Desarrollo seguro de Aplicaciones Web basado en OWASP

Por: Carlos Carreño,

OCP, ScrumMaster, Solution Architect

Email: ccarrenovi@Gmail.com

Unidad 3 Seguridad en la etapa de análisis

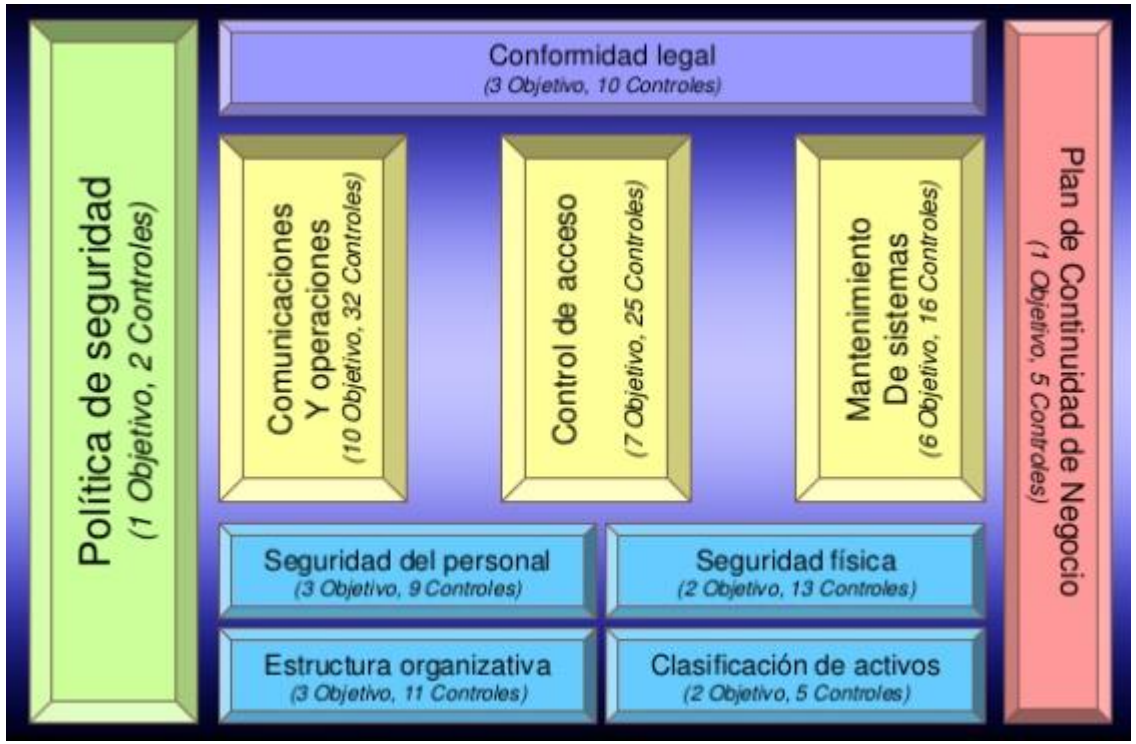
- Pautas de seguridad en el análisis de requerimientos.
- Desarrollo seguro y compliance / PCI, ISO27002

Pautas de seguridad en el análisis de requerimientos.

- Estándares y normas para la Ingeniería de Requisitos
  - ISO 29148 – Ingeniería de sistemas y software - Procesos del ciclo de vida - Ingeniería de requisitos
  - IEEE 830-1998 Prácticas recomendadas para la especificación de requisitos de software
  - IEEE 1233-1998 Guía para desarrollar especificaciones de requisitos de sistema
  - NC ISO/IEC 25010:2016 Ingeniería de software y sistemas – Requisitos de la calidad y evaluación de software (square) – Modelos de la calidad de software y sistemas
  - OWASP Testing Framework WSTG – v4-1

Desarrollo seguro y compliance / PCI, ISO 27002

- Modelo de Gestión de la Seguridad ISO 27002



Marcos de Trabajo de Ciberseguridad

- Comparativa

PCI DSS

- PCI Data Security Standard

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Laboratorio

- Lab 3 Crear un mapa conceptual de “Requisitos de Seguridad para aplicaciones web” identificados en el Paper: **“Security Requirements for web applications”**

Referencias

- https://www.techrepublic.com/article/popular-mobile-banking-apps-are-riddled-with-security-flaws-and-android-users-are-more-at-risk/
- http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992018000500015&lng=pt&nrm=iso&tlng=pt
- https://www2.deloitte.com/es/es/pages/risk/articles/los-cinco-mayores-ciberataques-de-la-historia.html
- https://www.complianceforge.com/product/iso-27002-based-security-documentation-wisp/
- https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

Autor: ccarrenovi@Gmail.com