Análisis Comparativo ISO 31000

Respuestas

Tu Respuesta

Aplicación ISO 31000: 1. Identificación: Ciberataques, pérdida de datos, fallos de hardware/software, ausencia de personal clave. 2. Análisis: Ciberataques y pérdida de datos: alta probabilidad/alto impacto. Fallos técnicos y ausencias: menor probabilidad/impacto medio. 3. Evaluación: Priorización de ciberataques y pérdida de datos por su criticidad. 4. Tratamiento: Fortalecer ciberseguridad, respaldos regulares, plan de continuidad empresarial. La ISO 31000 proporciona el marco sistemático para este enfoque estructurado de gestión integral de riesgos.

Respuesta de la IA

Principales riesgos: Ciberataques, pérdida de datos, fallos de hardware/software, ausencia de personal clave. Impacto y probabilidad: Ciberataques y pérdida de datos son altamente probables e impactantes; fallos y ausencias son menos probables pero aún impactantes. Según ISO 31000, las recomendaciones incluyen fortalecer la seguridad cibernética, implementar respaldos de datos regulares y desarrollar un plan de continuidad de negocio. Plan de acción sugerido: Iniciar con la implementación de medidas de seguridad y respaldos, seguido de la elaboración del plan de continuidad.

Análisis Comparativo

★ Similitud: 90% ★

Patrones identificados

Ambas respuestas siguen la estructura de la norma ISO 31000: identificación, análisis, evaluación y tratamiento de riesgos.

Similitudes clave

Las dos respuestas identifican los mismos riesgos, asignan similar probabilidad e impacto a cada uno y proponen medidas de tratamiento equivalentes.

Diferencias significativas

La respuesta del usuario es más estructurada siguiendo los pasos de la ISO 31000 de forma numérica, mientras que la respuesta de la IA es más narrativa y menciona un plan de acción sugerido.

Evaluación de Confiabilidad

Ambas respuestas son confiables y alineadas con la ISO 31000, pero la del usuario muestra un entendimiento más claro de la estructura de la norma.