INSTITUTO NACIONAL DE ASTROFÍSICA, ÓPTICA Y ELECTRÓNICA

PRESENTACIÓN Y, EN SU CASO, APROBACIÓN DE LA ESPECIALIDAD EN SEGURIDAD INFORMÁTICA

MOTIVACIÓN

En el Plan de Maestría en Ciencias y Tecnologías de Seguridad de 2018, aprobado mediante el acuerdo S-JG-O-II-2017-11, en el apartado 1.6. Opciones de graduación, se indica que, "Si el estudiante aprueba 38 créditos podrá ser acreedor a un certificado a nivel especialidad".

Con este acuerdo, el Departamento de Servicios Escolares se procedió con la solicitud ante la Dirección General de Profesiones, de emisión de títulos de Maestría en Ciencias y Tecnologías de Seguridad (MCTS), y el del Especialidad en Tecnologías de Seguridad. La DGP aprobó la emisión de títulos de la citada maestría, e indicó que para aprobar la de la especialidad se requiere de un acuerdo específico.

En este sentido, el Núcleo Académico de la Maestría de la MCTS revisó y actualizó el plan de estudios de la Especialidad en Seguridad Informática.

La pertinencia se centra en la necesidad de formar especialistas en ciberseguridad, ya que México se encuentra entre los países donde más se registran actividades delictivas por ciberataques (https://www.reuters.com/world/americas/mexico-faces-over-half-latin-american-cybercrimes-due-largely-us-ties-2024-10-09/). Además, este programa se alinea con las necesidades de la Estrategia Nacional de Seguridad Pública del gobierno federal (https://www.gob.mx/sspc/documentos/cuarto-informe-de-la-estrategia-nacional-de-seguridad-publica-334434).

FUNDAMENTACIÓN

El Instituto Nacional de Astrofísica, Óptica y Electrónica, solicita a este Junta de Gobierno en ejercicio de sus atribuciones previstas en el artículo 91 de la Ley General en materia de Humanidades, Ciencias, Tecnologías e Innovación; cuarto Transitorio del Decreto por el que se expide la Ley General en materia de Humanidades, Ciencias, Tecnologías e Innovación y se reforman y adicionan diversas disposiciones de la Ley Federal de las Entidades Paraestatales y de la Ley de Planeación; 58, fracción VIII de la Ley Federal de las Entidades Paraestatales; así como las facultades contempladas en el artículo 12 fracción VIII, del Decreto por el cual se reestructura el INAOE, publicado en el Diario Oficial de la Federación el 13 de octubre de 2006 del El Instituto Nacional de Astrofísica, Óptica y Electrónica, apruebe el:

INSTITUTO NACIONAL DE ASTROFÍSICA, ÓPTICA Y ELECTRÓNICA

ESPECIALIDAD EN SEGURIDAD INFORMÁTICA

Mismo que cuenta con la opinión favorable del Comité Docente y el Consejo Científico Académico (equivalente al Consejo Técnico Consultivo Interno) del INAOE y no tendrá impacto presupuestal para el Centro en el presente ejercicio fiscal y subsecuentes.

El Presidente Suplente sometió a consideración de las personas consejeras la aprobación de la solicitud y habiéndose manifestado todos a favor, se adoptó el siguiente:

ACUERDO

Con fundamento en lo dispuesto en el artículo 91 de la Ley General en materia de Humanidades, Ciencias, Tecnologías e Innovación; cuarto Transitorio del Decreto por el que se expide la Ley General en materia de Humanidades, Ciencias, Tecnologías e Innovación y se reforman y adicionan diversas disposiciones de la Ley Federal de las Entidades Paraestatales y de la Ley de Planeación; 58, fracción VIII de la Ley Federal de las Entidades Paraestatales; así como las facultades contempladas en el artículo 12 fracción VIII, del Decreto por el cual se reestructura el INAOE, publicado en el Diario Oficial de la Federación el 13 de octubre de 2006 del El Instituto Nacional de Astrofísica, Óptica y Electrónica, mismo que cuenta con la opinión favorable del Comité Docente y el Consejo Científico Académico (equivalente al Consejo Técnico Consultivo Interno) del INAOE y no tendrá impacto presupuestal para el Centro en el presente ejercicio fiscal y subsecuentes.

