Universidad Autónoma del Estado de México

Licenciatura en Informática Administrativa

PROGRAMA DE ESTUDIOS

GESTIÓN DE SEGURIDAD INFORMÁTICA

Elaboró:	L.I.A. Alejandro Domínguez Bond	Facultad de Contaduría y Administración.
	Dra. en S. Sara del Socorro Mota González	Facultad de Contaduría y Administración.
	Ing. en C. Adriana Trejo Patiño	Facultad de Contaduría y Administración.

	H. Consejo Académico	**H. Consejo de Gobierno**
Fecha de aprobación:		

Facultad de Contaduría y Administración

Índice

I. Datos de identificación.

Espacio académico donde se imparte	**Facultad de Contaduría y Administración** **Centro Universitario UAEM Atlacomulco** **Centro Universitario UAEM Ecatepec** **Centro Universitario UAEM Temascaltepec** **Centro Universitario UAEM Texcoco** **Centro Universitario UAEM Valle de México** **Centro Universitario UAEM Valle de Chalco** **Centro Universitario UAEM Teotihuacán**

Estudios profesionales	**Licenciatura en Informática Administrativa, 2018**						
Unidad de aprendizaje	**Gestión de seguridad informática**			Clave	**LIAA29**		
Carga académica	**2** Horas teóricas	**4** Horas prácticas	**6** Total de horas	**8** Créditos			
Carácter	**Obligatoria**	Tipo	**Taller**	Periodo escolar	**Séptimo**		
Área curricular	**Ingeniería y seguridad**		Núcleo de formación	**Integral**			
Seriación	**Ninguna** UA Antecedente		**Ninguna** UA Consecuente				

Formación común

No presenta	**X**

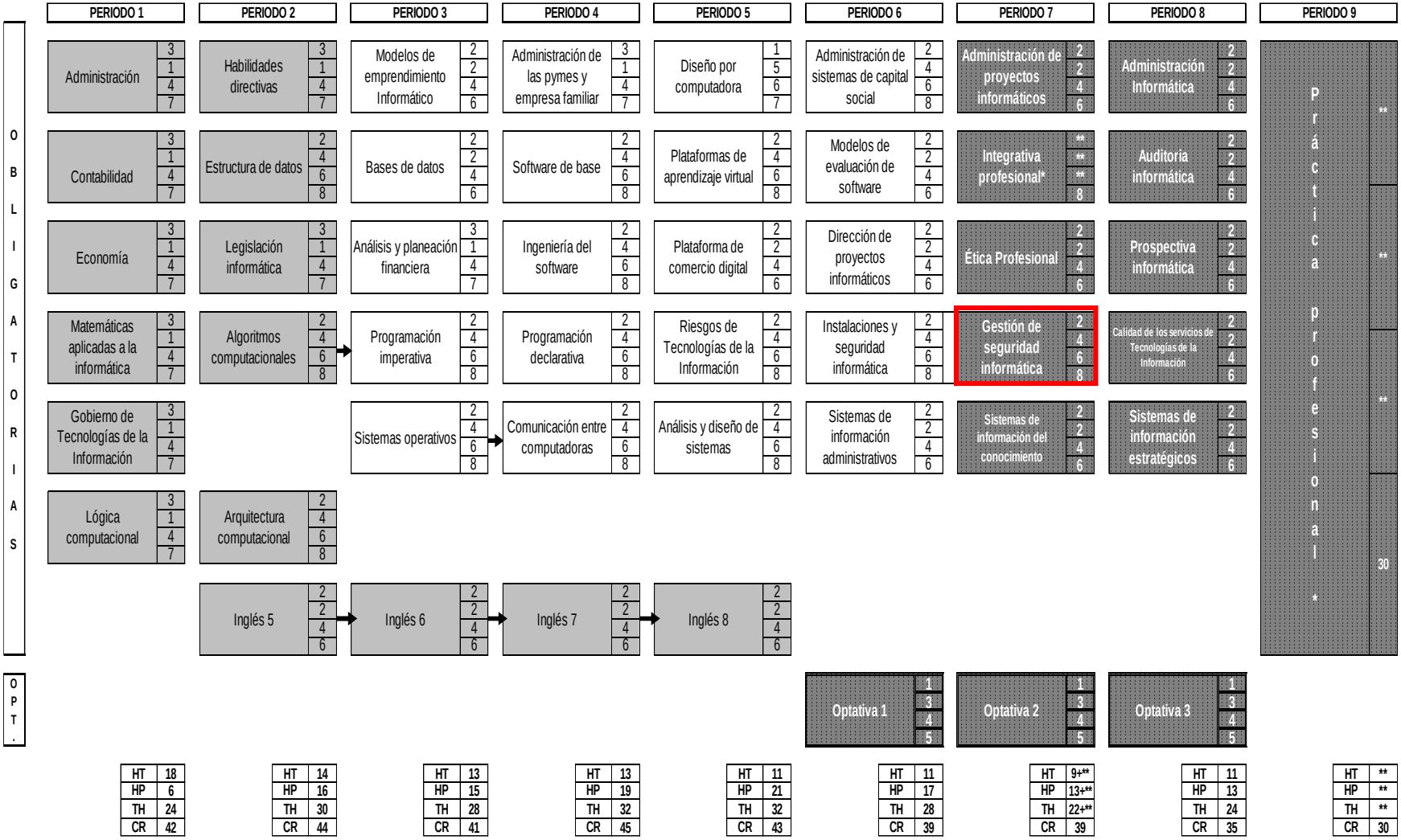
II. Presentación del programa de estudios

