INGENIERIA TECNOLOGÍAS DE LA INFORMACIÓN/SISTEMAS COMPUTACIONALES
EN COMPETENCIAS PROFESIONALES

ASIGNATURA DE SEGURIDAD INFORMÁTICA

PROPÓSITO DE APRENDIZAJE DE LA ASIGNATURA	El alumno establecerá estrategias de protección de la información mediante el uso de métodos y estándares de seguridad informática para preservar los activos informáticos de la organización.				
CUATRIMESTRE	Noveno				
TOTAL DE HORAS	PRESENCIALES	NO PRESENCIALES	**HORAS POR SEMANA**	PRESENCIALES	NO PRESENCIALES
	75	0		5	0

UNIDADES DE APRENDIZAJE	**HORAS DEL SABER**		**HORAS DEL SABER HACER**		**HORAS TOTALES**	
	P	**NP**	**P**	**NP**	**P**	**NP**
I. Fundamentos de seguridad	**10**	**0**	**5**	**0**	**15**	**0**
II. Seguridad física y lógica	**5**	**0**	**15**	**0**	**20**	**0**
III. Seguridad en redes e internet	**5**	**0**	**10**	**0**	**15**	**0**
IV. Tendencias en la seguridad informática	**10**	**0**	**15**	**0**	**25**	**0**
TOTALES	**30**		**45**		**75**	

ELABORÓ:	Comité de Directore de la ingenieria en tecnologías de la información/sistemas computacionales	**REVISÓ:**	Dirección Académica
APROBÓ:	C. G. U. T. y P.	**FECHA DE ENTRADA EN VIGOR:**	Septiembre 2018

COMPETENCIA A LA QUE CONTRIBUYE LA ASIGNATURA

De acuerdo con la metodología de diseño curricular de la CGUTyP, las competencias se desagregan en dos niveles de desempeño: Unidades de Competencias y Capacidades.

La presente asignatura contribuye al logro de la competencia y los niveles de desagración decritos a continuación:

COMPETENCIA: Desarrollar soluciones innovadoras de integración de tecnologías de la información mediante metodologías de desarrollo de software, diseño de base de datos, seguridad de la información y administración de proyectos; con base en los estándares aplicables para atender las áreas de oportunidad, resolver las necesidades y optimizar los procesos y recursos de la organización.

UNIDADES DE COMPETENCIA	CAPACIDADES	CRITERIOS DE DESEMPEÑO
Gestionar proyectos innovadores de integración de tecnologías de la información mediante metodología de investigación, herramientas administrativas y estándares aplicables para la optimización de procesos y recursos.	Diseñar proyectos innovadores de integración de tecnologías de la información de acuerdo a un diagnóstico de áreas de oportunidad empleando metodología de investigación, estándares y herramientas aplicables para la optimización de procesos y recursos de la organización.	Elabora un proyecto de integración de Tecnologías de la Información que especifique: - Descripción del proyecto. - Idea o planteamiento del problema - Diagnóstico situacional o Estado del Arte - Alcance - Justificación - Beneficios e impactos social y económico. - Beneficiarios directos, beneficiarios indirectos. - Objetivos y metas. - Planeación de las actividades a realizar - Cronograma especificando actividades, tiempos y responsables. - Requerimientos de infraestructura tecnológica y recursos humanos - Aspectos financieros - Presupuesto desglosado. - Propuesta de fuentes y formas de financiamiento - Asesoramiento especializado - Gestión de Riesgos - Estrategias de seguimiento - Indicadores de eficacia, eficiencia, impacto y sostenibilidad del proyecto - Momentos de evaluación, instrumentos a utilizar y medios de verificación. - Integración de tecnología con otros proyectos innovadores.