Instituto Nacional de Astrofísica, Óptica y Electrónica

Programa de Especialidad en Seguridad Informática

Plan de estudios 2024

Directorio

Dr. Julián David Sánchez de la Llave
Director General Interino

Dra. Claudia Feregrino Uribe
Encargada del Despacho de la Dirección de Investigación y Desarrollo Tecnológico

Dr. Francisco Javier Renero Carrillo
Encargado del Despacho de la Dirección de Formación Académica

Dr. Miguel Morales Sandoval
Coordinador de la Maestría en Ciencias y Tecnologías de Seguridad

Dra. Alicia Morales Reyes
Responsable Docente de la Maestría en Ciencias y Tecnologías de Seguridad

Contenido

1. PRESENTACIÓN....4
1.1. LÍNEAS DE ESPECIALIZACIÓN QUE OFERTA EL PROGRAMA....4
1.2. GRADO QUE SE OTORGA....4
1.3. MODALIDAD EN QUE SE IMPARTE....4
1.4. OBTENCIÓN DEL GRADO....4
2. PLAN DE ESTUDIOS....4
2.1. OBJETIVOS....4
2.2. PERFIL DE INGRESO....5
2.3. PERFIL DE EGRESO....5
2.4. MAPA CURRICULAR....6
2.5. ACTUALIZACIÓN DEL PLAN DE ESTUDIOS....8
2.6. OBTENCIÓN DEL GRADO....8

1. Presentación

1.1. Líneas de especialización que oferta el programa.

- LE1: Normatividad y políticas públicas (NPU)
- LE2: Seguridad y Criptografía aplicada (SCA)
- LE3: Hacking ético (HE)

1.2. Grado que se otorga.

Especialista en Seguridad Informática

1.3. Modalidad en que se imparte.

En línea

1.4. Obtención del grado.

- Tesis
- Tesina
- Obtención de alguna certificación en el ramo
- Continuar con estudios de maestría

2. Plan de estudios

2.1. Objetivos

Objetivo General

Contribuir al desarrollo científico y tecnológico del país mediante la formación de profesionistas capaces de adquirir, generar y aplicar conocimientos en el área de Seguridad Informática, específicamente de fundamentos de la seguridad informática, criptografía aplicada, ataques cibernéticos, internet de las cosas y hacking ético.

Objetivos Particulares

- Formar especialistas con los conocimientos, habilidades y aptitudes que les permitan liderar, analizar, diseñar, aplicar y evaluar ideas, proyectos y planes estratégicos de seguridad informática.

- Formar capital humano capaz de desarrollar soluciones inteligentes de seguridad, alineadas con los objetivos de las organizaciones; con estricto apego a los principios de actuación ética, estándares y regulaciones nacionales e internacionales en un marco legal de actuación.

2.2. Perfil de ingreso

El candidato al programa de Especialidad en Seguridad Informática debe cumplir con los siguientes requisitos:

- Tener el grado de ingeniería o licenciatura en Ciencias Computacionales, o afines (ej. Telecomunicaciones, Tecnologías de la Información, Ingeniería en Sistemas, Electrónica, Mecatrónica).
- Contar con un promedio mínimo de 8.0
- Aprobar el examen de admisión
- Demostrar vocación para los estudios de posgrado, la investigación o desarrollo tecnológico, estar preparado en los fundamentos de la computación y en los campos de especialidad del programa y tener la capacidad de aplicar el conocimiento en la solución de problemas específicos.

2.3. Perfil de egreso

Los egresados de la Especialidad en Seguridad Informática contarán con los conocimientos y la experiencia necesaria para el diseño, supervisión, vigilancia y construcción de sistemas informáticos seguros y una base sólida en los fundamentos de la seguridad informática, criptografía, ataques cibernéticos, el Internet de las Cosas y Hacking ético. Los graduados dominarán los conocimientos para convertirse en especialistas en el campo de la seguridad informática y concebir las tecnologías que se desarrollarán en el futuro. Ellos estarán preparados para trabajar en el ámbito de la seguridad informática en las tecnologías de información. También pueden optar por seguir adelante con estudios de maestría.

El egresado contará con los siguientes conocimientos:

- Los principales hechos, conceptos, principios y teorías relativas a la seguridad informática.
- Teoría, prácticas y herramientas para el diseño, implementación y evaluación de sistemas informáticos seguros.
- Teoría y práctica en implementación de sistemas de información seguros.

