I. Identificación del Curso

Carrera:	Desarrollo de Software			**Modalidad:**	Presencial	**Asignatura UAC:**	Seguridad en software			**Fecha Act:**	Diciembre, 2018
Clave:	18MPEDS0833	**Semestre:**	8	**Créditos:**	5.40	**División:**	Informática y Computación		**Academia:**	Informática	
Horas Total Semana:	3	**Horas Teoría:**	2	**Horas Práctica:**	1	**Horas Semestre:**	54	**Campo Disciplinar:**	Profesional	**Campo de Formación:**	Profesional Extendido

Tabla 1. Identificación de la Planificación del Curso.

II. Adecuación de contenidos para la asignatura

Proposito de la Asignatura (UAC)
Que el estudiante emplee técnicas y metodologías para la protección de datos persistentes en aplicaciones informáticas, así como el análisis de los principales elementos legales en el uso de información.
Competencias Profesionales a Desarrollar (De la carrera)
Identifica las premisas de diversos problemas del área de su competencia y propone soluciones aplicando la metodología adecuada.

Tabla 2. Elementos Generales de la Asignatura

III. Competencias de la UAC

Competencias Genéricas.*
5. Desarrolla innovaciones y propone soluciones a problemas a partir de métodos establecidos. 5.6 Utiliza las tecnologías de la información y comunicación para procesar e interpretar información. 8. Participa y colabora de manera efectiva en equipos diversos. 8.1 Propone maneras de solucionar un problema o desarrollar un proyecto en equipo, definiendo un curso de acción con pasos específicos.

Competencias Disciplinares Básicas**	Competencias Disciplinares Extendidas***
CO-12 Utiliza las tecnologías de la información y comunicación para investigar, resolver problemas, producir materiales y transmitir información.	Las competencias disciplinares no se desarrollarán explícitamente en esta UAC. Se presentan como un requerimiento para el desarrollo de las competencias profesionales

Competencias Profesionales Básicas	Competencias Profesionales Extendidas
- Analiza los algoritmos, herramientas y leyes actuales para la verificación y protección de la información en aplicaciones informáticas que manipulen información delicada, y que deben ser atendidas en la elaboración de un sistema informático seguro.	- Analiza los elementos legales involucrados en la administración de datos persistentes en aplicaciones informáticas, para la creación de sitios seguros y éticos.

Tabla 3. Competencias de la Asignatura.

* Se presentan los atributos de las competencias Genéricas que tienen mayor probabilidad de desarrollarse para contribuir a las competencias profesionales, por lo cual no son limitativas; usted puede seleccionar otros atributos que considere pertinentes. Estos atributos están incluidos en la redacción de las competencias profesionales, por lo que no deben desarrollarse explícitamente o por separado.

** Las competencias Disciplinares no se desarrollarán explícitamente en la UAC. Se presentan como un requerimiento para el desarrollo de las competencias Profesionales.

*** Cada eje curricular debe contener por lo menos una Competencia Disciplinar Extendida.

IV. Habilidades Socioemocionales a desarrollar en la UAC*8

Dimensión	Habilidad
No contiene	No contiene

Tabla 4. Habilidades Construye T

*Estas habilidades se desarrollarán de acuerdo al plan de trabajo determinado por cada plantel. Ver anexo I.

V. Aprendizajes Clave

Eje Disciplinar	Componente	Contenido Central
Desarrollo de tecnologías de la información.	Seguridad de TI.	1. La seguridad de la información en el desarrollo de software. 2. Técnicas y métodos para el aseguramiento de la información. 3. La era digital y el derecho informático. 4. Medidas de seguridad y vulnerabilidades informáticas.

