GRUPO 1 gracias <3

1. Agus Viruel
2. Sassali Constanza
3. Ximena Salamanca
4. Miranda Micaela

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. Crear un plan de seguridad

Seguridad lógica:

Cambiar que todos tengan el acceso y la visibilidad de los datos.

Física:

Consiste en el establecimiento de técnicas que permiten resguardar de cualquier tipo de daños a los equipos en los cuales se almacena los activos de una organización —sus datos—.
Dispositivos físicos de protección : Pararrayos, extintores, detectores de humo, alarma contra intrusos, entre otros.
UPS (Uninterruptable Power Supply) : Es un dispositivo electrónico que almacena energía por medio de una batería interna. Esto le permite a los dispositivos que están conectados al mismo, frente a un apagón eléctrico, seguir almacenando la información por un determinado tiempo.
Respaldo de datos: Es importante saber que los datos son los activos más importantes dentro de una organización, por tal motivo, es de suma importancia el manejo y cuidado de los mismos ya que pueden estar expuestos a muchos factores como hurto, alteración, virus, entre otros. Por tal motivo, se deben realizar copias de seguridad o backups de los datos completos e incrementales. El backup es un proceso por el cual se realiza la copia de los datos originales con el fin de prevenir cualquier tipo de pérdida de los mismos.
Sistemas redundantes : Son la copia de datos de mayor importancia. Cuando uno de los sistemas falla, no se pierde la información, sino que se recupera del otro lugar donde se encuentra.

Pasiva:

La realización de copias de seguridad de los datos en más de un dispositivo y/o en distintas ubicaciones físicas

Activa:

Uso de contraseñas
Encriptar los datos importantes (cifrar los datos o la información mediante un algoritmo de cifrado con una clave para que el dato/información sólo pueda ser leído si se conoce la clave de cifrado.)

Controles de medida de seguridad:

Controles de vulnerabilidades que podrían explotar los atacantes

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

Primer paso: se debe realizar una copia de seguridad de los datos, (puede ser en un disco externo o en la nube)

Segundo paso: el sistema debería requerir que los usuarios(tanto empleados cómo clientes) posean seguras contraseñas.

Tercer paso: Restringir acceso a la información para cierto tipo de usuarios.

Cuarto paso: Incorporación de un anti-virus

Quinto paso: utilizar la OPS para evitar que haya pérdida de información o rotura de equipos ante posibles dificultades eléctricas.

Sexto paso: realizar un cifrado de datos.

Sugerencias grupo 10:

Capacitar a los empleados como medida de protección proactiva preventiva.

En el paso 5 también agregar Dispositivos físicos de protección.