agesic

Estudio comparado de metodologías de análisis de riesgos para TI y Seguridad de la Información

Autor: Seguridad de la Información

Versión: 01

Año: 2021

Uruguay Presidencia

Resumen

Este documento presenta un análisis de las metodologías más relevantes de gestión de riesgos de Tecnologías de la Información (TI) y de Seguridad de la Información (SI), con el fin de ayudar a organizaciones de porte medio, a elegir la metodología o combinación de ellas que entienda adecuada para la gestión de sus riesgos. Entre los aspectos priorizados en este análisis, se destacan que la metodología se pueda aplicar de forma autodirigida y que pueda ser llevada a cabo por personas con distinto nivel de experiencia previa.

Palabras claves: análisis de riesgos, evaluación de riesgos, gestión de riesgos, ciberseguridad, metodología, método, Seguridad de la Información.

Introducción

La Seguridad de la Información es fundamental para mantener la confidencialidad, la disponibilidad e integridad de datos de una organización. Adoptar una metodología que ayude a formalizar un proceso continuo dentro de la organización, permitiendo identificar los riesgos a los que se puede exponer, e identificar las medidas que se deben adoptar para evitar su aparición o la mitigación del impacto, es un camino necesario para establecer ecosistemas cada vez más confiables y seguros.

La gestión de riesgos de SI puede ser parte del proceso de gestión de riesgos más amplio de una organización o puede llevarse a cabo por separado. En general, es un proceso sistemático que apunta a mantener el equilibrio entre el costo y los beneficios de la implementación de los controles para minimizar las vulnerabilidades y pérdidas, con el fin de proteger los objetivos de negocio.

En la medida que la TI en general y la SI en particular incorpora cada vez más tecnología a los procesos de negocio, se recomienda que la gestión de riesgos de SI se establezca como un proceso sistemático dentro de la organización.

Objetivo

El objetivo de este documento es presentar el análisis realizado de marcos y metodologías para la gestión de riesgos de TI y SI, con el fin de que las organizaciones, que requieran gestionar sus riesgos de tecnología, puedan seleccionar una metodología (o combinación de ellas) y aplicarla de forma ágil, simple y auto dirigida por personas con diferentes niveles de experiencia.

Principales desafíos

El propósito de la gestión de riesgos es la creación y la protección del valor, que contribuye a mejorar el desempeño, fomentar la innovación y contribuir al logro de objetivos de las organizaciones.

Los principales desafíos identificados vinculados a la gestión de riesgos son [1]:

- Baja conciencia de las actividades de gestión de riesgos dentro de las organizaciones del sector público y privado.
- Ausencia de un “lenguaje común” en el área de gestión de riesgos para facilitar la comunicación entre las partes interesadas.
- Falta de estudios sobre métodos, herramientas y buenas prácticas existentes.
- Problemas de interoperabilidad de los métodos y la integración con la estrategia de la organización.

Metodologías analizadas

En este capítulo se presenta una breve descripción de las metodologías analizadas. Se pueden distinguir:

- Estándares: que brindan pautas de alto nivel para los procesos de gestión de riesgos como ISO 31000, 27005; COBIT, NIST: SP 800-37, SP 800-30 y SP 800-39; OCTAVE: OCTAVE S, Allegro y FORTE.
- Metodologías más estructuradas que siguen fases o pasos específicos para implementar procesos de Gestión de Riesgos como MAGERIT, EBIOS, CORAS, etc.

1. ISO 31000:2018[2] - Gestión de riesgos – Directrices

Se presenta en esta guía varios principios que deberían considerarse al establecer un marco de referencia y procesos para la gestión de riesgos en una organización.

El desarrollo de un marco de referencia implica integrar, diseñar, implementar, valorar y mejorar la gestión de riesgos a lo largo de toda la organización, y permitirá que pueda aplicarse en todas sus actividades.

