PRESENTACIÓN EJECUTIVA PARA LA GERENCIA

1. Introducción

Este informe ejecutivo presenta un resumen detallado de los problemas de seguridad detectados, las soluciones implementadas y las recomendaciones estratégicas para fortalecer la ciberseguridad de la organización.

2. Resumen del Incidente

- **Fecha de detección:** 08/10/2024
- **Sistemas afectados:** Servidor web, base de datos, acceso remoto.
- **Tipo de ataque:** Acceso no autorizado, explotación de vulnerabilidad en Apache, uso de credenciales débiles en MySQL.
- **Impacto:** Posible fuga de datos, alteración de archivos críticos y compromiso de usuarios.

3. Problemas Detectados

1. **Fallas en autenticación y control de accesos:**
    - Uso de credenciales débiles y sin autenticación multifactor.
    - Configuraciones permisivas en SSH y base de datos.
2. **Vulnerabilidades en servidores y aplicaciones:**
    - Falta de actualización en Apache y MySQL.
    - Configuraciones de seguridad inadecuadas.
3. **Monitoreo y respuesta a incidentes insuficientes:**
    - Falta de alertas tempranas y auditoría de eventos.

4. Soluciones Implementadas

1. **Mejora en autenticación y control de accesos:**
    - Implementación de autenticación multifactor.

    - Restricción de accesos y revisión de permisos.
2. **Fortalecimiento de seguridad en servidores y aplicaciones:**
    - Aplicación de parches y actualizaciones en Apache y MySQL.
    - Configuración de reglas estrictas en firewall y acceso remoto.
3. **Implementación de monitoreo y respuesta a incidentes:**
    - Configuración de herramientas de detección de intrusos (IDS/IPS).
    - Auditoría de eventos críticos y generación de alertas automáticas.

5. Recomendaciones Futuras

1. **Capacitación continua del personal en ciberseguridad.**
2. **Realización de auditorías de seguridad trimestrales.**
3. **Implementación de políticas de gestión de incidentes y copias de seguridad.**
4. **Evaluación periódica de nuevas amenazas y ajuste de controles de seguridad.**

6. Conclusión

Las acciones implementadas han reducido significativamente el riesgo de futuros incidentes. Sin embargo, se recomienda mantener un enfoque proactivo en ciberseguridad, con revisiones periódicas y mejoras continuas en la infraestructura de TI. La inversión en seguridad es clave para la resiliencia y protección de la información empresarial.