Especialidad en Seguridad de la Información

IBERO
Ciudad de México • Tijuana ®

INDICE

ESTRUCTURA DEL PLAN DE ESTUDIOS

OBJETIVOS

GENERAL

Formar profesionales capaces de establecer estrategias de Seguridad de la Información, basadas en estándares internacionales y el marco normativo para el análisis, el diseño y el desarrollo de mecanismos y herramientas de seguridad de manera ética que fortalezcan los objetivos de las instituciones y el bienestar de las personas.

ESPECIFICOS

- Detectar necesidades de seguridad de la información alineadas a los objetivos del negocio.
- Identificar los riesgos y las mejores prácticas en la seguridad de la información para que las organizaciones logren sus objetivos.
- Utilizar técnicas y metodologías de seguridad de la información para la gestión de incidentes en los sistemas computacionales e informáticos.
- Aplicar metodologías y técnicas de protección de la información, de manera ética y con base en el uso de diversas herramientas de seguridad informática, y la normatividad sobre privacidad de datos y medidas de ciber seguridad.

PERFIL DE INGRESO

Conocimientos

- Medios y formatos electrónicos para la comunicación.
- Metodologías para recopilar, organizar, analizar y sintetizar la información empleando herramientas de la TI.
- Uso de información y selección de herramientas (tecnológicas) apropiadas para resolver problemas.

Habilidades

- Análisis y síntesis para consulta de información especializada.
- Elaboración de conclusiones y generalizaciones a partir de la información recopilada.
- Planeación y organización del trabajo con orientación hacia resultados.

- Comunicar ideas con claridad oralmente y por escrito.
- Abstracción de problemas de forma estructurada.
- Actitudes
- Disponibilidad para el trabajo en equipo.
- Responsabilidad social y laboral
- Interés por la tecnología.
- Interés por el entorno socioeconómico y productivo.
- Ética en todo su actuar
- Autoaprendizaje
- Actualización continúa.

REQUISITOS DE INGRESO

Egresados de Licenciaturas de las áreas de Ingeniería, Computación e Informática o programas afines, preferentemente con experiencia en el manejo de las áreas de sistemas de información, computación e informática en empresas industriales, de servicios o en instituciones de gobierno.

PERFIL DE EGRESO

El especialista de la Seguridad de la Información es un profesional capaz de integrar: la auditoría, los riesgos, la criptografía y la forencia de TI para lograr detectar y controlar vulnerabilidades en los sistemas organizacionales.

MAPA CURRICULAR

1er. semestre	2do. semestre	Verano
Administración de riesgos de tecnología de información	**Seguridad de tecnología de información**	**Herramientas de seguridad de la información**
4/2	4/2	6/4
Auditoría en tecnología de información	**Certificación y estándares de tecnología de información**	**Buenas prácticas de seguridad de la información**
4/2	4/2	6/4
Gestión del servicio de tecnología de información	**Dirección de proyectos de tecnología de información**	
4/2	4/2	

Gestión de incidentes	Tópicos de seguridad de TI
5/3	5/3

Nota: créditos / horas

DESCRIPCIÓN DE LAS ASIGNATURAS

NOMBRE DE LA ASIGNATURA	SIGLA			HSS	CRÉDITOS
ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN	PS1827	**TEORÍA**	X	2	4
		PRACTICA		0	0
	PERREQUISITOS	**TOTAL**		2	4

COORDINACIÓN
SIS POSGRADO EN SISTEMAS

Objetivos generales

Al final del curso el alumno será capaz de:

1. Analizar los estándares internacionales para la administración de riesgos en tecnología de información.
2. Explicar los elementos relevantes de la certificación en sistemas de información de riesgos y control (CRISC).
3. Valorar los riesgos de tecnología de información con base en los principios de gestión.

Temas principales

1. Conceptos básicos y factores de riesgos en la seguridad de la información.
2. La administración de riesgos y su relación con el gobierno de riesgos.
3. Gestión de riesgos y marcos de referencias: ISO 31000, ISO 27005.
4. Certificación de sistemas de información y control de riesgos (CRISC).
5. La evaluación de riesgos y su relación entre las mejores prácticas de tecnología de información.

Bibliografía

Bravo Mendoza, Oscar. Gestión Integral de Riesgos. Tomo I. Colombia Bravo & Sánchez, 2006.

Buchtik, Liliana. Secretos para dominar la Gestión de Riesgos en Proyectos. Montevideo, Uruguay: Buchtikglobal, 2016.

ISACA. The risk IT framework: principles, process details, management guidelines, maturity models. USA:ISACA, 2009.

NOMBRE DE LA ASIGNATURA	SIGLA			HSS	CRÉDITOS
AUDITORIA EN TECNOLOGIA DE INFORMACION	PS1828	**TEORÍA**	X	2	4
		PRACTICA		0	0
COORDINACIÓN	**PERREQUISITOS**	**TOTAL**		2	4
SIS POSGRADO EN SISTEMAS					

Objetivos generales

Al final del curso el alumno será capaz de:

1. Determinar los estándares, lineamientos y mejores prácticas de los objetivos de control de Tecnología de Información (COBIT) para los servicios de auditoría.
2. Identificar los elementos fundamentales para la protección de los activos de la información de una empresa.
3. Explicar los elementos relevantes de la certificación de auditoria en sistemas de información (CISA).

Temas principales

1. Introducción al proceso de control de tecnología de información.
2. Fundamentos de los objetivos de control para la información y tecnologías relacionadas (COBIT).
3. Proceso de auditoría de tecnología de información.
4. Continuidad del negocio y recuperación de desastres.
5. Certificación de auditoria en sistemas de información (CISA).

Bibliografía

ISACA. Sharepoint Deployment and Governance Using COBIT 4.1: A Practical Approach.USA: ISACA, 2010

IT Governance Institute.CIBIT 4.1: framerwork, control objetives, management guidelines, maturity models. USA: ISACA, 2007

Muñiz González, Luis. Como implantar y evaluar un sistema de control de gestión: incluye cuestionarios de evaluación. España: Profit Editorial, 2013

Piattini Velthuis, Mario, Emilio del Peso Navarrete y Mar de Peso Ruiz. Auditoria de tecnologías y sistemas de información.
España; Ra-Ma, 2008.

NOMBRE DE LA ASIGNATURA	SIGLA			HSS	CRÉDITOS
BUENAS PRACTICAS DE SEGURIDAD DE LA INFORMACION	PS1847	**TEORÍA**	X	2	4
		PRACTICA	X	2	2
	PERREQUISITOS	**TOTAL**		4	6
COORDINACIÓN					
SIS POSGRADO EN SISTEMAS					

Obejtivos generales

Al final del curso el alumno será capaz de:

1. Aplicar conceptos y principios de ingeniería social a un caso de ciberseguridad.
2. Desarrollar un modelo de gestión de la continuidad del negocio para prevenir y afrontar los riesgos que amenazan a la organización.
3. Utilizar las metodologías de pruebas de penetración en un prueba de haking ético.

Temas principales

1. Concienciación en seguridad de la información.
2. Resiliencia informática.
3. Continuidad del Negocio.
4. Hacking Ético.
5. Desarrollo de aplicaciones con seguridad de la información.

Bibliografía

Caballero Velasco, Maria Angeles, Diego Cilleros Serrano y Abtin Shamsaifar. . El libro del Hacker. España: Anaya, 2014.

Escrivá Gascó, Gema, Rosa Ma. Romero Serrano, David Jorge Ramada y Ramon. Onrubia Perez. Seguridad Informatica

Mexico: Macmillan ,, 2013

Gomez Vieites, Álvaro, Gestion de Incidentes de Seguridad Informatica.. España: Starbook, 2011.

Ramos Varon, Antonio Ángel, Carlos A. Barbero Muñoz, David Marugan Rodrigez y Ismael Gonzalo Duran. Hacking con Ingenieria Social: Tecnicas para Hackear Humanos.. Colombia: Ra-Ma, 2015.

