|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Características | Principios de Riesgo | Etapas/  Fases/  Pasos | Propósitos | Componentes | Objetivos | Roles |
| Magerit | Clasifica los riesgos según su impacto y probabilidad.  Clasifica el impacto según su naturaleza.  Analiza los activos en la organización con la intención de conocer las amenazas a las que están expuestos.  Ofrece tres clasificaciones de posibles salvaguardas/métodos de protección.  Cuantifica la probabilidad de riesgo y del impacto del mismo después de ser tratado. | Las amenazas soportadas por la metodología:  Origen Natural  Origen Industrial  Defectos  Aplicaciones Informáticas  Recurso  Humano no cualificado  Amenazas mal Intencionadas | Revisión de Activos  Amenazas    Determinación del impacto Potencial  Determinación del Riesgo Potencial  Las salvaguardas/ Métodos de Protección  El impacto Residual  El Riesgo residual | Es gestionar los riesgos en un orden de impacto y probabilidad de que se materialicen, para mantener un sistema optimo | Los componentes pueden ser definido como los tipos de protección:  Los preventivos  Las acciones de degradación  Los que influyen socialmente | Mitigar el impacto de los riesgos sobre los activos de la organización  Llevar un control sobre los activos para priorizar las amenazas identificadas en los mismo.  Prevenir la materialización de los riesgos identificados en los activos | --- |
| MEHARY | Implementa Herramientas Consistentes.  Posee una base de conocimiento que sustenta su análisis de los riesgos.  Maneja los riesgos de forma cuantitativa y cualitativa  Se enfoca en los activos de la seguridad de la información. | Este solo maneja riesgos que se pueden clasificar de manera cuantitativa y cualitativa. | Análisis y Evaluación de Riesgos  Análisis Sistemático de Evaluación de riesgo  Evaluación Seguridad  Análisis de Amenazas | Análisis y clasificación de amenazas  Evaluación de servicios  Análisis de riesgo | Esta está compuesta por:  Base de datos de conocimiento relacionado de situaciones de riesgo. Con el fin de facilitar el análisis de estas.  Herramientas consistentes, definidos como resultados reutilizables por otra herramienta u otro lugar del proceso. | Gestión de los activos de la seguridad de la información |  |
| CMMI | Se organiza en modelos CMMI  Maneja metas y prácticas para la obtención de estas  Clasifica los componentes en requeridos, Esperados e Informativos  Contempla 16 áreas de procesos en la que se puede presentar los modelos o marcos. | Estos se contemplan como incidentes en los servicios. | Capacitación, Disponibilidad y continuidad del servicio  Presentación del servicio  Prevención de Incidentes  Transición de servicio  Desarrollo del sistema del servicio | Es gestionar los servicios por medio de actividades para garantizar la correcta ´prestación del mismo | Este compuesto por un modelo de CMMI el cual contiene Marcos de CMMI conformados por metas y prácticas.  Las metas y practicas están clasificadas en 16 áreas de procesos y pueden clasificarse a su vez como requeridos , esperados o informativos. | Organizar y estructurar los servicios de tal forma que se garantice el buen funcionamiento de los mismos.  Analizar los incidentes que se pueden llegar a dar en los servicios prestados o presentes en la organización. |  |
| PRINCE2 | Es una metodología sencilla y con pasos reducidos.  Los involucrados son pocos, lo que proporciona mejor entendimiento y comunicación dentro del proyecto.  Permite un trato personal con los evaluadores del proyecto y distintas oportunidades para evaluar el mismo. | Los riesgos en la metodología de proyecto son la denegación de avanzar a la siguiente fase lo que traería consigo retraso y acciones contraproducentes al flujo normal del proyecto. A lo cual este debe estar preparado con acciones que se deben planear al principio del mismo. | Mandato de proyecto  Inicio de Proyecto  Ejecución (Control de fase/ Gestión de entrega de productos / Gestión de límites de cada fase)  Cierre de Proyecto | Es dar un orden a un proyecto para poder ejecutarlo de manera precisa y con una finalidad clara. | Los componentes son los entregables y diferentes documentos de control como revisiones o autorizaciones | Organizar y controlar la ejecución un proyecto siguiendo unas fases que permitan el análisis del mismo durante todo el proceso desde diferentes perspectivas para darle una correcta continuidad al mismo | Dirección de proyecto  Junta Proyecto  Equipo de trabajo |
