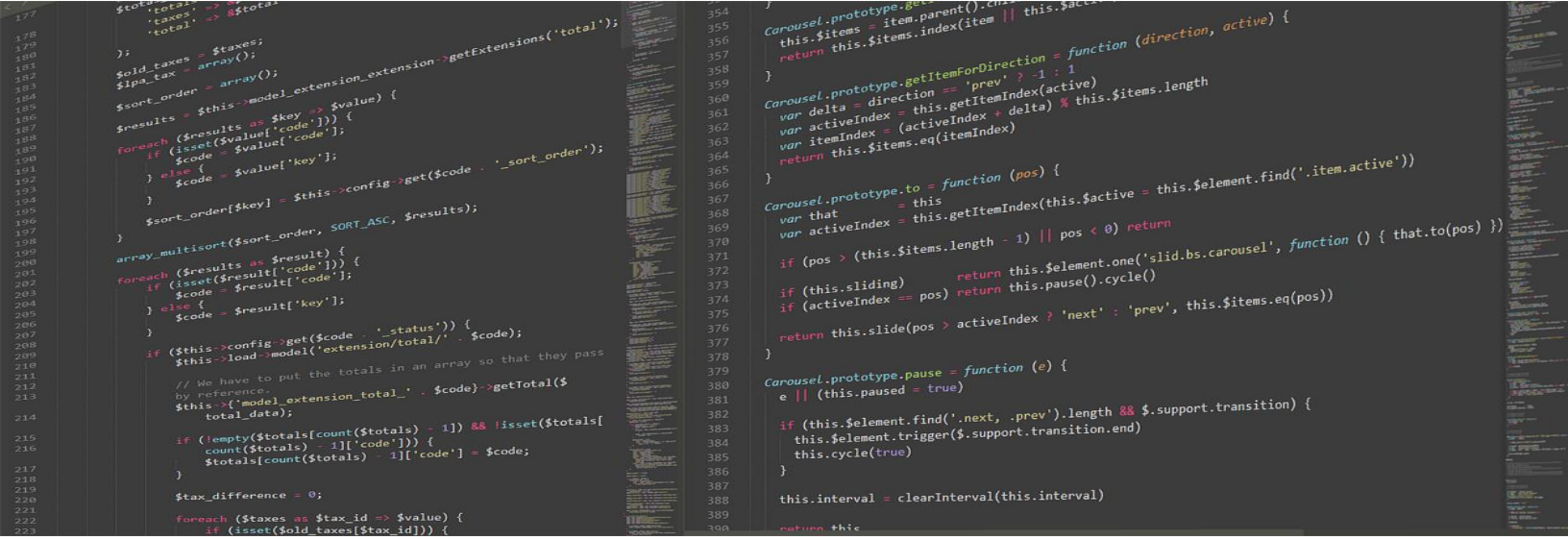


CURSO DE DESARROLLO SEGURO DE SOFTWARE

1. OBJETIVOS

Lograr que los asistentes al curso comprendan las metodologías de desarrollo de software seguro existentes en donde se establecen las etapas, actividades y técnicas necesarias para la construcción y mantenimiento de un proyecto de desarrollo de software, garantizando la obtención de productos de calidad y seguridad. Existen en la actualidad varias metodologías de desarrollo de software seguro. Entre ellas se encuentran Correctness by Construction (CbyC), Common Criteria, Comprehensive, Security Development Lifecycle (SDL), Cigital Touchpoints y Lightweight Application Security Process (CLASP). También OWASP, PCI DSS e ISO 27001:2013 ofrecen una serie de recomendaciones para mejorar la seguridad durante el ciclo de desarrollo.

2. ALCANCE

Las metodologías de desarrollo de software seguro definen las etapas y actividades que se deben seguir para la implementación de nuevos desarrollos, mejoras, desarrollos externos y para dar solución a fallos en el software, garantizando que estos procesos se realicen de forma eficiente, siguiendo las políticas y procedimientos establecidos. El alcance del curso está delimitado por los requerimientos de PCI (requerimiento 6) y las vulnerabilidades de OWASP.

3. MARCO TEÓRICO CONSIDERADO EN EL CURSO

La norma PCI DSS (**P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard) fue desarrollada por un conjunto de compañías de tarjetas de débito y crédito en el año 2006 entre las que estaban: America Express, Discover, JCB, Mastercard y VISA. De esta unión se creó el **P**ayment **C**ard **I**ndustry **S**ecurity **S**tandards **C**ouncil (PCI-SSC), el cual es responsable de la creación, desarrollo, y difusión de la norma PCI DSS.