NOMBRE DE LA ASIGNATURA	**SIGLA**			**HSS**	**CRÉDITOS**
CERTIFICACIONES Y ESTANDARES DE TECNOLOGIA DE INFORMACION	PS1829	**TEORÍA**	X	2	4
		PRACTICA		0	0
	PERREQUISITOS	**TOTAL**		2	4

COORDINACIÓN

SIS POSGRADO EN SISTEMAS

Objetivos generales

Al final del curso el alumno será capaz de:

1. Analizar las certificaciones y estándares internacionales para tecnología de información.
2. Explicar los elementos relevantes de la certificación en gobierno corporativo de tecnología de información (CGEIT).
3. Valorar las características principales de gobierno de tecnología de información.

Temas principales

1. Elementos fundamentales de las certificaciones y estándares de tecnología de información.
2. Certificaciones y estándares de tecnología de información y su relación con las buenas practicas.
3. Implementación del gobierno de tecnología de información.
4. Estándar ISO 38500.
5. Certificación en gobierno corporativo en tecnología de información (CGEIT).

Bibligrafía

Cohen, Daniel. Tecnologia de información en los negocios. Mexico: Mc Graw-Hill Interamericana, 2009.
Piattini Velthuis, Mario y Fernando Hervada Vidal. Gobierno de las tecnologías y los istemas de información. España: Ra-Ma, 2007.
Selm, Leo van. ISO/IEC 20000 una introducción. Holanda: Van Haren Publishing, 2009.

NOMBRE DE LA ASIGNATURA	SIGLA			HSS	CRÉDITOS
DIRECCION DE PROYECTOS DE TECNOLOGIA DE INFORMACION	PS1830	**TEORÍA**	X	2	4
		PRACTICA		0	0
COORDINACIÓN	**PERREQUISITOS**	**TOTAL**		2	4
SIS POSGRADO EN SISTEMAS					

Objetivos generales

1. Integrar los conceptos básicos, las técnicas y herramientas de las buenas prácticas del Instituto de Administración de Proyectos (PMI) para el desarrollo de proyectos.
2. Explicar los elementos relevantes de la certificación Certified Associate In Projetc Management (CAPM).
3. Diseñar una oficiana de administración de proyectos.

Temas principales

1. Elementos básicos de los proyectos de tecnología de información.
2. Fundamentos de dirección de proyectos.
3. Contexto de la dirección de proyectos en diversos ámbitos laborales.
4. Introducción y bases para la certificación de la administración de proyectos (CAPM),
5. Diseño de la oficina de la administración de proyectos.

Bibliografía

Gido. Jack y James P. Clements. Administración exitosa de proyectos. México: Cengage Learning. 2007.

Horine. Gregory. Manual imprescindible: Gestión de proyectos. España: Anaya Multimedia. 2009.
Klastorin. Ted. Administración de proyectos. México: Alfaomega, 2013

NOMBRE DE LA ASIGNATURA	SIGLA			HSS	CRÉDITOS
GESTION DE INCIDENTES	PS1843	**TEORÍA**	X	2	4
		PRACTICA	X	1	1
COORDINACIÓN					
SIS POSGRADO EN SISTEMAS	**PERREQUISITOS**	**TOTAL**		3	5

Objetivos generales

Al final del curso el alumno será capaz de:

1. Utilizar las herramientas de la seguridad de la información para la gestión, control, seguimiento, tratamiento y manejo de respuestas a incidentes.
2. Aplicar las fases o etapas del análisis forense para entornos informáticos y criminales.
3. Explicar la normatividad de la legislación de la de seguridad de la información con enfoque a las tendencias de la gestión de incidentes.

Temas principales

1. Fundamentos de la gestión de incidentes.
2. Monitoreo y seguimiento de incidentes.
3. Proceso de manejo de respuestas a incidentes.
4. Análisis Forense.
5. Legislación aplicable y tendencias.

Bibliografía

Cano, Jeimy. Computación Forense: Descubriendo los rastros informáticos. México: Alfaomega, 2015
Cowen, David. Computer Forensics Infosec Pro Guide.. USA: McGraw-Hill, 2013
Lázaro Domínguez, Francisco. Introducción a la Informática Forense.. España: Ra- Ma, 2013
Marras, Marie- Helen. Computer forensics: Cyber criminals, laws and evidence.. USA: Jones and Bartlett, 2014

NOMBRE DE LA ASIGNATURA	SIGLA			HSS	CRÉDITOS
GESTION DEL SERVICIO DE TECNOLOGIA DE INFORMACIÓN	PS1833	**TEORÍA**	X	2	4
		PRACTICA		0	0
COORDINACIÓN	**PERREQUISITOS**	**TOTAL**		2	4
SIS POSGRADO EN SISTEMAS					

Objetivos generales

1. Implementar un proceso de mejora continua con base en el ciclo de vida de un servicio de tecnología de información.
2. Analizar el estándar internacional ISO 20000 para la gestión de servicio de la tecnología de información.

Temas principales

1. Introducción a la biblioteca de Infraestructuras de tecnologías de información (ITIL).
2. Estrategia y diseño del servicio de tecnología de información.
3. Transición y operación del servicio de tecnología de información.
4. Mejora continua del servicio de tecnología de información.
5. Estándar internacional de gestión de servicio de tecnología de información (ISO 20000).

Bibliografía

Bon, Jan van. Transición der servicio basada en ITIL V3: guía de gestión. España: ITSM Library, 2008

Gallacher, Liz y Helen Morris. ITIL Foundation Exam Study Guide. Reino Unido: John Wiley & Sons, 2012

IT Governance Institute, Jan van Bon, Arjen de Jong, Axel Kolthof, Mike Peiper y Ruby Tjassing. Gestion de Servicios TI basado en ITIL V3: Guía de bolsillo. Países Bajos: Van Haren Publishing, 2008.

NOMBRE DE LA ASIGNATURA	SIGLA			HSS	CRÉDITOS
HERRAMIENTAS DE SEGURIDAD DE LA INFORMACIÓN	PS1842	**TEORÍA**	X	2	4
		PRACTICA	X	2	2
COORDINACIÓN	**PERREQUISITOS**	**TOTAL**		4	6
SIS POSGRADO EN SISTEMAS					

Objetivos generales

Al final del curso el alumno será capaz de:

1. Utilizar las herramientas de redes para el mapeo de puertos, un analizador de vulnerabilidades, y un detector de intrusos entre otros.
2. Identificar los tipos de problemas de seguridad de la información en las aplicaciones y las bases de datos durante el proceso de desarrollo y como solucionarlos utilizando las herramientas informáticas.
3. Diseñar estrategias de seguridad de la información con base en la inteligencia de amenazas utilizando los datos analíticos y las medidas correctivas que las organizaciones necesitan para mitigar el riesgo en sus operaciones.

Temas principales

1. Fundamentos de herramientas de seguridad de la información.
2. Herramientas para la red.
3. Herramientas para end point.
4. Herramientas para aplicaciones y base de datos.
5. Operación de la seguridad e inteligencia de amenazas.

Bibliografía

Fors, Luis Ricardo. Criptologia Quijotesca. España: Nabu Press, 2012.

Fuster Sabater, Amparo, Luis Hernandez Encinas, Agustin Martin Muñoz, Fausto Montoya Vitini y Jaime Muñoz Masque.
Criptografia: protección de datos y aplicaciones. Guia para estudiantes y preofesionales. España: Ra- Ma, 2012.

Hernandez Encinas, Luis. La Criptologia. España: La Catarata, 2016.

Maiorano, Ariel. Criptologia. Tecnicas de desarrollo para profesionales. España: Ra-Ma, 2010.

