Trabajo Práctico N° 3.1: "Seguridad de S.I."

Objetivos: Que los alumnos logren:

- Comprender la importancia del funcionamiento seguro de los SI/TI.
- Desarrollar habilidad de práctica para administrar los riesgos y planificar líneas de defensa en un ambiente informático.
- Conocer las principales normas y reglamentaciones que influyen en el funcionamiento seguro de los SI/TI.

Referencia Temática:

- ***Unidad III: La Administración de Recursos de SI/TI – Seguridad y Auditoría de Sistemas de Información***

Modalidad de Desarrollo: Grupal

Fecha de puesta en común: Miércoles 4/6/2025

NOTA: Para el desarrollo del Trabajo Práctico y a los efectos de lograr los objetivos de aprendizaje propuestos, se debe respetar el orden de las consignas.

Consignas:

PRECLASE. **Actividad individual disponible en el aula virtual.**

Casos de estudio para "MANAGEMENT SEGURO DE SI/TI"

Escuchar atentamente cada uno de los casos que se indican a continuación y **analizarlos** desde el punto de vista de cada uno los aspectos del ***"Management Seguro de SI/TI"***

EN CLASE.

a) **Actividad individual.** Leer el artículo "La seguridad paranoica"[1]. Identificar la/las amenazas, su comportamiento, impactos, activos en juego. Elaborar conclusiones. ¿Qué inquietud le genera lo que dice el artículo si usted fuese el Gerente de SI/TI de Agunsa?

b) **Actividad grupal.**

Suponiendo que AGUNSA cuenta con un depósito de almacenamiento en el Puerto de Barranqueras (Chaco), desarrollar los siguientes ejercicios:

i) Investigar en la W.W.W casos de fallas de seguridad informática en organizaciones similares.

ii) Desarrollar las etapas de Administración de Riesgos, en forma completa, a fin de elaborar el esquema de seguridad informática que consideren más adecuado para la sede local de AGUNSA, sabiendo que la principal aplicación utilizada es el nuevo Sistema de Gestión de Almacenes (WMS). Las medidas deben incluir políticas de seguridad acorde. Puede tomarse como guía las líneas de actuación planteadas por la norma ISO 27002. También, para el caso de la cuarta etapa, puede tomarse como orientación general lo indicado en el artículo "Plan B: Estrategias de Contingencia"[2].

Bibliografía de Referencia:

- ROBSON, Wendy. ***Decisiones Estratégicas en Sistemas de Información II***. Tomo 5. Colección Management Estratégico de Sistemas de Información. MP Ediciones. 2ª edición. 1999. Argentina.
- LARDENT, Alberto R. ***Sistemas de Información para la Gestión Empresaria – Procedimientos, Seguridad y Auditoría***. Editorial Prentice Hall Pearson Educación. 2001. Brasil.
- PIATTINI, Mario y DEL PESO, Emilio. ***"Auditoría informática: un enfoque práctico".*** Editorial Alfaomega-RA-MA. 2ª Edición ampliada y revisada. Noviembre 2006. O posteriores.

Revistas especializadas y fuentes de material de trabajo:

- Material complementario provisto por la Cátedra disponible en el aula virtual, en la sección *U.III.1) "Seguridad de SI"*

[1] Fernández, Pablo Martín. (2008). La seguridad paranoica. Information Technlology. 131. – Suplemento especial - Páginas 2 a 4.

[2] Giorgetti, Alicia. (2008) Plan, Estrategias de Contingencia. Information Technology. 130 – Páginas 88 a 94.