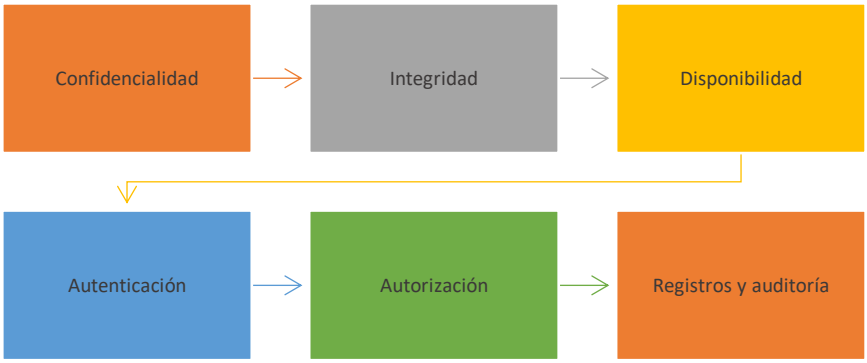
Las compañías autorizadas por el Concilio (PCI SSC) para realizar la validación de cumplimiento de la norma PCI DSS se conocen como QSA (Qualified Security Assessor), los cuales deben cumplir con una serie de requisitos como empresa y sus ingenieros deben ser entrenados directamente por esta asociación. La norma PCI es una de las normas más exigentes a nivel mundial en lo relacionado con la protección de la información sensible debido al énfasis que pone en los requerimientos de tipo tecnológicos y la rigurosidad que exige en el proceso de evaluación para otorgar la certificación de cumplimiento. La evaluación, para obtener la certificación, exige que el 100% de los requerimientos y sub-requerimientos (aproximadamente son 350) estén implementados correctamente.

PCI DSS procura que las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes protejan esta información con el fin de evitar fugas que involucren divulgación de información sensible. Este tipo de fugas podría afectar todo el ecosistema de tarjetas de pago incluyendo clientes, comercios e instituciones financieras. Estas entidades perderían credibilidad como consecuencias de fugas de información y quedarían expuestas a numerosas demandas económicas y en algunos casos su supervivencia en el tiempo quedaría seriamente comprometida.

Lograr el cumplimiento de PCI DSS es fundamental para el éxito a largo plazo de las organizaciones que procesan información sensible o realizan pagos con tarjetas. El cumplimiento involucra la identificación continua de amenazas y vulnerabilidades que podrían potencialmente afectar a dichas organizaciones. La mayoría de ellas nunca se recuperan totalmente de una infracción o fuga de sus datos ya que la pérdida o el impacto es mayor que los datos en sí mismos. Seguir la norma PCI es una gran oportunidad para realizar más negocios de manera segura. Por medio de esta norma se logra asegurar la salud y confianza en las transacciones de pago para cientos de millones de personas en el mundo que utilizan medios electrónicos para sus transacciones.

Finalmente, con el fin de poder desarrollar software que sea inmune a fallas y posibles amenazas siguiendo los lineamientos de PCI DSS, es importante incorporar los conceptos de seguridad desde la fase de requerimientos hasta la fase final de mantenimiento del ciclo SDLC (Software Development Life Cycle). Los conceptos de seguridad se deben considerar a lo largo de todo el ciclo de desarrollo y deben ser direccionados en cada fase. Si en alguna de las fases no se prestara atención suficiente a la seguridad de la información esto podría redundar en la disminución de los esfuerzos prestados a las fases previas.

Algunos de los conceptos más importantes para implementar la seguridad de la información en el desarrollo de software son:



DISPONIBILIDAD:
Propiedad que determina que la información sea accesible y utilizable por solicitud de una entidad autorizada.

CONFIDENCIALIDAD:
Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

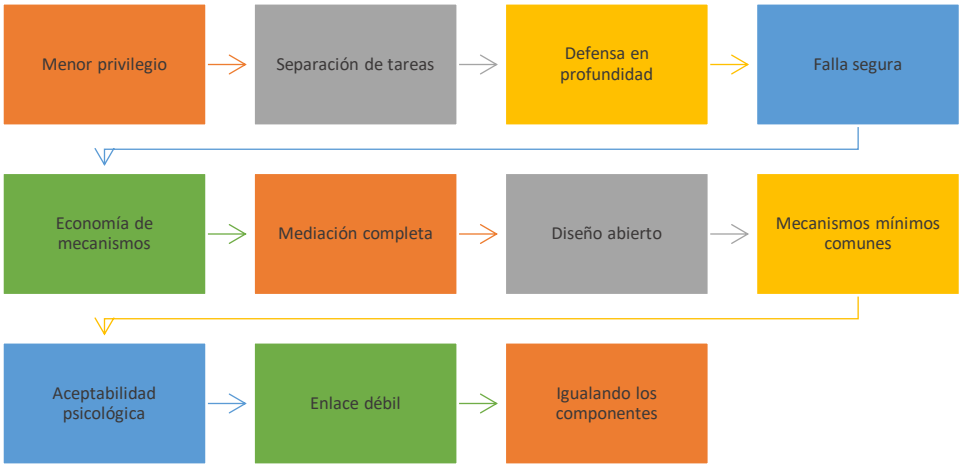
INTEGRIDAD:
Propiedad de salvaguardar la exactitud y estado completo de los activos.