Esta UA permitirá al egresado de la Licenciatura en Informática Administrativa identificar, diseñar, administrar y evaluar aspectos de seguridad y calidad de las TIC's en el ámbito de los negocios.

Asimismo, fomentar la aplicación de políticas, procedimientos, prácticas y estructuras organizacionales que permitan evaluar constantemente la función de las nuevas tecnologías y optimizar su potencial para las organizaciones, al mismo tiempo que las mantienen a salvo y proveer una garantía razonable de que sean alcanzados los objetivos y la continuidad del negocio. En esta UA se tiene la intención de formar profesionistas capaces de implementar sistemas de seguridad bajo políticas internas de las organizaciones y estándares aceptados.

Esta UA se encuentra estructurada por cinco unidades temáticas de tal manera que el aprendizaje es evolutivo en el conocimiento adquirido, iniciando con una perspectiva general de la gestión de riesgos, para después continuar con el aprendizaje de seguridad en sistemas, conocer el monitoreo de la seguridad informática, la Norma ISO 27000/2005 y finalizar con el conocimiento de los diferentes tipos de firewall para la protección de la información en las organizaciones.

III. Ubicación de la unidad de aprendizaje en el mapa curricular



DISTRIBUCIÓN DE LAS UNIDADES DE APRENDIZAJE OPTATIVAS

PERIODO 1	PERIODO 2	PERIODO 3	PERIODO 4	PERIODO 5	PERIODO 6	PERIODO 7	PERIODO 8	PERIODO 9
OPTATIVAS					Projects based on PMBok ï (1 3 4 5)	Gobierno de TI basados en COBIT (1 3 4 5)	Gestión y análisis de BIG DATA (1 3 4 5)	
					Desarrollo de proyectos complejos basados en SCRUM (1 3 4 5)	Servicios de IT basados en ITIL (1 3 4 5)	Arquitectura empresarial basada en TOGAF (1 3 4 5)	
					Inteligencia de negocios BI (1 3 4 5)	Lenguaje extensible de iinformes de negocios XBRL (1 3 4 5)	Sistemas de planificación de recursos empresariales ERP (1 3 4 5)	

SIMBOLOGÍA

Unidad de aprendizaje	HT: Horas Teóricas
	HP: Horas Prácticas
	TH: Total de Horas
	CR: Créditos

→ 5 líneas de seriación.
* Actividad académica.
** Horas de las actividades académicas
Créditos mínimos 20 y máximos 45 por periodo escolar.

- Núcleo básico obligatorio.
- Núcleo sustantivo obligatorio.
- Núcleo integral obligatorio.
- Núcleo integral optativo

PARÁMETROS DEL PLAN DE ESTUDIOS

Núcleo básico obligatorio: cursar y acreditar 15 UA	38 28 66 104	Total del núcleo básico: acreditar 15 UA para cubrir 104 créditos
Núcleo sustantivo obligatorio: cursar y acreditar 20 UA	41 63 104 145	Total del núcleo sustantivo acreditar 20 UA para cubrir 145 créditos
Núcleo integral obligatorio: cursar y acreditar 9 UA + 2*	18+** 20+** 38+** 94	Total del núcleo integral acreditar 12 UA +2* para cubrir 109 créditos
Núcleo integral optativo: cursar y acreditar 3 UA	3 9 12 15	

TOTAL DEL PLAN DE ESTUDIOS	
UA obligatorias	44 +2 Actividades académicas
UA optativas	3
UA a acreditar	47+2 actividades académicas
Créditos	358

IV. Objetivos de la formación profesional.

Objetivos del programa educativo:

Son objetivos de la licenciatura en Informática Administrativa, formar profesionales con conocimientos sólidos en Tecnologías de la Información que diseñen, innoven e implementen sistemas de información con el fin de aplicarlos a los procesos de planeación, organización, dirección y control de una organización y así coadyuvar a incrementar su eficiencia y productividad.