2. ISO/IEC 31010:2019 [3] - Gestión de riesgos: Técnicas de evaluación de riesgos

Esta guía proporciona información resumida de diferentes técnicas y referencias a otros documentos en los cuales se describen con más detalle, que pueden utilizarse en la evaluación de riesgos en una amplia gama de situaciones.

Está dirigida a las organizaciones que deben realizar evaluaciones de riesgos con fines de cumplimiento o conformidad, y se beneficiarían del uso de técnicas formales y normalizadas.

3. ISO/IEC 27005:2018 [4] - Tecnología de la Información. Técnicas de seguridad. Gestión del riesgo de Seguridad de la Información

Esta Norma Internacional, aplicable a todo tipo de organizaciones, proporciona pautas para la gestión de riesgos de seguridad de la información. Respalda los conceptos generales especificados en ISO/IEC 27001 y está diseñada para ayudar a la implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

El proceso de gestión de riesgos de Seguridad de la Información presentado en esta guía consiste en el establecimiento del contexto, la evaluación, el tratamiento, la aceptación, la comunicación y consulta del riesgo, seguimiento, revisión y mejora de la gestión del riesgo.

Un enfoque iterativo para realizar una evaluación de riesgos puede aumentar la profundidad y el detalle de la evaluación en cada iteración. El enfoque iterativo proporciona un buen equilibrio entre minimizar el tiempo y el esfuerzo dedicado a identificar los controles, al tiempo que garantiza que los altos riesgos se evalúen adecuadamente.

4. COBIT 5 for Risk

Cobit 5 for Risk se basa en el marco Cobit 5 con una orientación más detallada y práctica para el tratamiento de los riesgos.

Cobit 5 proporciona un marco integral, que ayuda a alcanzar los objetivos para el gobierno corporativo de las TI, al mantener un equilibrio entre la obtención de beneficios y la optimización de los riesgos y el uso de los recursos.

Presenta dos perspectivas sobre cómo usar Cobit 5 en un contexto de riesgo: función de riesgo y gestión de riesgo.

La primera se centra en lo que se necesita para construir y mantener la función de riesgo dentro de la empresa. La segunda tiene que ver con los procesos centrales de gobierno y gestión de riesgos sobre cómo optimizar el riesgo y cómo identificar, analizar, responder e informar sobre el riesgo a diario.

5. National Institute of Standard Technology Publicaciones especiales de la serie 800: 800-37 Rev 2[5], 800-39[6] y 800-30 Rev 1[7].

Guía 800-37 Risk Management Framework for Information Systems and Organizations., presenta al marco de gestión de riesgos como un proceso con 7 pasos:

- Prepararse para ejecutar el RMF
- Categorizar el sistema y la información procesada, almacenada y transmitida
- Seleccionar un conjunto inicial de controles para el sistema
- Implementar los controles
- Evaluar los controles para determinar si los controles se implementan correctamente
- Autorizar el sistema o controles comunes con base en la determinación de que el riesgo es aceptable
- Monitorear el sistema y los controles asociados de manera continua

Guía 800-39 Managing Information Security Risk Organization, Mission, and Information System View, plantea que la gestión de riesgos es una actividad holística, de toda la organización, abordado desde el nivel estratégico hasta el nivel táctico, con el objetivo de que la toma de decisiones basada en el riesgo se integre en todos los aspectos de la organización.

Guía 800-30 Guide for Conducting Risk Assessments, proporciona orientación para realizar evaluaciones de riesgos de sistemas y organizaciones, ampliando la orientación en la Publicación Especial 800-39.

Describe el proceso de evaluación del riesgo de seguridad de la información y las actividades necesarias para:

- prepararse para una evaluación de riesgos;
- realizar una evaluación de riesgos;
- comunicar los resultados de la evaluación de riesgos y compartir información relacionada con los riesgos en toda la organización; y
- mantener los resultados de una evaluación de riesgos.

Otras publicaciones que complementan este punto:

- 800-53- Recommended Security Controls for Federal Information Systems and Organizations.

- 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations.

