1. Un análisis de la situación actual de cada empresa que se les haya asignado.

Seguridad Lógica:
El control de acceso es nulo, ya que cualquiera puede acceder a la información sensible de la empresa, seguramente no debe haber ningún cifrado de datos de los clientes o usuarios, y habría que evaluar si usan algún antivirus y firewall.

Vulnerabilidad Física:
No cuenta con dispositivos físicos de protección, tampoco cuenta con Ups, Respaldo de datos o sistemas redundantes, pero en el escenario ideal es bueno que contenga algunas protecciones para salvaguardar los datos sensibles de la compañía.

Seguridad Pasiva:
No consideran conveniente la realización de copias de seguridad de los datos. No mencionan tampoco el uso de antivirus ni realización de controles periódicos para evitar ataques.

Seguridad Activa:
Las personas encargadas de sistemas manejan información sensible la cual está a la vista y siquiera está encriptada, los datos de los datos de compra de los clientes tampoco están encriptados. No se establecen parámetros de seguridad en cuanto a la creación e ingreso de usuarios, tampoco se posee ningún tipo de Software de seguridad como antivirus o antispyware

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.

Seguridad Lógica:
Primero que nada crearía un control a los accesos de la información sensible de la empresa, para que cualquiera en la misma no pueda acceder, también vería de agregar algún sistema de cifrado, para así poder dificultar el acceso de externos a esta información y en el caso de que no haya ningún antivirus o firewall, ver de agregarle a todos los equipos los mismos

Vulnerabilidad Física:
El Plan de trabajo propuesto arrancaría por incluir protección de dispositivos como pararrayos, alarmas, por otro lado sumariamos respaldo de datos.

Seguridad Pasiva:
Implementación de antivirus y la práctica de escaneos y limpiezas regulares de los equipos.
Crear particiones en el disco duro para contar al menos con zonas de almacenamiento independiente ya que no desean realizar copia de seguridad
Seguridad Activa:
Ya que se realizan compras mediante la web, es necesario que los usuarios tengan contraseñas y métodos de acceso adecuados.
Se deben implementar cifrados y software de seguridad informática.

Vulnerabilidad o Amenaza

La diferencia entre vulnerabilidad y amenaza es muy interesante, aunque son términos que se confunden a menudo. Veamos cómo se definen:

- Una vulnerabilidad (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.

- Por su parte, una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas.