Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final de la Especialización

ANÁLISIS DE METODOLOGÍAS DE LA GESTIÓN DEL RIESGO APLICABLES A LA NORMA ISO/IEC 27005:2018

Autor:

David Chacón Prieto

Tutor del Trabajo Final:

Marcia Maggiore

2020

Cohorte 2017

Declaración jurada de origen de los contenidos

“Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual”.

_____

David Chacón Prieto

DNI: 95.688.447

Resumen

En este documento de propósito investigativo se encuentran compiladas la descripción y análisis de las principales metodologías de la gestión del riesgo y las diferentes recomendaciones y directrices generales para la gestión de riesgo en Sistemas de Gestión de Seguridad de la Información, tomando como marco de referencia las normas ISO. En particular, la norma ISO/IEC 27005:2018[1].

De dichas metodologías se enfatizó en sus similitudes, diferencias, recomendaciones, aportes y directrices y posteriormente se enmarcó sobre el estándar mencionado para el correcto manejo de la incertidumbre generada a partir de una amenaza.

Palabras Clave: Activo, Amenaza, Vulnerabilidad, Riesgo, Incertidumbre, Análisis, Normas, Objetivos Corporativos, Tecnología Informática, Información, Continuidad, Auditoria, Seguridad de la Información.

[1] ISO/IEC 27005:2018 - Information Technology - Security Techniques - Information Security Risk Management

Índice General

Agradecimientos

A mi familia por hacer de mí la persona que soy hoy en día. Un logro que no lo considero personal sino nuestro.

Al cuerpo docente y amigos por su colaboración en el cumplimiento de esta nueva meta personal y profesional.

A la docente y tutora Marcia Maggiore, quien con su colaboración y guía me brindo el apoyo y detalle necesario para la elaboración de este documento.

Y con personal aprecio a mi novia Angelly Sanchez Luengas quien me ha acompañado en esta etapa de mi vida y ha sido un gran soporte para la consecución de este logro.

1- Introducción

Las empresas han ido evolucionando al ritmo de las necesidades generales como particulares de cada negocio y de los cambios sobre el ambiente en el cual se desenvuelven. Los avances a nivel tecnológico y de gestión han permitido que sus procesos tomen rumbos cada vez más automatizados a la hora del procesamiento de la información. La dependencia de la tecnología es cada vez mayor por el alto volumen de datos y procesamiento que se requiere para una correcta interpretación de los mismos, entregar resultados y en sí, poder administrar la entidad. Lo anterior ha dejado en evidencia necesidades que antes no lo eran tanto, o simplemente no eran tomadas en cuenta, como la integridad de los datos que se procesan, la disponibilidad de estos datos y la confidencialidad de los mismos.

Teniendo en cuenta lo anterior, la información se ha convertido en uno de los activos más relevantes de toda compañía y con este nuevo valor, se ha vuelto imperativa la necesidad de control, confianza y disposición de los datos. Para poder garantizar que este nuevo activo se encuentre seguro independientemente del medio y el lugar en el cual se encuentre se han generado metodologías, procesos y buenas prácticas. Es aquí donde los estándares y metodologías sobre gestión del riesgo empiezan a tomar un papel protagónico en el proceso de asegurar la información durante todo su ciclo de vida. Nos brindan una manera sistemática de tratar los riesgos asociados y una visión global del estado actual sobre esta temática, permitiendo así planificar los controles necesarios para cumplir con los requerimientos de seguridad de la información.

Uno de los estándares más reconocidos a nivel de gestión del riesgo de la seguridad de la información es la norma ISO/IEC 27005. Esta norma ofrece los lineamientos para la gestión de riesgos de seguridad de la información en una entidad, basándose puntualmente en el sistema de gestión de seguridad de la información especificado en el estándar ISO/IEC

27001:2013[2], teniendo como ventaja la adaptación a todo tipo de compañías.

