**Seguridad: Tema 6**

1. Auditoría de seguridad de sistemas de información

Una auditoría de seguridad estudia y analiza los sistemas para identificar y solucionar vulnerabilidades tras una revisión exhaustiva de la red, equipos y servidores. Permiten conocer el grado de protección de los equipos y las medidas de seguridad que tienen.

Una vez realizada debe reportarse a los responsables para que establezcan las medidas preventivas oportunas.

Es importante realizar una auditoría de seguridad al empezar a usar el sistema de información y luego seguir realizando auditorías de forma periódica (1 años aprox.) ya que los componentes HW y SW se van cambiando.

**Fases de una auditoría**

* Enumeración de redes, topologías y protocolos
* Identificación de los SO instalados
* Análisis de servicios y aplicaciones
* Detección, comprobación y evaluación de vulnerabilidades
* Medidas específicas de corrección
* Recomendaciones sobre implantación de medidas preventivas

**Tipos de una auditoría**

* Auditoría de seguridad interna: seguridad en redes locales y corporativas.
* Auditoría de seguridad perimetral: seguridad de la LAN ante la red externa.
* Test de intrusión: intentar acceder al sistema de forma no autorizada.
* Análisis forense: análisis posterior a incidentes.
* Auditoría de páginas web: comprobar vulnerabilidades, inyección SQL, XSS, etc.…
* Auditoría de código de aplicaciones: código de aplicaciones y páginas web.

1. Metodología de auditoría de seguridad

Las auditorías se deben realizar a través de buenas prácticas, definidas por estándares

Uno de ellos es el COBIT cuyo objetivo está garantizar la seguridad de los sistemas

También existe en estándar ISO 27002 que recoge buenas prácticas para tratar con información. El estándar ISO 27001 define los requisitos de una auditoría y de los sistemas de gestión de información

A través de la auditoría se verifica la autenticidad, confidencialidad, integridad, disponibilidad y auditabilidad de la información

Los objetivos de una auditoría son:

* Revisar la seguridad de los entornos y sistemas
* Verificar el cumplimiento de la normativa y legislación vigentes
* Elaborar un informe independiente

Fases de ejecución de una auditoría:

1. Definir el alcance de la auditoría.
2. Recopilación de información, identificación y realización de pruebas para la auditoría.
3. Análisis de las evidencias: documentación de los resultados obtenidos.
4. Informe de auditoría: se recogen las acciones realizadas y los fallos detectados.
5. Plan de mejora: recomendaciones para arreglar los fallos y mantener el sistema de seguridad estables.