* Empresa ya consolidada que se dedica a brindar servicios informáticos, la mayoría de sus empleados trabajan en remoto, pero hay algunos que van on site, necesitan una intranet más segura, y la información confidencial de la empresa tiene buena seguridad lógica pero muy poca física, aunque igualmente desean tener asesoramiento en seguridad lógica, no tienen problemas en invertir dinero pero sus empleados se resisten al cambio de nuevas restricciones. Poseen una página web donde brindan sus servicios y los clientes pueden contactarse a través de la misma.
* Hacer un análisis de la situación actual de cada empresa que nos toque.

Para cada escenario planteado, crear un plan de seguridad

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:

-Control de ac cesos: Generar contraseñas alfanuméricas y no repetirlas en otras cuentas.

-Mejora del firewall

-Actualización de antivirus de modo constante

-Cifrado de datos.

* Seguridad Física:

-Base de datos de respaldo (crear backups)

-Sistemas redundantes (Copia de datos de mayor importancia)

-UPS (Dispositivo que almacena energía en una batería interna, frente a un apagón eléctrico, permite seguir almacenando la info por un determinado tiempo)

-Dispositivos de protección (Pararrayos - Detectores de humo - Alarma contra \_\_\_\_\_\_-intrusos - Extintores)

* Seguridad Pasiva:

-Realización de copias de seguridad de los datos en más de un dispositivo y/o en distintas ubicaciones físicas

-Escanear y limpiar los equipos para evitar ataques malware

-Crear particiones de discos duro, para almacenar archivos y backups en unidades diferentes a donde se encuentra el sistema operativo

-Frente a un ataque, desconectar el equipo de la red hasta solucionar el problema

-Cuando haya una infección de virus, corroborar que el antivirus funcione correctamente

* Seguridad Activa:

-Mayor control en tipo de contraseñas de cada usuario

-Inhabilitar puertos USB (Manejo de información solo por correy y software de \_\_\_\_\_\_la empresa)

-Protocolo estándar para apertura de emails o archivos desconocidos

* Controles de medida de seguridad:

Proactivas:

-Directivas: Indican qué podemos y que no podemos hacer

-Disuasivas: Pueden desviar la intención del atacante

-Preventivas:

Reactivas:

