SEG 118 – Desarrollo Seguro basado en OWASP

Ing. Carlos Carreño

Nov, 2021

MODULO 3: SEGURIDAD EN LA ETAPA DE ANÁLISIS

- Pautas de seguridad en el análisis de requerimientos.
- Desarrollo seguro y compliance

Pautas de seguridad en el análisis de requerimientos.

- Arquitectura de la aplicación
  - ¿Cliente/servidor , Móvil o Desktop?
- Plataforma donde correrá la aplicación
  - PC / Android/iOS / Web / Serverless
- Tipos de datos que se almacenan o transfieren
  - Confidenciales / públicos
- Requerimiento de compliance con normativas y marcos regulatorios
  - SOX
  - PCI-DSS “A”
  - 4609
  - ISO-27002

…continua

- Tipos de registro que el sistema debe generar
  - Acceso a recursos, uso de privilegios, etc.
- Perfiles de usuario necesarios para la aplicación
  - Administrador, revisor, editor, usuario básico, etc.
- Tipos de acceso a los datos por parte de cada perfil
  - Lectura, escritura, modificación, agregado, borrado, etc.
- Acciones sobre el sistema que puede hacer cada perfil
  - Cambiar la configuración del sistema
  - Arrancar o detener servicios
- Modos de autenticación
  - Passwords, Tokens, Biométricos
  - 1 factor, 2 factores, etc

Desarrollo seguro y compliance

- Compliance es un término inglés que se traduce por ***cumplimiento normativo*** y hace referencia a las normas, tanto internas como externas, establecidas por una empresa, ente público o entidad

ISO 27002

- ¿Que es la ISO 27002?
  - En 1995, las organizaciones internacionales ISO (The International Organization for Standardization) e IEC (International Electrotechnical Commission) dieron origen a un grupo de normas que consolidan las directrices relacionadas al alcance de la Seguridad de la Información, siendo representada por la serie 27000. En este grupo se encuentra la **ISO/IEC 27002** (anteriormente denominada estándar 17799:2005), norma internacional que establece el *código de mejores prácticas para apoyar la implantación del Sistema de Gestión de Seguridad de la Información* (SGSI) en las organizaciones.
  - Establece con mas detalles los controles requeridos por la norma ISO 27001

Objetivos de la ISO 27002

- El principal objetivo de la **ISO 27002** es establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Esto también incluye la selección, implementación y administración de controles, teniendo en cuenta los entornos de riesgo encontrados en la empresa.

ISO 27002: Beneficios

- Mejor concienciación sobre la seguridad de la información.
- Mayor control de activos e información sensible.
- Ofrece un enfoque para la implementación de políticas de control.
- Oportunidad de identificar y corregir puntos débiles.
- Reducción del riesgo de responsabilidad por la no implementación de un SGSI o determinación de políticas y procedimientos.
- Se convierte en un diferencial competitivo para la conquista de clientes que valoran la certificación.
- Mejor organización con procesos y mecanismos bien diseñados y gestionados;
- Promueve reducción de costos con la prevención de incidentes de seguridad de la información.
- Conformidad con la legislación y otras reglamentaciones.

ISO 27002: Secciones

5. Politicas de Seguridad
6. Aspectos Organizativos de la Seguridad de la Informacion
7. Seguridad Ligada a los recursos humanos
8. Gestion de activos
9. Control de accesos
10. Cifrado
11. Seguridad Fisica y Ambiental
12. Seguridad operativa
13. Seguridad en las telecocumicaciones

… continua

- **Adquisicion, Desarrollo y Mantenimiento de los Sistemas de Informacion**
- Relaciones con proveedores
- Gestion de incidentes en la seguridad de la información
- Aspectos de seguridad de la información en la gestión de la continuidad del negocio

A14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

- Requisitos en la norma ISO 27001
- **Objetivo 1:** Requisitos de seguridad de los Sistemas de información
- **Objetivo 2:** Seguridad den los procesos de desarrollo y soporte

Objetivo 1: Requisitos de seguridad de los Sistemas de información

- 14.1.1 Análisis y especificación de los requisitos de seguridad
- 14.1.2 Aseguramiento de los servicios de aplicación en las redes públicas
- 14.1.3 Transacciones en línea

Objetivo 2: Seguridad en los procesos de desarrollo y soporte

- 14.2.1 Política de desarrollo seguro
- 14.2.2 Procedimiento de control de cambio del sistema
- 14.2.3 Revisión técnica de aplicaciones después de cambios de las plataformas operativas
- 14.2.4 Restricciones a los cambios en los paquetes de software
- 14.2.5 Principios de la ingeniería de Sistemas Seguros
- 14.2.6 Ambiente de desarrollo seguro
- 14.2.7 Desarrollo subcontratado
- 14.2.8 Pruebas de seguridad del sistema
- 14.2.9 Pruebas de aceptación del sistema

Practica

- Evaluar el cumplimiento de la sección 14 de la norma ISO 27002 en un sistema de información “core” de la empresa

Referencias

- https://normaiso27001.es/a14-adquisicion-desarrollo-y-mantenimiento-de-los-sistemas-de-informacion/