Cabe aclarar que el estándar ISO/IEC 27005 no determina o invita al uso de alguna metodología para la gestión del riesgo en particular, siendo ésta una decisión exclusiva de la entidad, dado que depende de varios factores como su tamaño, el ambiente en el que se desenvuelve, grado de aplicabilidad de la metodología y muchos otros factores que son determinantes a la hora de tomar esta decisión.

A partir de lo mencionado anteriormente, este trabajo de investigación busca describir, detallar y comparar las principales y más reconocidas metodologías para la gestión de riesgos, que sean compatibles para trabajar bajo la norma ISO/IEC 27005, efectuando un análisis a partir de sus características, su aplicación y entrega de resultados.

[2] ISO/IEC 27001:2013 - Information Technology - Security Techniques - Information Security Management Systems - Requirements

2- ISO/IEC 27005:2018 - Gestión de Riesgos de Seguridad de la Información

Cualquier actividad de una empresa involucra riesgos. Para conocerlos y medirlos, toda entidad debe realizarla gestión de riesgos a partir de su identificación, análisis y evaluación. Posteriormente tratará los riesgos de acuerdo con sus criterios, de manera tal que aquéllos no excedan su apetito de riesgo. Es aquí donde el estándar ISO/IEC 27005 toma importancia, proveyendo un marco para la gestión de riesgos, brindando una forma eficaz para desarrollar y evaluar los riesgos de seguridad de la información, particularmente en el contexto de la implementación de un sistema de gestión de seguridad de la información. Sin embargo no es una metodología, solo una guía que brinda los lineamientos para el correcto tratamiento de los riesgos, soportándose en los conceptos generales de la ISO/IEC 27001. Esta norma está redactada de manera muy técnica y direccionada a las personas que trabajan día a día con la seguridad de la información, sus líderes y también a los jefes de áreas de seguridad de la información (CISO´s[3]), personas que trabajen en el área de riesgos y auditores. A partir de su enfoque sistémico, desarrolla el proceso de gestión de riesgos, siendo así una guía para su implementación, mantenimiento y su mejora continua.

El proceso de gestión de riesgo de seguridad de la información busca evaluar las amenazas, sin importar su tamaño o naturaleza, ayuda a reconocer el riesgo en el cual se desenvuelve la empresa, brinda conciencia de las amenazas y vulnerabilidades que posee el ente, ofrece opciones acordes y efectivas para el tratamiento de los riesgos, y por ultimo establece los lineamientos para su revisión, monitoreo y comunicación de los resultados. Bajo un correcto proceso de documentación, proporciona información determinante a la organización en cualquier entorno, generando

[3] Chief Information Security Officers

un aumento de la madurez del sistema de gestión de seguridad de la información y su mejora continua.

La gran flexibilidad y adaptabilidad de este estándar implica poder aplicarlo de forma global o específica, siendo posible implementarlo en toda la organización o en áreas determinadas de la compañía. Dependiendo de las necesidades, se manifiesta el grado de especificidad de la aplicación de la gestión de riesgos, permitiendo un conocimiento puntual de los riesgos, de los controles y de su eficacia.

2.1- Términos Generales

Para poder contextualizar la información brindada en este trabajo es necesario inicialmente, familiarizarse con los conceptos y el lenguaje relacionados a este tópico, ya que por la diversa variedad de interpretaciones dada a los conceptos que abarcan esta temática y las múltiples perspectivas de abordaje es habitual que se presenten inconvenientes a la hora de interpretar y aplicar correctamente la gestión de riesgos. A continuación, se brindará el significado de cada uno de los términos más relevantes:

- Objetivo: Resultado que debe alcanzarse. (ISO/IEC 27000:2018[4])
- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
- Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. (ISO/IEC 27000:2018)
- Amenaza: Causa potencial de un incidente no deseado, que puede resultar en daños a un sistema u organización. (ISO/IEC 27000:2018)
- Consecuencia: Resultado de un acontecimiento que afecta a los objetivos (ISO Guide 73:2009[5]). Una consecuencia puede ser cierta o incierta y, en