| COBRA | Metodología que analiza los riesgos involucrando a todos los participantes dentro del riesgos.  Cuenta con un sistema de cuestionarios basado en usuarios expertos y una amplia base de conocimientos. | Mas conocidas como consecuencias se pueden clasificar en:  Perdida de cliente  Perdida financiera  Pérdidas económicas | Diseño  Desarrollo  Pruebas de Aceptación  Pruebas de Practicas/Solución  Reportes | Gestionar los riesgos, identificándolos por medio de cuestionarios, para posteriormente vincularles consecuencias. Con las cuales se justificará las soluciones de la mano con la base de conocimiento. | Maneja evaluaciones escritas en forma de informes para categorizar los riesgos  Maneja cuestionarios personalizados para la identificación de las amenazas  Maneja una base de conocimiento para sustentar sus recomendaciones | Generar una evaluación de las amenazas y vulnerabilidad para clasificar su importancia  Generar recomendaciones y soluciones adecuadas según la evaluación |  |
| GRAMM | Metodología de analizar riesgos basada en bases de conocimientos.  Basado en 400 tipos de activos, 25 tipos de impacto, 38 tipos de amenazas y 3500 salvaguardas | Clasifica los riesgos según el activo que afecta, ya sea físico o de software  Los riesgos pueden ser clasificados según su tipo nivel de amenaza | Establecimiento de objetivos de seguridad  Evaluación de riesgos  Identificación y selección de contramedidas | Manejar, identificar y monitorear las amenazas para mitigar el impacto de las mismas en la organización | Documento inicio de proyecto  Informe de análisis de riesgo  Informe de gestión de riesgo  Plan de implementación | Clasificar la medida de riesgo con las vulnerabilidades e impactos asociados a una amenaza.  Dar distintos salvaguardas a las diferentes amenazas que se presenten para otorgar mas de una opción para ser tratadas |  |
| OCTAVE | Modelo para creación de metodologías de análisis de riesgo  Es auto dirigido en cuanto a la implementación de los controles  Posee medidas adaptables a las necesidades.  Contempla un proceso continuo, definido y centrado en reducir el número de riesgos críticos | Este los clasifica según si son críticos o no, lo que le permite saber en qué medida hay que mitigarlos. | Visión Organizativa  Visión tecnológica  Estrategia y desarrollo de plan | Mitigar los riesgos a los activos críticos para garantizar sus funciones vitales y por consecuencia lo que depende de ellos. | Riesgos sobre activos críticos  Medidas contra los riesgos  Estrategias de Protección  Planes de mitigación de riegos  Vulnerabilidades  Componentes clave  Activos críticos | Clasificar los riesgos para mitigarlos.  Determinar estrategias para mitigar los riesgos  Ofrecer una visión tecnológica y organizativa de la manera de como mitigar los riesgos |  |
| NIST SP 800-30 | Gestiona los riesgos expresándolos de forma cuantitativa y cualitativa.  Los controles están orientados a preservar la rentabilidad de la organización  Tiene énfasis en asegurar el buen funcionamiento de los sistemas de información | Este maneja los riesgos con el fin de proveer información para los controles que deben cumplir con el parámetro de rentabilidad para la organización. | Esta se separa en dos grandes etapas: ANALISIS y GESTION.  Por un lado, análisis contienen 9 pasos internos que se ejecutan en paralelo a los 7 procesos internos de Gestión. | Administrar los riesgos para dar seguridad a la información | Evaluar  Monitorear  Responder  Marco | Asegurar que los sistemas de información almacenan , procesen y transmitan información  Gestionar los riesgos  Optimizar la gestión de riesgos en base a los resultados de analizar los riesgos |  |
| NTC 5254 | Norma para gestionar los riesgos.  Posee una guía genérica para el establecimiento e implementación de procesos de administración de riesgos  Plantea una gestión proactiva y no reactiva  Mejora conformidad con la legislación pertinente  Mejora la gestión de incidentes y reduce las perdidas y coste de los riesgos. |  | Establecimiento de contexto  Identificar Riesgos  Analizar riesgos  Evaluar riesgos  Tratar riesgos  Monitorear y revisar  Comunicar y Consultar | Reducir las pérdidas y coste de los riesgos de los activos por medio de un planteamiento proactivo a los salvaguardas de las amenazas detectados en el análisis de riesgos | Evaluación  Tratamiento  Monitoreo  Revisión de registros | Cumplir con la legislación pertinente en paralelo al mejoramiento de tratamiento de riesgos  Plantear una gestión proactiva  Reducir los costos de los riesgos |  |
| NTC-IEC / ISO 31010 |  | Los riesgos se pueden clasificar en tolerables y no aceptables.  La anterior clasificación se ayuda de dos parámetros el tipo y la extensión del riesgo. | Generalidades  Comunicación y consulta  Establecimiento de contexto  Valoración de riesgo  Tratamiento de riegos  Monitoreo y revisión | Suministrar Información y análisis de los riesgos. Con el fin de tomar decisiones. | Está compuesto por técnicas, riesgos, de la organización, procesos de la organización, rendimiento de cuentas y recursos disponibles. | Entender el riesgo y su impacto potencial en los objetivos de la organización  Comunicar riesgos e incertidumbres  Brindar información para aquellos que toman las decisiones |  |