También alcanzarán las siguientes habilidades:

- La capacidad de aplicar el conocimiento indicado anteriormente para el análisis de

un problema y el manejo seguro de la información.

- La capacidad para construir sistemas informáticos seguros, utilizando las herramientas más apropiadas para documentar todas las etapas de este proceso.
- La capacidad de descubrir vulnerabilidades y analizar riesgos.
- La capacidad de evaluar los sistemas de información con base en requisitos de seguridad informática.

2.4. Mapa curricular

La Especialidad en Seguridad Informática es en línea, en bloques de materias acumulables y no seriadas, teniendo como soporte tecnológico una plataforma informática dedicada para dicha finalidad.

La especialidad consta de tres períodos académicos divididos en diferentes materias, cada una de 64 horas totales, con 4 créditos asignados. Cuando el estudiante logre acumular 48 créditos, estará en condiciones de obtener el nivel especialidad de acuerdo con el apartado 1.4. Si el estudiante decide graduarse por tesina, esta será dirigida por un investigador del INAOE y podrá ser co-asesorada por un miembro externo perteneciente a alguna organización de seguridad informática relacionada con el tema a desarrollar.

El estudiante tendrá la oportunidad de reforzar sus habilidades de redacción a través de cursos optativos que se ofrecerán durante los periodos del plan de estudios. Para ambos cursos se realizará un examen de ubicación y no tendrán medida de carga académica (créditos).

A continuación se muestra cada uno de los tres niveles de formación y el mapa curricular:

Tabla 1. Mapa curricular de la Especialidad en Seguridad Informática.

PRIMERO		SEGUNDO		TERCERO	
C	4	C	4	C	4
Fundamentos de Seguridad Informática		Hacking ético		Integración de carpetas de investigación	
C	4	C	4	O	4

INSTITUTO NACIONAL DE ASTROFÍSICA, ÓPTICA Y ELECTRÓNICA

Marco normativo e interpretación	Criptografía aplicada	Optativa 5
O 4	O 4	O 4
Optativa 1	Optativa 3	Optativa 6
O 4	O 4	O 4
Optativa 2	Optativa 4	Optativa 7

C	Tronco común
O	Optativa
	Créditos

Carácter	LE	Periodo	Asignatura	Créditos	Clave
Tronco común	LE1	1	Marco Normativo e Interpretación	4	
Tronco común	LE2	1	Fundamentos de seguridad informática	4	
Optativa	LE3	1	Ataques Cibernéticos I	4	
Optativa	LE2/LE3	1	Internet de las cosas (IoT)	4	
Optativa	LE2	1	Estructuras de datos y algoritmos	4	
Optativa	LE2	1	Diseño de Sistemas de Gestión de Datos	4	
Tronco común	LE3	2	Hacking Ético	4	
Tronco común	LE2	2	Criptografía Aplicada	4	
Optativa	LE2	2	Seguridad en dispositivos móviles	4	

Optativa	LE2	2	Internet de las Cosas II	4	
Optativa	LE1/LE2	2	Administración y Protocolos de Seguridad en Redes de Computadoras	4	
Optativa	LE3	2	Ataques Cibernéticos II	4	
Tronco común	LE1	3	Integración de Carpetas de Investigación e Incidentes	4	
Optativa	LE2/LE3	3	Internet de las Cosas III	4	
Optativa	LE2/LE3	3	Sistemas Distribuidos y Cómputo en la Nube	4	
Optativa	LE3	3	Análisis de vulnerabilidades y pruebas de penetración	4	
Optativa	LE2	3	Seguridad y privacidad de datos	4	
Optativa	LE2	3	IA y seguridad	4	

2.5. Actualización del plan de estudios.

La revisión y actualización del Plan de estudios de la Especialidad en Seguridad Informática se realizará cada dos años, de acuerdo con lo establecido en el Reglamento de Posgrados vigente. Esta tarea será responsabilidad del grupo de expertos en Seguridad Informática que designe la DFA del INAOE.

2.6. Obtención del grado.

Para obtener el grado de Especialista en Seguridad Informática, la/el estudiante deberá cubrir 48 créditos y elegir alguna de las opciones de titulación referidas en la sección 1.4.