Los conceptos y principios contenidos en publicaciones del NIST implementan un sistema de gestión de Seguridad de la Información y un proceso de gestión de riesgos armonizados con las normas ISO/IEC 31000, ISO/IEC 31010, ISO/IEC 27001, y ISO/IEC 27005 mencionadas anteriormente.

6. OCTAVE [8] - Operational Critical Threat, Asset and Vulnerability Evaluation en sus tres versiones, OCTAVE S, Allegro y FORTE.

Es un marco para identificar y gestionar los riesgos de Seguridad de la Información, permite una evaluación estratégica basada en riesgos y una técnica de planificación para la seguridad. El enfoque se concentra en los activos, las amenazas y las vulnerabilidades.

OCTAVE es autodirigido, la técnica aprovecha el conocimiento de las personas sobre las prácticas y procesos relacionados con la seguridad en la organización para capturar el estado actual de las prácticas de seguridad en la misma. Los riesgos para los activos más críticos se utilizan para priorizar áreas de mejora y establecer la estrategia de seguridad para la organización.

A diferencia de la evaluación de otras metodologías centradas en la tecnología, que se enfocan en el riesgo tecnológico y en problemas tácticos, OCTAVE se enfoca en el riesgo organizacional y en problemas estratégicos relacionados con la práctica. Es una evaluación flexible que se puede adaptar para la mayoría de las organizaciones.

7. MAGERIT [9] - Metodología de Análisis y Gestión de Riesgos de IT

MAGERIT versión 3 se estructura en tres libros: "Método", "Catálogo de Elementos" y "Guía de Técnicas" implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Es mantenida por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital de España, con la colaboración del Centro Criptológico Nacional (CCN) del mismo país.

8. EBIOS [10] - Expression des Besoins et Identification des Objectifs de Sécurité

EBIOS se puede aplicar a toda una organización o a un componente de una aplicación. Presenta dos enfoques de identificación de riesgos: por cumplimiento (para

riesgos no intencionales) y por escenarios (para riesgos deliberados). Su objetivo es obtener una síntesis entre “cumplimiento” y “escenarios” al reposicionar estos dos enfoques complementarios donde aportan el mayor valor agregado.

Se proporciona una guía que describe 15 etapas de un enfoque progresivo para construir, paso a paso, una política de gestión de riesgos digitales dentro de una organización.

Este método adopta un enfoque iterativo mediante cinco talleres [11], propone una caja de herramientas, cuyo uso varía según el objetivo del proyecto y es compatible con los estándares de referencia vigentes, en términos de gestión de riesgos, con la norma ISO 31000:2018, así como en términos de ciberseguridad, con la serie ISO/IEC 27000.

9. CORAS [12] - Construct a platform for Risk Analysis of Security critical systems

CORAS es un método para realizar análisis de riesgos de seguridad, que proporciona un lenguaje personalizado para el modelado de amenazas y riesgos, y brinda directrices que explican cómo se debe usar el lenguaje para capturar y modelar información relevante durante las distintas etapas del análisis.

El método CORAS proporciona una herramienta diseñada para soportar la documentación, mantenimiento y reporte de resultados de forma coherente. Esta metodología brinda consejos detallados con respecto a qué modelos deben construirse y cómo deben expresarse.

10. CRAMM [13] Risk analysis and Management Method

CRAMM se divide en dos partes: el método, que proporciona orientación sobre cómo llevar a cabo evaluaciones de riesgos y revisiones de seguridad; y el software de soporte, que le ayuda a configurar y llevar a cabo las revisiones.

Ayudar a analizar los sistemas y redes de información, identificar los requisitos de seguridad y los requisitos de contingencia.

Es un método aplicable a todos los tipos de sistemas y redes de información pudiendo utilizarse en todas las etapas del ciclo de vida del sistema de información, desde la planificación y viabilidad, así como durante el desarrollo y la implementación.

11. FRAAP [14] - Facilitated of Risk Analysis and Assessment Process

FRAAP tiene como objetivo principal desarrollar un proceso eficiente y disciplinado para garantizar que los riesgos relacionados con la información para las operaciones

comerciales se consideren y documenten. Este proceso permite “preseleccionar” aplicaciones, sistemas u otros temas para determinar si se necesita un análisis más formal de riesgos y allí asignar los recursos.

Utiliza una metodología de implementación similar a OCTAVE.

12. Mehari [15] - Methode Harmonisée d’Analyse de Risques

El primer objetivo de Mehari es proporcionar un método para la evaluación y gestión de riesgos, concretamente en el dominio de la Seguridad de la Información, conforme a los requerimientos de la ISO/IEC 27005:2011, proporcionando el conjunto de herramientas y elementos necesarios para su implementación.

Otros objetivos adicionales son, permitir un análisis directo e individual de situaciones de riesgos descritas en escenarios, y proporcionar un conjunto de herramientas específicamente diseñadas para la gestión de la seguridad a corto, mediano y largo plazo, adaptables a diferentes niveles de madurez y tipos de acciones consideradas.

El enfoque proporcionado por MEHARI se basa en una base de datos de conocimientos y en procedimientos automatizados para la evaluación de los factores que caracterizan cada uno de los riesgos, y que permite evaluar su nivel. Este método también proporciona asistencia para la selección de planes de tratamiento adecuados.

13. ISRAM [16] - Information Security Risk Analysis Method

Presenta un enfoque cuantitativo para el análisis de riesgos y un modelo basado en encuestas, utilizado para analizar el riesgo en la Seguridad de la Información.

El método incluye dos atributos principales de riesgo: probabilidad y consecuencia, en base a dos encuestas separadas e independientes. Se basa en modelar el riesgo como una combinación de probabilidad y consecuencia de una violación de seguridad.

Comparación de metodologías

Cada una de las metodologías presentadas anteriormente, abordan el proceso de gestión de riesgos con diferentes enfoques, métodos y características, entre otros aspectos.

Los marcos de gestión de riesgo definen una estructura sobre la cual las organizaciones pueden construir todos los procesos relacionados con la identificación, el análisis, la evaluación y la gestión de los riesgos de seguridad de la información y las metodologías de gestión de riesgos proporcionan orientación sistemática sobre cómo identificar, analizar, evaluar y gestionar el riesgo, siendo menos flexibles que los marcos, debido a su especificidad.

Casi todas las metodologías analizadas están enfocadas en la gestión de los riesgos de la Seguridad de la Información, pero algunas, como la norma ISO 31000, se enfocan en la gestión de riesgos en general.

Para alcanzar los objetivos establecidos inicialmente, es necesario analizar y comparar cada una de las características de las diferentes metodologías.

Atributos comparables

Se definió un conjunto de criterios a partir de los cuales se compararon y evaluaron las diferentes metodologías presentadas en capítulo anterior.

En la siguiente tabla se detallan los criterios seleccionados y su valoración.

Criterio de evaluación	Descripción del criterio y valoración
Idioma	Lenguaje en el que está disponible la metodología o norma. Valoración: • 3: En español • 1: En inglés • 0: Distinto a español o ingles
Enfoque	Principal tema tratado por la metodología o norma; diferenciando si es orientado a los riesgos de Seguridad de la Información o por el contrario tiene un abordaje general. Valoración: • 3: En Seguridad de la Información • 1: En general
Procesos de gestión de riesgos	Procesos principales dentro de la metodología o norma. Valoración: • 2: Cuenta con la mayoría de los procesos principales • 1: No cuenta con la mayoría de los procesos principales
Apoyo	Si la metodología o norma cuenta con guías de apoyo para facilitar su uso. Valoración: • 3: Cuenta con guías de apoyo para la implementación • 0: Documentación general de la norma
Ayuda a la implementación	Plan de proyecto, técnicas, roles, comparativas, cuestionarios. Valoración: • 3: Cuenta con la mayoría de los elementos (4 o 5 de ellos) • 1: No cuenta con la mayoría de los elementos, tiene alguno de ellos (3 o menos de ellos) • 0: No cuenta con ayuda
Herramientas de soporte	Si la metodología o norma utiliza alguna herramienta ya sea free o premium.