AUTENTICACIÓN: Las aplicaciones en la gran mayoría de organizaciones procesan información sensible, por esta razón es importante que su acceso esté debidamente controlado y solamente aquellas personas o entidades estén debidamente autorizadas.

AUTORIZACIÓN: La autorización es el concepto dentro de la seguridad de la información en que los accesos a los diferentes objetos son controlados y está basado en los derechos y privilegios que son otorgados a los usuarios de acuerdo a las políticas y a los dueños de la información.

REGISTRO Y AUDITORÍA: La creación de registros de los diferentes componentes es importante para que en caso de un incidente de seguridad se pueda contar con la información respectiva que permita realizar la investigación de todos los eventos sucedidos.

A continuación, los conceptos de seguridad que serán tratados en el curso cuando se trate de diseñar la arquitectura de software segura:



4. CONTENIDO ESPECÍFICO DEL CURSO

DIA 1 (8 horas):

1. Introducción general al curso
2. Retos de la seguridad de la información en la actualidad
3. *Frameworks* de seguridad de la información relevantes
4. La norma PCI DSS V 3.2.1
5. La norma ISO 27001:2013
6. Introducción al desarrollo seguro
7. Metodologías y estándares de desarrollo seguro
8. Disminuyendo la brecha entre seguridad de la información y el desarrollo seguro
9. Seguridad durante todo el ciclo de desarrollo
10. Revisión de código
11. Separación de ambientes

DIA 2 (8 horas)

1. Mejores prácticas para el uso de datos en pruebas
2. Gestión de vulnerabilidades (OWASP, SANS, CWE, CERT secure coding)
3. Ataques de inyección de código (SQL, LDAP)
4. Buffers overflows
5. Transporte y almacenamiento criptográfico
6. Manejo de errores
7. Cross-site-scripting (XSS) y CSRF
8. Seguridad en los controles de acceso, protección de objetos e interfaces seguras.
9. Gestión de sesiones establecidas.
10. Sesión práctica para realizar ataques a las vulnerabilidades: (OWASP, SANS, CWE, CERT secure coding)
11. Cierre del curso y entrega de diplomas

5. CONFERENCISTAS

Gonzalo Rojas: Ingeniero de sistemas de la Universidad del Valle con experiencia en implementación de software para entidades financieras y del sector gobierno. Ha trabajada también en implementaciones de seguridad de la información y desarrollo seguro. Especialista en seguridad de la información y auditor Interno ISO 27001. En estas actividades ya completa 15 años de experiencia liderando proyectos de desarrollo partiendo de la arquitectura del sistema hasta su implementación e integración. Entre las plataformas preferidas está el framework de .NET.

Jairo García: El ingeniero Jairo García posee las certificaciones: LPT – Licensed Penetration Tester – (Expedida el 6 de marzo de 2014) EC – COUNCIL, ECSA – EC-Council Certified Security Analyst – (Expedida el 4 de octubre de 2013) EC – COUNCIL, CHFI – Computer Hacking Forensic Investigator – (Expedida el 5 de julio de 2013) EC - COUNCILCEH – Certified Ethical Hacker – (Expedida el 25 enero de 2013) EC – COUNCIL, CHackA0101 Founder THE EAGLE LABS https://www.theeaglelabs.com (4 de Junio de 2012), CIDF – Certificado en Investigación Digital Forense – (Expedida en noviembre de 2012) REDLIF - Red Latinoamericana de Informática Forense, también es Máster en Seguridad Informática – (Expedida el 2 de agosto de 2011) UOC - Universitat Oberta de Catalunya.

Rodrigo Ferrer V: Ingeniero eléctrico de la Universidad de la Andes**,** con estudios de especialización y maestría. Actualmente en desarrollo de estudios de doctorado. Ha realizado cursos de educación continua en la Universidad de Cambridge (Reino Unido). Certificado como ITIL, COBIT 5.0, CISSP (The World´s Premier Cybersecury Certification, ABCP (Associate Business Continuity Professional), Associate Member Business Continuity Institute (AMBCI), QSA (Qualified Security Assesor) PCI DSS, Auditor líder ISO 27001:2013, ISO 22301 (Business Continuity Lead Auditor), entre otros. Se ha desempeñado en compañías multinacionales como 3Com (hoy HP), Sonicwall (Implement cybersecurity solutions that are designed, deployed and managed specifically for small and medium-sized businesses (SMBs), Sisteseg Consulting Services (SCS), IQ Information Quality y Extreme Networks.