Acta: No. INAOE/CCA/2024-10-22/007/2024

22 de octubre de 2024

Aprobación del orden del día

Se aprueba por unanimidad.

Dirección General

- **Candidatos Honoris Causa**

Después de consultar con la academia de la Coordinación Ciencias Computacionales tenían dos candidatos y la votación favoreció ampliamente al Dr. Sergio Rajsbaum Gorodezky, por lo cual lo proponemos para que se le otorgue la distinción. Actualmente es investigador en el Instituto de Matemáticas en la UNAM, fue parte de la CDE por más de 6 años y tiene colaboración con varios miembros de la CCC.

Acuerdo CCA/2024-10-22/1: Se aprueba por unanimidad otorgarle dicha distinción al Dr. Sergio Rajsbaum Gorodezky.

La Coordinación de Óptica tenían dos candidatos y la votación favoreció ampliamente al Dr. Eugenio Rafael Méndez Méndez, egresado de la UAM y actualmente labora en el CICESES, ha participado en proyectos de investigación con diferentes investigadores del área y ha sido parte del CEE y miembro de la Junta de Gobierno del Instituto, ha ganado diferentes reconocimientos y el Premio Nacional de Ciencia y Tecnología en Baja California.

Acuerdo CCA/2024-10-22/2: Se aprueba por unanimidad otorgarle dicha distinción al Dr. Eugenio Rafael Méndez Méndez.

- **Reglamento de posgrados**

La DFA comenta que desde hace 14 años el Reglamento de posgrados no se ha actualizado por lo cual, se modificaron algunos artículos revisados ya por el Comité Docente y se agregó un artículo para los convenios de doble titulación; parte de las obligaciones de los estudiantes donde se generó un artículo para la baja definitiva.

Acuerdo CCA/2024-10-22/3: Se aprueba por unanimidad proponer como acuerdo ante el OG.

- **Especialidad en Seguridad Informática**

En el Plan de Maestría en Ciencias y Tecnologías de Seguridad de 2018, aprobado mediante el acuerdo S-JG-O-II-2017-11, en el apartado 1.6. Opciones de graduación, se indica que, "Si el estudiante aprueba 38 créditos podrá ser acreedor a un certificado a nivel especialidad".

Con este acuerdo, el Departamento de Servicios Escolares (DSE) procedió con las solicitudes, ante la Dirección General de Profesiones (DGP), de emisión de títulos de Maestría en Ciencias y Tecnologías de Seguridad (MCTS), y el del Especialidad en Tecnologías de Seguridad. La DGP aprobó la emisión de títulos de la citada maestría, e indicó que para aprobar la de la especialidad se requiere de un acuerdo específico.

En este sentido, el Núcleo Académico de la Maestría de la MCTS revisó y actualizó el plan de estudios de la Especialidad en Seguridad Informática.

Luis Enrique Erro No. 1, C.P. 72840, Tonantzintla, Pue., México.
Tel: (222) 266 3100 Fax: (222) 247 2580 difusion@inaoep.mx www.inaoep.mx

2024 AÑO DE Felipe Carrillo PUERTO

La pertinencia se centra en la necesidad de formar especialistas en ciberseguridad, ya que México se encuentra entre los países donde más se registran actividades delictivas por ciberastaques [https://www.reuters.com/world/americas/mexico-faces-over-half-latin-american-cybercrimes-due-largely-us-ties-2024-10-09/]. Además, este programa se alinea con las necesidades de la Estrategia Nacional de Seguridad Pública del gobierno federal [https://www.gob.mx/sspc/documentos/cuarto-informe-de-la-estrategia-nacional-de-seguridad-publica-334434]
Se llevará el tema al comité docente a más tardar el martes 23 de octubre, para aclarar los puntos importantes.

Acuerdo CCA/2024-10-22/4: Se aprueba por unanimidad proponer como acuerdo ante el OG.

- **Recomendaciones del CEE**

La DIDT menciona que se derivada de las observaciones de la CEE, algunas se han atendido, pero algunas otras se les debe de dar continuidad por lo que se requiere se participe en las actividades de investigación por ejemplo Seminario Institucional, colaboración con otras áreas y los temas de sinergia.

