Security risk assessment report

After inspecting the organization’s network, you discover four major vulnerabilities. The four vulnerabilities are as follows:

1. The organization’s employees' share passwords.
2. The admin password for the database is set to the default.
3. The firewalls do not have rules in place to filter traffic coming in and out of the network.
4. Multifactor authentication (MFA) is not used.

Part 1: Select up to three hardening tools and methods to implement
Después de realizar un análisis exhaustivo del incidente de seguridad que afectó a la organización, se han identificado cuatro vulnerabilidades críticas. Para mitigar estos riesgos y prevenir futuras brechas, se recomienda implementar las siguientes tres prácticas de hardening: 1. **Implementación de políticas de contraseñas seguras y gestión individualizada de credenciales.** 2. **Configuración estricta de firewalls con reglas claras de entrada y salida.** 3. **Activación de la autenticación multifactor (MFA) en todos los sistemas críticos.**

Part 2: Explain your recommendations
Políticas de contraseñas seguras y gestión individualizada: Esta práctica elimina el riesgo de accesos compartidos y promueve la trazabilidad de cada sesión de usuario. Es fundamental para prevenir accesos internos no autorizados y garantizar que cada acción en el sistema pueda ser auditada de forma precisa. Se recomienda aplicar esta política de forma permanente, acompañada de formación periódica para el personal cada 6 a 12 meses. **Configuración de reglas de firewall:** Los firewalls sin reglas activas no ofrecen protección real. Al configurar reglas estrictas —basadas en el principio de "denegar todo por defecto y permitir solo lo necesario"— se reduce drásticamente la superficie de ataque. Esta medida debe implementarse inmediatamente y revisarse mensualmente o ante cualquier cambio en la arquitectura de red. **Autenticación multifactor (MFA):** Añade una capa crítica de seguridad, especialmente frente a ataques de fuerza bruta, phishing o robo de credenciales. Aunque una contraseña sea comprometida, el segundo factor (como un token, app o biometría) detiene al atacante. Se recomienda activar MFA en todos los servicios críticos de inmediato y mantener una revisión de su efectividad cada seis meses.