UNIVERSIDAD DE GUADALAJARA

Red Universitaria e Institución Benemérita de Jalisco

Asignatura: Gestión de Riesgos de Sistemas

Material de Apoyo

El análisis de riesgo y su importancia

Hoy en día, y desde hace ya un tiempo, las organizaciones dependen del uso de la tecnología en donde el activo vital es la información, el aseguramiento de dicha información y de los sistemas que la procesan es (o debería ser) un objetivo de primer nivel dentro de la organización, por ello, la evaluación y gestión de riesgos surge como prioridad dentro de las organizaciones.

El análisis de riesgos es un proceso iterativo debido a los cambios constantes en las condiciones dadas y a la mejora continua en las organizaciones.

La administración de los riesgos es un análisis sistemático, que permite planear, identificar, analizar, evaluar, tratar y monitorear los riesgos asociados con una actividad, función o proceso, para que la organización pueda reducir pérdidas y aumentar sus oportunidades.

Existen varios (y diversos) tipos de gestión de riesgos en el área de tecnologías de la información, los cuales abarcan desde el desarrollo mismo de software pasando por la información hasta el entorno físico (la infraestructura tecnológica) necesaria para llevar a cabo los procesos y ámbitos tecnológicos que hoy en día requieren las organizaciones para operar.

Existen varios modelos de gestión de riesgos: CRAMM, COBIT, EBIOS, ITIL V3, MAGERIT, OCTAVE, RISK IT, y algunas normas ISO enfocadas en dar soporte a los riesgos, tales como: ISO/IEC 27000, ISO/IEC 27005, ISO/IEC 31010, AS/NZS ISO 31000, BS 7799-3:2006 y UNE 71504:2008. Desde su aparición, las normas y los modelos de riesgo han venido evolucionando de acuerdo con la forma como se administra la información en las empresas, brindando el conocimiento que permite tomar decisiones para disminuir costos y aumentar la rentabilidad. A continuación, se explican las normas y marcos de referencia:

BS 7799-3

Es una norma publicada por el British Standard Institute. Proporciona una guía para soportar los requisitos establecidos por ISO/IEC 27001:2005 con respecto a todos los aspectos que debe cubrir el ciclo de análisis y gestión del riesgo en la construcción de un sistema de gestión de la seguridad de la información (SGSI). El objetivo de esta norma es dar efectiva seguridad de la información a través de un programa permanente de actividades de gestión de riesgos. Además, incluye la identificación y evaluación del riesgo, mediante la implementación de controles para su reducción, monitoreo y revisión, y el mantenimiento y la mejora continua del sistema basado en el control del riesgo (BSI, 2006).

CRAMM

Es una metodología de análisis de riesgos desarrollada en el Reino Unido por la agencia central de cómputo y telecomunicaciones (CCTA). La primera versión apareció en 1987 y aún está vigente la versión 5.1. Es el método de análisis de riesgos preferido en los organismos de la administración pública. Se compone de tres etapas, cada una apoyada por cuestionarios, objetivos y directrices. Las dos primeras se encargan de identificar y analizar los riesgos para el sistema, y la tercera recomienda la manera en que estos riesgos deben ser gestionados (Seguridad Informática, 2005).

COBIT 4.1

Es un marco de referencia internacional aceptado por la mayoría de las empresas como buenas prácticas para el control interno de la información. COBIT ha sido diseñado para facilitar el uso de las TI desde un enfoque de inversión que debe estar bien administrado y está basado en los estándares y las mejores prácticas de la industria, y ayuda a salvar la brecha entre los riesgos del negocio, las necesidades de control y los aspectos propiamente técnicos. COBIT provee de buenas prácticas, gracias a un marco de dominios: planificar y organizar; adquirir e implementar; entrega y soporte; y monitorear y evaluar (EAFIT, 2007).

ISO 27005

Esta norma proporciona directrices para la gestión de riesgos de seguridad de la información. Es compatible con los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de elementos que permitan garantizar la seguridad de la información basada en un enfoque de gestión de riesgos. Es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que podrían comprometer la seguridad de su información (ISO/IEC, 2011a).

ISO 31010

Es una norma publicada por la Organización Internacional de Normalización [ISO] y la Comisión Electrotécnica Internacional [IEC] enfocada en la gestión de riesgos. Su propósito es brindar información basada en pruebas y análisis para tomar decisiones sobre cómo seleccionar y determinar el tratamiento de los riesgos. El marco de gestión del riesgo de esta norma proporciona las políticas, los procedimientos y las disposiciones organizativas que integran la gestión de riesgos en toda la organización a todos los niveles. Como parte de este marco, la organización debe tener una política o estrategia para decidir cuándo y cómo los riesgos deben ser evaluados (ISO/IEC, 2011b).

ITIL v3

Fue desarrollada al reconocer que las organizaciones dependen cada vez más de la informática para alcanzar sus objetivos corporativos, lo que ha dado como resultado la creciente necesidad de servicios informáticos de calidad que correspondan a los objetivos del negocio y que satisfagan los requisitos y las expectativas del cliente. A través de

los años, el énfasis pasó de estar en el desarrollo de las aplicaciones TI a la gestión de servicios TI. La aplicación TI sólo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones (Axwloa, 2011).