NOMBRE DE LA ASIGNATURA	**SIGLA**		**HSS**	**CRÉDITOS**
SEGURIDAD DE TECNOLOGIA DE INFORMACION	PS1834	**TEORÍA** X	2	4
		PRACTICA	0	0
COORDINACIÓN	**PERREQUISITOS**	**TOTAL**	2	4
SIS POSGRADO EN SISTEMAS				

Objetivos generales

Al final del curso el alumno será capaz de:

1. Analizar las buenas prácticas para la gestión de la seguridad informática.
2. Valorar el estándar internacional para la seguridad de la información.
3. Explicar las certificaciones profesionales internacionales para la seguridad de la información.

Temas principales

1. Fundamentos de la seguridad física y lógica.
2. Seguridad en redes y en internet.
3. Forensia informática.
4. Estándar ISO 27000.
5. Certificaciones en seguridad de la informacion.

Bibliografía

Areitio Bertolin, Javier. Seguridad de la información. Redes, Informática y sistemas de información. España. Paraninfo-Cengage Learning, 2008.
Cano, Jeimy, J.. Computacion forense: Descubriendo los rastros informáticos. Mexico Alfaomega, 2015.
Mcnab, Chris. Seguridad de redes. España: Anaya Multimedia, 2008.

NOMBRE DE LA ASIGNATURA	SIGLA			HSS	CRÉDITOS
TOPICOS SEGURIDAD DE TECNOLOGIA DE INFORMACION	PS1844	**TEORÍA**	X	2	4
		PRACTICA	X	1	1
COORDINACIÓN	**PERREQUISITOS**	**TOTAL**		3	5
SIS POSGRADO EN SISTEMAS					

Objetivos generales

Al final del curso el alumno será capaz de:

1. Analizar las leyes, normas y propuestas nacionales e internacionales del área de la seguridad de la información
2. Descubrir los fundamentos y conceptos generales de la normativa sobre privacidad de datos en el manejo de los niveles y medidas de seguridad de la información
3. Explicar las tendencias de frontera de conocimiento del área de seguridad de la información (computo en la nube, internet de las cosas entre otros)

Temas principales

1. Normatividad internacional en TI: impacto del marco legal nacional e internacional
2. Privacidad de datos
3. Seguridad en la nube
4. Ciberseguridad
5. Tendencias en la seguridad de la información

Bibliografía

Alegre Ramos, Maria Del Pilar y Alfonso Garcia- Cervigon Hurtado. Seguridad Informática- España: Paraninfo, 2011.
Buendia Roa. Seguridad informática GM. España: McGraw- Hill Interamericana, 2013.

Elisan, C, Christopher.. Advanced Malware Analysis. USA: McGraw-Hill, 2015.
Gomez Vieites, Alvaro. Enciclopedia de la seguridad Informática. España: Ra-Ma, 2011.
Miguel Perez, Julio Cesar. Proteccion de datos y seguridad información: guía practica para ciudadanos y empresas. España: Ra- Ma, 2015.

METODOLOGÍA DE ENSEÑANZA Y APRENDIZAJE

Los académicos del posgrado implementan diversas metodologías de enseñanza-aprendizaje algunos de ellos son: coloquio en pequeños grupos, educación tutorial, métodos de casos, aprendizaje por proyectos

COLOQUIO EN PEQUEÑOS GRUPOS

El estudiante adquiere conocimientos —especialmente sobre experiencias personales, valoraciones y propuestas— a través del intercambio de información y de opiniones con los demás participantes.

Otras denominaciones para el modelo: Círculo de estudios; coloquio (didáctico) en pequeños grupos; grupos de discusión; grupos pequeños de aprendizaje; mesa redonda. Micro-study circle; (mini-)discussion group; small-group learning; small group discussion.

EDUCACIÓN TUTORAL

El alumno aprende a través del enseñar. Para ello adquiere ciertos conocimientos que le permiten ayudar a otros alumnos, que están en un nivel de aprendizaje menos avanzado, y también aprende en ese proceso.

Otras denominaciones para el modelo: enseñanza con tutores; método de monitoría; método tutoría; tutoría de iguales o de pares. Learning by teaching; monitor (method); peer-teaching method; peer tutoring; tutorial method:

- Variantes.
- Método Bell-Lancaster.
- Sistema de ayudantes en clases.
- Tutorías autónomas.

MÉTODO DE CASOS

El alumno analiza individualmente, o en grupos, un conjunto de materiales que reconstruyen una situación pertinente de la práctica, a fin de adquirir conocimientos sobre esa práctica y desarrollar la capacidad de apreciar situaciones complejas y tomar decisiones adecuadas.

Otras denominaciones del modelo: Estudio de caso; método de caso; método casuístico. Case method; case study (method).
Variantes

- Caso de juicio o dictamen; Case problem method; Caso de decisión.
- Casos de información; Incident method.
- Método del papelero de correspondencia; In basket case method;
- Caso de determinación del problema.
- Caso de solución del problema; Case study method.Casos de investigación; Project case method.

APRENDIZAJE POR PROYECTOS

El Aprendizaje por Proyectos (ApP) se ha constituido en una herramienta útil para una gran cantidad de educadores; en la actualidad, se ha enriquecido con la utilización rutinaria de la Tecnología de la Información (TI) y se ha convertido en vehículo para el aprendizaje no solo del contenido de las materias académicas sino, también, del uso efectivo de las TI. El objetivo final del ApP es ayudar a los estudiantes a utilizar de manera efectiva tanto su mente (pensamiento de orden superior; capacidad de análisis y síntesis; y habilidades para resolver problemas) como las TI (computadores, Internet y software), a medida que planean y llevan a cabo proyectos interesantes y complejos. El aprendizaje por proyectos se enfoca en un problema que hay que solucionar o en una tarea que se debe realizar. La idea fundamental en la solución de problemas o la realización de tareas, es la de que estas se construyen sobre el trabajo que hayan realizado anteriormente. Cuando un alumno se enfrenta a un problema o tarea que constituye un desafío, utiliza el conocimiento, las habilidades, y las ayudas que otras personas han desarrollado, así como su propio conocimiento, habilidades y la experiencia adquirida en trabajos anteriores.

CRITERIOS Y PROCEDIMIENTOS DE EVALUACIÓN

La Evaluación Inicial es diagnostica y motivadora, por lo que se realiza al comienzo del proceso. Su objetivo es el de establecer el punto de partida y proporcionar información sobre la situación del alumno.

La Evaluación Continua es formativa, orientadora y reguladora, es decir, se realiza a lo largo del proceso de enseñanza y aprendizaje. Su objetivo no es solo calificar si no mejorar. Tiene dos consecuencias inmediatas: la retroalimentación del alumno y el docente para la detección de problemas y vías alternativas que permitan alcanzar unos mejores resultados.

La Evaluación Final es factible de considerarse como sumativa o terminal, por lo que se realiza al término de una fase de aprendizaje. Su objetivo es el de establecer el grado de

desarrollo de los conocimientos, competencias y habilidades de los objetivos por parte del alumno.

BIBLIOGRAFÍA RELEVANTE Y ACTUALIZADA

NOMBRE DE LA ASIGNATURA
ADMINISTRACION DE RIESGOS DE TECNOLOGIA DE INFORMACION

- Bravp Mendoza, Oscar. *Gestion integral de Riesgos*. Tomo I. Colombia: Bravo & Sanchez, 2006
- Buchtik, Liliana. *Secretos para dominar la gestión de riesgos en proyectos*. Montevideo, Uruguay. Buchtikglobal, 2016
- ISACA The risk IT framework: *Principles, process details, management guidelines, maturity models* USA: ISACA, 2009

NOMBRE DE LA ASIGNATURA
AUDITORIA EN TENOLOGIA DE INFORMACION

- ISACA. *Sharepoint Deployment and Governance Using COBIT 4.1: A Practical Approach*.USA: ISACA, 2010
- IT Governance Institute.CIBIT *4.1: framerwork, control objetives, management guidelines, maturity models*. USA: ISACA, 2007
- Muñiz González, Luis. *Como implantar y evaluar un sistema de control de gestión: incluye cuestionarios de evaluación*. España: Profit Editorial, 2013
- Piattini Velthuis, Mario, Emilio del Peso Navarrete y Mar de Peso Ruiz. *Auditoria de tecnologías y sistemas de información*.España; Ra-Ma, 2008.