VI. Contenidos Centrales de la UAC

Contenido Central	Contenidos Específicos	Aprendizajes Esperados	Proceso de Aprendizaje	Productos Esperados
1. La seguridad de la información en el desarrollo de software.	- La seguridad de la información como parte de una aplicación informática. - Factores de riesgo, amenazas y estimación de impacto.	- Comprende las características básicas de la seguridad de la información, sus aplicaciones, objetivos y tendencias. - Examina los factores de riesgo y amenazas en una aplicación y estima su impacto estructural. - Compara los distintos niveles de acceso a la información empleando privilegios de usuario, listas negras y blancas, mapas de puntos de exposición y pasillos de datos.	- Investiga la definición, objetivos de seguridad de la información, seguridad de software y ciberseguridad con la finalidad de crear un organizador gráfico. - Investiga en medios electrónicos las amenazas y factores de riesgo más comunes que afectan el desempeño de un sistema y genera un compendio donde se especifiquen sus características y repercusiones. - Investiga las características de las listas blancas y negras de software; componentes de mapas de exposición y pasillos de datos; y tipos y niveles de usuarios para un sistema informático, generando con ello un organizador gráfico. - Examina las características o necesidades de una empresa básica o ejemplificada para localizar una lista blanca y negra de software, un mapa de puntos de exposición y los pasillos de datos. - Elabora un análisis básico de riesgos y amenazas de un sistema CRUD básico previamente diseñado, incluyendo tipos y niveles de usuario.	- Organizador gráfico sobre los objetivos y características de la seguridad de software. - Compendio con definiciones y características de los diferentes tipos de amenazas y factores de riesgo en los sistemas. - Organizador gráfico sobre listas blancas y negras, mapas de puntos de exposición y pasillos de datos; tipos y niveles de usuario. - Reporte de listas blancas y negras, mapas de puntos de exposición y pasillos de datos, aplicado a un proyecto, sistema o práctica. - Reporte de análisis de riesgos aplicado a un proyecto, sistema o práctica.

2. Técnicas y métodos para el aseguramiento de la información.	- La criptografía, el cifrado y otras técnicas de protección de datos y procesos de desarrollo. - Los certificados y las firmas digitales en aplicaciones informáticas.	- Implementa sistemas criptográficos básicos, como medio de protección de información en medios temporales o persistentes de un sistema informático aplicando técnicas básicas de cifrado de datos (cifrado afín, por desplazamiento, por sustitución y transposición). - Implementa técnicas de protección ante ataques comunes (SQL injection, fallos de programación, PayLoad, Exploid, etc.) en un sistema en proceso de desarrollo. - Implementa los procesos de aseguramiento a través de certificados e incorpora a las aplicaciones la identificación de usuarios por firma digital.	- Investiga en diferentes fuentes electrónicas o físicas, el concepto de criptografía, su evolución, protocolos y estándares, para realizar una exposición empleando algún medio audiovisual y responde la pregunta ¿Cuál es la relación entre criptografía y cifrado?. - Organiza las características de la criptografía simétrica y asimétrica. - Compara los algoritmos relacionados a los distintos tipos de cifrado más utilizados (cifrado afín, por desplazamiento, por sustitución y transposición). - Realiza una lectura sobre los ataques más comunes a los sistemas (SQL injection, fallos de programación, PayLoad, Exploid, etc.), incluyendo frecuencia de ataque, característica, huecos de seguridad y malas prácticas de desarrollo. - Diseña un sistema básico donde proponga la solución a algunos de los ataques a sistemas más comunes e implemente un mecanismo de cifrado de datos. - Elabora un compendio sobre certificados y firmas de digitales con la definición, llaves públicas (definición, estructura y gestión) y	

	estándares de certificación, con la información proveniente de una exposición magistral. - Elabora una exposición de cómo incorporar certificados y firmas digitales a un sistema, empleando un medio audiovisual, partiendo de una investigación realizada previamente involucrando la información del API, sintaxis y los procesos de configuración del mismo.	- Cuadro comparativo de tipos de criptografías. - Cuadro sinóptico sobre ataques más comunes a sistemas informáticos. - Sistema de prueba y métodos de corrección de ataques. - Compendio de certificados y estructura firmas digitales.

3. La era digital y el derecho informático.	- La ética profesional como herramienta fundamental en el diseño de soluciones informáticas. - El derecho informático, como parte del desarrollo de aplicaciones.	- Identifica las características de un desarrollo ético y responsable en una aplicación que manipula o resguarda información de usuarios. - Comprende los derechos y obligaciones marcados en la legislación del derecho informático al desarrollar aplicaciones informáticas.	- Realiza una investigación sobre las características de un desarrollo ético y lo compara con el desarrollo que normalmente realiza. - Investiga la legislación nacional e internacional que rigen los modelos de desarrollo de software en cuestión de seguridad, haciendo énfasis en los derechos y obligaciones que competen a los desarrolladores de sistemas. - Enlista los delitos informáticos más comunes realizados por el desarrollador de software. - Investiga los conceptos de gobierno electrónico y propiedad intelectual, así como los requisitos necesarios para la redacción de un documento donde visualicen los procesos de registro en materia de propiedad intelectual de software.	- Cuadro comparativo sobre desarrollo ético y desarrollo típico. - Cuadro de derechos y obligaciones sobre la legislación nacional e internacional. - Lista de delitos informáticos y sus características. - Documento sobre procesos de propiedad intelectual.