Tabla de Metodologías

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | CARACTERISTICAS | Principios de riesgo | Etapas/Fases/Pasos | Propósito | Componentes | Objetivos | Roles |
| 38500 | Otorga conformidad con a organización  Mejora el desempeño de la organización  Permite evaluar , dirigir y monitorear el uso de TI en la organización | Los riesgos implicados, son aquello que afectan al tema de TI en la organización y por ende las funciones del mismo. | Evaluar  Dirigir  Monitorear | Fomentar el uso eficaz e eficiente y aceptable de la tecnología de la información. | Responsabilidad  Estrategia  Adquisición  Desempeño  Conformidad  Comportamiento Humano | Asegurar a las partes interesadas, dándoles confianza sobre la organización en aspectos de TI.  Informar y orientar a los directores sobre el gobierno del uso de TI | Altos directivos  Miembros de Grupos que monitorean  Distribuidores de software |
| COSO | Permite organizar la estructura de control interno en la organización.  Permite definir el concepto de control interno | El riesgo que contempla es el que puede llegar a afectar el proceso bajo el que trabaja el control interno | Ejecución  Estructura conceptual  Reportes  Herramientas para evaluación | Garantizar la eficiencia y eficacia de las operaciones | Ambiente de Control  Evaluación del riesgo  Actividades de control  Información  Comunicación  Supervisión de riesgo | Garantizar la confiabilidad de la información  Garantizar el cumplimiento de las leyes  Ofrecer reportes de lo que se debe realizar para el buen funcionamiento de un control interno |  |
| ITIL | Permite diseñar el de acción para desarrollar estrategias de servicios  Permite llevar trazabilidad en el ciclo de vida del servicio | Este contempla riesgos que afecten la estabilidad de los servicios, y como reestablecer en caso de que se llegan a materializar los riesgos. | Diseño de servicios  Operación de Servicios  Mejora continua de servicios  Transición de servicios | Gestionar de manera integral los servicios de TI dentro de la organización | Las diferentes partes de un servicio:  Arquitectura  Procesos  Políticas  Documentación  Capacitaciones  Continuidad | Diseñar un servicio optimizado para la organización  Garantizar la operación continua del servicio  Planear la transición a nuevos servicios. |  |
| RISK IT | Permite controlar los riesgos de manera coherente con una política de coste beneficio  Permite evaluar los riegos desde un gobierno de riesgo en donde el proceso es transparente  Permite clasificar los riesgos para ser tratados según la necesidad | Riesgos organizacionales los cuales se dividen en:  Riesgos Estratégicos  Riesgos Ambientales  Riesgos de mercado  Riesgos de crédito  Riesgos Operacionales  Riesgos de Cumplimiento | Gobierno de riesgos  Evaluación de riesgos  Respuesta de riesgos | Establecer prácticas de gestión de riesgo con el fin de implementar un marco que permita identificar, gobernar, administrar los riesgos asociados a su negocio. | Conectar a objetivos de negocio  Alinear gestión de riego con ERM  Equilibrar costo-beneficio  Promocionar participación y la comunicación  Establecer oportunidades  Funcionar como parte de las actividades diarias | Garantizar el manejo de riesgos de manera sustentada.  Equilibrar los costos de solución de riesgos con los beneficios que traerá tratar los mismos.  Alinea el control de riesgos con los objetivos de la organización | CONSEJO  CEO  CRO  CIO  CFO  Comité de organizaciones riesgos  Gestión de organización  RH |
| TOGAF | Identifica estrategias para el compromiso y participación de las distintas partes  Permite monitoreas y gestionar los procesos de información | Los riesgos a los que responde son lo que afecten los recursos de la organización | Implementación  Diseño  Estrategia  Monitoreo | Establecer una estrategia para utilizar los recursos de manera correcta | Bucket  Method  OUTPUT | Garantizar la confiabilidad de la información referente a los recursos dentro de la organización  Garantizar la trazabilidad de la información referente a los recursos |  |

Tabla de Marcos

# REFERENCIAS

## Magerit

- https://www.youtube.com/watch?v=J3fkKBfx-VE

## 31010

- ISO 31010.pdf

- NTC-IEC-ISO31010.pdf

## CMMI

- 2010\_019\_001\_28782.pdf

- CMMI\_for\_Services\_v1-3\_Spanish.pdf

## Cobra

- 00000744.pdf

## MEHARI

- MEHARI-2010-IntroduccionESP.pdf

## NIST SP 800-30

- 3. Trabajo de Titulación.pdf

-https://www.goconqr.com/mindmap/3511863/metodolog-a-de-gesti-n-de-riesgo-nist-800-30

## NTC 5254

- Norma Técnica NTC 5254.pdf

## PRINCE2

- PRINCE2.pdf

- <https://www.youtube.com/watch?v=QfpC-Iu8oNY>

## 31500

- NTC-ISO-IEC38500.pdf

- d15fa899df64c1e34d6c1623d10009abee73.pdf

- 20091126 Introducción ISO38500.pdf

## COSO

- normas\_ctrl\_interno.pdf

- COSO-Sesion1.pdf

## ITIL

- GSDE01.pdf

- itil\_MALC\_manual\_alumno\_nov12.pdf

## RISK IT

- Risk-IT-Framework\_fmk\_Spa\_0610.pdf

- Risk-IT-Framework-Excerpt\_fmk\_Eng\_0109.pdf

## TOGAF

- togaf-version9.pdf

- https://www.slideshare.net/netmindit/introduccin-a-togaf-para-el-desarrollo-de-enterprise-architecture