[4] ISO/IEC 27000:2018 - Information technology — Security techniques — Information security management systems — Overview and vocabulary
[5] ISO/Guide 73:2009 - Risk management — Vocabulary

el contexto de la seguridad de la información, suele ser negativa. (ISO/IEC 27000:2018)

- Probabilidad (likelihood): Posibilidad de que algo suceda. (ISO Guide 73:2009)
- Riesgo: Efecto de la incertidumbre sobre los objetivos. (ISO Guide 73:2009) El riesgo se caracteriza a menudo por la referencia a "acontecimientos" potenciales (tal como se definen en la Guía ISO 73:2009, 3.5.1.3) y "consecuencias" (tal como se definen en la Guía ISO 73:2009, 3.6.1.3), o una combinación de los mismos.
- Apetito de Riesgo: Cantidad y tipo de riesgo que una organización está dispuesta a buscar o retener.
- Nivel de Riesgo: Magnitud de un riesgo o combinación de riesgos, expresada en términos de la combinación de consecuencias y su probabilidad. (ISO Guide 73:2009)
- Riesgo Residual: Riesgo remanente después de su tratamiento. (ISO Guide 73:2009)
- Control: Medida para modificar el riesgo (ISO Guide 73:2009). Puede incluir políticas y procedimientos, directrices, prácticas o estructuras organizativas que pueden ser de carácter administrativo, técnico, de gestión o legal.
- Confidencialidad: Propiedad que la información no se pone a disposición o se divulga a individuos, entidades o procesos no autorizados.(ISO/IEC 27000:2018)
- Integridad: Propiedad de exactitud y completitud. (ISO/IEC 27000:2018)
- Disponibilidad: Propiedad de ser accesible y utilizable a petición de una entidad autorizada. (ISO/IEC 27000:2018)

2.2- Descripción del estándar ISO/IEC 27005:2018

2.2.1- Estructura de la norma

La norma ISO/IEC 27005 proporciona una serie de lineamientos sobre cómo gestionar los riesgos brindando un marco de gestión eficaz. Mediante una serie de cláusulas describe el proceso de gestión de riesgos de la

seguridad de la información, cada una de las cuales explica una parte esencial del proceso. De igual manera tiene una serie de anexos que soportan y brindan información adicional a la enunciada en las cláusulas que conforman el estándar. Cada una de ellas se encuentra segmentada de la siguiente manera:

- Requerimientos de Entrada: Se refiere a la identificación de la información necesaria para la toma de acciones.
- Acción: es la definición de la actividad a realizar.
- Guía de Implementación: En esta sección la norma brinda pautas, detalles e información adicional para realizar la actividad, indica el correcto deber ser de la actividad.
- Sección de Salida: Describe e identifica parte de la información resultante una vez realizada la actividad.

2.2.2- Visión general del proceso de gestión de riesgos

Para la gestión de riesgos de seguridad de la información es necesario un enfoque sistemático que permita identificar las necesidades de la organización con respecto a la seguridad de la información y crear un sistema de gestión efectiva de la seguridad de la información (SGSI).

Este enfoque debería ser adecuado para el entorno de la organización y, en particular, debería estar alineado con la gestión general de riesgos empresariales.

La gestión de riesgos de seguridad de la información debe ser un proceso continuo que puede ser aplicado a la organización como un todo, a un área en particular, a cualquier sistema de información o a aspectos particulares de un sistema complejo.

Cabe destacar que no todas las áreas/sistemas demandan un análisis completo y detallado. Muchas veces es suficiente con un análisis de alto nivel para poder tener los resultados esperados. Usualmente en ámbitos corporativos donde se focaliza el esfuerzo a partir de objetivos claros y un alcance definido, se procede a realizar un análisis global donde para los hallazgos de alta criticidad, o en los cuales no se pueda brindar una solución

sencilla, se realiza un análisis más detallado generando un grado más amplio a nivel de amenazas y posibilidades de mitigación.

