Programa de Modulo

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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** | PENDIENTE | | | | | | | | | |
| **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. | | | | | | | | | | |

|  |  |  |
| --- | --- | --- |
| Elaborador: Carlos Allendes Droguett Cargo: Especialista Técnico  Fecha: Marzo 2020 | Validador Técnico: Iván Peters Vera Cargo: Especialista Técnico  Fecha: Mayo 2020 | Validador Pedagógico: Felipe Cabaluz Rodríguez Cargo: Jefe de Diseño Curricular  Fecha: Mayo 2020 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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. | | 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. | Modelos de desarrollo de software  tradicionales y ágiles  -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 | |
| **Tipo de Habilidad asociada al AE**  Análisis | |
|  | |  |
| **Competencias personales, sociales y valóricas**  Respeto (R) | | 1.5.-Realiza las tareas asignadas respetando normas, protocolos  y necesidades en el contexto de su quehacer. (R) | -Uso de herramienta GIT | |
| 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. | | 1.6.-Sintetiza 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 | |
| **Tipo de Habilidad asociada al AE**  Aplicación | |
| **Competencias personales, sociales y valóricas**  Colaboración (Col) | | 1.10.-Trabaja de forma colaborativa y en red, a través de diversos  medios y soportes, adoptando diferentes roles. (Col) |

|  |  |  |
| --- | --- | --- |
| Elaborador: Carlos Allendes Droguett Cargo: Especialista Técnico  Fecha: Marzo 2020 | Validador Técnico: Iván Peters Vera Cargo: Especialista Técnico  Fecha: Mayo 2020 | Validador Pedagógico: Felipe Cabaluz Rodríguez Cargo: Jefe de Diseño Curricular  Fecha: Mayo 2020 |

|  |  |  |
| --- | --- | --- |
| 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. | -Vulnerabilidades y exposiciones comunes CVE  -Sistema de puntaje de vulnerabilidades comunes CVSS  -OWASP A9:2017: Uso de componentes con vulnerabilidades conocidas |
|  | 1.13.-Comprueba comunicaciones seguras y encriptación WS, SOAP y XML, de acuerdo con requerimientos técnicos. | -Plan de parchado de framework de desarrollo y de entornos seguros |
|  | 1.14.-Comprueba uso de CAPTCHAs y autenticación robusta centralizada en un entorno hardenizado. | -Comunicaciones seguras y encriptación: WS, SOAP, XML |
| **Tipo de Habilidad asociada al AE**  Aplicación |  | -CAPTCHAS y autenticación robusta centralizada |
|  |  |
| **Competencias personales, sociales y valóricas**  Autonomía (A) | 1.15.-Demuestra autonomía en actividades y funciones  especializadas en diversos contextos. (A) |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 principios de codificación segura, considerando gestión de riesgos, arquitectura de seguridad y registro de eventos y seguimiento. | | 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 a 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 OWASP A10:2017 asociado a registro y monitoreo insuficientes. | -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 A10:2017: Registro y monitoreo insuficientes | |
| **Tipo de Habilidad asociada al AE**  Aplicación | |
| **Competencias personales, sociales y valóricas**  Resolución de Problemas (RP) | | 2.5.-Tec-Detecta las causas que originan problemas de acuerdo a parámetros establecidos y en contextos propios de su actividad. (RP) |

|  |  |  |
| --- | --- | --- |
| Elaborador: Carlos Allendes Droguett Cargo: Especialista Técnico  Fecha: Marzo 2020 | Validador Técnico: Iván Peters Vera Cargo: Especialista Técnico  Fecha: Mayo 2020 | Validador Pedagógico: Felipe Cabaluz Rodríguez Cargo: Jefe de Diseño Curricular  Fecha: Mayo 2020 |

