INSTITUTO NACIONAL DE ASTROFÍSICA, ÓPTICA Y ELECTRÓNICA

PRESENTACIÓN Y, EN SU CASO, APROBACIÓN DE LA CREACIÓN DE UN MAESTRÍA EN CIENCIAS EN TENCOLOGÍAS DE SEGURIDAD

MOTIVACIÓN

El Programa de Maestría en Ciencias en Tecnologías de Seguridad es esencial para el desarrollo científico y tecnológico del país, por medio de la formación de recursos humanos de alto nivel, capaces de adquirir, generar y aplicar conocimientos en el área de Tecnologías de Seguridad, específicamente en los campos de ciberseguridad, criptografía, vigilancia de la red, loTs, seguridad de la información. Estos recursos humanos contribuirán al desarrollo de los sectores social, educativo, productivo, salud de la región y en el país, y que no tiene impacto presupuestal ya que la planta académica, estará conformada por los investigadores del INAOE, así como del personal vinculado con el Instituto.

FUNDAMENTACIÓN

El Instituto Nacional de Astrofísica, Óptica y Electrónica, solicita a este Órgano de Gobierno en ejercicio de sus atribuciones indelegables previstas en el 56, fracción I de la Ley de Ciencia y Tecnología, así como en sus facultades contempladas en el artículo 12, fracción V del Decreto por el cual se reestructura el Instituto Nacional de Astrofísica, Óptica y Electrónica, apruebe la creación de Maestría en Ciencias en Tecnologías de Seguridad y que tiene por objeto formar maestros en ciencias con los conocimientos, habilidades y actitudes que les permitan liderar, analizar, diseñar, aplicar y evaluar ideas, proyectos y planes estratégicos de seguridad cibernética conforme a las arquitecturas empresariales y alineadas con los objetivos de las organizaciones; todo ellos ligado a los principios de actuación ética como estándares y regulaciones nacionales e internacionales en un marco legal de actuación, mismo que no tiene un impacto presupuestal directo.

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

ACUERDO

Con fundamento en lo dispuesto por los artículos 56, fracción I de la Ley de Ciencia y Tecnología; así como en las facultades contempladas en el artículo 12, fracción V del Decreto por el cual se reestructura el Instituto Nacional de Astrofísica, Óptica y Electrónica, apruebe la creación de Maestría en Ciencias en Tecnologías de Seguridad y que tiene por objeto formar maestros en ciencias con los conocimientos, habilidades y actitudes que les permitan liderar, analizar, diseñar, aplicar y evaluar ideas, proyectos y planes estratégicos de seguridad cibernética conforme a las arquitecturas empresariales y alineadas con los objetivos de las organizaciones; todo ellos ligado a los principios de actuación ética como estándares y regulaciones nacionales e internacionales en un marco legal de actuación, mismo que no tiene un impacto presupuestal directo.

MAESTRÍA EN CIENCIAS EN TECNOLOGÍAS DE SEGURIDAD

INSTITUTO NACIONAL DE ASTROFÍSICA,
ÓPTICA Y ELECTRÓNICA

Tonantzintla, Puebla, México

Contenido

1. Presentación

1.1. Nombre del programa de estudios.

Maestría en Ciencias en Tecnologías de Seguridad

1.2. Líneas de Investigación que oferta el programa.

- Seguridad Informática
- IoT
- Seguridad de la Información
- Criptografía
- Minería de Datos
- Sistemas tiempo real
- Sistemas optrónicos

1.3. Título académico que se otorga.

Maestro en Ciencias en Tecnologías de Seguridad

1.4. Modalidad en que se imparte.

Escolarizada.

1.5. Obtención del grado.

Mediante la defensa de tesis.

2. Fundamentación y Antecedentes.

2.1. Introducción

Actualmente las tecnologías de la información, seguridad y las comunicaciones se han involucrado en todos los eslabones de la sociedad moderna, incluyendo las organizaciones públicas y privadas, que cada día se esfuerzan más por incorporar tecnologías de información, seguridad y comunicación en sus procesos, buscando así impulsar la optimización de tiempos y de recursos, la reducción de costos y la agilización en sus procesos. Este proceso incluye también el ciudadano normal, a través de la computación móvil, los teléfonos inteligentes, las iniciativas nacionales para facilitar el acceso a computadoras y conectividad de Internet así como los sistemas de seguridad física, tanto en casas habitación como en instalaciones sensibles.

Este nuevo paradigma ha generado una sociedad donde la información es el activo principal, en el cual, el concepto de ciberespacio ha adquirido dimensiones estratégicas y donde el cuidado de recursos y activos

informáticos y físicos se ha constituido en un foco fundamental. En contraste, podemos citar que hace algunos años, en el inicio de las redes y de la World Wide Web, la seguridad no era siempre un tema de gran importancia, de hecho, en las primeras facetas de ARPANET, una pequeña red fundada por el pentágono, se realizaron varias intrusiones por parte de estudiantes universitarios, similar a ataques cibernéticos que ocurren comúnmente hoy en día.

Es de resaltar que los cibercriminales y los ataques cibernéticos han estado presentes desde que las redes de computadoras estaban iniciando. Conforme las redes de computadoras y el internet fueron evolucionando también lo hicieron los ciberataques, desde un inicial Phreaking (acto de hackear líneas telefónicas para realizar llamadas gratuitas) hasta una gran variedad de virus y gusanos de computadora.

Recientemente la prensa ha destacado el efecto de los malware como Shamoon, Stuxnet y Flame en la comunidad empresarial. Estos ciberataques ilustran la vulnerabilidad de la industria y las operaciones del gobierno. El continuo crecimiento del uso de soluciones móviles y servicios de Cloud Computing añaden un riesgo adicional a estas actividades.

Hoy en día con toda la información que circula y se almacena en la nube, la ciberseguridad se ha vuelto un tema de suma importancia, no solo para los usuarios particulares, empresas u organizaciones sino también para organismos de seguridad nacional de todos los países ya que la información que se maneja no puede estar comprometida a través de la web. Es por esto que dichas organizaciones de seguridad han concentrado recursos en reunir y capacitar a personal especializado en ciberseguridad para poder prevenir, planificar, evaluar y posibilitar estrategias y capacidades de respuesta frente al creciente número de eventos de ciberataques y robo de información digital. Y aunque las violaciones de la seguridad informática son inevitables, este tipo de preparación por parte de las organizaciones minimiza el riesgo que pueda conllevar un ataque a la seguridad de su información digital.

Es importante resaltar la diferencia entre la seguridad de la información y la ciberseguridad. La seguridad de la información tiene un alcance mayor que la ciberseguridad, puesto que la primera busca proteger la información de riesgos que puedan afectarla, en sus diferentes formas y estados. Por el contrario, la ciberseguridad se enfoca principalmente en la información en formato digital y los sistemas interconectados que la procesan, almacenan o transmiten, por lo que tiene un mayor acercamiento con la seguridad informática.

Adicionalmente el aseguramiento de casas habitación como instalaciones estratégicas ha tomado una importancia excepcional en los últimos años, debido al avance de la inseguridad en México.

2.2. Fundamentación

El Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE) fue creado por Decreto Presidencial el 11 de noviembre de 1971. Este Decreto de Creación del INAOE se actualizó y publicó nuevamente en el Diario Oficial de la Federación el 30 de agosto de 2000; de este Decreto se reproduce el primer Artículo que a la letra dice:

> "Artículo 1º.- El Instituto Nacional de Astrofísica, Óptica y Electrónica, es un Organismo Público Descentralizado, con personalidad jurídica y patrimonio propio, con domicilio en Tonantzintla, Estado de Puebla, y tiene por objeto identificar y procurar la solución de problemas científicos y tecnológicos en los campos de astrofísica, óptica, electrónica, telecomunicaciones, computación, instrumentación y demás áreas afines, por medio de la investigación científica, básica y aplicada, el desarrollo experimental y la innovación tecnológica relacionados con las áreas mencionadas; preparar investigadores, profesores especialistas, expertos y técnicos en el campo del conocimiento referido, en los niveles de especialización, licenciatura, maestría, doctorado y postdoctorado, así como orientar

sus actividades de investigación y docencia hacia la superación de las condiciones y la resolución de los problemas del país, y podrá contar con establecimientos en cualquier otra parte de la República Mexicana."