A continuación se muestra gráficamente el proceso de gestión de riesgos:

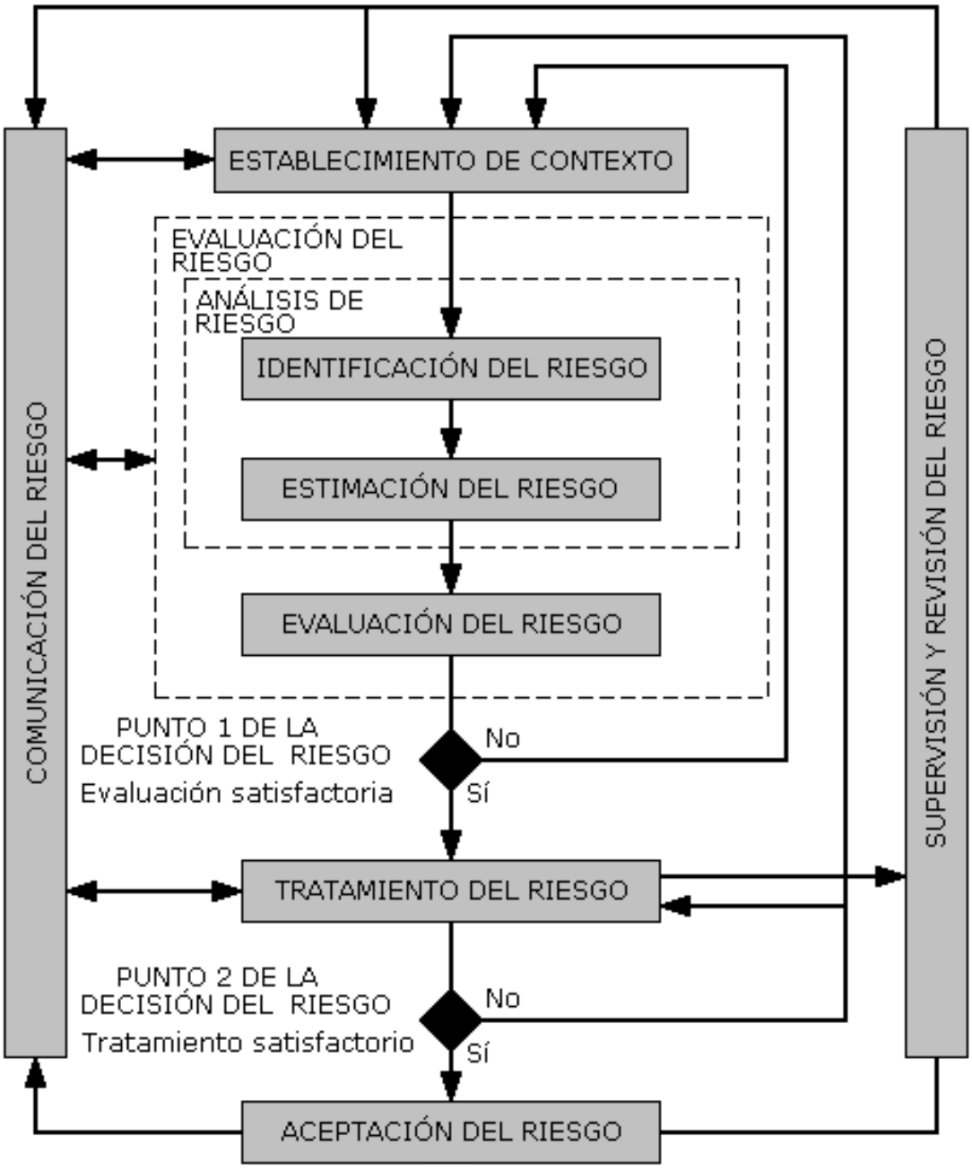

Ilustración 1: Proceso de para la Gestión del Riesgo ISO/IEC 27005:2018. Fuente: [9]

Como muestra la ilustración anterior, el proceso es iterativo, ya que es necesario realizar todos los pasos hasta obtener el nivel del riesgo y así poder compararlo con el apetito predefinido. Si el nivel de riesgo lo excede, se iniciará nuevamente el proceso hasta que dicho nivel quede por debajo.