- **Estacionamiento para visitantes**

Se buscará la opción para que puedan ingreso al Instituto con vehículos los visitantes previo registro, además de incluir a las mujeres posdoctorantes en el estacionamiento general derivada de los diferentes problemas derivados por la entrada del acceso del parque tecnológico.

- **Suficiencia presupuestal**

Se estará trabajando con las Coordinaciones para solicitar la suficiencia presupuestal al de Departamento de Finanzas y Control Presupuestal, y se les enviarán diferentes circulares para llevar un mejor control del presupuesto.

Nombre	Cargo	Firma
Dr. David Sánchez de la Llave	Director General Interino	
Dra. Claudia Feregrino Uribe	Encargada del Despacho de los Asuntos de la Dirección de Investigación y Encargada del Despacho de los Asuntos de la Dirección de Desarrollo Tecnológico	
Dr. Francisco Javier Renero Carrillo	Encargado del Despecho de los Asunto de Formación Académica	
Mtra. Petra Mares Martínez	Directora de Administración y Finanzas	
Dr. José Ramón Valdés Parra	Coordinador de Astrofísica	
Dr. Femín Salomón Granados Agustín	Coordinador de Óptica	

Luis Enrique Erro No. 1, CP. 72840, Tonantzintla, Pue., México.
Tel: (222) 266 3100 Fax: (222) 247 2580 difusion@inaoep.mx www.inaoep.mx

2024 Año de Felipe Carrillo PUERTO

Dr. Luis Hernández Martínez	Coordinador de Electrónica	
Dr. Jesús Ariel Carrasco Ochoa	Coordinador de Ciencia Computacionales	
Dr. Divakara Mayya	Secretario del CPA	
Dr. Alejandro Díaz Sánchez	Representante del CPA de la Coordinación de Electrónica	
Dr. Saúl Pomares Hernández	Representante del CPA de la Coordinación de Ciencias Computacionales	

Cierre de las sesiones 22 de octubre a las 12:15 horas.

Luis Enrique Erro No. 1, CP. 72840, Tonantzintla, Pue., México.
Tel: (222) 266 3100 Fax: (222) 247 2580 difusion@inaoep.mx www.inaoep.mx

RESULTADO DE LA EVALUACIÓN ACTUALIZACIÓN DEL PLAN DE ESTUDIOS DE LA ESPECIALIDAD EN SEGURIDAD INFORMÁTICA

La seguridad informática ha cobrado relevancia de manera sostenida en los últimos años, particularmente por el incremento significativo de ciberataques durante el periodo de pandemia que obligó a intensificar el uso de TIC para realizar las actividades incluso más comunes en la sociedad. Las ciberamenazas ha presentado un avance sin precedentes, ahora impulsadas por el auge de la IA generativa. El continuo crecimiento y dependencia en el uso de TIC así como ataques cada vez más sofisticados añaden un riesgo mucho mayor y una amenaza permanente a la seguridad de los sistemas, datos y dispositivos.

Hoy en día, con toda la información que circula y se almacena en la nube, y la mayoría de los servicios y aplicaciones que se acceden en línea, la ciberseguridad se ha vuelto un tema de suma importancia, para los usuarios particulares, empresas u organizaciones, gobierno y organismos de seguridad nacional, ya que la información que se maneja, si es sensible, debe protegerse.

En México, el panorama de ciberseguridad presenta avances, pero aún enfrenta desafíos significativos, especialmente en el desarrollo de talento y recursos humanos capacitados. De acuerdo con estudios del Consorcio Internacional de Certificación de Seguridad de Sistemas de Información (ISC2), “en la región de Latinoamérica existe una carencia de aproximadamente 2,2 millones de profesionales especializados en ciberseguridad”. Esto confirma que actualmente sigue existiendo una brecha considerable de personal cualificado que aborde las problemáticas de seguridad, lo que aumenta el riesgo creciente en esta materia tanto para organizaciones como para ciudadanos.

Debido a ello, es necesario formar recursos humanos especializados en ciberseguridad para poder prevenir, planificar, evaluar y posibilitar estrategias y capacidades de respuesta frente al creciente número de ciberataques y robo de información digital. Dada la naturaleza de las comunicaciones e información digitales, las violaciones de la seguridad informática son inevitables, por lo que especialistas en seguridad son indispensables para minimizar el riesgo de ataques cibernéticos.