Basado en este Artículo y cumpliendo lo que establece la Ley de Ciencia y Tecnología, de asociar el trabajo científico y la formación de recursos humanos de alto nivel al desarrollo del conocimiento y a la atención de las necesidades del sector productivo y la sociedad mexicana, es que se toma la decisión de crear la propuesta de este programa de Maestría en Ciencias en Tecnologías de Seguridad**,** cuyo objetivo principal es el de preparar recursos humanos capaces de identificar y resolver problemas científicos y tecnológicos en materia de seguridad cibernética y en el diseño y construcción de sistemas optrónicos para proveer la integridad física de instalaciones.

Dado el impacto económico, científico, social y benéfico que esta área tiene a nivel nacional, así como a nivel internacional; el INAOE consideró someter a evaluación la propuesta del Programa, puesto que es fundamental para el desarrollo de la ciencia y tecnología en el país.

2.3. Justificación del Programa

El ciberespacio es particularmente difícil de proteger contra ataques debido a diferentes factores tales como, la habilidad de personas maliciosas que operan desde diferentes lugares del mundo, los vínculos que existen entre el ciberespacio y los sistemas físicos, y la dificultad de disminuir vulnerabilidades en redes de computadoras de alta complejidad. Un fallo en dichas redes y/o infraestructura podría poner en peligro el suministro de numerosos servicios, algunos de ellos vitales para mantener el bienestar de una organización.

Las ciberamenazas pueden proceder de delincuentes bien organizados, de hackers o de un sistema de espionaje promovido por los poderes públicos. Los costes directos e indirectos provocados por los ciberincidentes a nivel mundial se han estimado recientemente en $388.000 millones de dólares; esto incluye, entre otros, los costes por robo, fraude, extorsión y pérdida de propiedad intelectual. Además del impacto financiero directo, incidentes recientes han puesto de manifiesto las graves implicaciones empresariales que suponen las ciberamenazas, desde el desplome del precio de las acciones y la pérdida del valor para los accionistas, hasta la pérdida de confianza por parte de los mercados y de los consumidores.

Es por estas razones que diferentes empresas, organizaciones y gobiernos han desplegado una serie de acciones para estar preparados en este tipo de eventualidades. En el caso de la Unión Europea, por ejemplo, se ha gestionado la creación de la Agencia Europea de Seguridad de las redes y de la información (ENISA), la elaboración de una "Estrategia para una sociedad de la información segura" y el "Plan de Ciberseguridad de la Unión Europea". Pero la rapidez con la que se desarrollan ahora los nuevos ataques y la complejidad del entorno de Internet hacen que esta forma de actuar ya no sea la adecuada, la evolución de las amenazas en el ciberespacio es tal que las organizaciones deben asumir ya que serán atacadas en algún momento y, quizás, de forma reiterada.

Es por esto que las organizaciones deben estar preparadas para definir los procesos y planes necesarios para poder priorizar las acciones de respuesta y mitigación, considerando la continuidad de los diferentes servicios en su conjunto, las operaciones y las relaciones públicas, además de las operaciones informáticas. También deben disponer de las aptitudes técnicas y las herramientas necesarias para evaluar el origen de la violación, llevar a cabo una investigación forense y probar la validez de la solución técnica.

Revisar de forma continua, mejorar y adaptar la capacidad de respuesta, además de modificar los perfiles de riesgo organizacional y las ciberamenazas.

Aunado a los sistemas software para la detección de amenazas, existen los sistemas basados en hardware que coadyuvan en la protección y defensa de instalaciones sensibles. Estos incluyen sistemas de vigilancia, sistemas de detección y seguimiento de intrusos y objetivos designados, así como sistemas de tiempo real para la ejecución de estrategias de defensa. En estas áreas el INAOE posee una experiencia de más de 20 años, diseñando y creando sistemas de este tipo.

3. Definición del Perfil Profesional

3.1. Misión

El INAOE, como Centro Público de Investigación contribuirá al desarrollo científico y tecnológico del país mediante la formación de investigadores de alto nivel, capaces de adquirir, generar y aplicar conocimientos en el área de Tecnologías de Seguridad, específicamente en los campos de: ciberseguridad, criptografía, vigilancia de la red, IoTs, seguridad de la información, sistemas de tiempo real y sistemas optrónicos. Estos recursos humanos deberán contribuir al desarrollo de los sectores social, educativo, productivo y de salud en la región y en el país.

3.2. Visión

La Maestría en Tecnologías de Seguridad será reconocida nacional e internacionalmente como un programa de posgrado líder en la innovación y generación de conocimiento científico y tecnológico en el área de seguridad cibernética y sistemas optrónicos.

3.3. Propuesta

La Maestría en Tecnologías de Seguridad proporcionará a los estudiantes los conocimientos y habilidades tanto intelectuales como técnicas y tecnológicas para hacer frente a amenazas actuales y futuras en el campo de la seguridad cibernética y el diseño de sistemas optrónicos con un fuerte fundamento legal.

3.4. Objetivo

Formar maestros en ciencias con los conocimientos, habilidades y actitudes que les permitan liderar, analizar, diseñar, aplicar y evaluar ideas, proyectos y planes estratégicos de seguridad cibernética y diseño de sistemas optrónicos, conforme a las arquitecturas empresariales y alineadas con los objetivos de las organizaciones; todo ello ligado a los principios de actuación ética como estándares y regulaciones nacionales e internacionales en un marco legal de actuación.

3.5. Perfil de Ingreso

El candidato al programa de Maestría en Tecnologías de Seguridad debe cumplir con los siguientes requisitos:

- Tener el grado de ingeniería o licenciatura en una especialidad afín (ej. Telecomunicaciones, Tecnologías de la Información, Computación, Ciencias Computacionales, Ingeniería en Sistemas, Electrónica, Mecatrónica, Derecho y Psicología)
- Contar con un promedio mínimo de 8.0
- Haber acreditado exámenes de control y confianza
- Aprobar el examen de admisión
- Demostrar claramente vocación para los estudios de posgrado, la investigación y desarrollo tecnológico, estar altamente 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 puntuales.

3.6. Perfil de Egreso

Los egresados de la Maestría en Tecnologías de Seguridad contarán con los conocimientos y la experiencia necesaria para el diseño, supervisión, vigilancia y construcción de sistemas seguros y una base sólida en la criptografía, seguridad de redes, programación segura, sistemas de tiempo real y sistemas optrónicos. Los graduados dominarán los conocimientos para convertirse en líderes en el campo de la seguridad cibernética y electrónica y concebir las tecnologías que se desarrollarán en el futuro. Ellos estarán preparados para trabajar en el desarrollo de software seguro dentro de la industria del software y de TI, para el diseño de sistemas electrónicos y optrónicos o para convertirse en consultores de seguridad. También pueden optar por seguir adelante con la investigación doctoral.

El egresado contara con los siguientes conocimientos, dependiendo de la línea que escojan:

- Los principales hechos, conceptos, principios y teorías relativas a la seguridad informática.
- Teoría apropiada, prácticas y herramientas para el diseño, implementación y evaluación de sistemas informáticos seguros.
- Teoría apropiada, prácticas y procedimientos para la gestión y gobernanza de la seguridad cibernética.
- Teoria y práctica en el diseño de sistemas en tiempo real y sistemas optrónicos.

También alcanzarán las siguientes habilidades:

- La capacidad de aplicar el conocimiento y la comprensión que se ha indicado anteriormente para el análisis de un problema de manejo de la información dada.
- La capacidad de especificar, diseñar y construir sistemas informáticos y optrónicos seguros, utilizando las herramientas más apropiadas para documentar todas las etapas de este proceso.
- La capacidad de descubrir vulnerabilidades en implementaciones.
- La capacidad de evaluar los sistemas de software-hardware basados en Internet en relación con los requisitos de seguridad informática dados.
- Correlacionar la información sobre el comportamiento de los delitos cibernéticos.
- Analizar y resolver incidentes de seguridad Informática, manejando la información de manera segura acorde con las políticas de seguridad.

3.7. Plan de estudios

La Maestría en Tecnologías de Seguridad es semipresencial, en bloques de materias acumulables y no seriadas donde se consideran las condiciones laborales de la población objetivo, teniendo como soporte tecnológico una plataforma informática dedicada para dicha finalidad.