UNIDADES DE COMPETENCIA	CAPACIDADES	CRITERIOS DE DESEMPEÑO
	Controlar la implementación del proyecto de tecnologías de la información empleando herramientas administrativas de control y software de administración de proyectos para garantizar el cumplimiento de los objetivos.	Realiza actividades de seguimiento y administración de recursos del proyecto de acuerdo con la planeación establecida y las documenta en reportes periódicos que incluyan: - Cumplimiento de Hitos - Porcentaje de avance del cronograma - Actualización de riesgos - Ajustes a la planeación - Presupuesto ejercido - Incidencias y acciones correctivas en: recursos humanos, económicas y técnicas. - Archivos en formato digital de avances - Acta de cierre del proyecto.
	Evaluar los resultados del proyecto de tecnologías de la información mediante estándares e indicadores para contribuir a la mejora continua y toma de decisiones.	Elabora un resumen ejecutivo de evaluación del proyecto que incluya: - Análisis de los indicadores de eficacia, eficiencia, impacto y sostenibilidad - Nivel de cumplimiento de los indicadores - Propuestas de mejora ""Elabora un resumen ejecutivo de evaluación del proyecto que incluya: - Análisis de los indicadores de eficacia, eficiencia, impacto y sostenibilidad - Nivel de cumplimiento de los indicadores - Propuestas de mejora

UNIDADES DE APRENDIZAJE

UNIDAD DE APRENDIZAJE	I. Fundamentos de seguridad							
PROPÓSITO ESPERADO	El alumno implementará políticas de seguridad para promover la seguridad de los procesos y activos que están sujetos a riesgo.							
HORAS TOTALES	**P**	**NP**	**HORAS DEL SABER**	**P**	**NP**	**HORAS DEL SABER HACER**	**P**	**NP**
	15	**0**		**10**	**0**		**5**	**0**

TEMAS	SABER DIMENSIÓN CONCEPTUAL	SABER HACER DIMENSION ACTUACIONAL	SER DIMENSIÓN SOCIAFECTIVA
Fundamentos de la seguridad informática.	Reconocer los conceptos de: - Transmisión. - Procesamiento. - Almacenamiento. Identificar elementos de la seguridad informática: - Seguridad física. - Seguridad lógica. - Cifrado. - Respaldo de información. - Buenas prácticas. Identificar los tres ejes rectores de la seguridad informática: - Confidencialidad. - Integridad. - Disponibilidad. Describir el proceso de detección de vulnerabilidades de los procesos y activos informáticos.	Detectar vulnerabilidades de los procesos y activos informáticos.	Analítico. Sistemático. Gestión de la información. Responsabilidad. Honestidad. Juicio. Resolución de problemas. Toma de decisiones. Orden. Organizar y planificar. Comunicación asertiva.
Gestión de la seguridad	Definir los conceptos de sistema de gestión de la seguridad informática y ciclo del	Seleccionar la metodología de análisis de riesgo de acuerdo a la problemáticas	Analítico. Sistemático.

informática	sistema de gestión de la seguridad informática. Describir los elementos del ciclo de gestión de la seguridad informática. - Planificar. - Hacer. - Verificar . - Actuar. Identificar las contramedidas de seguridad. Describir las metodologías de análisis de riesgo - ISTMO. - USAF. - TOP (ODAS). Describir el proceso de implementación de metodologías de riesgo.	Analizar el riesgo de los procesos y activos del negocio	Gestión de la información. Responsabilidad. Honestidad. Juicio. Resolución de problemas. Toma de decisiones. Orden. Organizar y planificar. Comunicación asertiva.
Políticas de seguridad informática.	Definir concepto de política de seguridad. Identificar los criterios de determinación de las políticas de seguridad. Describir el proceso de diseño e implementación de políticas de seguridad.	Diseñar políticas de seguridad. Implementar políticas de seguridad.	Analítico. Sistemático. Gestión de la información. Responsabilidad. Honestidad. Juicio. Resolución de problemas. Toma de decisiones. Orden. Organizar y planificar. Comunicación asertiva.

