Análisis general:

La empresa no cuenta con fondos grandes para implementar medidas, así que las medidas sugeridas son de bajo-medio costo.

Ya que los empleados trabajan en forma presencial no precisan implementar VPNs, ni sistemas de acceso remoto.

El acceso a la información no está limitado para los usuarios que lo precisan.

Las copias de seguridad DEBEN realizarse ya que pueden sufrir un ataque y perder toda la información.

Controles de medidas de seguridad y de vulnerabilidades:

Seguridad activa:
Uso y empleo adecuado de contraseñas.
Uso de software de seguridad informática, como antivirus, antiespías y cortafuegos.
Los antivirus, antiespías y cortafuegos deben ser actualizados cada día para actualizar las bases de datos de virus.
Encriptar los datos importantes.
Control de acceso limitado por perfil según necesidad de acceso a los datos.

Seguridad Pasiva:
Realizar copias de seguridad de los datos en más de un dispositivo o en distintas ubicaciones físicas por lo menos una vez por semana.
Escanear y limpiar continuamente los equipos para controlar y evitar ataques de malware.
Crear particiones en el disco duro para almacenar archivos y backups (copias de seguridad) en una unidad distinta a donde tenemos nuestro sistema operativo (Costo intermedio).

Sugerencias:

Frente a un ataque, desconectar el o los equipo/s de la red hasta que se pueda solucionar.
Es importante que cuando haya una infección por un virus, se compruebe que el antivirus funcione correctamente.

Generar modelos de procesos y dar charlas y capacitaciones para evitar problemas del tipo phishing en el email corporativo y uso de aplicaciones laborales.
Generar manuales para que los procesos se lleven a cabo sin errores y para que el uso indebido de las herramientas no genere vulnerabilidades en el sistema.