# Informe de evaluación de riesgos de seguridad

|  |
| --- |
| **Parte 1: Selecciona hasta tres herramientas y métodos de reforzamiento a implementar** |
| 1. **Implementar autenticación multifactor (MFA).** 2. **Establecer y aplicar políticas de contraseñas fuertes.** 3. **Configurar y mantener el firewall con reglas de filtrado.** |
|

|  |
| --- |
| **Parte 2: Explica tus recomendaciones** |
| 1. **Autenticación multifactor (MFA):**    * Requiere que los usuarios utilicen más de una forma de verificación, como contraseña más huella digital, tarjeta de identificación, PIN o aplicación de autenticación.    * **Eficacia:** reduce la probabilidad de accesos no autorizados, incluso si una contraseña es robada o compartida. También dificulta los ataques de fuerza bruta.    * **Aplicación:** debe implementarse de manera permanente, en especial para usuarios con privilegios de administrador. 2. **Políticas de contraseñas fuertes:**    * Se deben definir reglas claras sobre la longitud mínima, uso de caracteres especiales y caducidad periódica. También incluir bloqueo automático después de varios intentos fallidos y prohibición de compartir credenciales.    * **Eficacia:** aumenta la dificultad para que un atacante adivine o crackee contraseñas. Al reforzar la cultura organizacional con capacitaciones periódicas, se reduce el riesgo humano.    * **Aplicación:** las contraseñas deben renovarse cada 90 días y las capacitaciones a empleados realizarse al menos una vez al semestre. 3. **Mantenimiento y configuración de firewalls:**    * Consiste en revisar y actualizar las reglas de seguridad que filtran el tráfico entrante y saliente. Se deben bloquear puertos no usados y monitorear el tráfico sospechoso.    * **Eficacia:** protege contra ataques externos como DoS/DDoS y evita que software malicioso se comunique hacia afuera.    * **Aplicación:** debe mantenerse activo en todo momento y revisarse mensualmente o después de cualquier incidente de seguridad. |