Programa de Módulo

Nombre del Módulo	**PROGRAMACIÓN SEGURA**								**Horas de Clases**	72	
Código	PRO203		**Año Plan**	2020					**Créditos SCT-AIEP**	4	
Modalidad	**Presencial**	☒	**Semipresencial**	☐	**Online**	☐					
Horas en Espacio de Aprendizaje	**Aula**		**Laboratorio PC**	72	**Taller**		**Terreno**		**Aula Virtual**		
Tipo de Módulo	**Especialidad**	☒	**General**	☐	**Sello**	☐			**Semestre**	II	
Módulos Prerrequisito	**NO**	☒	**SI**	☐	**Módulo(s)**						
Tributación a la Competencia del Perfil de Egreso	-Diseñar sistemas de información seguros, considerando el levantamiento de requerimientos funcionales y no funcionales, además de los modelos de procesos de negocios resultantes según necesidades del cliente (Código SFIA: SWDN nivel 3, REQM nivel 3, BUAN nivel 4). (Téc) -Diseñar sistemas de información seguros, considerando el levantamiento de requerimientos funcionales y no funcionales, además de los modelos de procesos de negocios resultantes del levantamiento de necesidades del cliente (Código SFIA: SWDN nivel 3, REQM nivel 3, BUAN nivel 4). (Prof)										
Unidad de Competencia (UC): Al finalizar el módulo, los participantes serán capaces de: Aplicar técnicas y métodos de programación segura, considerando modelos y estándares internacionales para mitigación de vulnerabilidades.											

UNIDADES DE APRENDIZAJE		Secuenciales	
1° UNIDAD	**Programación segura para desarrollo – OWASP**	**HORAS DE CLASES**	**36**

APRENDIZAJE ESPERADO	CRITERIOS DE EVALUACIÓN	CONTENIDOS OBLIGATORIOS
1.-Analizan ciclos de vida SDLC asociados al desarrollo de software, considerando normativa vigente. **Tipo de Habilidad asociada al AE** Analizar **Espacio de Aprendizaje** Laboratorio PC	1.1.-Caracteriza modelos de desarrollo de software tradicionales y ágiles, considerando normativa vigente para desarrollo seguro. 1.2.-Identifica componentes de documentación y productos intermedios de trabajo en SDLC. 1.3.-Relaciona SDLC con calidad y seguridad del software, considerando normativa vigente ISO-9000 e ISO-27001. 1.4.-Relaciona SDLC con control de versiones, gestión de cambios y trazabilidad, considerando uso de herramienta GIT o similar.	<u>Modelos de desarrollo de software tradicionales y ágiles</u> -Cascada, Prototipado, Incremental, Espiral -RAD, CMMI y AGILE -Normativa vigente para desarrollo seguro -Ciclos de vida de desarrollo de software: SDLC -Documentación y productos intermedios de trabajo en SDLC -ISO-9000 e ISO-27001 -Repositorio de control de versiones -Gestión de cambios de ITIL -Concepto de Trazabilidad en SDLC -Uso de herramienta GIT
Competencias personales, sociales y valóricas Respeto	1.5.-Realiza las tareas asignadas respetando normas, protocolos y necesidades en el contexto de su quehacer.	
2.-Aplican modelo de seguridad para el diseño y modelamiento de software, considerando la adaptación de componentes del sistema, sus amenazas potenciales y normativa vigente. **Tipo de Habilidad asociada al AE** Aplicar **Espacio de Aprendizaje** Laboratorio PC	1.6.-Identifica conceptos de OWASP TOP10 y ASVS, considerando su aplicabilidad en programación segura y solución de vulnerabilidades frecuentes. 1.7.-Comprueba aplicación de norma PCI-DSS para desarrollo seguro de software, considerando la industria de pagos electrónicos. 1.8.-Determina amenazas de seguridad del enfoque STRIDE, considerando recomendaciones del modelo SDL. 1.9.-Implementa modelamiento de amenazas para sistema de software, considerando modelo SDL.	-OWASP TOP10: aplicabilidad en programación segura -OWASP ASVS: aplicabilidad en programación segura -Solución de vulnerabilidades frecuentes -Norma PCI-DSS: checklist selfassesment -Industria de pagos electrónicos -Microsoft STRIDE: amenazas de seguridad -Modelo de seguridad SDL -Modelamiento de amenazas
Competencias personales, sociales y valóricas Colaboración	1.10.-Trabaja de forma colaborativa y en red, a través de diversos medios y soportes, adoptando diferentes roles.	