PROCESO DE EVALUACIÓN		TÉCNICAS SUGERIDAS DE ENSEÑANZA Y APRENDIZAJE	ESPACIO DE FORMACIÓN			MATERIALES Y EQUIPOS
EVIDENCIA DE DESEMPEÑO	INSTRUMENTO EVALUACIÓN		AULA	TALLER	OTRO	
Elabora un reporte digital a partir de un caso práctico de un problema de seguridad informática en el que se propongan medidas de contención: - Resumen. - Introducción. - Desarrollo: - Descripción del problema de vulnerabilidad: - Seguridad física. - Seguridad lógica. - Cifrado. - Respaldo de información. - Buenas prácticas. - Metodología de análisis de riesgo elegida y su justificación - Documentación de las vulnerabilidades identificadas. - Determinación de políticas de seguridad a implementar a partir de las vulnerabilidades identificadas. - Conclusiones.	Caso práctico. Rúbrica.	Aprendizaje situado. Caso práctico. Prácticas de laboratorio.	X			Internet. PC. Laboratorio. Pintarrón. Cañón.

UNIDADES DE APRENDIZAJE

UNIDAD DE APRENDIZAJE	II. Seguridad física y lógica							
PROPÓSITO ESPERADO	El alumno auditará los sistemas informáticos para proponer políticas de seguridad.							
HORAS TOTALES	**P**	**NP**	**HORAS DEL SABER**	**P**	**NP**	**HORAS DEL SABER HACER**	**P**	**NP**
	20	**0**		**5**	**0**		**15**	**0**

TEMAS	**SABER DIMENSIÓN CONCEPTUAL**	**SABER HACER DIMENSION ACTUACIONAL**	**SER DIMENSIÓN SOCIAFECTIVA**
Ejes rectores de la seguridad informática	Definir el concepto del manejo seguro de datos. Describir las propiedades del manejo seguro de datos: - Confidencialidad de la información. - Integridad de la información. - Disponibilidad. Describir el proceso de desarrollo de las políticas relacionadas con el manejo seguro de datos.	Proponer políticas de manejo seguro de datos.	Analítico. Sistemático. Gestión de la información. Responsabilidad.
Cifrado	Identificar los tipos de cifrado: - Simétrico. - Asimétrico. Identificar las características del software de cifrado. Describir el proceso de selección de software de cifrado. Describir el proceso de cifrado de datos	Cifrar datos.	Analítico. Sistemático. Gestión de la información. Responsabilidad. Honestidad. Juicio. Resolución de problemas. Toma de decisiones Orden. Organizar y planificar. Comunicación asertiva.

Seguridad física	Definir el concepto de nivel de seguridad física. Describir las características de los niveles de seguridad física: - Desastres naturales. - Acceso a infraestructura. - Políticas sobre protección a la infraestructura. Describir el proceso de desarrollo de las políticas relacionadas con los niveles de seguridad física.	Proponer las políticas relacionadas con los niveles de seguridad física.	Analítico. Sistemático. Gestión de la información. Responsabilidad. Honestidad. Juicio. Resolución de problemas. Toma de decisiones. Orden. Organizar y planificar. Comunicación asertiva.
Auditoria	Describir las características de los procesos de: - Pruebas. - Técnicas de monitoreo. Describir las fases de la metodología de auditoria: - Estudio preliminar. - Planificación de la operación. - Desarrollo de la auditoría. - Fase de diagnóstico. - Presentación de conclusiones. - Información del plan de mejoras. Describir los procedimientos de desarrollo de auditoria.	Desarrollar auditorias.	Analítico. Sistemático. Gestión de la información. Responsabilidad. Honestidad. Juicio. Resolución de problemas. Toma de decisiones. Orden. Organizar y planificar. Comunicación asertiva.

PROCESO DE EVALUACIÓN		TÉCNICAS SUGERIDAS DE ENSEÑANZA Y APRENDIZAJE	ESPACIO DE FORMACIÓN			MATERIALES Y EQUIPOS
EVIDENCIA DE DESEMPEÑO	INSTRUMENTO EVALUACIÓN		AULA	TALLER	OTRO	

Elabora un reporte digital a partir de un caso práctico de un problema de seguridad informática que contenga:
 	
- Resumen
- Introducción
- Desarrollo
  - Propuesta de medidas de contención
  - Informe de auditoria
  - Documentación del plan de mejora.
  - Justificación de la propuesta de cifrado.
  - Propuesta de políticas para el manejo seguro de datos.
  - Propuesta de políticas relacionadas con los niveles de seguridad física.
- Conclusiones.
	Caso práctico.
	Rúbrica.
		Aprendizaje situado.
		Caso práctico.
		Prácticas de laboratorio.
				x		Internet.
						PC.
						Laboratorio.
						Pintarrón.
						Cañón.