La maestría consta de tres niveles divididos en diferentes materias, cada materia tiene asignado un número de créditos, cuando el estudiante logre acumular 82 créditos y la elaboración y aprobación de tesis, estará en condiciones de acreditar el nivel maestría. Si el estudiante junta 38 créditos podrá ser acreedor a un certificado a nivel especialidad.

El nivel básico de la maestría consta de 3 materias básicas de su elección y la materia de Marco Normativo e Interpretación. El nivel intermedio consta de 3 tópicos avanzados de su elección y el módulo de Metodología de la Investigación. En el nivel avanzado el estudiante cursará 2 materias de especialidad de su elección y el seminario de desarrollo tecnológico.

Finalmente, cuando el estudiante haya completado los tres niveles, el estudiante estará completamente dedicado al desarrollo de su tesis. La tesis será dirigida por un investigador del INAOE y co-asesorada por un miembro externo perteneciente a alguna organización de seguridad cibernética 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. Así mismo, se ofrecerán cursos optativos de inglés ya que es requisito obtener un puntaje de 500 puntos en el TOEFL para obtener el grado de Maestro.

Para ambos cursos se realizará un examen de ubicación y no tendrán medida de carga académica (créditos).

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

	Cursos	Créditos
NIVEL BÁSICO	3 Materias de Nivel Básico	24
	Marco Normativo e Interpretación	6
	Total	**30**
NIVEL INTERMEDIO	3 Materias de Nivel Intermedio	24
	Metodología de la Investigación	6
	Total	**30**
NIVEL AVANZADO	2 materias de Nivel Avanzado	16
	Seminario de Desarrollo Tecnológico	6
	Total	**22**
TESIS	Desarrollo y aprobación de tesis	0
	Total	**0**
Total		**82**

Nivel Básico				
Curso	**Descripción**	**Horas presenciales**	**Horas en plataforma**	**Créditos**
Marco Normativo e Interpretación	Marco legal, Tipificación de los delitos, Armonización legislativa en materia de delitos cibernéticos, Convenio de Budapest	32	32	8
Conductas Ilícitas	Suplantación de identidad, extorción, amenazas, ciberbullyng, grooing, sextorsion, pederastia, lenocinio, turismo sexual, trata de personas, corrupción de menores y pornografía infantil.	32	32	8

Cursos				Créditos
Estrategias de Prevención de Delitos Cibernéticos	Introducción a los delitos cibernéticos, seguridad de la información, la guerra de la información y la evolución del internet, principales actividades que realizan las personas en internet, las mejores prácticas en la prevención, monitoreo de la red pública.	32	32	8
Amenazas dentro del Internet	Buscadores y redes sociales, correo electrónico, compras y ventas, pago de servicios, descargas, localización, juegos, redes sociales, cámaras de vigilancia, fraude electrónico, Phising y Smishing, Virus informáticos, información pública, suplantación de identidad.	32	32	8
Delitos Electrónicos contra la Información	Infraestructura critica, empresas, instituciones académicas, instituciones privadas, seguridad de la información, seguridad lógica, seguridad física, seguridad administrativa, confidencialidad, tipos de amenazas, evaluación de riesgos, técnicas de aseguramiento.	32	32	8
Ataques Cibernéticos I	Alteración de contenidos web, infección por código malicioso, configuración de seguridad de sistemas, divulgación de información no autorizada, envió de correos spam, ingeniería social, como preservar evidencia digital.	32	32	8
Internet de las Cosas (IoT) I	Historia, arquitectura hardware/software de un IoT, plataformas de desarrollo, estándares, introducción al diseño de IoT.	32	32	8
Sistemas Embebidos	Se analizarán las arquitecturas típicas de sistemas hw/sw a la medida para aplicaciones específicas de alto rendimiento	32	32	8
Instrumentación	Se analizarán las técnicas de instrumentación industrial y militar para sistemas optrónicos según las especificaciones de diseño	32	32	8
Estructuras de Datos y Algoritmos	Requisitos previos: Programación, Estructuras de Datos y Algoritmos. Se realizará el estudio de los fundamentos de las estructuras de datos y algoritmos; se presentarán las definiciones, representaciones, algoritmos de procesamiento de estructuras de datos, diseño general y técnicas de análisis de algoritmos.	32	32	8
Sistemas en tiempo real	Requisitos previos: Electrónica digital. Programacion. Se realizará el estudio de los fundamentos de los sistemas basados en tiempo real; se presentarán las definiciones, representaciones, diseños funcionales y diseños a detalle de sistemas en tiempo real. Hilos de operación, semáforos, concurrencia.	32	32	8
Diseño de Sistemas de Gestión de Datos.	Requisito: Conocimiento de estructuras en C y de base de datos. Se obtendrá el conocimiento de las nociones fundamentales de la tecnología de base de datos relacional (propiedades matemáticas y el uso de lenguajes de programación de base de datos); los métodos de diseño de base de datos y el modelado conceptual; métodos de almacenamiento físico para la información de la base de datos (nociones fundamentales de control de concurrencia y recuperación en los sistemas de bases de datos).	32	32	8

Nivel Intermedio				
Curso	**Descripción**	**Horas presenciales**	**Horas en plataforma**	**Créditos**
Internet de las Cosas (IoT) 2	Plataformas de desarrollo Hw/Sw, almacenamiento en memoria, procesamiento digital de señales, sensores y actuadores, sistemas de comunicación inalámbrica, encriptado e integridad de la información, dispositivos híbridos, vulnerabilidades de los IoT	32	32	8
Diseño de sistemas de vigilancia	Plataformas de desarrollo Hw/Sw, almacenamiento en memoria, procesamiento digital de señales, sensores y actuadores, sistemas de comunicación, camáras de video, dispositivos mecánicos.	32	32	8
Sistemas Inerciales	El problemas de la estabilización, acelerómetros y giroscopos, algoritmos de sensado de posición, arquitecturas Hw/sw para sistemas de estabilización, implementación de algoritmos	32	32	8
Algoritmos de seguimiento y filtros	Analisis de algoritmos de procesamiento de imágenes y comparación de desempeño, filros predictivos, seguimiento de objetos en tiempo real.	32	32	8
Protocolos de comunicación	I2C, Can Bus, Ethercat, NMEA, Arink, 1553, Sercos, implementación de protocolos en tiempo real	32	32	8
Sistemas de Control:	Teoría de control, definición de requerimientos de sistemas optronicos, arquitecturas de control, implementación de algoritmos de control bajo	32	32	8

