En base a que somos:

Empresa emergente dedicada a la venta de productos fertilizantes para campos con una capacidad financiera acotada. Todos sus empleados trabajan on site y están dispuestos 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. Análisis de la situación actual de la empresa
   Al ser una empresa con una capacidad financiera acotada, con información sensible pero no crítica, con escaso personal de sistemas y nula capacitación del personal en medidas básicas de seguridad informática, se va a sugerir un Plan de Seguridad básico y de bajo costo, adecuado para las necesidades de la empresa, que tienda a proteger de las vulnerabilidades externas y que provea una educación en seguridad informática a todo el personal.

2. Plan de seguridad

Seguridad lógica:
- Control de accesos (proxy)
- Uso de antivirus

Seguridad física:
- Contratar un espacio en la nube para el respaldo de datos. Se deben realizar copias de la información y estar resguardadas en forma segura.

Seguridad pasiva:
- Capacitar a los empleados sobre cómo deben actuar en caso de que se presente un ataque (desconectar el equipo de la red, comprobar funcionamiento de antivirus).
- Instalación de Antivirus y AntiMalware gratuitos o asequibles al poder adquisitivo de la empresa.

Seguridad activa:

- Capacitación en uso adecuado de contraseñas
- Verificar que los dispositivos cuentan con software de seguridad: antivirus
- Encriptar los datos sensibles, y que cada usuario tenga acceso solamente a la información que requiere para su área de trabajo (definición de diferentes perfiles dentro de los sistemas)

Controles de medida de seguridad:
- Manual de Buenas prácticas informáticas (no colocación de USB en las PC, uso de claves personal e intransferible, no acceder a páginas web sospechosas)

Controles de vulnerabilidades:
- Contratación de una auditoría informática semestral, a efectos de evaluar vulnerabilidades y desvíos, e ir optimizando las buenas prácticas y robustecer la seguridad informática.