Elementos evaluados para determinar la pertinencia de la especialidad en Tecnologías de Seguridad

La seguridad informática es un área transversal y se ha convertido en una competencia necesaria en los profesionales de tecnologías de información. La seguridad de datos, sistemas y de dispositivos debe considerarse desde las etapas de análisis, diseño e

implementación en el ciclo de vida del software, de la creación de sistemas informáticos y de dispositivos computacionales de propósito específico, independientemente del dominio en el que dichos aplicaciones se orienten.

Las organizaciones están invirtiendo cantidades masivas para mitigar los riesgos cibernéticos. Se espera que el gasto mundial en soluciones de ciberseguridad alcance los $266 mil millones de dólares en 2027, según estimaciones de Gartner, lo que refleja el aumento en la preocupación por la seguridad digital. Todo esto, sin duda, implica una mayor y mejor formación de recursos humanos en seguridad informática.

Tan solo en nuestro país, en los últimos años ha habido varios ciberataques importantes que han menguado la fortaleza y credibilidad de instituciones, tal es el caso del ciberataque al gobierno de México por el grupo Guacamaya, así como los ataques previos realizados a Pemex, IMSS, CFE, la Lotería Nacional y el INAI. La capacidad de respuesta a incidentes y sobre todo la prevención de estos está fuertemente ligado a las capacidades y habilidades de los profesionistas en materia de seguridad informática. En NCI (National Cybersecurity Index) evaluó en 2022 a México con 37.66 puntos de 100 posibles, dejándolo en la posición 88 de 160 países, lo que deja ver la necesidad de avanzar, desde el punto de vista de la formación de recursos humanos, en materia de seguridad informática. De acuerdo con el Instituto Nacional de Ciberseguridad de España, se estima que el talento en ciberseguridad doblará su demanda en 2024, hasta alcanzar cerca de 83,000 profesionales. En México, la demanda en este sector ha crecido 64%.

Por lo anterior, se comienzan a observar esfuerzos de universidades y centros de investigación para integrar programas de formación específicos de ciberseguridad. Aunque la oferta de cursos y certificaciones ha crecido, el desarrollo de competencias técnicas y prácticas sigue siendo insuficiente en comparación con la demanda. Mientras que un posgrado tradicional está generalmente orientado a la investigación, para personas con dedicación de tiempo completo, gran parte de los profesionales en ciberseguridad en México han adquirido experiencia práctica en el campo laboral y no necesariamente cuentan con formación académica especializada. Esto crea una brecha entre los conocimientos teóricos y la experiencia práctica que se necesita en los entornos empresariales y críticos. Las personas o profesionales de este sector, con estas necesidades, son las que se pueden beneficiar de un programa de especialidad en Tecnologías de Seguridad como el que el INAOE tiene por objetivo ofertar.

Cabe resaltar que México cuenta con una Estrategia Nacional de Ciberseguridad, que tiene como objetivo fortalecer la infraestructura, mejorar la legislación y fomentar la colaboración internacional. Sin embargo, la implementación efectiva de estas

estrategias ha sido lenta y aún enfrenta desafíos, uno de ellos es el contar con recursos humanos especializados en Tecnologías de Seguridad.

En el INAOE se tiene la convicción de aprovechar su capacidad de infraestructura y de recursos humanos (investigadores) para desarrollar currículos orientados a ciberseguridad, enfocados en habilidades prácticas y en el uso de herramientas de protección y análisis, que coadyuven a proveer a los profesionales mexicanos las habilidades necesarias para competir en un mercado global, y ser una opción sólida para que individuos por cuenta propia o pertenecientes a empresas grandes y medianas en México se especialicen en temas de ciberseguridad, contribuyendo así a reducir vulnerabilidades internas en sus ámbitos de trabajo o personales y a fortalecer el ecosistema de seguridad en el país.