	especificaciones predeterminadas.			
Seguridad en dispositivos móviles	Definiciones y conceptos, arquitectura y diseño, dispositivos inalámbricos, vulnerabilidades, amenazas, legislación en redes inalámbricas, técnicas de ataques a plataformas inalámbricas, medidas de seguridad, sistemas Operativos, Bluetooth,	32	32	8
Malware amenazas y ataques	Seguridad informática, historia del malware, técnicas de propagación, entorno de análisis seguro, escaneo y perfilado, análisis estático y dinámico, herramientas para el análisis, herramientas de prevención y protección.	32	32	8
Ciberpatrullaje	Aplicación de navegadores/buscadores y herramientas especiales para realizar el Ciberpatrullaje. Elaborar informes del Ciberpatrullaje.	32	32	8
Ataques Cibernéticos 2	Navegadores, lenguaje HTML, navegación anónima, TOR, Whois, Maltengo,Kali Linux,Tweet Deck, Awesome Screenshot, Evil foca, BeCyPDF, MetaEdit, Aplicaciones para el monitoreo de Incidentes, Fraudes al sector financiero, Carding, Deep web.	32	32	8
Criptografía y Seguridad.	Este curso se estudiarán métodos computacionales que proporcionan una comunicación segura a Internet. Entre los temas que se tratan son: amenazas a la seguridad en los sistemas de comunicación; la criptografía convencional: códigos de sustitución y transposición; la distribución de la clave secreta a través de Internet; principios de la criptografía de clave pública; RSA y otros métodos de cifrado de clave pública; y el protocolo de firma digital.	32	32	8
Seguridad y Privacidad en Informática de Sistemas.	Requisitos previos: Conocimiento básico de los sistemas operativos, redes, algoritmos y estructuras de datos y capacidad de programar en Java y C / C ++. El curso cubre los principios fundamentales de la construcción de sistemas y técnicas seguras para garantizar la seguridad de los datos y la privacidad. Los temas incluyen mecanismos de control de acceso, seguridad de los sistemas de explotación, amenazas de código malicioso y seguridad de software, confiabilidad informática, protección de contenido y la seguridad de base de datos.	32	32	8
Internet y los protocolos de capa superior.	El curso introduce a los protocolos y estándares del conjunto de protocolos TCP / IP que rigen el funcionamiento de Internet; se discutirán los protocolos alternativos a la suite TCP / IP y nuevos protocolos adoptados por esta suite; se analizarán ejemplos numéricos relacionados con la planificación de la red y el funcionamiento proocol.	32	32	8
Protocolos de seguridad en la red.	Requisitos previos: Internet y los protocolos de capa superior y la capacidad de programar en Java y C / C ++. Este curso cubre la seguridad de los protocolos de red utilizados actualmente en Internet. Los temas incluyen sistemas de autenticación y seguridad de enrutamiento, cortafuegos, detección de intrusiones, sistemas trampa, seguridad de la red inalámbrica, el malware, la propagación y la detección y seguridad web.	32	32	8
Técnicas de Hacking Ético.	Requisitos previos: Seguridad y Privacidad en Informática de Sistemas, Gestión de Redes y Seguridad, Protocolos seguridad de la red. Este curso cubre técnicas avanzadas que pueden ser utilizados para objetivos ofensivas o defensivas en la red, sistemas y aplicaciones informáticas. Los temas cubiertos incluyen organizaciones de memoria del sistema, registros de la CPU, los fundamentos del lenguaje ensamblador, GNU y depuradores de inmunidad, fuzzing el desarrollo de pruebas de seguridad en base de exploits locales y remotos Linux y Windows, desarrollo de código shell, ataques sigilosos.	32	32	8
Gestión de Redes y Seguridad.	Requisitos previos: Redes Computacionales- Arquitecturas, protocolos y normas o Internet y los protocolos de capa superior o ordenadores Red Diseño y análisis. Se estudiará la tecnología de seguridad de red existente y las diversas técnicas prácticas que se han implementado para proteger los datos contra la divulgación, para garantizar la autenticidad de los mensajes, y para proteger los sistemas de los ataques basados en la red.	32	32	8
Redes de	Requisitos previos: Manejo de un lenguaje de programación de alto nivel.	32	32	8

Computacionales-arquitecturas, protocolos y normas.	Se estudiarán varios estándares de arquitectura de red y de protocolo; con énfasis en el modelo de sistemas abiertos Interconnetion (OSI). Los temas incluyen: la transmisión analógica y digital, circuitos y conmutación de paquetes, la Red Digital de Servicios Integrados (RDSI), Frame Relay, RDSI de banda ancha, teléfono Relay, SONET, redes de área local (CSMA / CD, Token Bus, Token Ring, se cambió y isócrona ethernets), redes de área metropolitana (FDDI FDDI-II, DQDB), redes inalámbricas y por satélite, control de sincronización y el error, la expedición y control de congestión, norma X.25.			

Nivel Avanzado				
Curso	**Descripción**	**Horas presenciales**	**Horas en plataforma**	**Créditos**
Integración de carpetas de investigación	Elaboración de carpetas de investigación relacionadas con delitos cibernéticos	32	32	8
Incidentes	Esquema general de recuperación de incidentes, ciclo de respuesta de incidentes, medidas preventivas, análisis de riesgos, procedimientos y políticas de seguridad, controles automatizados, equipo de respuesta a incidentes, simulacros, detección de incidentes, administración de incidentes, reportes de incidentes, procedimientos de contingencia, de respaldo de información, análisis forense de equipos de cómputo.	32	32	8
Sistemas de detección y prevención de intrusos	Seguridad informática, conceptos de detección y prevención, Tipos de IDS/IPS, amenazas persistentes avanzadas, metodologías de detección, progresión de la amenaza, reconocimiento, herramientas para la detección de trafico sospechoso, monitoreo de seguridad de red.	32	32	8
Análisis de vulnerabilidades y pruebas de penetración	Metodologías de pruebas de penetración, análisis de vulnerabilidades, recopilación de la información, reconocimiento, mapeo, descubrimiento, explotación, pruebas de penetración exterior e interior. Penetración al firewall, métodos de penetración a una aplicación web.			
Filtros para determinación de objetivos	Balística, problemas de apuntado, triangulación, alineación de sistemas de referencia, filtros predictivos, solución de apuntado por concurrencia en sistemas móviles, caracterización de blancos.	32	32	8
Diseño de sistemas mecánicos	Mejores prácticas. Definición de requerimientos, control de calidad, diseño, sistemas de simulación, problemas de alineación. Sistemas de construcción y máquinado. Verificación de funcionalidades.	32	32	8
Sincronización y caracterización de sistemas robóticos complejos	Paralelismo computacional, arquitecturas paralelas, señales de sincronización, sincronización de arquitecturas en tiempo real. Definición de protocoles de pruebas, cálculo de latencia, tiempos de respuesta, error total,	32	32	8
Sistemas Distribuidos.	En este curso de tratarán temas relativos al diseño e implementación de sistemas informáticos distribuidos, incluyendo la comunicación entre procesos, llamadas a procedimiento remoto, autenticación, protección, sistemas de archivos distribuidos, las transacciones distribuidas, los datos replicados, los protocolos de transmisión fiables y especificaciones de los programas distribuidos.	32	32	8
Marca de Agua Digital.	Se estudiará la marca de agua digital y la esteganografía su importancia para asegurar la seguridad de datos en multimedia. Marca de agua digital es una herramienta adecuada para identificar la fuente, creador, propietario, distribuidor o consumidor autorizada de un documento o una imagen esteganografía digital tiene por objeto ocultar la información digital en los canales secretos, así que uno puede ocultar la información y evitar la detección. Este curso se proporcionará a los estudiantes una visión general sobre diferentes aspectos de los mecanismos y técnicas para la marca de agua digital y la esteganografía.	32	32	8
Minería de datos.	Este curso cubre los principios de diseño y aplicación de sistemas de minería de datos. Presenta métodos para la asociación y análisis de la dependencia, así como la clasificación, predicción, y la agrupación. Los temas que se pueden incluir son: series de tiempo y minería gráfica, las tendencias actuales en la minería de datos, y minería de datos para aplicaciones científicas, económicas, de seguridad y de ingeniería.	32	32	8
Computación en la nube.	Requisitos previos: Sistemas Distribuidos, Internet y los protocolos de capa superior.	32	32	8

	Este curso presenta una visión de arriba hacia abajo de la computación en la nube, las aplicaciones y la administración de la programación y la infraestructura. Su atención se centra en las técnicas de programación paralela de la nube sistemas distribuidos a gran escala que forman la infraestructura de computación en la nube y. Los temas incluyen: visión general de la computación en nube, sistemas de nubes, el procesamiento paralelo en la nube, sistemas de almacenamiento distribuidos, virtualización, asegurar la computación distribuida, y la programación multinúcleo.			
Seguridad avanzada de datos y privacidad.	Requisitos previos: Criptografía y Seguridad , Seguridad y privacidad en Informática de Sistemas , Gestión de Redes y Seguridad. En este curso se analizan cuestiones de seguridad y privacidad asociados con la enorme cantidad de datos que se recogen, almacenan, comparten y distribuyen en la sociedad actual. Se necesitan nuevos paradigmas para abordar la seguridad / privacidad desafía cuando los datos se externaliza a los servidores no son de confianza (como en la computación en nube), cuando los datos se convierten en anónimos, a fin de ser compartido entre las partes no son de confianza, o datos cuando con derechos de autor debe ser protegido del uso no autorizado .	32	32	8
Auditoría Forense para la Seguridad de la computación.	En este curso se determinará cuando una auditoría forense informática es la adecuada para la identificación y recolección de evidencia informática, dado que los dispositivos están involucrados en violaciones de seguridad a través de delitos o violaciones políticas, o son blanco de un ataque. Los principales temas de este curso son la preservación, identificación, extracción, documentación, adquisición, análisis e interpretación de los datos informáticos.	32	32	8
Administración y Seguridad en Redes Inalámbricas.	Este curso introduce a los fundamentos de la seguridad de la red inalámbrica y la administración. Los temas incluyen: vulnerabilidades inalámbrica a internet, ataques inalámbricos pasivos y activos, seguridad de hardware inalámbrico de la empresa, la autenticación inalámbrica segura y la comunicación, detección de intrusiones inalámbricas y sistemas de prevención, WiFi y gestión de la red celular, privacidad de la ubicación, la administración de redes de área personal y la seguridad, la seguridad de IP para móviles , GSM, CDPD, 3G y 4G seguridad de la red.	32	32	8
Electrónica Forense.	Requerimientos previos: electrónica En este curso se analizan los componentes electrónicos y los métodos para extraer información de dispositivos electrónicos (celulares, PC´s, lap top, etc.) dañados sin comprometer la evidencia y preservando la información sensible.	32	32	8
Tratamiento Automático de Texto.	Este curso analiza métodos y algoritmos para el análisis de texto escrito en lenguaje natural, lo cual permite obtener información y relaciones implícitas.	32	32	8
Reconocimiento de Patrones.	Requisitos Previos: probabilidad y estadística. En este curso se estudiarán algoritmos para extracción de características para identificar, clasificar y relacionar entidades, lugares u objetos.	32	32	8
Análisis Digital de Imágenes.	Se analizaran los posibles problemas de las imágenes; métodos y algoritmos para la adquisición y procesamiento de imágenes a color y monocromáticas; procedimientos de realce de imágenes para corregir problemas de background y ruido, destacar bordes de objetos y segmentar determinadas características de la imagen; herramientas simples de medida para resolver problemas en morfometría, densitometría, conteo y análisis de objetos múltiples, para la extracción de información útil de acuerdo al contexto de análisis.	32	32	8