NOMBRE DE LA ASIGNATURA
BUENAS PRACTICAS DE SEGURIDAD DE LA INFORMACION

- Caballero Velasco, Maria Angeles, Diego Cilleros Serrano y Abtin Shamsaifar. *El libro del Hacke*r. España: Anaya, 2014.
- Escrivá Gascó, Gema, Rosa Ma. Romero Serrano, David Jorge Ramada y Ramón. Onrubia Perez. *Seguridad Informatica*. Mexico: Macmillan, 2013.
- Gomez Vieites, Álvaro, *Gestion de Incidentes de Seguridad Informatica*. España: Starbook, 2011.
- Ramos Varon, Antonio Ángel, Carlos A. Barbero Muñóz, David Marugan Rodrígez y Ismael Gonzalo Durán. *Hacking con Ingenieria Social: Tecnicas para Hackear Humanos*. Colombia: Ra-Ma, 2015.

NOMBRE DE LA ASIGNATURA
CERTIFICACIONES Y ESTANDARES DE TECNOLOGIA DE INFORMACION

- Cohen, Daniel. *Tecnologia de información en los negocios*. Mexico: Mc Graw-Hill Interamericana, 2009.
- Piattini Velthuis, Mario y Fernando Hervada Vidal. *Gobierno de las tecnologías y los istemas de información.* España: Ra-Ma, 2007.
- Selm, Leo van. ISO/IEC *20000 una introducción*. Holanda: Van Haren Publishing, 2009.

NOMBRE DE LA ASIGNATURA
DIRECCION DE PROYECTOS DE TECNOLOGIA DE INFORMACION

- Gido. Jack y James P. Clements. *Administración exitosa de proyectos*. México: Cengage Learning. 2007.
- Horine. Gregory. *Manual imprescindible: Gestión de proyectos*. España: Anaya Multimedia. 2009.
- Klastorin. Ted. *Administración de proyectos*. México: Alfaomega, 2013

NOMBRE DE LA ASIGNATURA
GESTION DE INCIDENTES

- Cano, Jeimy. Computación Forense: Descubriendo los rastros informáticos. México: Alfaomega, 2015
- Cowen, David. Computer Forensics Infosec Pro Guide.. USA: McGraw-Hill, 2013
- Lázaro Domínguez, Francisco. Introducción a la Informática Forense.. España: Ra-Ma, 2013
- Marras, Marie- Helen. Computer forensics: Cyber criminals, laws and evidence.. USA: Jones and Bartlett, 2014

NOMBRE DE LA ASIGNATURA
GESTION DEL SERVICIO DE TECNOLOGIA DE INFORMACION

- Bon, Jan van. *Transición der servicio basada en ITIL V3: guía de gestión*. España: ITSM Library, 2008
- Gallacher, Liz y Helen Morris. *ITIL Foundation Exam Study Guide*. *Reino Unido*: John Wiley & Sons, 2012
- IT Governance Institute, Jan van Bon, Arjen de Jong, Axel Kolthof, Mike Peiper y Ruby Tjassing. *Gestion de Servicios TI basado en ITIL V3: Guía de bolsillo*. Países Bajos: Van Haren Publishing, 2008.

NOMBRE DE LA ASIGNATURA
HERRAMIENTAS DE SEGURIDAD DE LA INFORMACION

- Fors, Luis Ricardo. *Criptologia Quijotesca*. España: Nabu Press, 2012
- Fuster Sabater, Amparo, Luis Hernandez Encinas, Agustin Martin Muñoz, Fausto Montoya Vitini y Jaime Muñoz Masque. *Criptografia: protección de datos y aplicaciones. Guia para estudiantes y preofesionales.* España: Ra- Ma, 2012
- Hernandez Encinas, Luis. *La Criptologia*. España: La Catarata, 2016
- Maiorano, Ariel. *Criptologia. Tecnicas de desarrollo para profesionales*. España: Ra-Ma, 2010

NOMBRE DE LA ASIGNATURA
SEGURIDAD DE TECNOLOGIA DE INFORMACION

- Areitio Bertolin, Javier. *Seguridad de la información. Redes, Informática y sistemas de información*. España. Paraninfo-Cengage Learning, 2008
- Cano, Jeimy, J. *Computacion forense: Descubriendo los rastros informáticos*. Mexico Alfaomega, 2015
- Mcnab, Chris. *Seguridad de redes*. España: Anaya Multimedia, 2008

NOMBRE DE LA ASIGNATURA
TOPICOS DE SEGURIDAD DE TECNOLOGIA DE INFORMACION

- Alegre Ramos, Maria Del Pilar y Alfonso Garcia- Cervigon Hurtado. *Seguridad Informática*- España: Paraninfo, 2011
- Buendia Roa. *Seguridad informática* GM. España: McGraw- Hill Interamericana, 2013
- Elisan, C, Christopher. *Advanced Malware Analysis*. USA: McGraw-Hill, 2015
- Gomez Vieites, Alvaro. *Enciclopedia de la seguridad Informática*. España: Ra-Ma, 2011
- Miguel Perez, Julio Cesar. *Proteccion de datos y seguridad información: guía practica para ciudadanos y empresas*. España: Ra- Ma, 2015

Número de estudiantes matriculados por cohorte generacional

Aún no se tiene la 1er Generación.

Núcleo académico básico

Profesores de Asignatura

Los académicos que forman el claustro de docentes es el siguiente:

Mtro. Pedro Fernando Solares Soto

Actualmente Coordinador del Programa Académico Técnico Superior Universitario en Software, Maestría en de Gobierno de TI y Especialidad en Seguridad de la Información. Los estudios académicos que ha cursado son: tres diplomados, una maestría y una especialidad. La experiencia docente en Instituciones Educativas, en la IBERO como académico de tiempo en el posgrado del área de sistemas, realizó actividades como jefe del área de Cultura Computacional en el Departamento de Sistemas. En la Universidad Autónoma de Hidalgo, fue académico de asignatura del posgrado en el Instituto de Ciencias Exactas.

Las actividades académicas realizadas son: evaluador Nacional de los Comités Interinstitucionales de la Evaluación de la Educación Superior (CIEES) del Comité de Ingeniería y Tecnología, así como revisor técnico de la editorial Pearson Prentice Hall en el área de TI.

En la experiencia profesional se ha desarrollado como consultor en las empresas CONSETI, en áreas de Seguridad de la Información, buenas prácticas de procesos de negocios, Gobierno de TI. En TenStep Latinoamérica, en áreas de dirección de proyectos, arquitectura empresarial. En SG SOFT, en arquitectura y calidad de software.

Los reconocimientos obtenidos: Diploma y Medalla al Mérito Universitario, así como Académico Numerario, las agrupaciones en las que ha sido fundador en la IBERO son; comunidad UIA-PMI, Club IBERO-TOASTMASTERS, la rama estudiantil IBERO-IEEE y la Cátedra “Gobierno de TI”.

Las asociaciones a las que pertenece actualmente son: miembro de la Vicepresidencia de Tecnología de Información de la Comisión Nacional de Desarrollo Empresarial de COPARMEX. Vicepresidente del Sector Educativo del Foro de Administración de Servicios de Tecnología de Información (ITSMF). Asesor en el Comité Directivo de la Asociación Latinoamericana de Profesionales en Seguridad de la Información (ALAPSI). Se

desempeñó como Vicepresidente de Relaciones con el Sector Gubernamental del ITSMF y Vicepresidente de la Academia Mexicana de la Ciencia de Sistemas.
Coordinador con ECORFAN en dos Handbook de TI con artículos de alumnos de la maestría, además de publicar varios artículos arbitrados en temas de: Gobierno y Riesgos de TI, Software, Protección de datos, Modelos de Ecuaciones Estructurales. Tiene un libro publicado en la Editorial Patria "Administración Informática: Análisis y evaluación de la TI". Coordino varios estudios de Percepción sobre la Seguridad de la Información en México. En la difusión académica a participado en diversos eventos académicos como ponente, conferencista y panelista. La actualización se desarrolla mediante la asistencia a diversos cursos, talleres, conferencias y congresos.