|  |  |  |
| --- | --- | --- |
| 5.-Aplican técnicas de programación segura de OWASP TOP10, considerando técnica de inyección, pérdida de autenticación, exposición de datos y entidades externas XML. | 2.6.-Determina ataques, considerando técnica de inyección asociada a riesgo A1:2017, de acuerdo a OWASP TOP10.  2.7.-Resuelve formas débiles de programación asociadas a la pérdida de autenticación, considerando técnicas de programación segura para mitigación de riesgo A2:2017.  2.8.-Resuelve formas débiles de programación asociadas a exposición de datos sensibles, considerando técnicas de programación segura para mitigación de riesgo A3:2017.  2.9.-Aplica técnicas para la mitigación de ataques asociados a A4:2017, considerando explotación de vulnerabilidades XXE o de entidades externas XML. | -OWASP Development Guide OWASP TOP10  -Riesgo A1:2017: Inyección  -Riesgo A2:2017: Pérdida de Autenticación  -Riesgo A3:2017: Exposición de datos  -Riesgo A4:2017: Entidades Externas XML, explotación de vulnerabilidades XXE |
| **Tipo de Habilidad asociada al AE**  Aplicación |
| **Competencias personales, sociales y valóricas**  Autonomía (A) | 2.10.-Demuestra autonomía en actividades y funciones especializadas en diversos contextos. (A) |
| 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 y deserialización insegura. | 2.11.-Resuelve formas débiles de programación asociadas a pérdida del control de acceso, considerando técnicas de programación segura para mitigación de riesgo A5:2017.  2.12.-Implementa métodos de programación segura para mitigación de riesgo A6:2017 asociado a configuración de seguridad incorrecta.  2.13.-Implementa métodos de programación segura para mitigación de riesgo A7:2017 asociado a Cross-Site Scripting XSS.  2.14.-Implementa métodos de programación segura para mitigación de riesgo A8:2017 asociado a deserialización insegura. | -OWASP Development Guide OWASP TOP10  -Riesgo A5:2017: Pérdida del control de acceso  -Riesgo A6:2017: Configuración de seguridad Incorrecta  -Riesgo A7:2017: Cross-Site Scripting XSS  -Riesgo A8:2017: Deserialización Insegura |
| **Tipo de Habilidad asociada al AE**  Aplicación |
| **Competencias personales, sociales y valóricas**  Resolución de Problemas (RP) | 2.15.-Tec-Detecta las causas que originan problemas de acuerdo a parámetros establecidos y en contextos propios de su actividad. (RP) |

|  |  |  |
| --- | --- | --- |
| Elaborador: Carlos Allendes Droguett Cargo: Especialista Técnico  Fecha: Marzo 2020 | Validador Técnico: Iván Peters Vera Cargo: Especialista Técnico  Fecha: Mayo 2020 | Validador Pedagógico: Felipe Cabaluz Rodríguez Cargo: Jefe de Diseño Curricular  Fecha: Mayo 2020 |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **PERFIL DOCENTE** | | | | | | | | | | |
| **Formación Académica** | Profesional o Técnico de Nivel Superior | **Área de Formación** | Informática, Programación, Ciberseguridad y 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** | | |
| **AUTOR/A/S** | **TÍTULO** | **EDITORIAL, AÑO** |
| Fundación OWASP | OWASP Top10 | OWASP, 2020: [www.owasp.org](http://www.owasp.org/) |

|  |  |  |
| --- | --- | --- |
| Elaborador: Carlos Allendes Droguett Cargo: Especialista Técnico  Fecha: Marzo 2020 | Validador Técnico: Iván Peters Vera Cargo: Especialista Técnico  Fecha: Mayo 2020 | Validador Pedagógico: Felipe Cabaluz Rodríguez Cargo: Jefe de Diseño Curricular  Fecha: Mayo 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: |
| 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. | Listas de verificación Escalas de apreciación Matrices de valoración  (Rúbricas) |

|  |  |
| --- | --- |
| **MATRIZ DE EVALUACIONES** | |
| **N° de horas de clases (pedagógicas) por Unidad de Aprendizaje (U.A.)** | **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. |

|  |  |  |
| --- | --- | --- |
| Elaborador: Carlos Allendes Droguett Cargo: Especialista Técnico  Fecha: Marzo 2020 | Validador Técnico: Iván Peters Vera Cargo: Especialista Técnico  Fecha: Mayo 2020 | Validador Pedagógico: Felipe Cabaluz Rodríguez Cargo: Jefe de Diseño Curricular  Fecha: Mayo 2020 |