3.8. Formas de evaluación

Las formas de evaluación de la Maestría en Ciencias en Tecnologías de Seguridad son las siguientes:

- Exámenes parciales y examen final.
- Reportes de trabajos de investigación.
- Prácticas de laboratorio y reportes de las mismas.
- Realización de simulaciones y reportes de las mismas.
- Realización de proyectos y presentación o reportes de los mismos.

4. Factibilidad Académica

La planta docente de este nuevo programa está conformada por investigadores adscritos a las coordinaciones del INAOE. Todos ellos tienen los conocimientos y experiencia necesarios para participar en este programa y cumplir los objetivos del mismo.

La planta docente de la Maestría en Tecnologías de Seguridad estará conformada inicialmente por 13 investigadores del INAOE.

En la siguiente tabla se enlista el nombre de los investigadores pertenecientes al núcleo académico básico, el tipo de nombramiento en el INAOE, su nivel en el SNI, así como la coordinación de adscripción.

Investigador	Nivel SNI	Coordinación
Dr. Saúl Eduardo Pomares Hernández	I	Ciencias Computacionales
Dra. Hayde Peregrina Barreto	C	Ciencias Computacionales
Dr. Reydezel Torres Torres	II	Electrónica
Dr. Eduardo F. Morales Manzanares	III	Ciencias Computacionales
Dra. Claudia Feregrino Uribe	I	Ciencias Computacionales
Dr. René A. Cumplido Parra	II	Ciencias Computacionales
Dr. José Martínez Carranza	C	Ciencias Computacionales
Dra. Alicia Morales Reyes	I	Ciencias Computacionales
Dr. Leopoldo Altamirano Robles	II	Ciencias Computacionales
M.C. Iván Olivera Romero	-	Ciencias Computacionales
M.C. David Tenorio Pérez	-	Ciencias Computacionales

Síntesis curricular de la planta académica.

Dr. Saúl Eduardo Pomares Hernández
Nivel SNI: I

Estudió la Ingeniería en Ciencias Computacionales en el Instituto Tecnológico de Veracruz, cursó la Maestría en Ciencias en Ingeniería Eléctrica y Telecomunicaciones en el Centro de Investigaciones y de Estudios Avanzados del Instituto Politécnico Nacional en Guadalajara. Y el Doctorado en el área de Ciencias Computacionales y Telecomunicaciones en el Institute National Polytechnique de Toulouse en Francia. Hizo una estancia doctoral en el Centre National de la Recherche Scientifique en Francia. Actualmente es investigador y Coordinador de Ciencias Computacionales en el Instituto Nacional de Astrofísica Óptica y Electrónica.

Publicaciones más recientes/relevantes:

- "The Minimal Dependency Relation for Causal Event Ordering in Distributed Computing," Saul e. Pomares Hernandez, Applied Mathematics & Information Systems, Eds, Natural Publ., Vol. 9, No. 1, 2015.
- "Temporal alignment model for data streams in wireless sensor networks based on causal dependencies," Jose Roberto Perez Cruz, Saul E. Pomares Hernandez, International Journal of Distributed Sensor Networks, Eds. Hindawi, Vol. 2014, No. 938698, 2014.
- "A Scalable Communication-Induced Checkpointing Algorithm for Distributed System," Alberto Calixto, Saul E. Pomares Hernandez, Jose Roberto Perez Cruz, Pilar Gomez-Gil and Khalil Drira, Transactions on Information Systems, Eds. IEICE, Vol. E96-D, No. 4, 2013, pp. 886-896.
- "From the Happened-Before Relation to the Causal Ordered Set Abstraction," Saul E. Pomares Hernandez, Jose Roberto Perez Cruz and Michel Raynal, Journal of Parallel and Distributed Computing (JPDC), Eds. Elsevier, Vol. 72, No. 6, 2012, pp. 791-795, ISSN: 0743-7315, http://dx.doi.org/10.1016/j.jpdc.2012.02.015.

Dra. Hayde Peregrina Barreto
Nivel SNI: C

Obtuvo su Doctorado en Ingeniería por la Universidad Autónoma de Querétaro. Ha trabajado en la Universidad Autónoma de Querétaro, Universidad de Guanajuato, Universidad Politécnica de Puebla y el Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE). Actualmente es Investigador Titular A en la Coordinación de Ciencias Computacionales del INAOE.

Publicaciones más recientes/relevantes:

- D. Hernandez-Contreras, H. Peregrina-Barreto, J. Rangel-Magdaleno, J. Ramirez-Cortes, F. Renero-Carrillo (2015). Automatic Classification of Thermal Patterns in Diabetic Foot based on Morphological Pattern Spectrum, Infrared Physics & Technology, 73, 149-157 (Q2 JCR)
- Reta, C., Altamirano, L., Gonzalez, J. A., Diaz-Hernandez, R., Peregrina, H., Olmos, I., Alonso, J., & Lobato, R (2015). Segmentation and Classification of Bone Marrow Cells Images Using Contextual Information for Medical Diagnosis of Acute Leukemias. PloS one, 10(6), e0130805. (Q1 JCR)
- Arias-Cruz, J. A., Perez-Corona, C. E., Peregrina-Barreto, H., Ramos-Garcia, R., & Ramirez-San-Juan, J. C. (2015, August). Visualization of deep blood vessels in speckle imaging using homogeneity measurement of the co-occurrence matrix. In SPECKLE 2015: VI International Conference on Speckle Metrology (pp. 96601O-96601O). International Society for Optics and Photonics.
- Hernandez-Contreras, D., Peregrina-Barreto, H., Rangel-Magdaleno, J., Ramirez-Cortes, J., Renero-Carrillo, F., & Avina-Cervantes, G. (2015, May). Evaluation of thermal patterns and distribution applied to the study of diabetic foot. In Instrumentation and Measurement Technology Conference (I2MTC), 2015 IEEE International (pp. 482-487).

- Peregrina-Barreto, H., Morales-Hernandez, L. A., Rangel-Magdaleno, J. J., Avina-Cervantes, J. G., Ramirez-Cortes, J. M., & Morales-Caporal, R. (2014). Quantitative estimation of temperature variations in plantar angiosomes: a study case for diabetic foot. Computational and mathematical methods in medicine, 2014. (Q4 JCR)

- Herrera-Navarro, A. M., Terol-Villalobos, I. R., Jiménez-Hernández, H., Peregrina-Barreto, H., & Gonzalez-Barboza, J. J. (2014). Detection and Measurement of the Intracellular Calcium Variation in Follicular Cells.Computational and mathematical methods in medicine, 2014. (Q4 JCR)

Dr. Reydezel Torres Torres
Nivel SNI: II

Estudió la Ingeniería en Electrónica, en el Instituto Tecnológico de Querétaro, cursó la Maestría en Ciencias con Especialidad en Electrónica en el Instituto Nacional de Astrofísica, Óptica y Electrónica INAOE, fue estudiante doctoral visitante en la Universidad Católica de Lovaina, obtuvo el Doctorado en Ciencias con Especialidad en Electrónica en el INAOE. Actualmente es investigador de tiempo completo en el INAOE.

