UNIVERSIDAD AUTÓNOMA DE SINALOA
SECRETARÍA ACADÉMICA UNIVERSITARIA
Coordinación General de Evaluación, Innovación y Calidad Educativa
UNIDAD ACADÉMICA: FACULTAD DE INFORMÁTICA CULIACÁN

PROGRAMA DE ESTUDIOS

1. DATOS DE IDENTIFICACIÓN			
UNIDAD DE APRENDIZAJE	Seguridad en Software		
Clave:	**4016**		
Horas y créditos:	Teóricas**: 60**	Prácticas: **20**	Estudio Independiente: **15**
	Total de horas: 80	**Créditos: 5**	
Tipo de unidad de aprendizaje:	**Teórico:**	**Teórico-práctico:X**	**Práctico:**
Competencia (s) del perfil de egreso que desarrolla o a las que aporta.	Hábil para el manejo de las tecnologías de la información y comunicaciones. Actúa de manera socialmente responsable con ética y respeto al marco jurídico. Tiene los conocimientos necesarios para crear y administrar empresas o proyectos de Tecnologías de la información y comunicación		
Cursos consecuentes relacionados:		**Cursos subsecuentes relacionados:**	
Responsables de elaborar y/o actualizar el programa:	LI. Fidel Bojorquez Solis MC. Javier Muro García MC. Gerardo Beltrán Gutiérrez		
Fecha de elaboración:	**Junio 2011**	**Actualización: Agosto 2018**	

2. PROPÓSITO

El alumno será capaz de conocer la terminología básica acerca de la seguridad informática y de la información, las metodologías para el análisis de riesgos informáticos y las normas de certificación correspondientes, además de los tipos de criptografía y métodos criptográficos y su implementación, la metodologías de seguridad en el desarrollo de sistemas, las mejores prácticas en el desarrollo de código, la configuración de seguridad básica en diferentes entornos de trabajo, para proteger la confidencialidad, integridad y disponibilidad de la información en las organizaciones.

3. SABERES

Teóricos:	Conoce la terminología de seguridad informática, criptografía y métodos criptográficos, las metodologías para el análisis de riesgos informáticos, normas y procesos de certificación, las mejores practicas para el desarrollo de sistemas y código seguro y la configuración básica de seguridad en diferentes entornos de trabajo
Prácticos:	Elabora mapas conceptuales acerca de la seguridad y su clasificación, de criptografía, sus tipos y métodos utilizados. Desarrolla proyecto de análisis y gestión de riesgos informáticos, proyecto de sistema de gestión de seguridad de la información basado en norma de certificación.

	Desarrolla código para la implementación de métodos criptográficos que propicien la seguridad de la información Desarrolla procedimientos y código utilizando las mejores prácticas y configura entornos de trabajo en relación con la seguridad de la información
Actitudinales:	Actúa de manera socialmente responsable con ética y respeto al marco jurídico. Es capaz de solucionar problemas por su cuenta, investigando, trabajando en equipo positivamente y con respeto de ideologías.

4. CONTENIDOS

BLOQUE I: Introducción a la seguridad	**Aprendizajes Esperados**
1.1 Seguridad Informática.	Describe el significado de seguridad informática y reconoce su importancia
1.2 Seguridad de la Información.	Describe el significado de seguridad de la información y reconoce su importancia
1.3 Controles de Seguridad	Reconoce los controles utilizados en seguridad y describe su clasificación
1.4 Confidencialidad, Integridad y Disponibilidad	Expresa con claridad el significado de los principios básicos en la seguridad de la información y su importancia
1.5 Vulnerabilidades	Reconoce las vulnerabilidades de un activo informático y describe su clasificación
1.6 Amenazas	Reconoce las amenazas de un activo informático y describe su clasificación
1.7 Riesgos	Reconoce los riesgos y el impacto de un activo informático y describe su clasificación
1.8 Modelado de Riesgos y Amenazas 1.8.1 STRIDE (Amenazas) 1.8.1.1 Spoofing 1.8.1.2 Tampering 1.8.1.3 Repudiation 1.8.1.4 Information Disclousure 1.8.1.5 Denial of Service 1.8.1.6 Elevation of Privilege	Describe las principales amenazas que pueden afectar a la seguridad, el impacto y su clasificación y el proceso para el análisis de riesgos
1.8.2 DREAD (Riesgos) 1.8.2.1 Damage 1.8.2.2 Reproducibility 1.8.2.3 Exploitability 1.8.2.4 Affected Users 1.8.2.5 Discoverability	Describe los principales riesgos que pueden afectar a la seguridad, el impacto y su clasificación y el proceso para el análisis de riesgos.
1.9 Políticas, Requisitos y Procedimientos	Establece las políticas, requisitos y procedimientos para implementar un plan de seguridad informática