3.-Implementan adaptación de hardening de sistemas, considerando listas de vulnerabilidades y exposiciones comunes, plan de parchado de framework, comunicaciones seguras y autenticación robusta.	1.11.-Adapta vulnerabilidades y exposiciones comunes CVE, y sistema de puntaje de vulnerabilidades comunes CVSS para la creación de modelo de hardening de sistemas. 1.12.-Configura plan de parchado de framework de desarrollo y entornos seguros de sistemas operativos hardenizados, considerando requerimientos técnicos. 1.13.-Comprueba comunicaciones seguras y encriptación WS, SOAP y XML, de acuerdo con requerimientos técnicos. 1.14.-Comprueba uso de CAPTCHAs y autenticación robusta centralizada en un entorno hardenizado.	-Vulnerabilidades y exposiciones comunes CVE -Sistema de puntaje de vulnerabilidades comunes CVSS -OWASP A06:2021: Componentes Vulnerables y Desactualizados -Plan de parchado de framework de desarrollo y de entornos seguros -Comunicaciones seguras y encriptación: WS, SOAP, XML -CAPTCHAS y autenticación robusta centralizada
Tipo de Habilidad asociada al AE Aplicar		
Espacio de Aprendizaje Laboratorio PC		
Competencias personales, sociales y valóricas Autonomía	1.15.-Demuestra autonomía en actividades y funciones especializadas en diversos contextos.	

UNIDADES DE APRENDIZAJE		Secuenciales	
2° UNIDAD	**Prácticas de programación segura para desarrollo – OWASP**	**HORAS DE CLASES**	**36**

APRENDIZAJE ESPERADO	CRITERIOS DE EVALUACIÓN	CONTENIDOS OBLIGATORIOS
4.-Aplican codificación segura, considerando gestión de riesgos, arquitectura de seguridad, registro y seguimiento de eventos.	2.1.-Determina gestión de riesgos y clasificación de activos de negocio, considerando principios de codificación segura. 2.2.-Implementa arquitectura de seguridad, de acuerdo con principios de codificación segura. 2.3.-Construye escala de riesgo basada en clasificación de riesgos DREAD, considerando codificación segura. 2.4.-Implementa registro de eventos y seguimiento LOGs, considerando categoría OWASP A09:2021 asociada a fallas en el registro y monitoreo.	-OWASP Development Guide: Principios de codificación segura -Gestión de riesgos y clasificación de activos -Arquitectura de seguridad: por defecto, privilegio mínimo, defensa en profundidad -Confección de escala de riesgo -Clasificación de riesgos DREAD -Registro de eventos y seguimiento LOGs -OWASP A09:2021: Fallas en el registro y monitoreo
Tipo de Habilidad asociada al AE Aplicar		
Espacio de Aprendizaje Laboratorio PC		
Competencias personales, sociales y valóricas Resolución de Problemas	2.5.-Tec-Detecta las causas que originan problemas de acuerdo a parámetros establecidos y en contextos propios de su actividad.	

5.-Aplican técnicas de programación segura de OWASP TOP10, considerando riesgo de inyección, fallas de identificación y autenticación, fallas criptográficas y configuración de seguridad incorrecta.	2.6.-Determina ataques, considerando técnica de inyección asociada a riesgo A03:2021, de acuerdo con OWASP TOP10. 2.7.-Resuelve formas débiles de programación asociadas a fallas de identificación y autenticación, considerando técnicas de programación segura para mitigación de riesgo A07:2021. 2.8.-Resuelve formas débiles de programación asociadas a fallas criptográficas y exposición de datos sensibles, considerando técnicas de programación segura para mitigación de riesgo A02:2021. 2.9.-Aplica técnicas para la mitigación de ataques asociados a riesgo A05:2021, considerando configuración de seguridad incorrecta.	-OWASP Development Guide OWASP TOP10 -Riesgo A03:2021: Inyección -Riesgo A07:2021: Fallas de Identificación y Autenticación -Riesgo A02:2021: Fallas Criptográficas. / CWE-259: Uso de contraseña en código fuente / CWE-327: Algoritmo criptográfico vulnerado o inseguro / CWE-331: Entropía insuficiente -Riesgo A05:2021: Configuración de Seguridad Incorrecta
Tipo de Habilidad asociada al AE Aplicar		
Espacio de Aprendizaje Laboratorio PC		
Competencias personales, sociales y valóricas Autonomía	2.10.-Demuestra autonomía en actividades y funciones especializadas en diversos contextos.	
6.-Aplican técnicas y métodos de programación segura de OWASP TOP10, considerando pérdida de control de acceso, configuración de seguridad incorrecta, Cross-Site Scripting XSS, fallas en el software y en la integridad de los datos.	2.11.-Resuelve formas débiles de programación asociadas a pérdida de control de acceso, considerando técnicas de programación segura para mitigación de riesgo A01:2021. 2.12.-Implementa métodos de programación segura para mitigación de riesgo A05:2021 asociado a configuración de seguridad incorrecta. 2.13.-Implementa métodos de programación segura para mitigación de riesgo A03:2021, considerando Cross-Site Scripting XSS. 2.14.-Implementa métodos de programación segura para mitigación de riesgo A08:2021 asociado a fallas en el software y en la integridad de los datos.	-OWASP Development Guide OWASP TOP10 -Riesgo A01:2021: Pérdida de control de acceso -Riesgo A05:2021: Configuración de seguridad Incorrecta -Riesgo A03:2021: Inyección -Riesgo A08:2021: Fallas en el Software y en la Integridad de los Datos
Tipo de Habilidad asociada al AE Aplicar		
Espacio de Aprendizaje Laboratorio PC		
Competencias personales, sociales y valóricas Resolución de Problemas	2.15.-Tec-Detecta las causas que originan problemas de acuerdo a parámetros establecidos y en contextos propios de su actividad.	