Conclusión

México presenta una notable carencia de expertos en ciberseguridad en el país. Según estimaciones de organizaciones como la Organización de Estados Americanos (OEA), México necesitaría decenas de miles de profesionales más para cubrir las demandas actuales. El desarrollo de la ciberseguridad en México se encuentra en aún en crecimiento, con importantes áreas de oportunidad, entre ellas, la necesidad de contar con más y mejores recursos humos especializados en ciberseguridad. Con iniciativas como la creación de una especialidad en Tecnologías de Seguridad, pertinente en el contexto actual, futuro y global, se contribuye a mejorar la capacidad del país para hacer frente a las amenazas cibernéticas. El impulso de la educación en ciberseguridad es un componente esencial para que México avance y sea competitivo en este ámbito.

Referencia – correo electrónico del Dr. Miguel Morales en atención al Dr. Francisco Renero, sobre la actualización del plan de estudios de la Especialidad de Seguridad Informática. Adjunto a este documento

ESTUDIO DE FACTIBILIDAD

De la actualización del plan de estudios de la Especialidad en Seguridad Informática se concluyó que, *La seguridad informática ha cobrado relevancia de manera sostenida en los últimos años, particularmente por el incremento significativo de ciberataques durante el periodo de pandemia que obligó a intensificar el uso de TIC para realizar las actividades incluso más comunes en la sociedad. Las ciberamenazas ha presentado un avance sin precedentes, ahora impulsadas por el auge de la IA generativa. El continuo crecimiento y dependencia en el uso de TIC así como ataques cada vez más sofisticados añaden un riesgo mucho mayor y una amenaza permanente a la seguridad de los sistemas, datos y dispositivos.*

Hoy en día, con toda la información que circula y se almacena en la nube, y la mayoría de los servicios y aplicaciones que se acceden en línea, la ciberseguridad se ha vuelto un tema de suma importancia, para los usuarios particulares, empresas u organizaciones, gobierno y organismos de seguridad nacional, ya que la información que se maneja, si es sensible, debe protegerse.

En México, el panorama de ciberseguridad presenta avances, pero aún enfrenta desafíos significativos, especialmente en el desarrollo de talento y recursos humanos capacitados. De acuerdo con estudios del Consorcio Internacional de Certificación de Seguridad de Sistemas de Información (ISC2), "en la región de Latinoamérica existe una carencia de aproximadamente 2,2 millones de profesionales especializados en ciberseguridad". Esto confirma que actualmente sigue existiendo una brecha considerable de personal cualificado que aborde las problemáticas de seguridad, lo que aumenta el riesgo creciente en esta materia tanto para organizaciones como para ciudadanos.

Adicionalmente, de acuerdo con los datos reportados por la empresa de ciberseguridad Fortinet, en México se presentaron 85,000 millones de intentos de ciberataques durante el primer semestre de 2022. Esta cifra es alarmante debido a que corresponde a más de la mitad de los 137,000 millones de intentos en toda Latinoamérica. En este escenario la población mexicana tiene 28% más posibilidades de ser víctima de ciberataques. En otras palabras, México se encuentra entre los países donde más se registran actividades delictivas por ciberastaques (https://www.reuters.com/world/americas/mexico-faces-over-half-latin-american-cybercrimes-due-largely-us-ties-2024-10-09/).

Para atender este rezago en ciberseguridad, en 2017 se publicó la Estrategia Nacional de Ciberseguridad (ENCS), en la que se establece la visión de estado mexicano en la materia, teniendo como objetivo identificar y establecer las acciones aplicables a los ámbitos social, económico y político. La ENCS plantea ocho ejes transversales: 1) cultura de ciberseguridad, 2) desarrollo de capacidades, 3) coordinación y colaboración, 4) investigación, desarrollo e innovación, 5) estándares y criterios técnicos, 6) infraestructuras críticas, 7) marco jurídico y autorregulación y 8) medición y seguimiento (https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria_y_Recomendaciones_ENCS.pdf, https://www.gob.mx/sspc/documentos/cuarto-informe-de-la-estrategia-nacional-de-seguridad-publica-334434)

Este escenario muestra la necesidad de formar recursos humanos especializados en ciberseguridad para poder prevenir, planificar, evaluar y posibilitar las estrategias y las capacidades de respuesta frente al creciente número de ciberataques y robo de información digital. Dada la naturaleza de las comunicaciones e información digitales, las violaciones de la seguridad informática son inevitables, por lo que especialistas en seguridad son indispensables para minimizar el riesgo de ataques cibernéticos.