	Valoración: • 3: Existen herramientas libres, pero no las requiere • 2: Existen herramientas de pago, pero no las requiere • 1: No requiere de herramientas • 0: Requiere de herramientas
Acceso a la metodología	Tipo de acceso: libre o sin costo, o mediante pago. Valoración: • 3: Libre • 2: Algunos materiales restringidos • 1: Pago
Elementos	Procesos, Activos, Recursos, Vulnerabilidades, Amenazas y Controles. Valoración: • 3: Cuenta con todos los elementos. • 2: Cuenta con la mayoría de los elementos (4 o 5 de ellos). • 1: Tiene alguno de ellos (2 o 3 de ellos)
Tipo de empresas	Pequeña, mediana, grande. Valoración: • 2: Aplica para la mayoría de las empresas • 1: Aplica para las empresas medianas y grandes • 0: Aplica solo a empresas grandes
Tipo de análisis	Cualitativo, cuantitativo. Valoración: • 3: Cuenta con ambos tipos de análisis • 2: Cuenta sólo con análisis cualitativo • 1: Cuenta sólo con análisis cuantitativo
Complejidad (necesidad de experiencia)	Complejidad baja, media y alta. Valoración: • 3: Baja • 2: Media • 1: Alta

A cada uno de los criterios de evaluación definidos, se le asignó una valorización de entre 0 y 3 puntos, con el fin de asignarle un puntaje mayor a aquellos aspectos que son más importantes al momento de cumplir con los objetivos iniciales de este trabajo.

Por ejemplo, respecto al idioma, se asignó un valor de 3 puntos a las metodologías que disponen de su documentación original en español, un valor de 1 punto a las que disponen de la documentación en inglés, pero no en español, y un valor de 0 punto, a las que no disponen de documentación ni en español ni en inglés. De este modo, aquellas metodologías cuya documentación no esté publicada en español o en inglés, no recibirán puntos, pues resulta más difícil la comprensión de idiomas particulares diferentes del español o el inglés.

Resultados comparados

Una vez analizadas cada una de las metodologías y asignados los puntos de valoración de acuerdo con los criterios definidos se presentan los resultados en la siguiente Tabla:

Criterio de evaluación / Metodología	Idioma	Enfoque	Procesos	Apoyo	Ayuda a la implementación	Herramientas de soporte	Acceso a la metodología	Elementos	Tipos de empresas	Tipo de análisis	Complejidad	TOTAL
ISO 31000:2018	3	1	2	0	1	3	1	2	2	3	2	20
ISO/IEC 31010:2019	3	1	2	3	1	3	1	2	2	3	2	23
ISO/IEC 27005:2018	3	3	2	0	1	3	1	2	2	3	2	22
COBIT 5 for Risk	3	3	2	0	1	3	1	2	2	3	2	22
NIST SP.800-37,39 y30	1	3	2	3	3	3	3	2	2	2	2	26
OCTAVE	1	3	2	3	3	3	2	3	2	2	2	26
MAGERIT	3	3	2	3	3	1	3	1	2	3	2	26
EBIOS	3	3	2	3	1	3	3	1	2	1	2	24
CORAS	1	3	2	0	1	1	3	2	2	2	2	19
CRAMM	1	3	2	0	3	1	1	2	2	2	2	19
FRAP/FRAAP	1	3	2	0	3	1	3	1	2	2	2	20
MEHARI	1	3	2	3	3	1	3	2	2	2	2	24
ISRAM	1	3	2	0	1	3	3	1	2	1	2	19

Resultados

Los marcos de gestión de riesgo definen una estructura sobre la cual las organizaciones pueden construir todos los procesos relacionados con la identificación, el análisis, la evaluación y la gestión de los riesgos de seguridad de la información y las metodologías de gestión de riesgos proporcionan orientación sistemática sobre cómo identificar, analizar, evaluar y gestionar el riesgo, siendo menos flexibles que los marcos, debido a su especificidad.