Mtro. Carlos Zamora Sotelo

Carlos Zamora Sotelo es un profesional con Licenciatura y Maestría en Tecnologías de Información, es experto en materia de Administración de Riesgos Financiero, Legal, Operativo y Tecnológico, ha participado en estudios de especialización y posgrado en materia financiera, de seguridad y dirección en Instituciones académicas entre las que destacan, la Universidad Iberoamericana, ITAM, ITESM y la Universidad de Berkeley en California E.E.U.U.

Ha fungido como catedrático de la materia de Auditoría de Sistemas y Gobierno de Tecnologías de Información universidades nacionales y extranjeras, ha capacitado a más de 3500 Profesionales en temas de Auditoría, Gobierno de T.I., riesgos y seguridad en Latinoamérica.

Ha impartido conferencias sobre Peritajes, Auditorías, Seguridad, Riesgos y Fraudes en México, Centro y Sudamérica y el Caribe.

Cuenta con las certificaciones con validez Internacional en Auditoría, Seguridad, Riesgos y Gobierno de Tecnologías de Información emitidas por ISACA, asociación internacional con más de cien mil miembros en el mundo de la cual fue presidente del capítulo Mexicano durante el periodo 2004 -2009.

Ha participado como perito y arbitro en las controversias relacionadas con contratos en materia de Tecnología de Información en la administración pública.

Actualmente se desempeña como perito único en materia de Ingeniería de Sistemas en el Poder Judicial de la Federación.

Participó en el diseño del modelo de Gobierno de Tecnologías de Información para el sector salud y su último proyecto fue participar con el Instituto Nacional de Administración Pública en la evaluación del padrón de beneficiarios del Seguro Popular de la CNPSS; Actualmente se encuentra cursando y desarrollando su tesis doctoral en Administración Pública, sustentada en un modelo de transparencia, gobernabilidad y aseguramiento de la gestión de contratos en la administración, gobernabilidad y aseguramiento de gestiatos ón pública Federal denominado Método Pakal.

Director del Proyecto TISS 2013/14 "Situación Actual de las Tecnologías de Información en los tres pilares fundamentales para la cobertura universal de Salud en México".

Mtro. Fernando Solares Valdés

Es ingeniero en cibernética y sistemas computacionales por la universidad la Salle, cuenta con un Master en Gobierno de Tecnologías de Información y Comunicaciones por la universidad de Deusto en España, así como una Maestría en Administración de Servicios de TI por la Universidad Iberoamericana.

El maestro cuenta con las certificaciones de ITIL v3, COBIT, ISO 20000 e ISO 27001.

Actualmente es Director General Adjunto de Tecnologías de la Información y Comunicaciones de la Secretaria de Gobernación, el Maestro es especialista en temas tales como, seguridad de la información, riesgos corporativos, riesgos de TI, gobierno de Tecnologías de la Información, Gobierno Corporativo, Procesos de negocio, sistemas de Gestión, Arquitectura Empresarial y Administración de Proyectos.

Ha impartido conferencias, cursos y seminarios en materia de protección de datos personales, gobierno de las Tecnologías de la Información, ISO 27001, ISO 9000, ISO 2000, COBIT e ITIL.

Mtro. Omar Sánchez Cázares

Omar Sánchez es Ingeniero en Comunicaciones y Electrónica por el Instituto Politécnico Nacional y egresado de la Maestría en Administración de

Servicios de TI de la Universidad Iberoamericana.

Tiene 22 años de experiencia en las Tecnologías de Información y cuenta con diversas certificaciones en el ámbito de las TI.

Ha colaborado en compañías nacionales y transnacionales de diversos sectores como servicios, medios de comunicación, farmacéutico y consultoría y ha participado en proyectos con cobertura nacional e internacional, liderando equipos multidisciplinarios y multiculturales.

Como parte de su desempeño profesional, imparte cursos, talleres y conferencias sobre diversos aspectos de las mejores prácticas de TI como ITIL, ISO-20000, Gestión de Riesgos, o Análisis de Negocio.

Es miembro profesional del AXELOS, IIBA y de ISACA.
A partir de Julio de 2015, es el presidente del IT Service Management Forum México, cuya misión es generar, divulgar y promover las mejores prácticas de TI.

Actualmente es Director General de la consultora O2 Systems, siendo sus principales intereses la evangelización sobre la creación de valor de negocio mediante las mejores prácticas de TI, para ayudar a los CIOs, Directores y Gerentes de TI a encontrar su propia visión en sus organizaciones.

Mtro. Jorge Garibay Orozco

Es Licenciado en Informática por la UPIICSA-IPN.
Tiene Maestría en Alta Dirección de Empresas (MBA) por el IPADE (Instituto Panamericano de Alta Dirección de Empresas).
Cuenta con la certificación CISSP otorgado por ISC2.
Cuenta con la certificación CISA de ISACA..
Cuenta con la certificación CRISC de ISACA.
Es Auditor e Implementador Líder de ISO 22301:2012 por el PECB de Canadá.
Es Auditor e Implementador Líder de ISO 27001:2005 por el PECB de Canadá.
Es Risk Manager de ISO 27005 por el PECB de Canadá.
Fue Subdirector del Centro de Cómputo de la Secretaría de Salud en México.
Director de Proyectos de SAIT primera empresa mexicana en integrar proyectos llave en mano de instalaciones de fibra óptica y enlaces de redes abiertas para empresas privadas.

Fue socio fundador y director de SEG.COM, empresa dedicada a integrar soluciones de seguridad informática de 1997 a 2000.

Fue Director de Tecnologías de Información (CIO) dentro del Grupo Metronet / Xertix desde el 2001 hasta el 2012, ahora RedIT, empresa pionera en México en el suministro de redes de telecomunicaciones de fibra óptica y en proveer servicios administrados de TI, a través de 3 Centros de datos en el país y 2 en los Estados Unidos (San Diego, California). Durante este tiempo llevó a cabo la implementación de los sistemas de gestión de seguridad de la información y de administración de tecnología para recibir la certificación ISO 27001 e ISO 20000 para la organización, siendo la primera empresa en México en ostentar la certificación ISO 20000 y la primera en el mundo en obtener ambas certificaciones de manera simultánea. Asimismo, participó en la definición de la estrategia no sólo de TI del grupo, sino en la definición de negocio que hoy en día posiciona a RedIT como una empresa multinacional siendo una de las 500 empresas más importantes de México.

Fue Director General de Let´s Cloud IT y de Servicios de Valor de TI; empresas dedicadas al desarrollo de soluciones de software en la nube, así como a la consultoría y capacitación en temas de Procesos, Seguridad de la Información, Análisis de Riesgos y Administración de Tecnología de Información.

Es Director Ejecutivo de Riesgos, Seguridad y Continuidad de Pink Elephant para América Latina desde 2014, teniendo a su cargo el desarrollo de estas prácticas en México y la región.

Es miembro y socio de asociaciones nacionales en seguridad como la ALAPSI e ISACA capítulo Cd. de México y de instituciones internacionales de seguridad como el CSI, ISC2, y MIS Institute.

Ha sido profesor de la UPIICSA – IPN por más de 14 años en temas de TI como Auditoria de Sistemas de Información, seguridad informática, redes globales, informática empresarial, sistemas analógico-digitales, entre otras materias.

Es Miembro del BOARD de Relaciones Gubernamentales y con Asociaciones de ISACA Internacional, como Chair de América Latina en consejos a nivel mundial. Presidió este Consejo en la región de 2010 a 2013.

