UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

LICENCIATURA EN INFORMÁTICA ADMINISTRATIVA

GUÍA DE EVALUACIÓN DEL APRENDIZAJE

GESTIÓN DE SEGURIDAD INFORMÁTICA

Elaboró:	M. en C.C Juan Carlos Cisneros Rasgado	Centro Universitario UAEM Valle de Chalco

	H. Consejo Académico	**H. Consejo de Gobierno**
Fecha de aprobación:	15 de julio de 2021	15 de julio de 2021

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	Horas teóricas	Horas prácticas	Total de horas	Créditos
	2	**4**	**6**	**8**

Carácter	Tipo	Periodo escolar
Obligatoria	**Taller**	**Séptimo**

Área curricular	Núcleo de formación
Ingeniería y seguridad	**Integral**

Seriación	UA Antecedente	UA Consecuente
	Ninguna	**Ninguna**

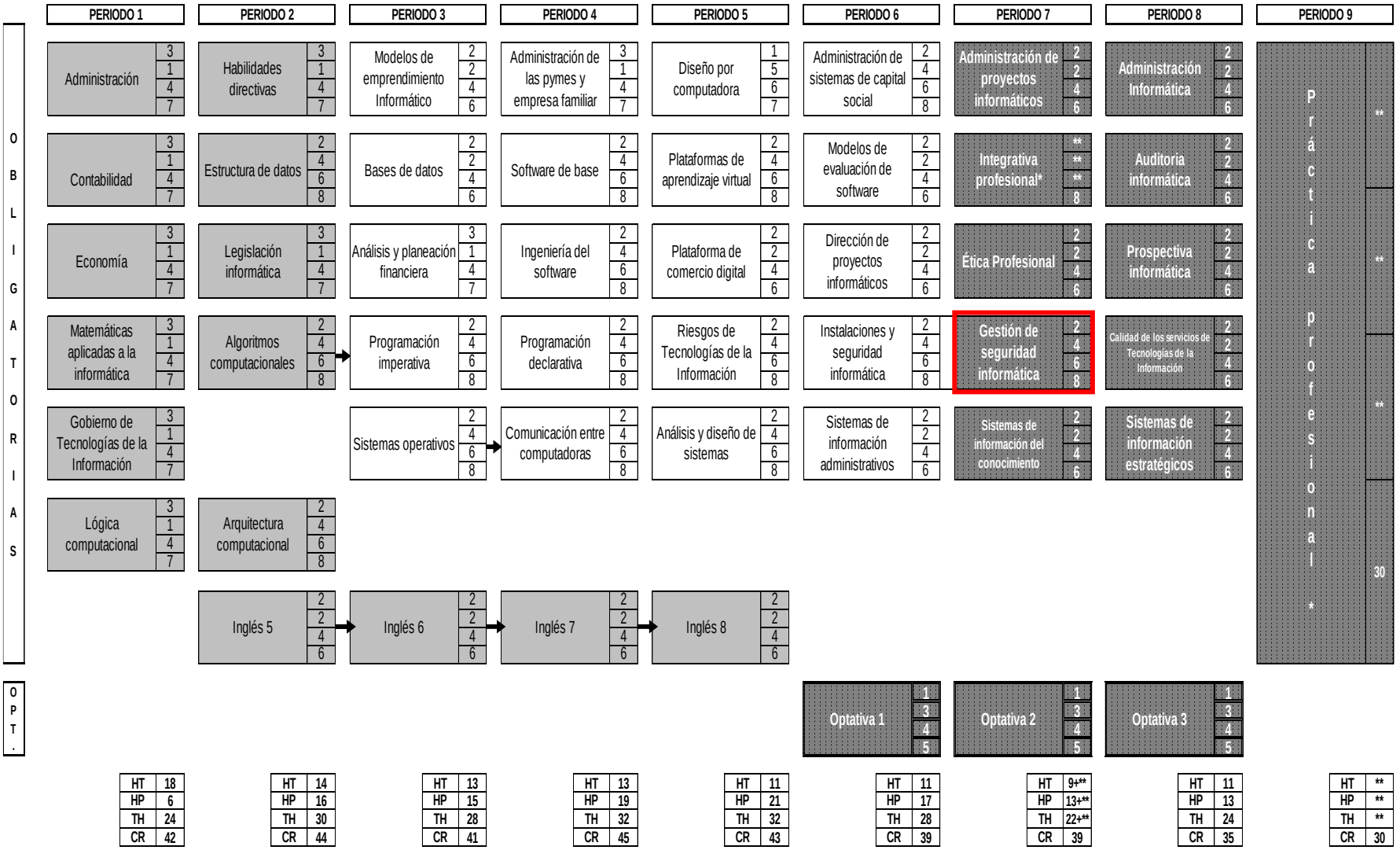
Formación común

No presenta	**X**

II. Presentación de la Guía.

La unidad de aprendizaje de gestión de Seguridad Informática habilita al estudiante de Licenciatura en Informática Administrativa en los conocimientos y habilidades para diseñar y gestionar normas de seguridad y estándares para el aseguramiento de los activos informáticos de las organizaciones mediante la elaboración de reportes, infogramas, proyectos, manuales, entre otros instrumentos que se evaluarán a treves de listas de cotejo, guías de observación y exámenes, con el fin de lograr el objetivo de la UA.