A partir del puntaje obtenido por cada una de las metodologías analizadas, se profundizó en las metodologías que obtuvieron un puntaje superior a los 25 puntos.

Las metodologías que obtuvieron un puntaje superior son OCTAVE, NIST y MAGERIT con 26 puntos.

Se analizaron las ventajas y desventajas de dichas metodologías conforme al objetivo del presente documento.

OCTAVE [17,18]

Ventajas:

- Auto dirigible. Se puede desarrollar por personas de la misma organización, utilizando un equipo multidisciplinario.
- Involucra a personas de todas las áreas.
- Permite construir perfiles de amenazas basados en los activos.
- Permite identificar las vulnerabilidades.
- Facilita el desarrollo de planes y estrategias de seguridad.
- Comprende las etapas de análisis y gestión de riesgos.
- Involucra procesos, activos, dependencias, recursos, vulnerabilidades, amenazas y contramedidas.
- Relaciona amenazas y vulnerabilidades.
- Su uso es gratuito.

Desventajas:

- Utiliza muchos documentos anexos para llevar a cabo el proceso de análisis de riesgos, lo que puede resultar tedioso y complicado de entender.
- Se requiere habilidades previas en gestión de riesgos.
- Se debe solicitar autorización al SEI para la utilización completa o parcial del material específico aclarando que intención de distribución se tiene.

NIST [19,20]

Ventajas:

- Proporciona un conjunto de guías para la gestión y evaluación de riesgos de Seguridad de la Información. (SP 800-30, SP 800-37, SP 800-53, SP 800-53A)
- Presenta un resumen de los elementos clave de las pruebas de seguridad técnica y la evaluación con énfasis de técnicas específicas, sus beneficios, limitaciones y recomendaciones para su uso.
- Las guías proveen herramientas para la valoración y mitigación de riesgos.
- Asegura los sistemas informáticos que almacenan, procesan y transmiten información.
- Mejora la administración a partir de los resultados del análisis de riesgos.
- Se aplica a todas las etapas del proceso de gestión de riesgos.

Desventajas:

- En el modelo no se tiene contemplados elementos como los procesos, los activos ni las dependencias.

MAGERIT [21], [22]

Ventajas:

- Alcance completo en el análisis y gestión de riesgos.
- Está bien documentado en cuanto a recursos de información, amenazas y tipos de activos.
- Utiliza un completo análisis de riesgo cuantitativos y cualitativos.
- El libre y no requiere autorización para su uso.
- Divide los activos de la organización en diferentes grupos, para identificar más riesgos y poder tomar contramedidas para evitar así cualquier riesgo.
- Se centra en tres objetivos: concientizar sobre la existencia de los riesgos de la necesidad de atajarlos a tiempo, ofrecer un método sistemático para analizar tales riesgos, ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación.
- Posee una buena base documental en tres libros: El método, Catálogo de elementos, y Guía de Técnicas, que son de accesos público.
- Posee herramientas para el análisis de riesgo como PILAR.

Desventajas:

- En su modelo no involucra los procesos, ni vulnerabilidades.

Conclusión

Los marcos seleccionados son aplicables a cualquier organización de Uruguay.

La metodología OCTAVE en su versión especialmente desarrollada para empresas PYMES, requiere que el equipo que realiza la implementación cuente con cierta experiencia en la gestión de riesgos.

Por su parte, la metodología MAGERIT requiere de un inventario de los activos con la correspondiente valoración de los mismos.

Finalmente, el marco de gestión de riesgo de NIST con sus guías complementarias, ofrece un conjunto de documentos, que permiten cubrir todos los posibles enfoques del proceso de gestión de riesgos.

Adicionalmente la metodología de gestión de riesgos desarrollada por el NIST está alineada con el marco de ciberseguridad desarrollado por dicha institución, y dicho marco es la base del Marco de Ciberseguridad desarrollado por Agesic.