Es Coordinador Suplente de México, del Grupo de Trabajo de la Organización Internacional de Estándares ISO JTC 1 / Subcomité 27 “Técnicas de Seguridad de la Información”.

Es Coordinador Titular de México, del Grupo de Trabajo de la Organización Internacional de Estándares ISO JTC 292 / Subcomité 223 “Continuidad de Negocio y Recuperación de Desastres”.

Mtro. Luis Pérez del Real

Candidato a Doctor por la Universidad La Salle, investigando seguridad en PyME’s. Maestro en seguridad de las tecnologías de información en la Universitat Ramon Llull en Barcelona, España. Ingeniero en Cibernética y Sistemas Computacionales egresado de la Universidad La Salle; egresado del MBA en la Universidad La Salle. Es catedrático en la escuela de ingeniería de la Universidad La Salle, Universidad Anáhuac y colaborador de la Universidad Iberoamericana.

Ha participado en diversas startups relacionadas con tecnología, cuenta con experiencia profesional en Latinoamérica y Europa. Ha laborado en IBM, S21sec, Scitum e IXE Grupo Financiero y actualmente es arquitecto de soluciones en Verint, diseñando soluciones de ciber-seguridad y proporcionando consultoría a clientes en diferentes industrias y verticales de negocio. Cuenta con las cerficaciones CISA, CRISC, CISSP-ISSAP, OPST, OPSA, CCSA, CCSE, Auditor Líder ISO 27001, ITIL.

Mtra. Maricarmen García de Ureña

Administrativa del Instituto Politécnico Nacional donde cursó la carrera como Licenciado en Ciencias de la Informática.

Cuenta con el diploma de “Sistemas de Información Bajo Ambiente Web” del Instituto Tecnológico de Estudios Superiores de Monterrey y especialización en “Alta Dirección en Informática Gubernamental” por el Instituto Nacional de Administración Pública.

Ha realizado estudios en temas como: administración de tiempo por el Covey Leadership Center, Oracle por Destra Consultores, Psicología Trascendental por el Centro deIntegración de Conciencia, productividad y calidad por el Instituto Politécnico Nacional, normas técnicas de competencia laboral para la consultoría general y evaluación de competencias laborales por la Cámara de Comercio, Servicios y Turismo, ética y valores por el ITAM, evaluación y avances de calidad, redefinición de estándares de calidad, elaboración y difusión de estándares de calidad por el CECAL, auditoria pública por SECODAM, entre otros.

Inicio su carrera dirigiendo proyectos de tecnología comercial en la "Secretaría de Comercio y Fomento Industrial" actualmente conocida como Secretaría de Economía.
Trabajó como Auditor de sistemas para la contraloría Interna de la "Secretaría de Hacienda y Crédito Público".

Colaboró como Project Leader para "Marsh & McLennan Companies", en las diversas áreas Europea, Americana y Asiática.
Laboró como Consultor y Administrador de proyectos para las firmas de consultoría "Consult International "y "Destra Consultores".

Ejerció el cargo de Titular del Área de Tecnologías de Información y Comunicaciones para la empresa "Talleres Gráficos de México".

Certificaciones

- CBCP (Certified Business Continuity Professional)
- ISO27001-2005 Information Security Management System Lead Auditor Certificate Number: 3687684-61096
- BS25999-2 Business Continuity Management System Lead Auditor Certificate Numbrer: 7855893-49816.
- ISO22301-2012 Business Continuity Management System Lead Auditor

Otros

- Premio de la Asociación Latinoamericana de Continuidad, ALCONT 2013 al "Liderazgo e innovación en Continuidad del Negocio".
- Cuenta con el Diploma en Seguridad Informática – Tecnológico de Monterrey.
- Cuenta con la certificación FCSP (Fortinet Certified Sales Professional).
- Ha participado en seminarios de seguridad, relacionados con herramientas y tecnologías de seguridad informática.
- Es miembro de la Asociación Latinoamericana de Profesionales de Seguridad Informática A.C. (ALAPSI) y la Asociación Latinoamericana de Seguridad (ALAS).
- Ganadora del premio ALCONT 2013 otorgado por la Asociación Latinoamericana de Continuidad del Negocio en la categoría de "Liderazgo e Innovación en Continuidad del Negocio".
- Miembro del consejo editorial del Disaster Recovery Journal (DRJ) en español.
- Conferencista recurrente en eventos internacionales, tales como ISACA Latin
- CACS, DRJ Conference, Conferencia Iberoamericana de Continuidad del Negocio, Día de la Seguridad de la Información, Conferencia Latinoamericana de Continuidad del Negocio y Seguridad de la Información, ALCONT Continuity and Recovery, Week, entre otros.

Lic. Mario Ureña Cuate

Mario es consultor en continuidad del negocio, gestión de riesgos, auditoria, control y seguridad de la información. Académicamente, es Licenciado en Ciencias de la Informática egresado de la Unidad Profesional Interdisciplinaria de Ingeniería y Ciencias Sociales y Administrativas del Instituto Politécnico Nacional en la Ciudad de México.

A la fecha, ha realizado revisiones y trabajos de consultoría de diversos tipos como son de controles generales de Tecnología de Información (COBIT), auditoria de aplicaciones, proyectos especiales de análisis de datos, implementación de ISO22301/ISO27001/ISO20000/BS25999/ISO27005/ISO31000, creación del marco normativo de seguridad, reingeniería de procesos de administración de TI, implantación de herramientas de seguridad, análisis forense de datos, análisis de vulnerabilidades, pruebas de penetración y hackeo ético, análisis de riesgos, análisis de impacto al negocio, revisiones de seguridad en ambientes multiplataforma y gestión de la continuidad del negocio.

Certificaciones

- CISSP (Certified Information Systems Security Professional) Certificate Number: 41645.
- CISA (Certified Information Systems Auditor) Certificate Number: 0645165.
- CISM (Certified Information Security Manager) Certificate Number: 0605757.
- CGEIT (Certified in the Governance of the Enterprise IT) Certificate Number: 0901850.
- ISO22301-2012 Business Continuity Management System Lead Auditor.
- BS7799-2002 Information Security Management System Lead Auditor Certificate Number: 4674145-30417.
- BS25999-2006 Business Continuity Management System Lead Auditor Certificate Number: 7359871-30417.
- ISO27001-2005 Information Security Management System Lead Auditor Certificate Number: 7387684-30417.

Otros

- Especialización en auditoria de equipos IBM AS/400 y sistemas OS/400 por Wayne O. Evans Consulting.

- Especialización en auditoria de seguridad en Internet, auditoria de aplicaciones del negocio y auditoria del ciclo de desarrollo de sistemas por el MIS Training Institute.
- Expositor de temas de Tecnologías de Información, Seguridad informática y Continuidad del negocio en diversos foros especializados e instituciones de reconocido prestigio, incluyendo LatinCACS 2007 (Monterrey, México) 2008 (Santiago, Chile) 2009 (San José, Costa Rica) 2011 (San Juan, Puerto Rico),
- Conferencia Internacional ISACA 2010 (Cancún, México), Information Security and Risk Management Conference 2009 (Bogotá, Colombia), Information Security Forum 2008 (Ciudad de México, México), BSI Communication Days 2008 y 2009, Lima Full Day 2012, DRJ Conference 2012 (Punta Cana, República Dominicana),
- ALCONT Continuity and Recovery Week 2013 (Bogotá, Colombia), entre otros.
- Es miembro activo de la Information Systems Audit And Control Association (ISACA), International Information Systems Security Certification Consortium (ISC2),
- Information Systems Security Association (ISSA), Asociación Latinoamericana de Profesionales en Seguridad Informática (ALAPSI) y Asociación Latinoamericana de Seguridad (ALAS).
- Miembro del CISA Quality Assurance Team (QAT) y External Advocacy Committe (EAC) de ISACA internacional.
- Participó en la creación del curso de gestión de riesgos basado en ISO27005 para el British Standards Institution que se imparte actualmente.
- Participó en la redacción del capítulo de gestión de riesgos del manual de certificación CISM 2009 para ISACA internacional.
- Instructor oficial del British Standards Institution para los cursos de Interpretación, implementación y auditoría de sistemas de gestión y estándares ISO, incluyendo ISO22301, ISO27001, ISO20000, ISO27005, BS25999.

