ANEXO2: Programa del Curso "Desarrollo Seguro" (28 horas)

Objetivo General:	Entregar a los asistentes, los conocimientos necesarios para entender y aplicar: Técnicas de desarrollo seguro. Uso de API's segura (ESAPI) para .NET, PHP y JAVA, para mitigar vulnerabilidades utilizando métodos de análisis, diseño y codificación orientado a prácticas seguras, basado en normativas de OWASP (Top10, Proactive Controls, Secure Web Application Framework) y JAVA(Guías de programación Segura) • Uso de información sensible. El correcto tratamiento, retención y eliminación de los datos sensibles de clientes, tales como números de tarjetas de crédito, códigos de seguridad o valores de verificación de tarjetas, datos de transacciones electrónicas, registros, historiales o bitácoras, etc.-. Basado en normativa de PCI-DSS. Los asistentes serán capaces de identificar vulnerabilidades típicas, mediante la comprensión de la teoría y la ejecución de ejercicios prácticos. Al finalizar el curso el alumno estará en condiciones de: ➢ Conocer los conceptos principales del modelo de desarrollo seguro de OWASP ➢ Conocer y entender las prácticas seguras para desarrollar aplicaciones. ➢ Conocer las recomendaciones de la norma PCI-DSS para la protección de información sensible de clientes y transacciones electrónicas.
Contenido y Objetivos Específicos:	Los contenidos están alineados con: • OWASP TOP10, los cuales son normas y prácticas de referencia a nivel mundial sobre riesgos en aplicaciones Web y su mitigación. • PCI-DSS y los requisitos para protección de datos sensibles de tarjetahabientes, y las recomendaciones para desarrollar y mantener sistemas y aplicaciones seguras. • **Unidad 1. Introducción a la Seguridad de Aplicaciones Web (05 hrs.)** U1.1 Nociones básicas de Seguridad de la Información

	U1.2 Normativas ISO27001 y PCI-DSS U1.3 Propósito de acatar una norma y efectos de incumplirla U1.4 Riesgos y resguardos en Internet, Correo y Redes Sociales U1.5 Riesgos y resguardos en el puesto de trabajo U1.Evaluación: La unidad tiene ejercicios de tipo práctico que enfrentan al alumno con situaciones cotidianas, alineado a los temas entrenados. • **Unidad 2. Laboratorio de revisión sobre un proyecto de prueba (03 hrs.)** U2.1 Introducción al laboratorio de revisión asistida U2.2 Ejemplos prácticos de amenazas U2.Evaluación: La unidad se entrena con ejercicio simulados en un entorno de pruebas. • **Unidad 3. Entendiendo los riesgos de seguridad y como mitigarlos (20 hrs.)** U3.1 Inyección U3.2 Secuencia de Comandos en Sitios Cruzados (XSS) U3.3 Perdida de Autenticación y Gestión de Sesiones U3.4 Referencia directa insegura a objetos U3.5 Falsificación de Peticiones en Sitios Cruzados (CSRF) U3.6 Inadecuada Configuración de Seguridad U3.7 Almacenamiento Criptográfico Inseguro U3.8 Fallo de Restricción de Acceso a URL U3.9 Protección Insuficiente en la Capa de Transporte U3.10 Redirecciones y Re-envíos No Validado

	U3.Evaluación: La unidad tiene ejercicios de tipo práctico que requieren un desarrollo analítico por parte del alumno, alineado a los temas entrenados.
Requisitos:	Conocimiento básico de Seguridad de la Información. Conocimiento de Lenguaje(s) de programación. Conocimiento de algún modelo de desarrollo (Cmmi, PRINCE2, etc.) Lectura de Inglés Técnico. Equipo PC o notebook individual (CPU 64-bit x86 , OS win7 o win8, 4GB RAM)
Duración:	28 Horas Cronológicas.
Orientado a:	Personal que realiza desarrollo de aplicaciones, testeadores, auditores de seguridad.