SEGURIDAD INFORMÁTICA

2º DE SISTEMAS MICROINFORMÁTICOS Y REDES

Noelia Huguet Chacón

TOBALCAIDE

TEMA 6: AUDITORÍAS DE SEGURIDAD

1. Auditoría de seguridad en sistemas de información
2. Metodología de auditoría de seguridad

6.1 AUDITORÍA DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN

- Una **auditoría de seguridad informática** o auditoría de seguridad de sistemas de información (SI) es el estudio que comprende el **análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades** que pudieron presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.
- Una vez obtenidos **los resultados, se detallan, archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo,** siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.
- Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

6.1 AUDITORÍA DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN

- Realizar auditorías con cierta frecuencia asegura la integridad de los controles de seguridad aplicados a los sistemas de información.
- Acciones como el constante cambio en las configuraciones, la instalación de parches, actualizaciones de software y la adquisición de nuevo hardware hacen necesario que los sistemas estén continuamente verificados mediante auditoría.

6.1 AUDITORÍA DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN

FASES DE UNA AUDITORÍA:

- Los servicios de auditoría constan de las siguientes fases:
  - Enumeración de redes, topologías y protocolos.
  - Identificación de los sistemas operativos instalados.
  - Análisis de servicios y aplicaciones.
  - Detección, comprobación y evaluación de vulnerabilidades.
  - Medidas específicas de corrección.
  - Recomendaciones sobre implantación de medidas preventivas.

6.1 AUDITORÍA DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN

TIPOS DE UNA AUDITORÍA:

- Los servicios de auditoría pueden ser de distinta índole:
  - Auditoría de seguridad interna.
  - Auditoría de seguridad perimetral.
  - Test de intrusión.
  - Análisis forense.
  - Auditoría de páginas web.
  - Auditoría de código de aplicaciones.

6.1 AUDITORÍA DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN

TIPOS DE UNA AUDITORÍA:

- **Auditoría de seguridad interna.** En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno.
- **Auditoría de seguridad perimetral.** En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores.
- **Test de intrusión.** Es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.

6.1 AUDITORÍA DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN

TIPOS DE UNA AUDITORÍA:

- **Análisis forense.** Es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperabilidad del sistema, el análisis se denomina análisis *postmortem*.
- **Auditoría de páginas web.** Entendida como el análisis externo de la web, comprobando vulnerabilidades como la inyección de código SQL, Verificación de existencia y anulación de posibilidades de Cross Site Scripting (XSS)…
- **Auditoría de código de aplicaciones.** Análisis de código tanto de aplicaciones de páginas web como de cualquier tipo de aplicación, independientemente del lenguaje empleado.

6.2 METODOLOGÍA DE AUDITORÍA DE SEGURIDAD

- Una auditoría se realiza con base a un patrón o conjunto de directrices o **buenas prácticas sugeridas.**
- Existen estándares orientados a servir como base para auditorías de informática.
- Uno de ello es **COBIT** (Objetivos de Control de las Tecnologías de la Información), dentro de los objetivos definidos como parámetros, se encuentra el de "garantizar la seguridad de los sistemas".
- Adicional a este estándar podemos encontrar el estándar **ISO 27002,** el cual se conforma como un código internacional de buenas prácticas de seguridad de la información, este puede constituirse como una directriz de auditoría aoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoría y sistemas de gestión de seguridad, como lo es el estándar **ISO 27001**.

6.2 METODOLOGÍA DE AUDITORÍA DE SEGURIDAD

- Con una auditoría de seguridad se da una visión exacta del nivel de exposición de sus sistemas de información a nivel de seguridad.
- En la auditoría se verifica la seguridad en la autenticidad, confidencialidad, integridad, disponibilidad y auditabilidad de la información tratada por los sistemas.
- Los **objetivos** de una auditoría de seguridad de los sistemas de información son:
  - Revisar la seguridad de los entornos y sistemas.
  - Verificar el cumplimiento de la normativa y legislación vigentes.
  - Elaborar un informe independiente.

6.2 METODOLOGÍA DE AUDITORÍA DE SEGURIDAD

- La metodología para una auditoría de sistemas de información establece su **ejecución por fases**:
  1. **Definir el alcance de la auditoría**: análisis inicial y plan de auditoría.
  2. **Recopilación de información, identificación y realización** de pruebas de auditoría, incluyendo, si se acuerda, acciones de hacking ético o análisis de vulnerabilidad de aplicaciones.
  3. **Análisis de las evidencias**, documentación de los resultados obtenidos y conclusiones.
  4. **Informe de auditoría** en el que se recogen las acciones realizadas a lo largo de la auditoría y las deficiencias detectadas. El informe contiene un resumen ejecutivo en el que se resaltan los apartados más importantes de la auditoría.
  5. **Plan de mejora** con el análisis y las recomendaciones propuestas para subsanar las incidencias de seguridad y mantener en el futuro una situación estable y segura de los sistemas de información.