4. Medidas de seguridad y Vulnerabilidades informáticas.	- Los mecanismos internos y externos para la revisión de vulnerabilidades de sistemas. - Instrumentos legales para el fomento de un uso seguro y confiable de un sistema.	- Compara las técnicas de revisión básicas implementadas durante las fases de diseño y prueba de un sistema informático. - Compara las técnicas de revisión externas de un sistema, así como la legalidad de su implementación. - Elabora un documento de políticas de uso y privacidad básicos con base en legislaciones nacionales o internacionales actuales.	- Investiga en medios electrónicos, estadísticas sobre las fallas más comunes en materia de seguridad de sistemas que se cometen durante las fases de prueba o diseño de un sistema con la finalidad de evaluar un sistema prediseñado con dichas fallas. - Investiga las características del hacker ético y el pentesting como herramientas de análisis de fallas en la seguridad de los sistemas. -Analiza la legalidad del uso de algunas de las herramientas de análisis de fallas en la seguridad (hackers ético y pentesting) y las repercusiones en su uso. -Emplea la normatividad sobre los avisos de privacidad, confidencialidad y uso en los sistemas informáticos expuesta en clase por el docente o el alumno (previa investigación) usando algún medio audiovisual, para proponer uno o varios documentos similares básicos que serán aplicados en un proyecto o sistema informático elaborado por el estudiante.	- Lista de fallas de seguridad encontradas durante el proceso de diseño o prueba, aplicados a un sistema prediseñado. - Resumen sobre las características y repercusiones legales del hacker ético y del pentesting. - Documentos de los avisos de privacidad, confidencialidad y uso en los sistemas.

VII. Recursos bibliográficos, hemerográficos y otras fuentes de consulta de la UAC

Recursos Básicos:
- Espino, L. (2016). Criptografia [Kindle version]. - Gómez, A. (2017). Enciclopedia de la seguridad informática (2nd ed). España: Ra-Ma. - Congreso de la Unión. (2015). Ley general de transparencia y acceso a la información. DOF 04-05-2015 . Recuperado en noviembre del 2018 en http://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf - Congreso de la Unión. (2018). Ley federal de derecho de autor. DOF 15-06-201. Recuperado en noviembre del 2018 en http://www.diputados.gob.mx/LeyesBiblio/pdf/122_150618.pdf
Recursos Complementarios:
- Pacheco, F. y Jara, H. (2013). Hackers manual al descubierto. Buenos Aires: Fox andina. - González, L. y De Fuentes, J. (2010). Sistemas seguros de acceso y transmisión de datos. LC editorial.

VIII. Perfil profesiográfico del docente para impartir la UAC

Recursos Complementarios:
Área/Disciplina: Informática Campo Laboral: Servicios Tipo de docente: Profesional Formación Académica: Licenciatura o Ingeniería, en Electrónica, Sistemas Computacionales e Informática y carreras afines. Constancia de participación en los procesos establecidos en la Ley General del Servicio Profesional Docente, COPEEMS, COSDAC u otros.

XI. Fuentes de Consulta

Fuentes de consulta utilizadas*
- Acuerdo Secretariales relativos a la RIEMS.
- Planes de estudio de referencia del componente básico del marco curricular común de la EMS. SEP-SEMS, México 2017.
- Guía para el Registro, Evaluación y Seguimiento de las Competencias Genéricas, Consejo para la Evaluación de la Educación del Tipo Medio Superior, COPEEMS.
- Manual para evaluar planteles que solicitan el ingreso y la promoción al Padrón de Buena Calidad del Sistema Nacional de Educación Media Superior PBC-SINEMS (Versión 4.0).
- Normas Generales de Servicios Escolares para los planteles que integran el PBC. SINEMS
- Perfiles profesiográficos COPEEMS-2017
- SEP Modelo Educativo 2016.
- Programa Construye T