UNIDAD DE APRENDIZAJE	III. Seguridad en redes e internet							
PROPÓSITO ESPERADO	El alumno propondrá herramientas de contención de riesgo en redes e internet para preservar los activos informáticos de la organización.							
HORAS TOTALES	**P**	**NP**	**HORAS DEL SABER**	**P**	**NP**	**HORAS DEL SABER HACER**	**P**	**NP**
	15	**0**		**5**	**0**		**10**	**0**

TEMAS	SABER DIMENSIÓN CONCEPTUAL	SABER HACER DIMENSION ACTUACIONAL	SER DIMENSIÓN SOCIAFECTIVA
Gestor unificado de amenazas	Definir el concepto de gestor unificado de amenazas. Describir las funciones del gestor unificado de amenazas: - Firewall. - Antivirus. - Antispyware. - Antispam. - Detección-prevención de intrusos. Describir el proceso de configuración del gestor unificado de amenazas.	Configurar gestores unificados de amenazas.	Analítico. Sistemático. Gestión de la información. Responsabilidad. Honestidad. Juicio. Resolución de problemas. Toma de decisiones. Orden.
Listas de acceso	Reconocer características y funciones de listas de acceso. Reconocer los tipos de listas de acceso. Describir el proceso de implementación de listas de acceso.	Implementar listas de acceso.	Analítico. Sistemático. Gestión de la información. Responsabilidad. Honestidad. Juicio. Resolución de problemas. Toma de decisiones.
Seguridad en redes inalámbricas	Reconocer las características de los protocolos de autenticación de red inalámbrica. Describir el proceso de selección y	Seleccionar los protocolos de seguridad de redes inalámbricas. Configurar los protocolos de acceso de redes inalámbricas.	Analítico. Sistemático. Gestión de la información. Responsabilidad. Honestidad.

	configuración de protocolos de autenticación de red inalámbrica.		Juicio. Resolución de problemas. Toma de decisiones.
Redes privadas virtuales	Describir el concepto y características de redes privadas virtuales. Describir el proceso de configuración de las redes privadas virtuales.	Configurar redes privadas virtuales.	Analítico. Sistemático. Gestión de la información. Responsabilidad. Honestidad. Juicio. Resolución de problemas. Toma de decisiones.
Certificados de seguridad y firmas digitales	Definir los conceptos de certificado digital y firma digital. Explicar el proceso de construcción de certificados y firmas digitales.	Construir certificados y firmas digitales.	Analítico. Sistemático. Gestión de la información. Responsabilidad. Honestidad. Juicio. Resolución de problemas. Toma de decisiones.

PROCESO DE EVALUACIÓN		TÉCNICAS SUGERIDAS DE ENSEÑANZA Y APRENDIZAJE	ESPACIO DE FORMACIÓN			MATERIALES Y EQUIPOS
EVIDENCIA DE DESEMPEÑO	INSTRUMENTO EVALUACIÓN		AULA	TALLER	OTRO	
Elabora un reporte digital a partir de un caso práctico de seguridad en la red e internet que contenga: - Resumen - Introducción - Desarrollo - Propuesta de configuración del gestor unificado de amenazas. - Propuesta de lista de acceso. - Propuesta de selección e implementación de protocolos de redes inalámbricas. - Propuesta de la configuración de redes privadas virtuales. - Propuesta de creación de certificados y firmas digitales. - Conclusiones.	Caso práctico. Rúbrica.	Aprendizaje situado. Caso práctico. Prácticas de laboratorio.		x		Pintarrón. Cañón. Internet. Firewall. Software de simulación. Access Point. Routers. Switch.

