Elección de teoría sustente de la situación problemática
- Diseño de propuesta de solución
- Ensayo de solución
- Resultados obtenidos

Curso: Investigación Práctica Aplicada Avanzada I

Créditos: 3

Descripción del curso:

En el presente curso, el estudiante desarrolla la fase de identificación de la situación problemática de una investigación práctica aplicada compleja relativa a una situación que está caracterizada por un conjunto de elementos que se relacionan entre sí y cuyo comportamiento y propiedades no son evidentes a simple vista. El estudiante deberá identificar la situación “problema” a partir de una situación problemática que requiere ser intervenida y mejorada. Se debe describir sistemáticamente esa situación problema, de manera que se justifique con criterios relevantes su orden práctico.

Además, deberá hacer la selección de la teoría sustenten, que dé una explicación de la situación problemática identificada.

Objetivo general:

Al finalizar el curso el estudiante desarrollará la identificación de la situación problemática de una investigación práctica aplicada compleja y la sustentación teórica en que se basa dicha situación.

Temática:

- Identificación de la situación problemática
- Elección de teoría sustente de la situación problemática
- Escritura parcial de informe científico (paper u otro formato) de la investigación práctica que está desarrollando

Curso: Investigación Práctica Aplicada Avanzada II

Créditos: 3

Descripción del curso:

En el presente curso, el estudiante desarrolla la fase de diseño de la propuesta de solución para una investigación práctica avanzada aplicada en una situación compleja. Allí se examina la situación "problema" a la luz de la teoría seleccionada, de ésta se diseña un prototipo de acción (propuesta de solución), con el cual se busca resolver favorablemente la situación "problema". En él se contempla la descripción sistemática con sus secuencias e instrumentaciones pues resultará ser el método y/o un modelo a emplear y comprobar en este proceso práctico aplicado. Adicionalmente, el estudiante deberá desarrollar el ensayo de solución, que tiene como fin ejercitar y probar la propuesta de solución para determinar la probabilidad o viabilidad que tiene el modelo aplicativo para resolver la situación "problema".

Objetivo general:

Al finalizar el curso el estudiante desarrollará un diseño de la propuesta de solución y su correspondiente ensayo de solución para la investigación práctica aplicada compleja.

Temática:

- Diseño de propuesta de solución
- Ensayo de solución
- Escritura parcial de informe científico (paper u otro formato) de la investigación práctica que está desarrollando.

Curso: Investigación Práctica Aplicada Avanzada III

Créditos: 3

Descripción del curso:

Este curso es el tercero de una secuencia de tres que en conjunto permiten el desarrollo de una investigación práctica aplicada avanzada que será desarrollada en forma individual. Para tal fin el estudiante contará con un profesor asesor el cual le guiará en el proceso. En el presente curso, el

estudiante identifica y analiza los resultados obtenidos de la investigación avanzada aplicada en situación compleja. Se completa el proceso de análisis de la práctica investigativa al detallar los resultados obtenidos y, por último, elegir el formato adecuado para presentar el informe final escrito. Es importante destacar que la comunicación de resultados debe ser presentada por medio de un informe escrito que tenga calidades para ser publicado en revistas, journals, o presentado en conferencias, u otros medios para divulgar los resultados obtenidos de la investigación práctica aplicada

Objetivo general:

Al finalizar el curso el estudiante desarrollará el análisis de resultados para la investigación práctica aplicada compleja.

Temática:

- Resultados obtenidos
- Escritura de informe científico (paper u otro formato)

Curso: Presentación de Proyecto de Investigación Práctica Aplicada Avanzada

Créditos: 3

Descripción del curso:

En el presente curso, el estudiante presenta los resultados obtenidos de la investigación avanzada aplicada en situación compleja.

Objetivo general:

Al finalizar el curso el estudiante presentará de resultados de la investigación práctica aplicada avanzada desarrollada en los cursos anteriores de investigación práctica avanzada aplicada, ante un tribunal de la institución.

Temática:

Ver Reglamento o normas de evaluación de Trabajos Finales de Graduación (TFG).