BLOQUE II: Criptografía, Certificados y Firmas Digitales	
2.1 Comunicación en la Historia	Describe la evolución de la comunicación en la historia en una línea de tiempo
2.2 Criptografía 2.2.1 Historia de los sistemas criptográficos 2.2.2 Características de los sistemas de seguridad 2.2.3 Criptografía simétrica y asimétrica 2.2.4 Algoritmos (DES, AES, RSA)	Describe en una línea de tiempo la evolución de la Criptografía. Define los conceptos de criptografía y sus características Clasifica y describe los tipos de criptografía y los métodos de criptografía tradicionales y modernos.
2.3 Certificados Digitales	Describe el significado y usos de un certificado digital, el proceso para su obtención o generación y su implementación
2.4 Firma Electrónica	Describe el significado y usos de una firma digital, el proceso para su obtención o generación y su implementación
2.5 PKI (Infraestructura de Clave Pública)	Describe el significado de PKI, su uso y como se implementa en seguridad informática.
BLOQUE III: Introducción a la Seguridad en el SDLC	
3.1 Metodologías para la incorporación de seguridad en el SDLC 3.1.1 Proceso CLASP 3.1.2 OpenSAMM	Reconoce y utiliza las metodologías para el desarrollo de sistemas seguros
3.2 Análisis de Código (Mejores prácticas) 3.2.1 Race Conditions 3.2.2 Input Validation 3.2.3 Exceptions 3.2.4 SQL Injection 3.2.5 Buffer Overflows 3.2.6 Stack Overflows 3.2.7 Integer Overflows	Reconoce e implementa a través de código las herramientas para las mejores practicas en la seguridad de los programas
BLOQUE IV: Prácticas de Seguridad en Servidores WEB	
4.1 Seguridad Básica en Servidor Apache con Sistema Operativo LINUX CentOS 7	Conoce las herramientas y opciones de configuración de seguridad básica en Sistemas Operativos. Realiza la configuración de seguridad básica en un sistema operativo

4.2 Seguridad Básica en Servidor MySQL con Sistema Operativo LINUX CentOS 7	Conoce las herramientas y opciones de configuración de seguridad básica en Servidor de Base de Datos Realiza la configuración de seguridad básica en un Servidor de Base de Datos
4.3 Seguridad Básica en Servidor LINUX CentOS 7 (o Windows 2012/2016)	Conoce las herramientas y opciones de configuración de seguridad básica en Sistemas Operativos. Realiza la configuración de seguridad básica en un sistema operativo
4.4 Configuración Básica en PHP. (o X Lenguaje)	Conoce las herramientas y opciones de configuración de seguridad básica en un Lenguaje Realiza la configuración de seguridad básica en un Lenguaje
4.5 Configuración de Certificados en Servidor LINUX CentOS 7 (o en IIS con Windows)	Conoce las herramientas y opciones de configuración de certificados en un Servidor LINUX o Windows. Realiza la configuración de certificados en un sistema operativo
4.6 Penetration Testing	Conoce las herramientas para realizar pruebas de penetración a sistemas, sitios web, etc. Implementa o realiza pruebas de penetración a sistemas y sitios web para determinar vulnerabilidades

5. ACTIVIDADES PARA DESARROLLAR LAS COMPETENCIAS

Actividades del maestro.

- Actividades de inicio: técnica expositiva, conferencia, la pregunta.
- Actividad de desarrollo: panel, simposio, investigación bibliográfica, estudio supervisado, diálogo, mesa redonda con moderador y/o relator,

Actividad de evaluación: informe de investigación documental, ensayo, mapa conceptual, cuadro sinóptico, cuadro comparativo, portafolio de evidencias, rúbrica.

Actividades del estudiante.

- Actividades de inicio: Diario, fichas de trabajo, memoria, lluvia de ideas
- Actividades de desarrollo: concordar y discordar, realizar código de programas, exposiciones

Actividades finales: Informe de investigación documental o de campo, ensayo, mapa conceptual, cuadro sinóptico, cuadro comparativo, portafolio de evidencias, rúbrica, entrega de implementación de código, proyecto de seguridad, practica de configuración de seguridad

6. EVALUACIÓN DE LAS COMPETENCIAS

6.1. Evidencias de aprendizaje	6.2. Criterios de desempeño	6.3. Calificación y acreditación
• Escala de rango • Rúbrica • Cuestionario • Mapa conceptual, cuadro sinóptico • Elaboración de proyecto de seguridad • Escritura de programas • Implementar configuración de seguridad	• Obtener 80% de asistencia a clase • Entrega de tareas y trabajos de investigación • Realizar exposición en clase • Desarrollo de programas • Elaboración de Proyecto de Seguridad Informática • Implementar en programas las mejores prácticas para la seguridad • Implementar la configuración básica en sistemas operativos, Servidores y Lenguajes • Realizar pruebas de penetración a sistemas y sitios web	• 10% de asistencia • 20% Tareas, trabajos de investigación • 40% Calificación aprobatoria en exámenes parciales • 30% Entrega y Revisión del producto requerido

7. FUENTES DE INFORMACIÓN

Bibliografía:

(http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf)
(http://www.iso27000.es/download/ControlesISO27002-2013.pdf)
(https://www.us-cert.gov/bsi/articles/best-practices/architectural-risk-analysis/architectural-risk-analysis)
https://www.us-cert.gov/bsi/articles/best-practices/requirements-engineering/introduction-to-the-clasp-process
http://www.opensamm.org/downloads/resources/OpenSAMM-1.0-es_ES.ppt
https://www.us-cert.gov/bsi/articles/best-practices/code-analysis/code-analysis

8. PERFIL DEL PROFESOR:

Licenciatura en Informática, Ingeniería en Sistemas Computacionales