También podría suceder que al aplicar determinado tratamiento del riesgo no se obtenga un nivel correcto de riesgo residual, lo cual demandará una nueva iteración. Esta vez relacionada con la aplicación de nuevos controles o cambios de estrategia en el tratamiento del riesgo.

Por otro lado, encarar la gestión de riesgos desde un enfoque iterativo, permitiría aumentar la profundidad y el grado de detalle de la evaluación en cada iteración.

Los criterios a utilizar en cada parte del proceso deben ser una decisión exclusiva de los responsables de la entidad.

Asimismo, una comunicación efectiva de la evaluación de riesgos a todas las partes interesadas posibilita una correcta implementación de controles y seguimiento de los mismos.

Por último, la documentación del proceso es esencial, así como el correcto registro de los resultados obtenidos, necesarios para llevar control y seguimiento de la gestión realizada.

A continuación se presentan las cláusulas que componen la norma, donde se describen los componentes de la gestión.

2.2.3- Establecimiento del Contexto para la Gestión del Riesgo

Actualmente, la seguridad de la información abarca varios ítems relacionados entre sí, como lo son la continuidad del negocio, las tecnologías de la información y la ciberseguridad.

Ilustración 2: Correlación entre la Continuidad del Negocio, Ciberseguridad y las Tecnologías de la información. Fuente: [25]

Como se muestra en el gráfico anterior, la gestión del riesgo es una labor que debe ser afrontada de manera integral. Para ello es necesario establecer previamente las bases de dicha gestión.

Con relación al contexto de la gestión de riesgos, la norma hace referencia a los objetivos y al área en la que se le realizará la implementación. Es decir que su definición es flexible y los deja a disposición de la interpretación y necesidades de la entidad, entendiendo que cada caso es diferente y teniendo en cuenta que el enfoque que se puede aplicar dependerá de los recursos con los que se cuente.

Para establecer el contexto interno y externo de la gestión de riesgos es necesario definir los criterios a utilizar respecto de la evaluación de riesgos, de la consecuencia y de la aceptación del riesgo, así como la definición de alcance, límites y el establecimiento del marco organizativo.

Criterio de Evaluación del Riesgo: Cómo proceder con respecto a la evaluación del riesgo es una decisión que debe considerar varios temas relacionados con el negocio, como son los objetivos de la organización, el valor y criticidad de los activos informáticos a nivel operacional y estratégico, el entorno jurídico, legal, los requerimientos regulatorios asociados a la

actividad de la compañía y cualquier otro factor decisivo que considere la entidad.

Criterio para Especificar las Consecuencias: Este criterio debe ser desarrollado en términos de la magnitud del daño o de los costos que podrían surgir de materialización de riesgos de seguridad de la información tales como generación de daños personales, pérdidas financieras, interrupción del servicio, pérdida de reputación y/o imagen de la entidad, incumplimiento de regulaciones, requisitos contractuales y/o legales.

En algunas entidades, la consecuencia se valora en términos del costo derivado del valor de los activos afectados y los daños producidos en el propio activo. Es importante resaltar que a la hora de asignar valores para la consecuencia, éstos se expresen en magnitudes, ya que esto ayuda al proceso de evaluación y permite generar con mayor exactitud el umbral de riesgo, o como usualmente se conoce, el apetito de riesgo. Cabe aclarar que también se puede realizar un análisis cualitativo, aunque es de menor precisión.

Criterio de Aceptación del Riesgo (Apetito de Riesgo): Este criterio a menudo depende de las políticas, metas y objetivos de la organización así como de las necesidades y expectativas de las partes interesadas. Se debe tener en cuenta que el criterio de aceptación puede ser diferente al evaluar diferentes riesgos y que también es posible la existencia de distintos niveles de apetito de riesgo.

