**GRUPO 10**:

Empresa ya consolidada que se dedica a brindar servicios informáticos. La mayoría de sus empleados trabajan de forma remota, pero hay algunos que lo hacen on site. Necesitan una intranet más segura. 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.

**Seguridad lógica**: Control de acceso, cifrado de datos y antivirus para cada uno de las computadoras personales que los empleados utilizan para hacer home office.  
Uso de VPN para el personal conectados desde sus hogares.  
Seguridad perimetral mediante IPS y firewall.

**Seguridad física**: Dispositivos físicos informáticos almacenados en un data center que estén en la empresa física + respaldo de datos para computadoras en oficina y las que se utilizan de Home Office.  
Acceso al data center mediante acceso biométrico solo para personal autorizado,

**Seguridad pasiva**: Como acciones se pueden realizar copias de seguridad programadas cada un mes, y programar limpiezas y escaneos de cada equipo tanto en la empresa como en las PC de Home Office cada 45 días. Antivirus funcionando activamente y actualización cada una semana. Programación de backup de información cada 15 días

**Seguridad activa**: ​​  
- Instalación de software antivirus eficaces y actualizados en equipos, redes y sistemas de la empresa, con el fin de combatir los principales tipos de malware (virus informático).   
- Diseñar e implantar políticas efectivas de gestión de contraseñas, credenciales y permisos de los usuarios. Deberán actualizarse cada 10 días.

**Controles de medida de seguridad:** Se implementarán mecanismos acciones y herramientas para la detección de errores. Este proceso se realizará cada 24 horas programando a las 02 Am   
Contar con un personal profesional y especializado en el área de informática

**Vulnerabilidades**: Debido a que los empleados permanecen conectados constantemente a internet se encuentran expuestos a malwares como phishing, ingeniería social, adware, troyanos,   
  
Cuando las credenciales de autenticación se ven comprometidas, las sesiones de usuario y las identidades pueden ser secuestradas por actores maliciosos para hacerse pasar por el usuario original.

Ataque DDoS (Denegación de servicio): Un ataque de denegación de servicio distribuido (*DDoS*) se produce cuando un servidor recibe muchas peticiones de acceso, sobrecargando el sistema y haciendo que el servidor caiga o funcione de forma incorrecta (acceso lento o rebotando mensajes de errores). Para realizar este tipo de ataques se utilizan muchos ordenadores (bots) que de forma automatizada hacen peticiones a ese servidor.

Los ataques DDoS son muy habituales contra servidores o servidores web de empresas, por lo que es muy importante disponer de medidas protectoras contra esta peligrosa amenaza que puede dejar fuera de servicio la actividad de una empresa.