# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| En este caso aplicaremos los siguientes métodos de seguridad que harán mejorar y endurecer la seguridad e integridad de la red;   * Autenticación Multifactor (MFA) * Mantenimiento del firewall * Políticas de contraseñas * Tutorías y charlas educativas sobre ciberseguridad | |
|

| **Part 2: Explain your recommendations** |
| --- |
| **Charlas y talleres regulares:** Realizaremos sesiones informativas donde explicaremos claramente los riesgos de compartir contraseñas (accesos no autorizados, fugas de información, dificultad para rastrear responsabilidades, etc.).  **Políticas de seguridad para contraseñas**: Aplicaremos políticas de seguridad de contraseñas para el usuario Administrador, con una longitud de por ejemplo, 15-20 caracteres o más.  **Autenticación MFA:** Activaremos la autenticación MFA en la que los usuarios requerirán de un código en la app autenticadora o código SMS para poder realizar el inicio de sesión que solicitan.  **Mantenimiento del Firewall:** Es importante que apliquemos reglas de seguridad y mantengamos actualizado nuestro firewall para estar al tanto de los últimos parches de seguridad.  **Autenticación Multifactor (MFA):** Implementar **lo antes posible** y mantener **siempre activa** al iniciar sesión. Revisar la cobertura **anual o semestralmente**.  **Mantenimiento del Firewall:**   * **Reglas**: Revisar **trimestral o semestralmente** o después de cada cambio en la red. * **Firmware**: Actualizar parches críticos **inmediatamente**; otras actualizaciones según el proveedor. * **Logs**: Monitorizar alertas **en tiempo real**; revisar logs generales **diaria o semanalmente**.   **Políticas de contraseñas:** Establecer **inicialmente** y revisar/actualizar **anualmente**. El cumplimiento técnico debe ser **siempre activo**. Enviar recordatorios a los usuarios **trimestralmente**.  **Tutorías y Charlas de Ciberseguridad:** Para nuevos empleados, **inmediatamente** en el onboarding. Formación general **anual**. Campañas específicas **mensual o trimestralmente**. Simulacros de phishing **trimestralmente**. |