Publicaciones más recientes/relevantes:

- J. Molina, R. Torres-Torres, A. Ranjan, and K.-L. Pey, "Accurate modeling of gate tunneling currents in Metal-Insulator-Semiconductor capacitors based on ultra-thin atomic-layer deposited Al2O3 and post-metallization annealing," Thin Solid Films, Vol. 638, No. 1, pp. 48–56, Sep. 2017. ISSN: 0040-6090.
- D.M. Cortés-Hernández and R. Torres-Torres, "Modeling the Frequency-Dependent Series Parasitics of Ground–Signal–Ground Pads Used to Probe On-Wafer Microstrip-Line-Fed Devices," IEEE Transactions on Microwave Theory and Techniques, Vol. 65, No. 6, pp. 2085–2092, Jun. 2017. ISSN: 0018-9480.
- J. Molina, R. Torres-Torres, A. Ranjan, and K.-L. Pey, "Resistive switching characteristics of MIM structures based on oxygen variable ultra-thin HfO2 and fabricated at low temperature," Materials Science in Semiconductor Processing, Vol. 66, No. 1, pp. 191–199, Aug. 2017. ISSN: 1369-8001.
- A. Ortiz-Conde, A. Sucre-González, F. Zárate-Rincón, R. Torres-Torres, R.S. Murphy-Arteaga, J.J. Liou, and F.J. García-Sánchez, "A review of DC extraction methods for MOSFET series resistance and mobility degradation model parameters," Microelectronics Reliability, Vol. 69, No. 1, pp. 1–16, Feb. 2017. ISSN: 0026-2714.
  CITES:
  R. Trevisoli, R. Trevisoli D., M. de Souza, S. Barraud, M. Vinet, M. Cassé, G. Reimbold, O. Faynot, G. Ghibaudo, and M.A. Pavanello, "A New Method for Series Resistance Extraction of Nanometer MOSFETs," IEEE Transactions on Electron Devices. Volume 64, Issue 7, pp. 2997–2803, Jul. 2017.
- H. Cuchillo-Sánchez, F. Zárate-Rincón, and R. Torres-Torres, "Alternative Determination of the Intrinsic Cut-Off Frequency Applied to a Degraded MOSFET," IEEE Microwave and Wireless Components Letters, Vol. 26, No. 9, pp. 693–695, Sep. 2016. ISSN: 1531-1309.

  CITES:
  Z. Zhan, E. Colomés, and X. Oriols, "Limitations of the Intrinsic Cutoff Frequency to Correctly Quantify the Speed of Nanoscale Transistors," IEEE Transactions on Electron Devices. Volume 64, Issue 6, pp. 2617–2624, Jun. 2017.
- A. Ortiz-Conde, A. Sucre-González, R. Torres-Torres, J. Molina, R. S. Murphy-Arteaga, and F.J. García-Sánchez, "Conductance-to-Current-Ratio-Based Parameter Extraction in MOS Leakage Current Models," IEEE Transactions on Electron Devices, Vol. 63, No. 10, pp. 3844–3850, Oct. 2016. ISSN: 0018-9383.

Dr. Eduardo F. Morales Manzanares
Nivel SNI: III

Estudió la Licenciatura en Ingeniería Física en la Universidad Autónoma Metropolitana, cursó la Maestría en Information Technology: knowledge-based systems en la Universidad de Edimburgo, Edimburgo, Reino Unido. Y el Doctorado en Computación The Turning Institute – Universidad de Strathclyde. Actualmente es investigador de tiempo completo en el Instituto Nacional de Astrofísica Óptica y Electrónica.

Publicaciones más recientes/relevantes:

- Maxhuni, P. Hernandez-Leal, L.E. Sucar, V. Osmani, E.F. Morales, O. Mayora (2016). Stress Modelling and Prediction in Presence of Scarce Data. Journal of Biomedical Informatics 63: 344-356.
- E. Munoz de Cote, E.O. Garcia, E.F. Morales (2016). Transfer Learning by Prototype Generation in Continous Spaces. Adaptive Behavior: 1-15.
- A.C. Tenorio, E.F. Morales (2016). Automatic Discovery of relational concepts by an incremental graph-based representation. Robotics and Autonomous Systems 83: 1-14.
- A. Maxhuni. A. Muñoz-Meléndez, V. Osmani, H. Perez, O. Mayora, E.F. Morales (2016). Clasification of bipolar disorder based on analysis of voice and motor activity of patients. Pervasive and Mobile Computing 31: 50-66. DOI: 10.1016/j.pmcj.2016.01.008.

Dra. Claudia Feregrino Uribe
Nivel SNI: I

Estudió la Ingeniería en Sistemas Computacionales en el Instituto Tecnológico de Querétaro, cursó la Maestría Ingeniería Eléctrica con Especialidad en Telecomunicaciones en el Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional en Guadalajara. Y el Doctorado en Ingeniería Electrónica en Loughborough University, Reino Unido. Actualmente es investigadora de tiempo completo en el Instituto Nacional de Astrofísica Óptica y Electrónica.

Publicaciones más recientes/relevantes:

- Lázaro Bustio-Martínez, René Cumplido, Raudel Hernández-León, José M. Bande-Serrano, Claudia Feregrino-Uribe, On the design of hardware-software architectures for frequent itemsets mining on data streams, Journal of Intelligent Information Systems, May 2017, pp. 1-26. DOI 10.1007/s10844-017- 0461-8.
- Menéndez-Ortíz A., Feregrino-Uribe C., García-Hernández J.J., Guzman-Zavaleta Z.J., Self-recovery Scheme for Audio Restoration after a Content Replacement Attack, Multimedia Tools and Applications (2017), 76(12), 14197-14224. doi:10.1007/s11042-016-3783-6. (Online 11 August 2016).
- Jezabel Guzman-Zavaleta, Claudia Feregrino-Uribe, Miguel Morales-Sandoval, Alejandra Menendez-Ortiz, A robust and low-cost video fingerprint extraction method for copy detection, Multimedia Tools and applications. 2016, issn: 1573-7721, pp. 1-21. doi:10.1007/s11042-016-4168-6.
- Guzman-Zavaleta ZJ, Feregrino-Uribe C (2016) Towards a Video Passive Content Fingerprinting Method for Partial-Copy Detection Robust against Non-Simulated Attacks. PLoS ONE 11(11): e0166047. https://doi.org/10.1371/journal.pone.0166047

Dr. René Armando Cumplido Parra
Nivel SNI: II

Estudió la Ingeniería en Sistemas Computacionales en el Instituto Tecnológico de Querétaro, cursó la Maestría en Ciencias de la Ingeniería Eléctrica con Especialidad en Telecomunicaciones en el Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional en Guadalajara. Y el Doctorado en Ingeniería Electrónica con Especialidad en Sistemas Digitales, en la Universidad de Loughborough, Reino Unido. Actualmente es investigador de tiempo completo en el Instituto Nacional de Astrofísica Óptica y Electrónica.

Publicaciones más recientes/relevantes:

- "Improving the construction of ORB through FPGA-based acceleration", Roberto de Lima, Jose Martinez-Carranza, Alicia Morales-Reyes, Rene Cumplido. Machine Vision and Applications, August 2017, Volume 28, Issue 5-6, pp 525-537. Doi.org/10.1007/s00138-017-0851-5.
- "On the design of hardware-software architectures for frequent itemsets mining on data streams", Lázaro Bustio-Martínez, Rene Cumplido, Raudel Hernández-León, José M. Bande-Serrano, Claudia Feregrino-Uribe. Journal of Information Intelligent Systems, Springer. DOI 10.1007/s 10844-017-0461-8.
- "A Scalable and Customizable Processor Array for Implementing Cellular Genetic Algorithms", Martin Letras, Alicia Morales-Reyes, Rene Cumplido. Neurocomputing. Elsevier. Volume 175, Part B, 29 January 2016, Pages 899-910. ISSN: 0925-2312. DOI doi: 10.1016/j.neucom.2015.05.128.
- "Analysis of an Adaptive Watermarking Scheme Designed for Video Copyright Protection", Pedro Aaron Hernández-Grácidas, Ignacio Algredo-Badillo. International Journal of Computer Science and Information Security, IJCSIS, Vol. 14, No. 12, December Issue 2016.