PERFIL DOCENTE										
Formación Académica	Profesional o Técnico de Nivel Superior	**Área de Formación**	Informática/ Programación/ Ciberseguridad/ Tecnologías de la Información	**Competencias TIC**	Ofimática Básica	☒	**Años de Experiencia Laboral en la Especialidad**	+ de 2 años	**Años de Experiencia en Docencia y/o Capacitación**	+ de 2 años
					Navegadores	☒				
					Entornos Virtuales de Aprendizaje	☒				

BIBLIOGRAFÍA BÁSICA OBLIGATORIA
Ver detalle en documento Bibliografía Básica Obligatoria Planes de Estudio Carreras 2020

ESTRATEGIAS Y TÉCNICAS DE APRENDIZAJE-EVALUACIÓN			
Estrategia Formativa	**Técnicas de Aprendizaje Sugeridas**	**Técnicas de Evaluación Sugeridas**	**Instrumentos de Evaluación asociados**
Aprendizaje Basado en Casos	Aula invertida, lluvia de ideas, mapas mentales, redes semánticas, ensayo, simulación de procesos, juego de roles, aprendizaje colaborativo, informe.	Retroalimentación formativa, pruebas de comprensión sin o con apoyo de textos, resúmenes y organizadores gráficos previos al análisis de casos, reportes de conclusiones individuales/grupales posteriores al análisis de casos, debates, paneles de discusión, auto y coevaluación.	Registros de actividades de evaluación formativa y sumativa. Pautas de corrección de respuestas abiertas y/o cerradas. Pautas de observación directa/indirecta de desempeños esperados: Listas de verificación Escalas de apreciación Matrices de valoración (Rúbricas)
Aprendizaje Basado en Problemas	Aula invertida, mapas mentales, redes semánticas, ensayo, simulación de procesos, juego de roles, aprendizaje colaborativo.	Retroalimentación formativa, pruebas de comprensión sin o con apoyo de textos, pruebas de desempeño/ejecución, organizadores gráficos (mapas mentales, redes semánticas), reportes temáticos escritos tipo ensayo, auto y coevaluación.	
Aprendizaje Basado en Proyectos	Lluvia de ideas, aprendizaje colaborativo, mapas mentales, redes semánticas, simulación de procesos, pasantías formativas, informes, Aprendizaje + Servicio.	Retroalimentación formativa, pruebas de desempeño/ejecución, presentaciones de progreso/efectividad del proyecto, evaluación docente compartida con otros docentes/socios comunitarios, portafolios, diarios personales de clase, auto y coevaluación.	
Aprendizaje Basado en el Pensamiento	Aula invertida, lluvia de ideas, método de las preguntas, aprendizaje colaborativo, mapas mentales, redes semánticas.	Retroalimentación formativa, organizadores gráficos (mapas mentales, redes semánticas), pruebas de desempeño/ejecución, portafolios, diarios personales de clase, auto y coevaluación.	

MATRIZ DE EVALUACIONES	
N° de horas de clases (pedagógicas) por Unidad de Aprendizaje (UA)	**N° mínimo de evaluaciones sumativas (calificadas)**
Menor o igual a 36 horas	1 evaluación parcial
Mayor que 36 y menor que 72 horas	2 evaluaciones parciales
Mayor o igual que 72 horas	3 evaluaciones parciales