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 I (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 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.

V. Diseño de la evaluación: Factores, Criterios e Indicadores.

Unidad 1. Mecanismos y herramientas de protección.

Factores	Criterios	Indicadores
Aplicar los mecanismos y herramientas de protección para el cuidado de la seguridad informática en una organización de manera física y lógica.	1.1 Sistemas y Mecanismos de Protección. 1.1.1. Seguridad Física. 1.1.2. Seguridad Lógica. 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: 1.2.5. 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. 1.3.4. Filtrado de MAC Address. 1.3.5. RADIUS Authentication. 1.3.6. WLAN VPN. 1.3.7. Seguridad sobre 802.11(x).	Reconoce y emplea con claridad los conceptos y técnicas de encriptado mediante la elaboración de un reporte. Elabora un infograma que incluye las herramientas para mitigar amenazas informáticas que pongan en riesgo la integridad de la información.

Unidad 2. Seguridad en Sistemas.		
Factores	**Criterios**	**Indicadores**
Aplicar los mecanismos y herramientas de protección para el cuidado de la seguridad informática en una organización.	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.	Integra proyectos de seguridad en la instalación, despliegue y respaldos de Sistemas de Información. Diseña algoritmos de control de acceso en los Sistemas de Información.

Unidad 3. Monitoreo de la seguridad informática.		
Factores	**Criterios**	**Indicadores**
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.	3.1 Administración de la Seguridad Informática. 3.2 Detección de Intrusos.	Emplea distintas herramientas computacionales que permite detectar intrusos.

<table>
<tr><td colspan="3">Unidad 4. Norma ISO 27001.</td></tr>
<tr><th>Factores</th><th>Criterios</th><th>Indicadores</th></tr>
<tr><td rowspan="2">Analizar la norma ISO 27001 para su aplicación.</td><td rowspan="2">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.</td><td>Conoce eficientemente las normas ISO, lo que permite el manejo de las políticas de calidad en seguridad informática, para organizar y administrar con éxito los archivos de la organización.</td></tr>
<tr><td>Gestiona eficiente de los temas que permitan la operabilidad de las tecnologías de comunicación.</td></tr>
</table>

Unidad 5. Firewalls como Herramientas de Seguridad.		
Factores	**Criterios**	**Indicadores**
Evaluar los diferentes tipos de firewall como método de protección de una red de computadoras para proteger la información de las organizaciones.	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.	Aplica los firewalls de software y hardware como coadyuvantes en la integridad de los datos.
	5.2 Ventajas de un firewall.	
	5.3 Limitaciones de un firewall.	
	5.4 Políticas del firewall.	

VI. Diseño de los instrumentos de observación

a) Mediciones que derivan en puntajes

Indicador	Evaluación	Instrumento
Reconoce y emplea con claridad los conceptos y técnicas de encriptado mediante la elaboración de un reporte.	Formativa Sumativa	Guía de observación de Reporte
Elabora un infograma que incluye las herramientas para mitigar amenazas informáticas que pongan en riesgo la integridad de la información.		Lista de Cotejo para Infograma
Integra proyectos de seguridad en la instalación, despliegue y respaldos de Sistemas de Información.	Sumativa	Guía de observación para Proyecto
Diseña algoritmos de control de acceso en los Sistemas de Información.		Lista de Cotejo de Algoritmo
Emplea distintas herramientas computacionales que permite detectar intrusos.	Formativa Sumativa	Guía de observación
Conoce eficientemente las normas ISO, lo que permite el manejo de las políticas de calidad en seguridad informática, para organizar y administrar con éxito los archivos de la organización.	Formativa Sumativa	Guía de observación
Gestiona eficiente de los temas que permitan la operabilidad de las tecnologías de comunicación.		Lista de Cotejo
Aplica los firewalls de software y hardware como coadyuvantes en la integridad de los datos	Sumativa	Guía de observación

b) Estimaciones no cuantificables

Evaluación	Instrumento	¿Qué evalúa?
Evaluación diagnostica	Examen	Conocimientos previos

VII. Administración de los instrumentos y registro de evidencias.

Período	Indicador	Evidencias	Instrumento	Puntaje
Primera evaluación parcial	Reconoce y emplea con claridad los conceptos y técnicas de encriptado mediante la elaboración de un reporte.	Desempeño	Guía de observación de Reporte	10%
	Elabora un infograma que incluye las herramientas para mitigar amenazas informáticas que pongan en riesgo la integridad de la información.	Producto	Lista de Cotejo para Infograma	10%
	Integra proyectos de seguridad en la instalación, despliegue y respaldos de Sistemas de Información.	Desempeño	Guía de observación para Proyecto	20%
	Diseña algoritmos de control de acceso en los Sistemas de Información.	Producto	Lista de Cotejo de Algoritmo	20%
			Examen	40%
			Total	**100%**

