# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| **Encryption using the latest standards**  **Configuration checks**  **Disabling unused ports**  **Firewall maintenance**  **Multifactor authentication (MFA)**  **Network access privileges**  **Password policies**  **Penetration test (pen test)**  **Port filtering** | |
|

| **Part 2: Explain your recommendations** |
| --- |
| 1. Esta recomendación es para mitigar que la información comprometida no sea legible a las personas que la hayan captado si el tráfico fue comprometido. 2. Validar si la información en las bases está cifrada, es muy importante para mantener la integridad de los datos. 3. Deshabilitar puertos, tener el mínimo acceso es muy importante para no dejar brechas a ataques que puedan encaminarse por estos puertos habilitados. 4. Es importante realizar el mantenimiento de las reglas de firewall, validarlas, actualizarlas. 5. El MFA, es indiscutible para asegurar correctamente la autenticación a las cuentas y mitigar accesos no autorizados. 6. Los privilegios de acceso a la red, importante que tipo de permisos tiene, escritura, a los puertos esto para mitigar el alcance del permiso. 7. Es importante definirla para crear contraseñas seguras, que se puedan almacenar en sistemas cifrados y minimizar esa superficie. 8. El pen test, cada cierto periodo de tiempo, al menos dos veces al año para validar que puertas están abiertas, qué vulnerabilidades existen y de esta manera mitigar. 9. Filtrado de puertos, es importante en el firewall para minimizar estas puertas abiertas a ataques relacionados con puertos expuesto en los sistemas de la organización. |