-Detectivas

-Correctivas

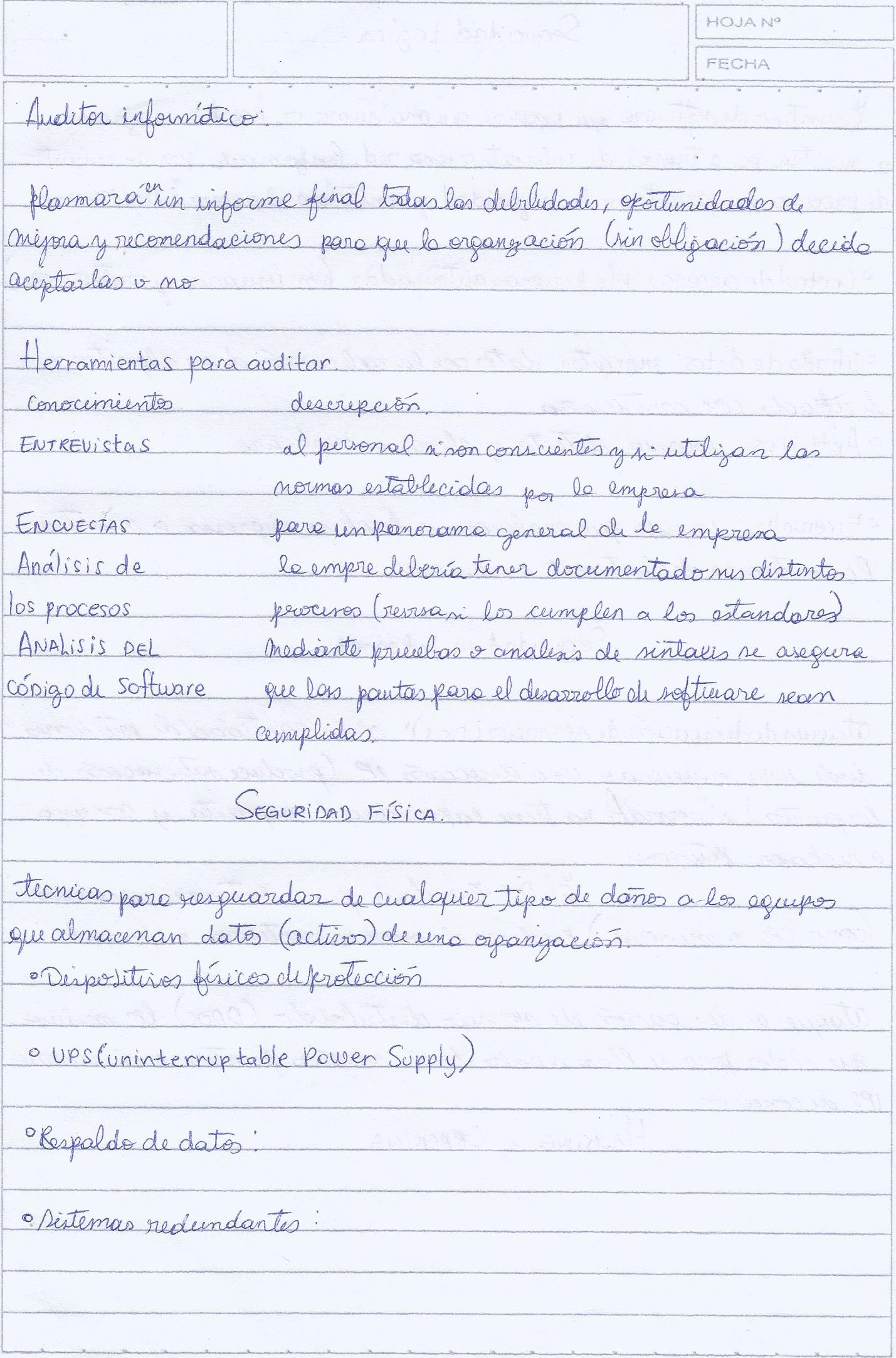
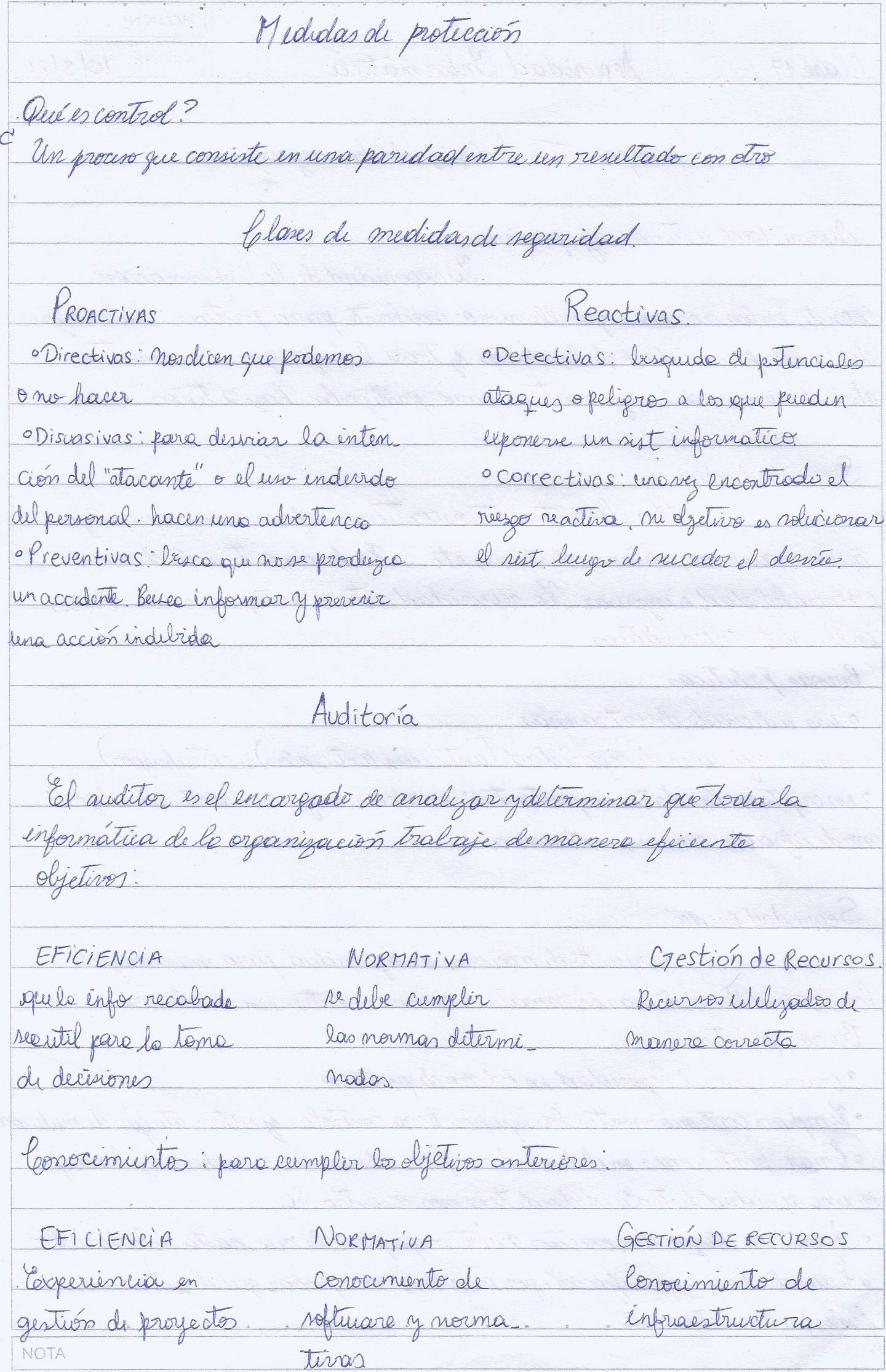
* Vulnerabilidades que podrían explotar los atacantes:

Captación de información por parte de personas que se encuentren en la planta física

**Resumen de plan de trabajo**

1. Inhabilitar puertos USB (Manejo de información solo por correy y software de lla empresa)
2. UPS (Dispositivo que almacena energía en una batería interna, frente a un apagón eléctrico, permite seguir almacenando la info por un determinado tiempo)
3. Dispositivos de protección (Pararrayos - Detectores de humo - Alarma contra intrusos - Extintores)
4. Base de datos de respaldo (crear backups)
5. Capacitación a empleados sobre nuevas políticas

Imagen que contiene texto, documento

Descripción generada automáticamenteTexto, Carta

Descripción generada automáticamente