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

Empresa emergente dedicada a la venta de productos fertilizantes para campos, con una capacidad financiera acotada, todos sus empleados trabajan on site y están dispuesto 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. Hacer un análisis de la situación actual de cada empresa que nos toque.
2. Para cada escenario planteado, crear un plan de seguridad
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.

Casos de acción

1. **Seguridad lógica:** generar controles de acceso para limitar el acceso a información sensible, como así también cifrar las comunicaciones relacionadas a las transacciones de venta dentro de la plataforma.
    a. Implementar un esquema de seguridad que permita el acceso a elementos de sistemas únicamente a personal autorizado.

Instalar antivirus y firewalls en todos los equipos de la red local y en los backups remotos.

2. **Física:** Realizar copias de seguridad de los datos.
    a. Faltaría implementar UPS, sistemas redundantes y protección ante amenazas externas como pararrayos, alarmas contra incendio e intrusos, extintores.
3. **Pasiva:** En el disco duro generar backups en una unidad distintas a el S.O. y backups versionados on-cloud.
    a. Programar actualizaciones y escaneos periódicos del antivirus corporativo.

4. **<u>Activa</u>:** Encriptar los datos para que no tengan acceso todos los usuarios a la info sensible.
    a. Establecer políticas de contraseñas seguras para empleados y modificar el login en la página para que solo permita crear cuentas bajo el cumplimiento de dichas políticas.
5. **<u>Controles de seguridad</u>:** dado que los empleados están dispuestos a recibir capacitación, se pueden usar medidas preventivas: informando qué es lo que puede suceder dadas ciertas acciones indebidas, para poder prevenirlas.
6. **<u>Vulnerabilidades</u>:** información sensible no confidencial (cualquier usuario puede verla). Capacitar a los empleados, educando sobre ataques de ingeniería social (realizar simulacros de phishing, rondas informativas, etc.).

Enviar al equipo de sistemas a la DEFCON 21 (https://www.defcon.org/)