MAGERIT

Es un método formal para investigar los riesgos que soportan los sistemas de información. Es una norma establecida por el Gobierno español con el fin de brindar una metodología de sistemas de información de riesgos en su análisis y gestión. El propósito de MAGERIT está relacionado con el uso de medios electrónicos, informáticos y tecnológicos, sujetos a ciertos riesgos que se deben minimizar con medidas de seguridad, para mitigar la desconfianza en el uso de estos medios. Su utilización está enfocada en las personas que utilizan los sistemas de información y sobre los riesgos y vulnerabilidades a que está expuesta la información (MHAP, 2012).

OCTAVE

Es una técnica efectiva de evaluación de riesgos desarrollada en el Centro de Coordinación CERT en Carnegie Mellon University. Octave es un conjunto de herramientas, técnicas y métodos para la evaluación del riesgo. Tiene en cuenta también la definición de los activos incluyendo: personas, hardware, software, información y sistemas. Hay tres componentes que conforman la base de su cuerpo de conocimiento:

Octave, en su metodología original, definida para las grandes empresas, que describe conjuntos de criterios (i.e., principios, atributos y resultados);

Octave-S, similar a la original, pero dirigido a empresas con garantía limitada; y Octave Allegro, un enfoque simplificado para la evaluación de la información de seguridad y garantía (CERT, 2008).

Octave proporciona una línea base que se puede utilizar para enfocar la mitigación y mejorar de actividades; asimismo, equilibra los riesgos operativos, las prácticas de seguridad y la tecnología, lo cual permite tomar decisiones de protección de información con base en los riesgos de confidencialidad, integridad y disponibilidad de los bienes relacionados con la información crítica (CERT, 2008).

Existen varios criterios de Octave que definen un conjunto de enfoques para la evaluación de los riesgos en una organización, en la seguridad de la información, utilizando un conjunto de principios, atributos y salidas (CERT, 2008).

RISK IT

Es un marco de trabajo a nivel mundial enfocado a las TI y publicado por ISACA. RISK IT proporciona una visión global sobre los riesgos empresariales asociados con todas las actividades relacionadas con TI. RISK IT pretende ser una herramienta práctica para la gestión de riesgos basada en los conceptos de valor y beneficios que la

organización obtiene a través de sus iniciativas de TI. Al igual que COBIT, RISK IT se concentra en el cumplimiento de los objetivos de la organización. Este modelo puede personalizarse para cualquier tipo de empresa en cualquier ubicación geográfica. RISK IT se define como una serie de guías para la gestión eficaz de los riesgos de TI. Dichas guías se basan en los principios comúnmente aceptados en ERM, que se han aplicado en el ámbito de las TI. El modelo del proceso de los riesgos de TI está diseñado y estructurado para que las organizaciones puedan poner los principios en práctica y comparar sus resultados (ISACA, 2013).

UNE 71504

Es una norma realizada por la Asociación Española de Normalización y Certificación [AENOR], orientada al análisis y la gestión de riesgos para los sistemas de información. Esta norma define la gestión de riesgos con base en las siguientes fases principales: caracterización de activos, caracterización de las amenazas, cálculo del riesgo intrínseco, caracterización de las salvaguardas, cálculo del riesgo efectivo, evaluación de riesgos, tratamiento de riesgos, y administración de la gestión de los riesgos (Agendum, 2007).

Modelo	Organización	Publicación	Actualización	País	Estructura
AS/NZS ISO31000	ISO	2004	2009	Australia Nueva Zelanda	11 principios / 5 procesos
BS 77993	BSI	2006	-	Reino unido	6 procesos
COBIT	CCTA	2003	-	Reino unido	5 principios / 37 procesos
CRAMM	ISACA	2008	2012	Estados Unidos	3 Fases
EBIOS	ANSSI	2002	2010	Francia	5 Fases
ISO/IEC 27005	ISO	2008	-	Suiza	6 Procesos
ISO/IEC 31010	ISO	2009	-	Suiza	4 principios / 5 procesos
ITIL	ITIL	2001	2011	Suiza	5 principios
MAGERIT	Gobierno de España	2006	2012	España	Vol. 1, Método / Vol.2, Catálogo / Vol. 3 Guía
OCTAVE	SEI	2001	2007	Estados Unidos	Octave: 3 fases / Octave s: 3 fases / Octave allegro: 4 fases
RISK IT	ISACA	2009	2011	Estados Unidos	3 Principios
UNE 71504	AENOR	2008	-	España	4 Fases

Bibliografía

Ramírez Castro, Alexandra, & Ortiz Bayona, Zulima (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería*, *16*(2),56-66.[fecha de Consulta 2 de Febrero de 2022]. ISSN: 0121-750X. Disponible en: https://www.redalyc.org/articulo.oa?id=498850173005

Sánchez Peña, Juan José, & Fernández Vicente, Eugenio, & Moratilla Ocaña, Antonio (2013). ITIL, COBIT and EFQM: Can They Work Together?. *International Journal of Combinatorial Optimization Problems and Informatics*, *4*(1),54-64.[fecha de Consulta 2 de Febrero de 2022]. ISSN: . Disponible en: https://www.redalyc.org/articulo.oa?id=265225625006

Velásquez Pérez, Torcoroma, & Puentes Velásquez, Andrés Mauricio, & Pérez Pérez, Yesica María (2015). Un enfoque de buenas prácticas de gobierno corporativo de TI. *Tecnura*, *19*,159-169.[fecha de Consulta 2 de Febrero de 2022]. ISSN: 0123-921X. Disponible en: https://www.redalyc.org/articulo.oa?id=257059815014