Dr. José Martínez Carranza
Nivel SNI: C

BSc. in Computer Science, 2004 en la Benemérita Universidad Autónoma de Puebla, cursó la Maestría en Ciencias Computacionales en el Instituto Nacional de Astrofísica, Óptica y Electrónica, INAOE. Y su Doctorado en Ciencias Computacionales en la Universidad de Bristol. Facultad de Ingeniería .Bristol UK. Actualmente es investigador de tiempo completo en el INAOE.

Publicaciones más recientes/relevantes:

- De lima ,R, Martinez –Carranza ,J., Morales –Reyes , A . et. Al Machine Vision and (2017)28: 525.doi .org 1007/s00138-017-0851-5
- Cruz Martinez C.,Martinez , J Mayol-Cuevas , W . jrEAL- time Image Proc (2017).doi 10.1007/s11554-017-0707-2.
- H Jair Escalante , V Ponce –López ,S Escalera , X .Baró , A . Morales –Reyes , José Martínez – Carranza .E Voling weightingschemes for the Bag of Visual WORDS. Neural Computing and AppLICATIONS, PP.1-11 March 2016DOI:10.1007/s00521-0162223x

- Hugo Jair Escalante , MAURICIO García –Limón, Alicia Morales- Reyes, Graff, Manuel Montes y Gómez, Eduardo Morales, José Martínez Carranza "term- Weighting via Genetic y Gómez, Eduardo F. Morales," Programming for Tex Classification" , volumen 83,july 2015 pages 176-186 . DOI :10.1016/J knosys.2015.03025.
- Hugo Jair Escalante, Mauricio García-Limón, Alicia Morales-Reyes, Mario Graff, Manuel Montesy-Gómez, Eduardo F. Morales, José Martinez-Carranza. "Term-Weighting Learning via Genetic Programming for Text Classification". Knowledge-based Systems Journal, Elsevier. Volume 83, July 2015, Pages 176–189. DOI:10.1016/j.knosys.2015.03.025. 6. José Martínez-Carranza, Richard Bostock, Simon Willcoxb, Ian Cowling, Walterio MayolCuevas. Indoor MAV Auto-Retrieval Using Fast 6D Relocalisation. Advanced Robotics. pages 119- 130. Volume 30, Issue 2, February, 2015. DOI: 10.1080/01691864.2015.1094409.

Dra. Alicia Morales Reyes
Nivel SNI: I

Obtuvo una Licenciatura en Ingeniería Eléctrica y Electrónica de la Universidad Nacional Autónoma de México, Obtuvo una Licenciatura en Ingeniería Eléctrica y Electrónica de la Universidad Nacional Autónoma de México, terminó sus estudios doctorales en el Insitute for Integrated Micro and Nano Systems" (IMNS) de la Universidad de Edimburgo en Escocia, Reino Unido. Actualmente, colabora con el grupo de investigación en Ingeniería en Sistemas, en la coordinación de
Ciencias Computacionales del INAOE, como parte del programa de repatriación CONACyT

Publicaciones más recientes/relevantes:

- Jorge Echavarria, Alicia Morales-Reyes, Rene Cumplido, Miguel A. Salido, Claudia Feregrino-Uribe. "IP Cores Watermarking Scheme at Behavioral Level using Genetic Algorithms". Submitted to Expert Systems with Applications Journal (JCR 2.240), Elsevier. June 2015.
- Alicia Morales-Reyes, Hugo Jair Escalante, Martin Letras, Rene Cumplido. "An Empirical Analysis on Dimensionality in Cellular Genetic Algorithms". GECCO 2015: Proceedings of the 2015 Genetic and Evolutionary Computation Conference. ACM. July 11-15, 2015. Madrid, Spain. DOI: Pending.
- Hugo Jair Escalante, Mauricio García-Limón, Alicia Morales-Reyes, Mario Graff, Manuel Montes-y-Gómez, Eduardo F. Morales, and José Martinez-Carranza. "Term- Weighting Learning via Genetic Programming for Text Classification". Knowledge-based Systems Journal, Elsevier (JCR 2.947). Volume 83, July 2015, Pages 176–189. doi:10.1016/j.knosys.2015.03.025.

- Martin Letras-Luna, Alicia Morales-Reyes, Rene Cumplido. "A Scalable and Customizable Processor Array for Implementing Cellular Genetic Algorithms". Accepted for publication, Neurocomputing Journal, Elsevier (JCR 2.083). May 2015. doi: pending

Dr. Leopoldo Altamirano Robles
Nivel SNI: II

Estudió Licenciatura en Computación en la Universidad Autónoma de Puebla, cursó la Maestría en Ingeniería Eléctrica con Especialidad en Computación en el CINVESTAV. Y el Doctorado en Informática por la Universidad Técnica de Munich, Almania. Actualmente es Director General del Instituto Nacional de

Astrofísica, Óptica y Electrónica.

Publicaciones más recientes/relevantes:

- "A quantitative index for classification of plantar termal changes in the diabetic foot", D Hernandez-Contreras, H Peregrina-Barreto, J Rangel-Magdaleno, JA Gonzalez-Bernal, L Altamirano-Robles, Infrared Physics & Technology, Vol. 81, Pag. 242-249, 2017. 2015 Impact Factor 1.588. ISSN: 1350-4495. http://dx.doi.org/10.1016/j.infrared.2017.01.010.
- "Latent fingerprint identification using deformable minutiae clustering" Miguel Angel Medina-Pérez, Aythami Morales Moreno, Miguel Ángel Ferrer Ballester, Milton García-Borroto, Octavio Loyola-González, Leopoldo Altamirano-Robles. Neurocomputing. Volume 175, Part B, 29 January 2016, Pages 851-865. Impact Factor: 2.392 Cited: 1. ISSN: 0925-2312. http://dx.doi.org/10.1016/j.neucom.2015.05.130
- Automatic approach to solve the morphological galaxy classification problem using the sparse representation technique and dictionary learning", R Díaz-Hernández, A Ortiz-Esquivel, H Peregrina-Barreto, L Altamirano-Robles, J Gonzalez-Bernal, Experimental Astronomy, Vol. 41, Pag. 409-426, 2016. Impact Factor 2.867. ISSN: 0922-6435 (Print) 1572-9508 (Online). DOI 10.1007/s10686-016-9495-0
- "Segmentation and Classification of Bone Marrow Cells Images Using Contextual Information for Medical Diagnosis of Acute Leukemias" Carolina Reta, Leopoldo Altamirano, Jesus A. Gonzalez, Jose E. Alonso, Ruben Lobato. Published: June 24, 2015, PLoS ONE 10(7): e0134066. doi: 10.1371/journal.pone.0134066. Impact Factor: 4.411 Cited 4 no auto cited. ISSN 1932-6203. DOI:10.1371/journal.pone.0130805.

M.C. Iván Olivera Romero

Estudió la Licenciatura en Ciencias de la Computación en la Benemérita Universidad Autónoma de Puebla, cursó la Maestría en Ciencias Computacionales en el Instituto Nacional de Astrofísica, Óptica y Electrónica, INAOE y realizó un Master of Science in Technology Commercialization en el Centro de Investigación en Materiales Avanzados y The University of Texas al Austin. Actualmente es Director de Desarrollo Tecnológico en el INAOE.

Publicaciones más recientes/relevantes:

- I. Olivera Romero, L. Altamirano Robles y M. Arias Estrada. Segmentación temporal aplicada a la detección de objetos en movimiento en imágenes infrarrojas. Mexican International Conference on Artificial Intelligence, Taller de Análisis de Imágenes y Reconocimiento de patrones, 371-379, 2002.
- J. Cruz, J. Pedroza, L. Altamirano, and I. Olivera, A Performance Comparison of Estimation Filters for Adaptive Imagery Tracking. Proceedings of the Third IASTED International Conference on Signal Processing, Pattern Recognition and Application (SPRA 2006), Innsburuck, Austria. Pp. 20-25. February 2006.
- Altamirano Robles L., Olivera Romero I., García Flores H., Arenas Fernández J., Zenteno Guevara F. A., Sierra Rodríguez B., Hernández Blas J.E. Análisis de la criticidad de modos y efectos de

falla de subestaciones eléctricas de distribución de Comisión Federal de Electricidad. VII congreso Internacional en Innovación y Desarrollo Tecnológico, 7 al 9 de octubre de 2009, Cuernavaca, Morelos, México.

