AUDITORIA GRUPO 3

Escenarios para grupos 1, 3, 5, 7, 9, 11

Empresa emergente dedicada a la venta de productos fertilizantes para campos con una capacidad financiera acotada. Todos sus empleados trabajan on site y están dispuestos a recibir capacitación. Poseen actualmente dos personas encargadas de sistemas, las cuales manejan información sensible, pero que todos los usuarios pueden ver (no es política de la empresa). No realizan copias de información porque no las creen convenientes. Poseen una página web donde hay catálogos y los clientes pueden hacer compras a través de la misma.

- Seguridad lógica: Antivirus Windows Defender
- Seguridad física: UPS para prevenir cortes o fallas eléctricas y dar tiempo de guardado y correcto apagado de equipos.
- Seguridad activa: usuario y contraseña para cada empleado de la empresa.
- Seguridad pasiva: realización de backups en cortos plazos para resguardo de datos.
- Control de vulnerabilidad: encriptación de datos personales para clientes que compran en la página web.
- Control de medida de seguridad:Crear particiones en el disco duro para almacenar archivos y backups en una unidad distinta a donde tenemos nuestro sistema operativo.

Microdesafío

1. Utilizando el documento de presentación de la actividad, cada mesa deberá colocar el link al documento del plan de seguridad diseñado en la actividad anterior, para que otro grupo pueda acceder y analizarlo.

2. Realizar una auditoría del plan de seguridad de uno de los grupos en base a los escenarios planteados.

3. Buscar vulnerabilidades y fallas que faltaron solventar. Cuando se encuentre una falla, hay que explicar por qué es una vulnerabilidad y cómo podríamos atacar. A su vez, se debe explicar cómo solucionar dicha vulnerabilidad.

Analizada el informe del plan de auditoría, se realiza/n la/s siguiente/s observación/es:

1- Vista de información sensible por todos los usuarios. Debería existir perfiles y accesos a sistemas en función de los mismos.