Práctica integradora Equipo 7

Objetivo
Para empezar a poner en práctica los conocimientos adquiridos, realizaremos la siguiente actividad. Se crearán grupos, divididos en sus respectivas salas y realizarán la siguiente ejercitación.

Microdesafío.
La empresa que se les haya asignado los contrata como asesores de seguridad, ya que creen que es una parte fundamental para resguardar sus activos. En base a lo visto en clase y clases anteriores deben hacer:

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

1. **Un análisis de la situación actual de cada empresa que se les haya asignado**.
   La empresa no cuenta con niveles de seguridad físicos ni lógico para poder resguardar la información, estas medidas de seguridad se tienen que adoptar como políticas de seguridad de la empresa.

2. Para cada escenario planteado, crear un plan de seguridad
   Respuesta: En primer lugar, el plan de seguridad seria restringir el acceso al personal no autorizado y de esta forma resguardar la información sensible, Es necesario realizar copias de seguridad a las bases de datos en caso tal exista un percance en la compañía y de esta manera podamos acceder al backup. Con esto podríamos resguardar la información de los clientes.

3. Este plan debe ser de 6 pasos e incluir: seguridad lógica, física, pasiva, activa y controles de medida de seguridad y de vulnerabilidades que podrían explotar los atacantes.

    - Seguridad lógica:
        - Limitar el acceso a programas y archivos
        - La información debe ser recibida por el solo destinatario
        - Autenticación de doble factor para los accesos a las cuentas
        - Actualización de contraseñas
    - Seguridad física
        - Bases de datos
        - Ups
        - Discos raid
        - Accesos

- Pasiva
    - Backup’s en distintos dispositivos
    - Escaneos de seguridad
    - Particiones de discos
    - Inactivar los puertos de red si se encuentra un virus en el sistema
- Activa
    - Actualización de contraseñas
    - Antivirus
    - Firewalls
    - Encriptar los datos importantes
- Controles de medida de seguridad
    - usuarios con diferentes niveles de acceso.
- Vulnerabilidades:
    - Contraseñas inseguras
    - Capacitación al personal