ANEXO II. Vinculación de las competencias con Aprendizajes esperados

Aprendizajes Esperados	Productos Esperados	Competencias Genéricas con Atributos	Competencias Disciplinares	Competencias profesionales
- Comprende las características básicas de la seguridad de la información, sus aplicaciones, objetivos y tendencias. - Examina los factores de riesgo y amenazas en una aplicación y estima su impacto estructural. - Compara los distintos niveles de acceso a la información empleando privilegios de usuario, listas negras y blancas, mapas de puntos de exposición y pasillos de datos.	- Organizador gráfico sobre los objetivos y características de la seguridad de software. - Compendio con definiciones y características de los diferentes tipos de amenazas y factores de riesgo en los sistemas. - Organizador gráfico sobre listas blancas y negras, mapas de puntos de exposición y pasillos de datos; tipos y niveles de usuario. - Reporte de listas blancas y negras, mapas de puntos de exposición y pasillos de datos, aplicado a un proyecto, sistema o práctica. - Reporte de análisis de riesgos aplicado a un proyecto, sistema o práctica.	5. Desarrolla innovaciones y propone soluciones a problemas a partir de métodos establecidos. 5.6 Utiliza las tecnologías de la información y comunicación para procesar e interpretar información.	CO-12. Utiliza las tecnologías de la información y comunicación para investigar, resolver problemas, producir materiales y transmitir información.	Básica: - Analiza los algoritmos, herramientas y leyes actuales para la verificación y protección de la información en aplicaciones informáticas que manipulen información delicada, y que deben ser atendidas en la elaboración de un sistema informático seguro.

- Implementa sistemas criptográficos básicos, como medio de protección de información en medios temporales o persistentes de un sistema informático aplicando técnicas básicas de cifrado de datos (cifrado afín, por desplazamiento, por sustitución y transposición). - Implementa técnicas de protección ante ataques comunes (SQL injection, fallos de programación, PayLoad, Exploid, etc.) en un sistema en proceso de desarrollo. - Implementa los procesos de aseguramiento a través de certificados e incorpora a las aplicaciones la identificación de usuarios por firma digital.	- Cuadro comparativo de tipos de criptografías. - Cuadro sinóptico sobre ataques más comunes a sistemas informáticos. - Sistema de prueba y métodos de corrección de ataques. - Compendio de certificados y estructura firmas digitales.	5. Desarrolla innovaciones y propone soluciones a problemas a partir de métodos establecidos. 5.6 Utiliza las tecnologías de la información y comunicación para procesar e interpretar información. 8. Participa y colabora de manera efectiva en equipos diversos. Atributos: 8.1 Propone maneras de solucionar un problema o desarrollar un proyecto en equipo, definiendo un curso de acción con pasos específicos.	CO-12. Utiliza las tecnologías de la información y comunicación para investigar, resolver problemas, producir materiales y transmitir información.	Básica: - Analiza los algoritmos, herramientas y leyes actuales para la verificación y protección de la información en aplicaciones informáticas que manipulen información delicada, y que deben ser atendidas en la elaboración de un sistema informático seguro.

- Identifica las características de un desarrollo ético y responsable en una aplicación que manipula o resguarda información de usuarios. - Comprende los derechos y obligaciones marcados en la legislación del derecho informático al desarrollar aplicaciones informáticas.	- Cuadro comparativo sobre desarrollo ético y desarrollo típico. - Cuadro de derechos y obligaciones sobre la legislación nacional e internacional. - Lista de delitos informáticos y sus características. - Documento sobre procesos de propiedad intelectual.	8. Participa y colabora de manera efectiva en equipos diversos. 8.1 Propone maneras de solucionar un problema o desarrollar un proyecto en equipo, definiendo un curso de acción con pasos específicos.	Las competencias disciplinares no se desarrollarán explícitamente en esta UAC. Se presentan como un requerimiento para el desarrollo de las competencias profesionales.	Extendida: - Analiza los elementos legales involucrados en la administración de datos persistentes en aplicaciones informáticas, para la creación de sitios seguros y éticos.

- Compara las técnicas de revisión básicas implementadas durante las fases de diseño y prueba de un sistema informático. - Compara las técnicas de revisión externas de un sistema, así como la legalidad de su implementación. - Elabora un documento de políticas de uso y privacidad básicos con base en legislaciones nacionales o internacionales actuales.	- Lista de fallas de seguridad encontradas durante el proceso de diseño o prueba, aplicados a un sistema prediseñado. - Resumen sobre las características y repercusiones legales del hacker ético y del pentesting. - Documentos de los avisos de privacidad, confidencialidad y uso en los sistemas.	8. Participa y colabora de manera efectiva en equipos diversos. 8.1 Propone maneras de solucionar un problema o desarrollar un proyecto en equipo, definiendo un curso de acción con pasos específicos.	Las competencias disciplinares no se desarrollarán explícitamente en esta UAC. Se presentan como un requerimiento para el desarrollo de las competencias profesionales.	Extendida: - Analiza los elementos legales involucrados en la administración de datos persistentes en aplicaciones informáticas, para la creación de sitios seguros y éticos.