Informe de evaluación de riesgos de seguridad

Parte 1: Selecciona hasta tres herramientas y métodos de reforzamiento a implementar

- Establecer una política de contraseñas
- Mantenimiento de cortafuego
- Autenticación de múltiples factores (MFA)

Parte 2: Explica tus recomendaciones

Política de contraseñas:

- **Salting y Hashing:** Implementar técnicas de salting y hashing para almacenar contraseñas. El salting añade un valor aleatorio a cada contraseña antes de ser hasheada, lo que protege contra ataques de fuerza bruta y diccionario. El hashing convierte las contraseñas en valores fijos de longitud que no pueden revertirse a su estado original, aumentando la seguridad.
- Desarrollar una política de contraseñas que establezcan unos requisitos mínimos de longitud, caracteres…
- **Prohibir el Uso de Contraseñas Predeterminadas:** Las contraseñas predeterminadas son conocidas y fácilmente explotables. Se debe requerir que todos los usuarios y administradores cambien las contraseñas predeterminadas al configurarlas por primera vez, asegurando que las nuevas contraseñas sean únicas y complejas.

Sistema de MFA,

Queremos también establecer un doble sistema, para ello cuando se introduzca se enviará un código al móvil.

Gestión del cortafuegos.

- **Establecimiento de Reglas de Cortafuegos:** Configurar reglas específicas en los firewalls para controlar el tráfico que entra y sale de la red. Esto incluye bloquear accesos no autorizados y permitir solo tráfico legítimo.

Actualización y Revisión Regular: Actualizar las reglas del cortafuegos semanalmente y aumentar la frecuencia de revisiones durante períodos de alta actividad. Esto asegura que las políticas de seguridad estén siempre alineadas con las amenazas actuales.