Análisis de Métodos de Evaluación de Riesgos (Enfoque México)

Introducción

El presente documento compara tres metodologías de análisis de riesgos ampliamente utilizadas y evalúa su aplicabilidad en México, considerando marcos regulatorios como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y las guías del INAI. Asimismo, se relacionan estas metodologías con normas mexicanas como la NMX-I-27001-NYCE-2015 y la NMX-CC-9001-IMNC-2015.

Tabla Comparativa de Métodos de Análisis de Riesgos

Método	Datos Generales (México)	Principios y Objetivos	Pasos de Implementación
FMEA	Aplicado en México principalmente en industrias automotriz, alimentaria, manufactura y sectores regulados por normas oficiales (NOM-251-SSA1-2009, NMX-CC-9001-IMNC-2015).	Identificar modos de falla, causas y efectos para prevenir riesgos operativos y de proceso.	1) Definir alcance. 2) Identificar componentes. 3) Identificar fallas. 4) Calificar severidad/ocurrencia/detección. 5) Calcular RPN. 6) Priorizar riesgos. 7) Implementar acciones.
ISO 31000	Reconocida en México por organismos públicos y privados. Compatible con LFPDPPP, LGPDPPSO, guías del INAI y normas mexicanas como NMX-I-27001-NYCE-2015.	Establecer un sistema de gestión integral del riesgo adaptable a cualquier organización.	1) Establecer contexto. 2) Comunicar. 3) Identificar riesgos. 4) Analizar. 5) Evaluar. 6) Tratar. 7) Monitorear. 8) Registrar.
OCTAVE Allegro	Recomendado por el INAI en México como método adecuado para análisis de riesgos relacionados con datos personales. Utilizado en dependencias públicas y sector educativo.	Evaluar riesgos que afectan activos de información desde un enfoque organizacional.	1) Criterios de medición. 2) Perfil de activos. 3) Identificar amenazas. 4) Mapear contenedores. 5) Escenarios. 6) Evaluar riesgos. 7) Mitigación. 8) Plan.

Conclusión

De las metodologías comparadas, ISO 31000 es la más útil y aplicable al contexto mexicano. Su compatibilidad con la LFPDPPP, la LGPDPPSO y las guías del INAI la convierte en la opción más sólida para organizaciones públicas y privadas. Además, su alineación con normas mexicanas como la NMX-I-27001-NYCE-2015 permite integrar la gestión del riesgo en sistemas de seguridad de la información y en modelos de gestión de calidad. Por su enfoque integral y adaptabilidad, ISO 31000 ofrece la mejor base para una estrategia formal de gestión de riesgos en México.

Referencias

Carnegie Mellon University, Software Engineering Institute. (2007). *OCTAVE® Allegro: Improving the Information Security Risk Assessment Process*. CERT.

Hassan Montero, Y., & Martín Fernández, F. J. (2003). *Guía de Evaluación Heurística de Sitios Web*. No Solo Usabilidad. Recuperado de http://www.nosolousabilidad.com/articulos/heuristica.htm

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2015). *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales*. INAI. Recuperado de http://transparencia.udg.mx/sites/default/files/Gu%C3%ADa%20para%20la%20implementaci%C3%B3n%20de%20un%20SGSDP.pdf