# METODOLOGIÁS DE GESTION DE RIESGO

**PABLO ANDRÉS BRICEÑO**

**briceandres02@gmail.com**

**TRABAJO DE CONSULTA**

**CORPORACÓN UNIVERSITARIA AUTÓNOMA DE NARIÑO**

**INGENIERÍA INFORMÁTICA**

**PASTO 2020**

# METODOLOGÍAS DE GESTIÓN DEL RIESGO

La correcta gestión de una empresa conlleva el contar con una metodología que le ayude a asumir los riesgos que esta tiene día a día, y que lleve a alcanzar los objetivos estratégicos que dicha empresa haya plantado [1].

**Metodología Octave.**

Es un modelo para la creacion de metodologías de análisis de riesgos el cual fue desarrollado por la Universidad de Carnegie Mellon. Sus acrónimos en ingles significan "**O**perationally **C**ritical **T**hreat, **A**sset and **V**ulnerability **E**valuation", estudia los riesgos en base a tres principios los cuales son: Confidencialidad, Integridad y Disponibilidad, esta metodología es empleada por varias agencias gubernamentales como el Departamento de Defensa de Estados Unidos [2].

Octave es auto – dirigido, lo que quiere decir que el personal es el responsable de llevar a cabo su implementación dentro de la organización. La técnica aprovecha el conocimiento de los relacionados con los procesos para terminar el estado de seguridad actual dentro de la organización [3].

Tiene 3 variantes las cuales son:

- **Octave:** Metodología original, definida para grandes organizaciones.
- **Octave-s:** Metodología definida para pequeñas organizaciones.
- **Octave Allegro:** Metodología definida para analizar riesgos con un mayor enfoque en los activos de información, en oposición a enfoque en los recursos de información [2], [3].

Cuanta con 3 fases durante el proceso del desarrollo de la metodología:

- **Fase 1,** esta contempla la organización, se construyen los perfiles activo-amenaza, recogiendo los principales activos, así como las amenazas y requisitos como imperativos legales que puede afectar a los activos, las medidas de seguridad implantadas en los activos y las debilidades organizativas.
- **Fase 2,** se identifican las vulnerabilidades a nivel de infraestructura de TI.
- **Fase 3,** se desarrolla un plan y una estrategia de seguridad, siendo analizados los riesgos en esta fase en base al impacto que puede tener en la misión de la organización [2].

Los criterios que forman el núcleo de Octave son los siguientes:

- Auto-dirigida:
    - Equipo de análisis.

    - Capacidades del equipo de análisis.
- Medidas adaptables a las necesidades:
    - Catálogo de prácticas.
    - Perfil genérico de amenazas.
    - Catálogo de vulnerabilidades.
- El proceso debe ser definido:
    - Actividades de evaluación definidas.
    - Documentación de los resultados de evaluación.
    - Alcance de la evaluación.
- El proceso debe ser continuo:
    - Próximos pasos.
    - Catálogo de prácticas.
- El proceso debe seguirse con visión de futuro:
    - Enfoque en riesgos.
- El proceso debe centrarse en un reducido número de riesgos críticos:
    - Alcance de la evaluación.
    - Actividades enfocadas.
- Gestión integrada:
    - Aspectos organizativos y tecnológicos.
    - Participación de negocio y de áreas tecnológicas.
    - Participación de la alta dirección.
- Comunicación abierta:
    - Enfoque colaborativo.
- Perspectiva global:
    - Aspectos organizativos y tecnológicos.
    - Participación de negocio y de áreas tecnológicas.
- Equipo de trabajo:
    - Equipo de análisis.
    - Capacidades del equipo de análisis.
    - Participación de negocio y de áreas tecnológicas.
    - Enfoque colaborativo.

**Metodología NIST 800 – 30**

Sus siglas en ingles significan “**N**ational **I**nstitute of **S**tandards and **T**echnology”, es una guía de gestión de riesgo para sistemas de tecnología de información. Esta guía propone un conjunto de recomendaciones y actividades para una adecuada gestión de riesgos como parte de la gestión de la seguridad de la información. Se necesita del apoyo de toda la organización para que se cumplan los objetivos y el alcance de la gestión de riesgos se concluya con éxito [4].

Esta metodología está compuesta por cuatro pasos básicos los cuales son:

- **Preparación para la evaluación.** Las actividades claves para este paso son: la identificación del propósito y el alcance de la evaluación de riesgos, identificar suposiciones y limitaciones bajo las cuales se realiza la evaluación del riesgo, identificar las fuentes de información sobre amenazas, vulnerabilidades e impactos en la evaluación de riesgos.
- **Evaluación de la conducta.** En este paso se realizan las siguientes tareas: identificar amenazas relevantes para la organización, identificar vulnerabilidades dentro de la organización que pueden ser explotadas por fuentes de amenazas, determinar la probabilidad de que las fuentes de amenazas identificadas inicien eventos de amenaza específicos y la probabilidad de que los eventos de amenaza sean exitosos, determinar los impactos adversos a las operaciones de la organización y activos y determinar los riesgos para la seguridad de la información como una combinación de la probabilidad de una amenaza de explotación de vulnerabilidades y el impacto de dicha explotación.
- **Comunicar resultados.** En este paso, las actividades claves son: determinar el método apropiado para comunicar a las partes interesadas los riesgos tal como un informe de resultados basándose en las políticas de la organización.
- **Mantener la evaluación.** Las tareas a realizar en este paso son: determinar los factores de riesgo clave que se han identificado para el monitoreo continuo, su frecuencia y las circunstancias bajo las cuales se necesita actualizar la evaluación de riesgo, llevar a cabo tareas de evaluación según sea necesario y comunicar los resultados de la evaluación de riesgos posteriores al personal de la organización.

Se destaca por la gestión de riesgos en proyectos de TI y alcanza niveles satisfactorios en hardware, software, bases de datos, redes y telecomunicaciones, pues en su estructura se establecen criterios de seguridad, siendo los más comunes, la confidencialidad, integridad y disponibilidad, los cuales son la base para realizar el análisis y valorar la materialización de amenazas e impactos sobre los elementos de TI. No obstante, al ser una metodología tan robusta, esta propiedad se convierte en una limitante para su aplicación en pequeñas empresas con altas limitaciones de recursos humanos.

## REFERENCIAS BIBLIOGRAFICAS


[1] EALDE, «Metodologías en Gestión de Riesgos», *EALDE Business School*, jul. 19, 2016. https://www.ealde.es/metodologias-gestion-riesgos/ (accedido mar. 29, 2020).

[2] A. Huerta, «Introducción al análisis de riesgos – Metodologías (II)», *Security Art Work*, abr. 02, 2012. https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-–-metodologias-ii/ (accedido mar. 29, 2020).

[3] J. N. R. Pinzon, «METODOLOGÍA PARA IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS Y SALVAGUARDAS EN UNA MESA DE AYUDA TECNOLÓGICA», p. 80.

[4] «Vista de Metodologías para el análisis de riesgos en los sgsi | Publicaciones e Investigación». https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874 (accedido mar. 29, 2020).