Dr. Francisco Valdés Souto

Certificaciones

- Project Management Institute.
- Project Manager Professional.
- PMP Number: 452946.
- Common Software Measurement International Consortium (COSMIC).
- COSMIC Certification Entry-Level (CCFL) (Primer Mexicano).
- COSMIC International Advisory Council (IAC) para México.

- Certified Scrum Master (CSM).
- The Scrum Alliance, Inc. MEMBER: 000127605.

Experiencia laboral

- Departamento de Matemáticas de la Facultad de Ciencias (FC) de la Universidad Nacional Autónoma de México (UNAM).
- Profesor Asociado “C”.
- Investigación en Ingeniería de Software.
- Vinculación con la Industria.
- Asociación Mexicana de Métricas de Software (AMMS).

Fundador

- Creación de la Asociación Mexicana de Métricas de Software (AMMS) en 2015.
- Realización de 1er Congreso Nacional de Medición y Estimación de Software 15.

Fundador y Socio

- Impulso del método de medición estándar COSMIC en México, a través de capacitación y exámenes de certificación desde 2008.
- Fomento de prácticas formales de medición y estimación en la industria de software mexicana a través de investigación aplicada y el desarrollo del sitio MEPE (www.mepe.com.mx), sitio que expone mecanismos formales sobre estimación y evaluación de proyectos basados en investigación aplicada.
- Creación del Special Interest Group in COSMIC /México, como parte del Consorcio Internacional COSMIC, encargado de la difusión del estándar internacional en México con impacto en LATAM.
- Propuesta del Plan Estratégico de TIC para el estado de Veracruz y realización de evaluación de desempeño de distintos proyectos.

Instituto Mexicano del Seguro Social

- Director de Área de Portafolio de Servicios y Diseño de Soluciones
- Definición y negociación de nueva propuesta de gestión de servicios de Tecnología de Información y Comunicaciones para IMSS. Se replantearon los servicios de TIC que se proporcionaban con la finalidad de poder llegar a tener mediciones y evaluaciones que permitieran la mejora continua, así como garantizar la continuidad de los procesos de negocio soportados por servicios informáticos.

Dr. José de Jesús Vázquez Gómez

Doctor en Informática por la Universidad de Rennes I en Francia.

Distinciones

- 2011: Nombramiento como “Director de Planeación”, otorgado por la Asociación Latinoamericana de Profesionales en Seguridad A.C.
- 2009: Nombramiento como “Especialista en Tecnologías de Información”, otorgado por el Banco de México.
- 2006: Acreedor a la Medalla “San Ignacio de Loyola”, otorgada por la Universidad Iberoamericana.
- 2006: Premio “B-Secure Award 2006” otorgado por Netmedia.

Publicaciones

- 2007: Libro “La Seguridad de la Información”, Enrique Daltabuit, Leobardo Hernández Audelo, Guillermo Mallén y Jesús Vázquez, 776 p, ISBN: 968-18- 6935-4, Ed. Grupo Noriega Editores, 2007.
- 2006: "A Tool for Managing Security Policies in Organisations", con varios autores, publicado en “Lecture Notes in Computer Science", Ed. Springer Berlin/Heidelberg, Volume 4266/2006, pp. 378-388, Book “Advances in Information and Computer Security”, ISSN 0302-9743, ISBN 978-3-540-47699- 3, 2006.
- Entrevista publicada en la revista “B-Secure”, Vol. 3, No 26, Febrero de 2006 Pag. 12, Netmedia.
- 2005: “An Artificial Manager for Security Policies in Organizations”, Research on Computing Science, Vol. 17, pp 97-106, Volume Editors Alexander Gelbukh and Raúl Monroy, CIC IPN, 2005.
- Entrevista sobre seguridad de la información publicada en la revista “Contaduría Pública” Año 33, Num.395, 2005, México.
- “Seguridad en el Internet de mañana”, capítulo en el libro “Internet, columna vertebral de la sociedad de la información”, 2005, Editorial Porrúa, México.
- 2003 “Arquitectura de Seguridad Informática en Banco de México”, con varios autores, 2003 en la XXX Reunión de Sistematización de Banca Central. CEMLA. La Antigua, Guatemala.
- 2000 “Definiendo un esquema de seguridad para redes ATM en base a firewalls”, Proceedings CLEI'2000, 18-22 Septiembre 2000, México D.F. “Importancia de la seguridad informática en Internet”, Cap. 15 de “Internet: el medio inteligente”, Ed. CECSA, 2000.
- ISBN 970-24-0112-7 “Revista Enlace de Banco de México”, editor y autor de artículos de la Dirección de Sistemas para concientización en aspectos de seguridad informática (de 2000 a la fecha)
- 1998 “Caracterización de Ataques Informáticos”, Día Internacional de la Seguridad en Cómputo, México, DGSCA- UNAM, Diciembre de 1998.
- Entrevista publicada en Computer World Año 19, Núm. 590, Noviembre 9 de 1998. “Académicos hablan sobre seguridad”.
- 1995 Manual del Curso “Seguridad Computacional Tomo I” CR95516, Publicado por la Rectoría de Universidad Virtual del ITESM, 1995. CURRICULUM VITAE Enero de 2012 5/18

- “Internet Security”. 3rd ISAAC´95, Monterrey, México, Octubre de 1995.
- “Seguridad en Internet” . XXI Conferencia Latinoamericana de Informática Panel 95. Brasil, 1995.
- 1994 “Contribution a la Modélisation de la Sécurité Multidomaine”. Tesis de Doctorado de la Universidad de Rennes I. Francia, 1994. Num. national de thèse : 1994REN10082. [Note(s) : [160 p.]] (bibl.: 36 ref.) (Année de soutenance : 1994) (No : 94 REN1 0082). Localisation / Location INIST-CNRS, Cote INIST : T 97382.
- ”Multidomain Security”. Computers & Security , vol. 13, no. 2, United Kingdom, 1994.
- “Sécurité des systémes informatiques: Des systémes centralisés aux réseaux”. Revue Réseaux et Informatique Répartie, vol. 4, no. 1. France, 1994.
- 1993 “Modelling Multidomain Security”. ACM-SIGSAC New Security Paradigms Workshop II, Rhode Island, USA , 1993.
- 1991 “ Sécurité des systémes informatiques”. Rapport interne No. 91-001, Ecole Supérieure d´Eléctricité, France, 1991.
- 1987 “Rutas de Distancia Mínima sobre representaciones jerárquicas de terreno”, Tesis de Maestría del Centro de Investigación y de Estudios Avanzados del I.P.N., México, 1987.

Últimos Cursos y Certificaciones

- Certificado “ITIL v3 Foundation Examination”, 30 de mayo de 2011.
- Curso de “Harvard Business Review”, 2010.
- Curso de “Introducción a ITIL”, Banco de México, Septiembre de 2009.
- Curso de “Administración de Proyectos”, Alpha Consultoría, PMI, Abril de 2008.
- Curso de “Microsoft Project Profesional”, Alpha Consultoría, PMI, Abril de 2008.
- Participación IV Evento Internacional de Seguridad Informática 2006, Retos Actuales, ALAPSI, 31 de octubre de 2006, México.

Líneas de generación y/o aplicación del conocimiento del programa

A partir de la experiencia institucional desarrollada en posgrados, se propone crear la “Cátedra Seguridad de la Información” que apoyara la movilidad de investigadores, académicos y alumnos en la construcción de redes de estudio y enseñanza superior en Seguridad de la Información. Sera un espacio generador de estrategias teórico-metodológicas que favorecerán la articulación de la especialidad en la construcción de una cultura de a la seguridad en TI. Los temas de trabajo son:

- Auditoría de TI.
- Administración de Riesgos de TI.
- Ciberseguridad.