Generales

- Asumir los principios y valores universitarios, y actuar en consecuencia.
- Ampliar su universo cultural para mejorar la comprensión del mundo y del entorno en que vive, para cuidar de la naturaleza y potenciar sus expectativas.
- Cuidar su salud y desarrollar armoniosamente su cuerpo; ejercer responsablemente y de manera creativa el tiempo libre.
- Desarrollar la sensibilidad y el arte como base de la creatividad.
- Reconocer la diversidad cultural y disfrutar de sus bienes y valores.
- Tomar decisiones y formular soluciones racionales, éticas y estéticas.
- Ejercer el diálogo y el respeto como principios de la convivencia con sus semejantes, y de apertura al mundo.
- Cuidar su salud y desarrollar armoniosamente su cuerpo; ejercer responsablemente y de manera creativa el tiempo libre.

Particulares

- Gestionar sistemas de información administrativa, mediante métodos de algoritmos, de programación, entre otros para detectar y controlar problemas informáticos como el mal uso de software, virus, entre otros, dentro de una organización.
- Diseñar proyectos informáticos innovadores que optimicen los recursos tecnológicos de una organización mediante el uso de las nuevas tecnologías de la información como los servicios de mensajería instantánea, el comercio electrónico, e- gobierno, banca en línea, servicios peer-to-peer, correo electrónico, etc. empleando habilidades lingüístico-comunicativas en una segunda lengua para comprender el avanzado cambio tecnológico.
- Auditar sistemas de seguridad de la información de una organización a través de la incorporación de estrategias y métodos de análisis de datos e información como la visualización de datos, la minería de datos, los análisis semánticos de textos, la programación y optimización matemática, las redes neuronales, entre otros para llevar a cabo procesos informático-administrativos y proveer agilidad a las organizaciones.

Objetivos del núcleo de formación:

Proveerá al alumno de escenarios educativos para la integración, aplicación y desarrollo de los conocimientos, habilidades y actitudes que le permitan el desempeño de funciones, tareas y resultados ligados a las dimensiones y ámbitos de intervención profesional o campos emergentes de la misma.

Objetivos del área curricular de curricular o disciplinaria:

Diseñar y justificar el aseguramiento de la integridad y confidencialidad de la información por medio de herramientas como ingeniería de software, ciberseguridad, sistemas distribuidos para desarrollar proyectos que incrementen la seguridad y productividad de los sistemas de información de una organización.

V. Objetivos de la unidad de aprendizaje

Organizar conocimientos científicos y tecnológicos en la solución de problemas en el área Informática con un enfoque interdisciplinario; a través de la selección óptima de técnicas y herramientas computacionales actuales y emergentes y la aplicación de normas, marcos de referencia, estándares de calidad, seguridades vigentes en el ámbito del desarrollo y gestión de tecnologías y sistemas de información.

VI. Contenidos de la unidad de aprendizaje, y su organización.

Unidad 1. La Denominación de las Unidades, debe ser breve, interesante, debe guardar coherencia con su objetivo y los temas que la integran. Sin negritas.
Objetivo: Aplicar los mecanismos y herramientas de protección para el cuidado de la seguridad informática en una organización de manera física y lógica.
Temas: 1. Sistemas y Mecanismos de Protección. 1.1.1. Seguridad Física. 1.1.1.1. Protección del hardware. 1.1.1.2. Contratación de Personal. 1.1.2. Seguridad Lógica. 1.1.2.1. Identificación y Autenticación. 1.1.2.2. Control de Acceso Interno. 1.1.2.3. Control de Acceso Externo. 1.2. Seguridad en Redes de Datos. 1.2.1. Amenazas y Ataques a Redes. 1.2.2. Elementos Básicos de Protección. 1.2.3. Introducción a la Criptografía. 1.2.4. Seguridad de la Red a nivel: 1.2.4.1. Aplicación. 1.2.4.2. Transporte. 1.2.4.3. Red. 1.2.4.4. Enlace. 1.2.5. Monitoreo. 1.3. Seguridad en Redes Inalámbricas. 1.3.1. Seguridad en el Access Point. 1.3.2. SSID (Service Set Identifier). 1.3.3. 1.3.3 WEP (Wired Equivalent Privacy). 1.3.4. Filtrado de MAC Address. 1.3.5. RADIUS Authentication. 1.3.6. WLAN VPN. 1.3.7. Seguridad sobre 802.11(x).