- L. Altamirano Robles, I. Olivera romero, F. A. Zenteno Guevara, L. A. Pérez Peláez, H. García Flores, B. Sierra Rodríguez, J. E. Hernández Blas, C. Fajardo Caja. Guía rápida para la identificación de fallas y acciones correctivas inmediatas en los transformadores de distribución que emplea la CFE, basado en la metodología del Análisis de los Modos y Efectos de Fallas (AMEF). VII Congreso Internacional en Innovación y Desarrollo Tecnológico, 7 al 9 de octubre de 2009, Cuernavaca, Morelos, México.

M.C. David Tenorio Pérez

Estudió la Ingeniería en Electrónica en la Benemérita Universidad Autónoma de Puebla, cursó la Maestría en Ciencias con Especialidad en Electrónica en el Instituto Nacional de Astrofísica, Óptica y Electrónica, INAOE. Actualmente es el Responsable del Laboratorio de Visión por Computadora en el INAOE.

Publicaciones más recientes/relevantes:

- Ecualización de Imágenes Implementadas en un FPGA, Diciembre 2002
- Arquitectura de Hardware para la Detección Sub-pixel de Bordes en Tiempo Real, Enero 2004
- Cuarto encuentro de Investigación INAOE. Visión Estéreo Empleando Detección de Contornos e Interpolación Sub-pixel, Septiembre 2003
- Congreso Internacional de Cómputo Reconfigurable y FPGAs (ReConFig04), Arquitectura Hardware para la Detección Sub-pixel de Bordes en Tiempo Real, David Tenorio Pérez, Miguel Arias Estrada, Octubre 2004

5. Apoyo Institucional e Infraestructura.

5.1. Apoyo Institucional.

El Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE) está totalmente comprometido con el desarrollo exitoso de los programas de posgrado ofrecidos. En el decreto de creación del INAOE se establece que la formación de recursos humanos altamente preparados es uno de los ejes de la actividad científica en el INAOE.

La totalidad de la planta de investigadores (132 a finales de 2015) colabora en los programas de posgrado en todos los aspectos (impartición de cursos, asesorías, seminarios, dirección de tesis, etc.). El INAOE provee todo el apoyo administrativo necesario para el desarrollo de los programas de posgrado a través de la Dirección de Formación Académica (DFA), el Departamento de Servicios Escolares de la DFA, y de cada Academia con la cual se asocia el programa de posgrado. La comunicación ágil y expedita entre estas instancias contribuye al buen funcionamiento y desarrollo de los diversos programas de posgrado ofrecidos por el Instituto.

El Instituto cuenta con los suficientes espacios físicos para las diferentes labores académicas, como son biblioteca, aulas, auditorios, laboratorios bien equipados, talleres y oficinas para estudiantes.

Todos los programas de posgrado del INAOE han recibido un fuerte y decidido apoyo de las autoridades, con los suficientes recursos económicos y humanos para su desarrollo y mejora continua. La Dirección General del INAOE asigna un presupuesto anual a la Dirección de Formación Académica para el apoyo a los diversos programas de posgrado. Este presupuesto (administrado por la DFA) se calendariza para las diferentes actividades en las que se apoya económicamente a los estudiantes: apoyo a estancias cortas de investigación en otras instituciones, gastos de asistencia a congresos (nacionales y en el extranjero), cursos de idiomas, compra de libros, fotocopias, etc.

Además de cursos inglés, el INAOE imparte cursos de redacción en español para sus estudiantes, en el siguiente cuadro se describen los cursos de inglés ofrecidos en el Instituto.

Cursos de Inglés
Inglés Básico I
Inglés Básico II
Inglés Intermedio I
Inglés Intermedio II
Inglés Avanzado I
Inglés Avanzado II
Taller de Conversación, Lectura y Redacción
Preparación al TOEFL

Después de que el estudiante concluya con sus estudios, deberá entregar un comprobante de aprobación de 550 puntos TOEFL o equivalente (requisito de egreso).

5.2. Infraestructura.

5.3. Espacios y Equipamiento

Se cuenta con 80 oficinas destinadas a la matrícula estudiantil, con una capacidad total de 400 estudiantes aproximadamente. Cada estudiante cuenta con un equipo de cómputo para la realización de sus actividades académicas. Además, se cuenta con salones de clase para que los estudiantes puedan implementar el plan de estudios de acuerdo a los programas que ofrece el INAOE.

5.4. Laboratorios

El posgrado a crear, cuenta con el apoyo de todas las Coordinaciones del INAOE, en cuanto a infraestructura utilizará Laboratorios de las Coordinaciones de Electrónica y Ciencias Computacionales.

En el caso de la Coordinación de Electrónica se utilizará:

- Laboratorio de Instrumentación. En la actualidad opera como un laboratorio de electrónica general y sus actividades comprenden el soporte experimental para los cursos del posgrado en electrónica y el soporte para desarrollo de tesis que involucran la construcción de sistemas electrónicos. En cuanto a su infraestructura cuenta con mesas de trabajo, equipos de medición y pruebas,

osciloscopios, generadores de funciones, fuentes, analizadores de espectro, etc. Cuenta con componentes electrónicos diversos y circuitos integrados.

- Laboratorio de Microelectrónica. En el laboratorio se ha desarrollado un proceso de fabricación CMOS de Circuitos Integrados (CIs), con geometría mínima de 10 micras. Con esta tecnología se han diseñado y fabricado CIs digitales de propósitos específicos. La inclusión de materiales compatibles con esta tecnología ha resultado en la obtención de sensores y transductores novedosos a los que se ha integrado la electrónica necesaria para su operación y lectura de señales eléctricas de salida en un solo CI. Actualmente se encuentra bajo desarrollo un proceso de fabricación BiCMOS con geometría mínima de 0.8 mm.
- Laboratorio de Procesamiento Digital de Señales. El objetivo principal del laboratorio de DSP (Procesamiento de Señales Digitales), es desarrollar nuevos algoritmos, técnicas y herramientas de diseño en varias áreas de DSP y dar a los estudiantes de posgrado la oportunidad de producir el más alto nivel de investigación en DSP. El enfoque adicional es sobre implementación de nuevos algoritmos de DSP, que permita a los estudiantes desarrollar las habilidades necesarias para trabajar con modernos sistemas DSP.
- Laboratorio de Pruebas y Caracterización de Circuitos Integrados. El objetivo del laboratorio es medir el desempeño de los dispositivos y circuitos integrados fabricados, a nivel encapsulado y/o nivel oblea, considerando características tales como: frecuencia de operación, ganancia, márgenes de fase, consumo de potencia, robustez a ruido, tolerancia a fallas, efectos de variaciones de proceso y ambientales (temperatura, ruido, radiación, etc.). Con base en los resultados obtenidos de estas mediciones, es posible sugerir mejoras a los dispositivos y circuitos integrados con el fin de lograr el desempeño deseado.

En el caso de la Coordinación de Ciencias Computacionales se utilizará:

- Laboratorio de Cómputo y Procesamiento Ubicuo. El objetivo principal es proporcionar un espacio de trabajo para los investigadores del INAOE, estudiantes de posgrado e invitados, donde puedan desarrollar proyectos científicos y tecnológicos en las áreas relacionadas con cómputo y procesamiento ubicuo.
- Laboratorio de Visión por Computadora. El laboratorio de Visión por Computadora pertenece a la Coordinación de Ciencias Computacionales. En el laboratorio se realiza investigación básica y aplicada, así como prestación de servicios a la industria nacional. Sus principales áreas de investigación son: Análisis de Imágenes, Sistemas de Información, Simulación, Confiabilidad de Equipos, Ingeniería de Software y Aplicaciones Industriales de la Visión por Computadora
- Laboratorio de Súper computo con una capacidad de 12 teraflops, servirá de apoyo para las pruebas de laboratorio de diferentes algoritmos, big Data y minería de datos.

En cuanto a Servicios Tecnológicos se empleará:

- Laboratorio de Diseño Mecánico. El laboratorio fue fundado en 2002 como parte de un Plan Estratégico de la Dirección de Desarrollo Tecnológico del INAOE, para desarrollar la mecánica de alta precisión. El propósito fundamental es el desarrollo de sistemas opto-mecánicos, sistemas robóticos e instrumentos auxiliares que pueden ayudar a las pruebas de laboratorio, la ejecución o instalación de los sistemas desarrollados.