- Seguridad de la Información.
- Gestión de Incidentes.
- Privacidad de Datos.
- Forensia de TI.

Estándares Internacionales

- ISO 27000 (Seguridad de la Información).
- ISO 20000 (Gestión de Procesos de TI).
- ISO 31000 (Riesgos).
- ISO 21500 (gestión de proyectos).

Certificaciones internacionales profesionales

- CISA (Auditoria de sistemas).
- CISM (Seguridad de Sistemas de Información).
- CSX (Cybersecurity Fundamentals Certificate).
- CISSP (Seguridad en Sistemas).
- PMP (Profesional en la Administración de Proyectos).
- ITIL (Gestión de Procesos de TI).
- CEH (Certified Ethical Hacking).
- OPST (Seguridad de la Información).
- Resiliencia Cibernética.
- CCC (Professional Cloud Administrator).
- Cloud Computing Foundation.

Seguimiento de la trayectoria escolar (tutores – estudiantes)

La Tutoría Académica está orientada a fortalecer la práctica de la docencia, brindando a los estudiantes atención personalizada o grupal durante su proceso formativo, con el propósito de detectar de manera oportuna y clara los factores de riesgo que pueden afectar el desempeño académico de los alumnos.

La actividad tutorial contempla la realización de actividades planificadas y responsables que en suma busquen:

Mejorar el proceso de aprendizaje, generando actitudes de conocimiento crítico y participativo.

Trabajar el proceso de crecimiento personal del alumnado, sin dejar de lado las problemáticas y experiencias particulares.

Analizar el ámbito contextual, laboral y profesional, favoreciendo una construcción como sujetos activos de la sociedad.

Cada docente tiene asignado máximo 3 a 5 alumnos por periodo escolar, para su seguimiento se tiene un formato que es llenado por el académico en una entrevista.

Productividad académica relevante

En proceso.

Vinculación con otros sectores de la sociedad

Se tienen formalizados los siguientes convenios institucionales:

- IBM
- Microsoft
- Secretaria de la Defensa Nacional (SEDENA)
- Asociación Nacional de Institutos y Escuelas de Tecnología de Información (ANIEI)
- Asociación Latinoamericana de Profesionales de Seguridad de la Información (ALAPSI)
- Instituto de Administración de Proyectos (PMI)
- CANACINTRA
- TOASTMASTERS
- Instituto Internacional de Análisis de Negocios (IIBA).
- Foro de Administración del Servicio de Tecnología de Información (ITSMF).

En proceso

- Open Group
- ISACA
- IEEE
- COPARMEX
- AMESOL
- HUAWEI

Los organismos colegiados (Consejos Consultivo y Técnico) está integrado por los presidentes de los organismos, asociaciones e instituciones del ámbito de la Tecnología de Información como: ISACA, OPEN GROUP, PMI, ITSMF, TOASTMASTERS, ALAPSI, ANIEI entre otros.

Trámites administrativos

REQUISITOS

- Título de licenciatura en los programas señalados.
- Manejo de la lectura del idioma inglés equivalente al menos a 1000 puntos en el Examen EXANI III de ingreso a posgrado de CENEVAL o similar.

PROCESO DE ADMISIÓN

- Realizar cita para entrevista con el Coordinador (14:00 a 20:00) lunes a viernes.
- Hacer el pago del trámite de admisión.
- Realizar entrevista con el Coordinador (tiempo aproximado 30 minutos).
- Entregar en el momento de la entrevista:
    - Curriculum vitae.
    - Una carta explicando los motivos por los que desea ingresar a la maestría.
    - Dos cartas de recomendación (por su experiencia, cualidades, crecimiento profesional, etc.)
- Análisis de información, otorgamiento de veredicto.
- Resultado de aceptación y entrega de carta de aceptación en su caso.

DOCUMENTACIÓN

- Acta de nacimiento original.
- Título y Cédula Profesional, original y copia.
- Recibo de pago de inscripción.
- Carta de aceptación.
- Solicitud de ingreso al Posgrado (formato Ibero)
- Solicitud de materias (formato Ibero)
- Carta compromiso firmada (formato Ibero)
- Si eres extranjero, copia fotostática de la forma migratoria FM-2.

DURACIÓN DE LA ESPECIALIDAD

- Un año y un verano.

HORARIOS

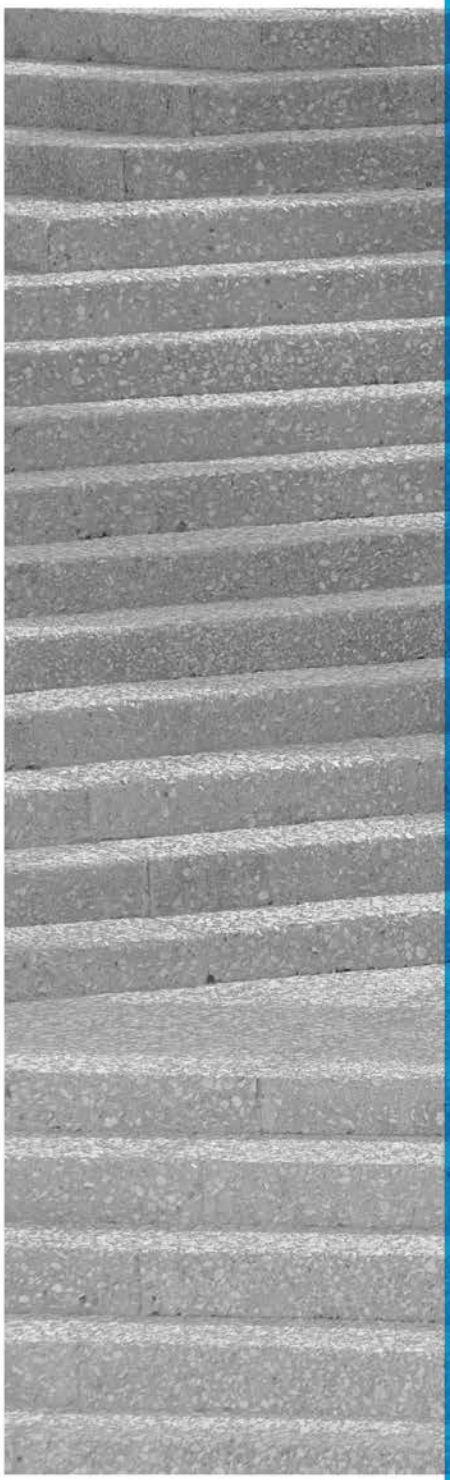
- Lunes y Miércoles de 18:00 a 20:00 y de 20:00 a 22:00 hrs. (1er. y 3er. semestre).
- Martes y Jueves de 18:00 a 20:00 y de 20:00 a 22:00 hrs. (2do. y 4to. semestre).

CONTACTOS

M. en C. Pedro Solares Soto
Coordinador de la Especialidad en Seguridad de la Información
Tel.: 52 (55) 5950-4000
Ext.: 4720
pedro.solares@ibero.mx

Erika Ton Sánchez
Asistente de la Especialidad en Seguridad de la Información
Tel.: 52 (55) 5950-4000
Ext.: 4298
erika.ton@ibero.mx

Para obtener más información sobre el Programa de Posgrado
Coordinación de Promoción del Posgrado
Tel. +52 (55) 5950-4000 ext. 7518 y 7534
atencion.posgrado@ibero.mx



IBERO
Ciudad de México • Tijuana ®

ATENCIÓN A ASPIRANTES DE POSGRADO

Tel. 5950 - 4000 exts. 4530, 7534 y 7518
atencion.posgrados@ibero.mx
www.ibero.mx/posgrados

Prol. Paseo de la Reforma 880
Lomas de Santa Fe, CP 01219
Ciudad de México