ANEXO C

PROFESORES DE LOS CURSOS DE LA MAESTRÍA EN CIBERSEGURIDAD DEL INSTITUTO TECNOLÓGICO DE COSTA RICA

ANEXO C

PROFESORES DE LOS CURSOS DE LA MAESTRÍA EN CIBERSEGURIDAD DEL INSTITUTO TECNOLÓGICO DE COSTA RICA

CURSO	PROFESOR
Análisis de Datos en Ciberseguridad	Luis Alexander Calvo Valverde María Mora Cross
Seguridad y Criptografía	Francisco Torres Rojas
Principios de Seguridad en Sistemas Operativos	Francisco Torres Rojas Rodrigo Bogarín Navarro
Políticas y Gobernanza de la Ciberseguridad	Mauricio Arroyo Herrera Roberto Cortés Morales
Blockchain y Ledger Distribuidos	Kevin Moraga García Carlos Roberto Vargas Montero
Seguridad en Sistemas Ciberfísicos	Herson Esquivel Vargas
Seguridad de Software Avanzado	Herson Esquivel Vargas Ignacio Trejos Zelaya
Tecnologías para Mejorar la Privacidad	Kevin Moraga García
Seguridad e Internet de las Cosas	Herson Esquivel Vargas
Seguridad en la Nube	Kevin Moraga García Herson Esquivel Vargas
Seguridad de Redes Avanzadas	Emmanuel Ramírez Segura
Defensa y Ataque de Sistemas	Herson Esquivel Vargas
Ingeniería Inversa	Kevin Moraga García
Administración Segura de Datos	Luis Alexander Calvo Valverde
Respuesta ante Incidentes	Mauricio Arroyo Herrera
Cibercrimen	Camila Delgado Agüero Freddy Ramírez Mora
Taller de investigación práctica aplicada	Mauricio Arroyo Herrera
Investigación Práctica Aplicada (todo el proceso)	Herson Esquivel Vargas Kevin Moraga García Luis Alexander Calvo Valverde Mauricio Arroyo Herrera Ignacio Trejos Zelaya Freddy Ramírez Mora María Mora Cross Francisco Torres Rojas Rodrigo Bogarín Navarro Roberto Cortés Morales

ANEXO D

PROFESORES DE LOS CURSOS DE LA MAESTRÍA EN CIBERSEGURIDAD DEL INSTITUTO TECNOLÓGICO DE COSTA RICA Y SUS GRADOS ACADÉMICOS

ANEXO D

PROFESORES DE LOS CURSOS DE LA MAESTRÍA EN CIBERSEGURIDAD DEL INSTITUTO TECNOLÓGICO DE COSTA RICA Y SUS GRADOS ACADÉMICOS

MAURICIO ARROYO HERRERA

Bachillerato en Ingeniería en Computación, Instituto Tecnológico de Costa Rica. Maestría en Administración de Negocios, Universidad Estatal a Distancia.

RODRIGO BOGARÍN NAVARRO

Licenciatura en Computación e Informática, Universidad de Costa Rica. Maestría en Computación, Instituto Tecnológico de Costa Rica.

LUIS ALEXANDER CALVO VALVERDE

Bachillerato en Ingeniería en Computación, Instituto Tecnológico de Costa Rica. Licenciatura en Ingeniería Informática, Universidad Estatal a Distancia.

ROBERTO CORTÉS MORALES

Bachillerato en Computación e Informática, Universidad de Costa Rica. Maestría en Computación e Informática, Universidad de Costa Rica.

CAMILA DELGADO AGÜERO

Licenciatura en Psicología, Universidad de Costa Rica. Maestría en Psicología Clínica, Universidad de Iberoamérica.

HERSON ESQUIVEL VARGAS

Bachillerato en Ingeniería en Computación, Instituto Tecnológico de Costa Rica. Maestría en Computación, Instituto Tecnológico de Costa Rica.

MARÍA MORA CROSS

Bachillerato en Computación e Informática, Universidad de Costa Rica. Maestría en Computación, Instituto Tecnológico de Costa Rica.

KEVIN MORAGA GARCÍA

Bachillerato en Ingeniería en Computación, Instituto Tecnológico de Costa Rica. Maestría en Computación, Instituto Tecnológico de Costa Rica.

EMMANUEL RAMÍREZ SEGURA

Bachillerato en Ingeniería en Sistemas de Información, Universidad Nacional. Licenciatura en Informática, Licenciatura en Ingeniería Electrónica, Instituto Tecnológico de Costa Rica. Maestría en Computación e Informática, Universidad de Costa Rica.

FREDDY RAMÍREZ MORA

Bachillerato en Ingeniería en Computación, Instituto Tecnológico de Costa Rica. Maestría en Computación, Instituto Tecnológico de Costa Rica.

FRANCISCO TORRES ROJAS

Doctorado en Computación, Instituto de Tecnología de Georgia, Estados Unidos de América.

IGNACIO TREJOS ZELAYA

Bachillerato en Ingeniería en Computación Administrativa, Instituto Tecnológico de Costa Rica. Maestría en Computación, Universidad de Oxford, Inglaterra.

CARLOS ROBERTO VARGAS MONTERO

Bachillerato en Ingeniería en Computación, Instituto Tecnológico de Costa Rica. Maestría en Computación, Instituto Tecnológico de Costa Rica.

CONSEJO NACIONAL
DE RECTORES

UCR TEC UNA UNED UTN Universidad Técnica Nacional