Período	Indicador	Evidencias	Instrumento	Puntaje
Segunda evaluación parcial	Emplea distintas herramientas computacionales que permite detectar intrusos.		Guía de observación para Reporte	20%
	Conoce eficientemente las normas ISO, lo que permite el manejo de las políticas de calidad en seguridad informática, para organizar y administrar con éxito los archivos de la organización.		Guía de observación para Mapa metal	10%
	Gestiona eficiente de los temas que permitan la operabilidad de las tecnologías de comunicación.		Lista de Cotejo de manual	20%
	Aplica los firewalls de software y hardware como coadyuvantes en la integridad de los datos		Guía de observación para Reporte	10%
			Examen	40%
			Total	**100%**
Evaluación ordinaria	Organizar conocimientos científicos y tecnológicos en la solución de problemas en el área Informática	Conocimiento Desempeño Producto	Examen	100%
Evaluación extraordinaria		Conocimiento Desempeño Producto	Examen	100%

Período	Indicador	Evidencias	Instrumento	Puntaje
Evaluación a Título de suficiencia	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.	Conocimiento Desempeño Producto	Examen	100%

VIII. Evaluación del aprendizaje.

a) Interpretación de apreciaciones y/o datos.

La unidad de aprendizaje que se presenta se desarrolla de manera práctica y teórica por lo que es importante lograr que los estudiantes elaboren ejercicios a través de los cuales desenvuelvan su potencial en tecnología de manera aplicada. Derivado de lo anterior se considera pertinente la creación de guías de observación y listas de cotejo para llevar a cabo la evaluación de los estudiantes permitiendo al docente verificar las practicas que se realizan a lo largo del desarrollo de las unidades ya que estos instrumentos reflejaran el conocimiento adquirido.

Se constituye el temario agrupando los contenidos de la UA en cinco unidades temáticas, distribuyendo los conceptos teóricos que ayudan a lograr un conocimiento adecuado e interpretación de las prácticas que se desarrollan durante el curso, lo cual permitirá la obtención de las competencias que esta UA proporciona.

La unidad uno incluye el análisis de los principales conceptos de importancia para el curso, que permite aplicar efectivamente los mecanismos y herramientas de protección para el cuidado de la seguridad informática en una organización de manera física y lógica.

En la segunda unidad se analizan los sistemas de información para aplicar los mecanismos y herramientas de protección para el cuidado de la seguridad informática en una organización.

La unida tres demandas de la aplicación de técnicas que permitan administrar la seguridad y las tecnologías de detección de intrusos para la protección de redes y sistemas dentro de una organización.

La unidad cuatro analiza la norma ISO 27001 para su aplicación garantizando buenas prácticas de seguridad informática con procedimientos establecidos de calidad.

Finalmente, la unidad cinco tiene como propósito evaluar los diferentes tipos de firewall como método de protección de una red de computadoras para proteger la información de las organizaciones.

b) Juicios y conclusiones valorativas.

EL alumno debe asistir en tiempo y forma a por lo menos el 80% a sus actividades presenciales o en línea y cumplir con los horarios establecidos para la unidad aprendizaje. Participar en el proceso de enseñanza-aprendizaje con estudio, iniciativa y proactividad. Entregar los trabajos asignados en tiempo y forma, respetando los lineamientos establecidos al inicio del curso. Participar en el intercambio de experiencias e ideas. El alumno deberá mantener un comportamiento y lenguaje respetuoso en el aula y/o en línea.

c) Asignación, entrega y revisión de resultados.

El docente se compromete a desarrollar cada uno de los temas, resolver dudas y realizar ejemplos de tal forma que los estudiantes asimilen el conocimiento al máximo.

Calificar según lo planteado en esta Guía de Observación, listas de cotejo, por unidad y dos exámenes uno por parcial, así como el proyecto integrativo final.

El docente también se compromete a entregar las calificaciones en tiempo y forma como lo estipula el reglamento, así mismo a dar revisión conforme a la presente Guía de observación a cada uno de los alumnos, respetando el porcentaje obtenido por cada uno y los tiempos reglamentarios. Y en su caso si el estudiante solicita revisión de la calificación asentada durante los primeros cinco días naturales posteriores.

Por otro lado, se solicita al estudiante se comprometa a cumplir con las asistencias que marca el reglamento de facultades y escuelas, a presentarse en las fechas estipuladas a realizar el examen correspondiente, así como llevar a cabo todas las practicas que indique el docente para ser evaluado de acuerdo con las rubricas y listas de cotejo.

El estudiante debe respetar los tiempos estipulados en el calendario escolar oficial. El docente y el alumno se comprometen a mantener una relación de respeto, mediante una actitud positiva, de manera colaborativa, con constante comunicación en pro del desarrollo educativo y con el objetivo de lograr el mayor desempeño académico.