Unidad 2. Seguridad en Sistemas.
Objetivo: Aplicar los mecanismos y herramientas de protección para el cuidado de la seguridad informática en una organización.
Temas: 2.1 Riesgos de Seguridad en Sistemas. 2.2 Arquitectura de los Sistemas. 2.3 Problemas Comunes de Seguridad. 2.4 Instalación Segura de Sistemas. 2.5 Administración de Usuarios y controles de acceso. 2.6 Administración de Servicios. 2.7 Monitoreo. 2.8 Actualización de los Sistemas. 2.9 Mecanismos de Respaldo.

Unidad 3. Monitoreo de la seguridad informática.
Objetivo: Aplicar técnicas que permitan administrar la seguridad y las tecnologías de detección de intrusos para la protección de redes y sistemas dentro de una organización.
Temas: 3.1 Administración de la Seguridad Informática. 3.1.1 Administración de cumplimiento de Políticas. 3.1.2 Administración de Incidentes. 3.1.3 Análisis de nuevas Vulnerabilidades en la Infraestructura. 3.1.4 Monitoreo de los Mecanismos de Seguridad. 3.2 Detección de Intrusos. 3.2.1Sistemas Detectores de Intrusos. 3.2.2 Falsos Positivos. 3.2.3 Falsos Negativos. 3.2.4 Métodos de Detección de Intrusos. 3.2.4.1 Análisis de Tráfico. 3.2.4.2 HIDS (Host Intrusión Detection System). 3.2.4.3 NIDS (Network Intrusión Detection System). 3.2.4.4 Nuevos métodos de detección. 3.2.5. Identificación de Ataques. 3.2.6. Análisis del Tiempo de Respuesta de los IDS.

Unidad 4. Norma ISO 27001.
Objetivo: Analizar la norma ISO 27001 para su aplicación.
Temas: 41 Evolución de la familia ISO 27001. 4.2 Objetivos de control y controles. 4.2.1 Política de seguridad. 4.2.2 Organización para la seguridad de la información. 4.2.3 Administración de activos. 4.2.4 Seguridad de los recursos humanos. 4.2.5 Seguridad física y ambiental. 4.2.6 Gestión de las comunicaciones y operaciones. 4.2.7 Control de accesos. 4.2.8 Adquisición, desarrollo y mantenimiento de sistemas de información. 4.2.9 Gestión de incidentes de la seguridad de la información. 4.2.10 Gestión de la continuidad del negocio. 4.2.11 Cumplimiento.

Unidad 5. Firewalls como Herramientas de Seguridad.
Objetivo: Evaluar los diferentes tipos de firewall como método de protección de una red de computadoras para proteger la información de las organizaciones.
Temas: 5.1 Tipos de firewall: de software y de hardware. 5.1.1 Firewall de capas inferiores. 5.1.2 Firewall de capa de aplicación. 5.1.3 Firewall personal. 5.2 Ventajas de un firewall. 5.3 Limitaciones de un firewall. 5.4 Políticas del firewall.

VIII. Acervo bibliográfico.

Básico:

- Baca, Gabriel. (2018). Introducción a la Seguridad Informática. Primera Edición, Grupo Editorial Patria
- Cano, Jeimy (2009). Computación Forense Descubriendo los Rastros Informáticos. Alfaomega
- Garrido, Juan (2009). Análisis Forense Digital en Entornos Windows. Informática 64
- Gómez, Álvaro (2011) Enciclopedia de la Seguridad Informática. Alfaomega Ra.Ma
- González, Gilberto. (2019) Manual del Hacker Ético Proyectos prácticos de seguridad informática. Six Ediciones
- Jara, Hector. (2009). Hackers al descubierto. Six Ediciones
- Stallings, W., Fundamentos de seguridad en redes. Aplicaciones y estándares. Segunda Edición, Editorial Pearson. ISBN 84-205-4002-1

Complementario:

- Aguirre, Jorge R. “Libro Electrónico de Seguridad Informática y Criptografía”. (2006); Depósito Legal M-10039-2003. Disponible en Internet en http://www.criptored.upm.es/guiateoria/gt_m001a.htm
- Becerril, L., Diego (2007). Instalaciones Eléctricas Prácticas. ESIME. IPN
- De la Torre, C., Sánchez, P, & Vélez, M. (2018). Sistemas de Prevención de Intrusos (IDS) en la gestión de la información. Guayaquil: Centro de Investigación y Desarrollo Profesional CIDEPRO. Recuperado de https://www.researchgate.net/publication/328007416_Sistemas_de_Prevencion_de_Intrusos_IDS_en_la_Gestion_de_la_Informacion
- Martinez, G., Ocampo, C. & Bermúdez, Y. (2017). Sistema de detección de intrusos en redes corporativas. Scientia et technica, 22(1), 60-68. DOI: https://doi.org/10.22517/23447214.9105
- Norma ISO 27001:2005.