INFORME DE EVALUACIÓN DE RIESGOS DE SEGURIDAD

Parte 1: Selección de herramientas y métodos de reforzamiento
Para abordar las vulnerabilidades detectadas, la organización puede implementar las siguientes herramientas de reforzamiento: 1. **Autenticación multifactor (MFA)**: Esta herramienta requiere que los usuarios utilicen más de un método para verificar su identidad antes de acceder a una aplicación. Los métodos pueden incluir escaneos de huellas dactilares, tarjetas de identificación, números PIN y contraseñas. 2. **Políticas de contraseñas fuertes**: Estas políticas pueden definir requisitos específicos para la longitud de las contraseñas, el uso de caracteres permitidos y establecer directrices para evitar el intercambio de contraseñas. Además, se pueden implementar medidas como bloquear el acceso a la red después de varios intentos de inicio de sesión fallidos. 3. **Mantenimiento regular del firewall**: Este proceso implica la revisión y actualización continua de las configuraciones de seguridad del firewall para anticiparse a posibles amenazas.

Parte 2: Recomendaciones
La implementación de la autenticación multifactor (MFA) disminuye la probabilidad de que un atacante pueda acceder a la red mediante ataques de fuerza bruta u otros métodos similares. Además, dificulta el intercambio de contraseñas entre los miembros de la organización, lo cual es crucial, especialmente para empleados con privilegios de administrador. La MFA debe aplicarse de forma constante. Establecer y hacer cumplir una política de contraseñas dentro de la empresa aumenta la seguridad de la red al dificultar el acceso para los atacantes. Es esencial que estas políticas se apliquen de manera continua para proteger la información de los usuarios. El mantenimiento del firewall debe realizarse de manera regular. Es fundamental actualizar las reglas del firewall ante cualquier evento de seguridad, especialmente aquellos que permitan el tráfico sospechoso en la red, para proteger contra ataques DoS y DDoS.