En este sentido la Especialidad en Seguridad Informática atenderá de manera específica la educación en ciberseguridad proveyendo de los especialistas que requiere el país. Al ser un programa de un año, el programa favorece la atención a personas que se encuentran laborando y requieren de este conocimiento de forma expedita, precisa y profunda.

La especialidad está respaldada por investigadores del Núcleo Básico de la Maestría en Ciencias y Tecnologías de Seguridad del Instituto.

Referencia - Dirección de Formación Académica.

Estudio de Impacto Presupuestal
Apertura de la Especialidad en Seguridad Informática
Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE)

---

1. Introducción

El presente estudio tiene como objetivo evaluar el impacto presupuestario de la apertura de la "Especialidad en Seguridad Informática" en el INAOE, en cumplimiento con la normativa vigente en materia de presupuesto y financiamiento.

2. Marco normativo y disposiciones legales

Para la estimación del impacto presupuestario, se deben considerar las siguientes disposiciones y marcos legales aplicables:

- Decreto por el que se reestructura el INAOE.
- Ley General en Materia de Humanidades, Ciencias, Tecnologías e Innovación.
- Ley Federal de Presupuesto y Responsabilidad Hacendaria.
- Ley Federal de Entidades Paraestatales.
- Presupuesto de Egresos Autorizado al INAOE.
- Análisis Funcional Programático.
- Clasificador por Objeto del Gasto.
- Plantilla de Personal.

3. Programa presupuestario

La "Especialidad en Seguridad Informática " se enmarca en el Programa Presupuestario E003: Desarrollo e Innovación Tecnológica, cuyo objetivo es fomentar la formación de profesionales capacitados en áreas tecnológicas avanzadas. A través de este programa, se buscará impulsar la investigación aplicada y la formación de recursos humanos especializados en el campo de la seguridad tecnológica.

4. Fuente de financiamiento

La fuente de financiamiento para la apertura de la especialidad será con cargo a los Recursos fiscales a la partida 33104 “Otras asesorías para la operación de programas”, el cual estará sujeto a la disponibilidad presupuestal.

5. Impacto presupuestario por fuente de financiamiento

Concepto	Fuente de Financiamiento	Impacto Presupuestal	
		Importe anual	Observaciones
Servicios personales (plantilla de personal docente)	Recursos Fiscales	-	Se operará con la misma plantilla de docentes que imparte la Maestría en Ciencias y Tecnologías de Seguridad.
Infraestructura (espacios físicos, mobiliario y equipo)	Recursos Fiscales	-	Se ocupará la infraestructura con la que cuenta actualmente la Dirección de Formación académica
Gastos de operación (papelería, servicio de impresión)	Recursos Fiscales	-	Se operará con los recursos con que actualmente tiene asignados la Dirección de Formación Académica.
Personal docente externo especializado en materia de Tecnologías de Seguridad y ciberseguridad.	Recursos Fiscales	100,000.00	Solicitara la Suficiencia presupuestal correspondiente
Impacto Presupuestal		**100,000.00**	

6. Consideraciones presupuestaria

Para asegurar la correcta ejecución del presupuesto, es fundamental tener en cuenta las siguientes consideraciones:

- ***Cupo mínimo:*** Es necesario establecer un número mínimo de aspirantes para asegurar el uso eficaz y eficiente de los recursos fiscales asignados.
- ***Anualidad:*** La especialidad se impartirá dentro del ciclo presupuestario, que va del 1 de enero al 31 de diciembre de cada año.
- ***Remanentes:*** Los recursos fiscales no ejercidos antes de diciembre deberán ser reintegrados.

7. Conclusiones y recomendaciones

El impacto presupuestario de la apertura de la "Especialidad en Seguridad Informática " dependerá de una correcta administración de los recursos asignados. Es fundamental mantener y respetar los costos operativos, como se menciona en el apartado 5, para garantizar que el programa se ejecute dentro de los márgenes presupuestarios anuales establecidos por las leyes correspondientes.

Se recomienda implementar un plan de monitoreo y evaluación anual para asegurar el cumplimiento de los objetivos presupuestarios y la correcta utilización de los recursos.

Mtra. Gema Ibáñez Flores
Jefa del Departamento de Programación y Presupuesto

C.P. Faustino Notario González
Encargado del Despacho de los Asuntos de la Subdirección de Finanzas y Control Presupuestal