Teniendo en cuenta todos los aspectos presentados, se entiende que cualquiera de estas tres metodologías aporta al abordaje integral de los riesgos de una organización de porte medio, con una curva de aprendizaje relativamente rápida que además está apoyada por documentación y herramientas disponibles de manera gratuita.

Referencias

[1] ENISA (The European Union Agency for Cybersecurity). Inventory of Risk Management / Risk Assessment Methods and Tools. Online: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory.

[2] ISO (International Organization for Standardization). ISO 31000:2018(es) Gestión del riesgo — Directrices. Risk management — Guidelines. Online: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es.

[3] Gamont QM. La nueva ISO 31010: 2019, cuáles son los cambios relevantes. Online: https://gamontqm.com/2019/08/11/la-nueva-iso-31010-2019-cuales-son-los-cambios-relevantes/.

[4] ISO (International Organization for Standardization). ISO/IEC 27005:2018(en) Information technology — Security techniques — Information security risk management. Online: https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27005:ed-3:v1:en.

[5] NIST (National Institute of Standards and Tecnology) SP 800-37 Rev. 2 Online: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

[6] NIST (National Institute of Standards and Tecnology) SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View Online: https://csrc.nist.gov/publications/detail/sp/800-39/final.

[7] NIST (National Institute of Standards and Tecnology) SP 800-30 Guide for Conducting Risk Assessments, Online: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

[8] SEI (Software Engineering Institute). Christopher J. Alberts, Audrey J. Dorofee , James F. Stevens y Carol Woody. Introduction to the OCTAVE® Approach. Online: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=51546.

[9] CSAE (Consejo Superior de Administración Electrónica). MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. Online: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

[10] ANSSI. Agence Nacionale de la Sécurité des systems d'information. Ebios Risk Manager. Online: https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/.

[11] ANSSI y AMRAE (Management des Risques et des Assurances de.'Enterprise). Online: https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf.

[12] CORAS – A Framework for Risk Analysis of Security Critical Systems. Ketil Stolen, Oslo.

[13] Servicio de Seguridad en nombre del Gobierno del Reino Unido. CRAMM Version 5.1 User Guide _0.2_.doc.

[14] Thomas R. Peltier. Information Security Risk Analysis, Second Edition, Auerbach Publications, 2005.

[15] CLUSIF. (Club de la Securite de L'information Français). Mehari 2010 Introducción. Online: http://meharipedia.x10host.com/wp/wp-content/uploads/2016/12/MEHARI-2010-IntroduccionESP.pdf

[16] Vivek Agrawal. The Norwegian Information Security laboratory – NISLAB, Gjøvik University College, Gjøvik, Indian. A Comparative Study on Information Security Risk Analysis Methods. December 2015. Online: http://www.jcomputers.us/vol12/jcp1201-06.pdf.

[17] Juan Santoja Lillo. Análisis y correlación entre probabilidad e impacto de los riesgos. Online: https://rua.ua.es/dspace/bitstream/10045/93271/1/Analisis_y_correlacion_entre_probabilidad_e_impacto_de_l_Santonja_Lillo_Juan.pdf.

[18] Alemán, H. & Rodríguez, C. (). Metodologías para el análisis de riesgos en los sgsi. Universidad Nacional Abierta y a Distancia, UNAD. Repositorio Institucional UNAD. Online; https://repository.unad.edu.co/handle/10596/29673.

[19] López, Ramirez, Marxela. Análisis de Riesgos en un sistema de gestión de seguridad de la información (SGSI) con metodologías complementarias, Online: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2913/00004422.pdf.

[20] Risk Management Framework Process Map – 2018.

[21] Juan Santonja Lillo. Análisis y correlación entre probabilidad e impacto del riesgo. Online: https://rua.ua.es/dspace/bitstream/10045/93271/1/Analisis_y_correlacion_entre_probabilidad_e_impacto_de_l_Santonja_Lillo_Juan.pdf.

[22] Alemán, H. & Rodríguez, C. (). Metodologías para el análisis de riesgos en los sgsi. Universidad Nacional Abierta y a Distancia, UNAD. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/29673.