UNIDAD DE APRENDIZAJE	IV. Tendencias en la seguridad informática							
PROPÓSITO ESPERADO	El alumno analizará áreas emergentes relacionadas con la seguridad informática para prevenir riesgos debidos a técnicas emergentes.							
HORAS TOTALES	**P**	**NP**	**HORAS DEL SABER**	**P**	**NP**	**HORAS DEL SABER HACER**	**P**	**NP**
	25	**0**		**10**	**0**		**15**	**0**

TEMAS	**SABER DIMENSIÓN CONCEPTUAL**	**SABER HACER DIMENSION ACTUACIONAL**	**SER DIMENSIÓN SOCIAFECTIVA**
Legislación informática	Identificar las leyes internacionales, nacionales y locales en materia de seguridad informática. Comparar el marco legislativo de seguridad informática local, nacional e internacional. Describir el proceso de comparación de las políticas de seguridad de la organización y el marco legislativo.	Determinar el cumplimiento del marco legislativo de seguridad informática de la organización.	Analítico. Sistemático. Gestión de la información. Responsabilidad. Honestidad. Juicio Resolución de problemas. Toma de decisiones.
Hacking ético	Definir el concepto de Hacking ético. Identificar las técnicas de aplicación del Hacking ético.	Reportar resultados del hacking ético.	Analítico. Sistemático. Gestión de la información. Responsabilidad. Honestidad. Juicio. Resolución de problemas. Toma de decisiones.
Cómputo forense	Definir el concepto de cómputo forense. Describir las actividades involucradas en el análisis de cómputo forense: - Adquirir. - Preservar. - Analizar.	Presentar resultados del cómputo forense.	Analítico. Sistemático. Gestión de la información. Responsabilidad. Honestidad. Juicio. Resolución de problemas.

	- Documentar. - Presentar.		Toma de decisiones.
Nuevas amenazas de ciberseguridad	Identificar nuevas amenazas de ciberseguridad. Identificar amenazas de ciberseguridad en: - Sistemas ciberfísicos - Internet de las cosas - Internet de los servicios Describir el proceso de implementación de buenas prácticas de prevención de ciberamenazas.	Desarrollar acciones de prevención de ciberamenazas.	Analítico. Sistemático. Gestión de la información. Responsabilidad. Honestidad. Juicio. Resolución de problemas. Toma de decisiones.

PROCESO DE EVALUACIÓN		TÉCNICAS SUGERIDAS DE ENSEÑANZA Y APRENDIZAJE	ESPACIO DE FORMACIÓN			MATERIALES Y EQUIPOS
EVIDENCIA DE DESEMPEÑO	INSTRUMENTO EVALUACIÓN		AULA	TALLER	OTRO	

Elabora un reporte digital a partir de un caso práctico de un problema de seguridad informática que incluya:
 	
- Resumen.
- Introducción.
- Desarrollo:
  - Marco legislativo aplicable.
  - Resultados de la aplicación de técnicas de Hacking ético.
  - Resultados del análisis de cómputo forense.
  - Propuesta de implementación de las buenas prácticas.
 	
- Conclusiones.
	.	Aprendizaje situado.
		Caso práctico.
		Prácticas de laboratorio.
				x		Software especializado (KALI Linux, software para forense).
						Bibliografía.

REFERENCIAS BIBLIOGRÁFICAS

AUTOR	AÑO	TÍTULO DEL DOCUMENTO	LUGAR DE PUBLICACIÓN	EDITORIAL	ISBN
Michael E. Whitman, Herbert J. Mattord	2012	Principles of Information Security	Canada	Course Technology, Cengage Learning	978-1-111-13821-9
Álvaro Gómez Vieites	2013	Enciclopedia de la Seguridad Informática	México	Alfaomega Ra-Ma	978-607-707-181-5
Julio Téllez Valdéz	4a. Ed 2014	Derecho Informático	México	Mc Graw Hill	978-970-10-6964-6

REFERENCIAS ELECTRÓNICAS

AUTOR	TÍTULO DEL DOCUMENTO	FECHA DE RECUPERACIÓN	VÍNCULO
Computer Security	Computer Security Org	1/15/2017	http://computersecurity.org
NIST	Cybersecurity	1/15/2017	https://www.nist.gov/topics/cybersecurity
USA-CERT	US-CERT	3/17/2017	https://www.us-cert.gov/
UNAM-CERT	UNAM-CERT	3/17/2017	http://www.cert.org.mx/index.html