Alcance y límites: Es necesario definir el alcance de la gestión de riesgos y se debe asegurar que en él se incluyen todos los activos relevantes. También deberán establecerse los límites para considerar los riesgos que pueden surgir fuera de los límites.

Para definir el alcance y los límites la organización debe contemplar, entre otros, los objetivos estratégicos, las políticas, el ambiente socio-cultural, los procesos y procedimientos internos, el enfoque de seguridad de la información, la legislación y normativa aplicable y la estructura organizacional.

Establecimiento del Marco Organizativo: Todo lo anterior genera los pilares necesarios para la creación del proceso de gestión del riesgo, el cual debe estar contenido en un marco organizativo y estructural, con los recursos necesarios y el establecimiento de funciones, roles y responsabilidades. Adicionalmente se debe identificar y crear las relaciones necesarias para el correcto flujo de trabajo de la gestión de riesgos con las partes interesadas, las áreas de involucradas y la alta y media gerencia.

2.2.4- Valoración del Riesgo

En este punto la norma ISO/IEC 27005 determina la valoración de los riesgos de seguridad de la información como un proceso compuesto por la identificación de todos los elementos partícipes y la definición del análisis del riesgo.

Los elementos a identificar son los activos, las amenazas, las vulnerabilidades, los controles existentes y las consecuencias. En base a los elementos identificados se valora el nivel de riesgo a partir de una posibilidad real de ocurrencia. La valoración que se produce en este proceso puede ser de carácter cuantitativo o cualitativo.

Es importante resaltar que todas estas actividades generarán un alto volumen de información debido a la gran cantidad de datos a manejar y todas las posibles combinaciones a tener en cuenta a la hora de evaluar. Esto hace imperativo la implementación de una metodología y un proceso estructurado, sistemático y riguroso de evaluación de riesgos y del uso de herramientas automatizadas de gestión que implementen alguna metodología con el agregado de listas de activos, amenazas, controles y sus combinaciones posibles.

2.2.4.1- Introducción a la Identificación del Riesgo

El propósito de la identificación de riesgos es encontrar los eventos que puede causar daño y profundizar respecto cómo, dónde y por qué dichos eventos pueden suceder.

A continuación se detallan los pasos que indica la norma para lograr la identificación de riesgos (ítems 2.2.4.2 a 2.2.4.6).

2.2.4.2 - Identificación de Activos

Los activos pueden ser de diversa índole y de diversas fuentes. A continuación se hace mención a las diferentes categorías de activos de información:

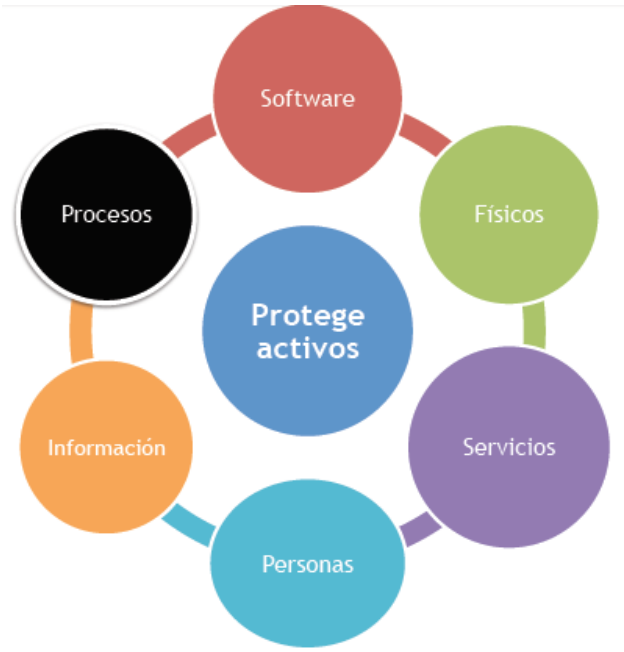

Ilustración 3: Categorías de Activos. Fuente: [12]

Como ejemplos de las categorías mencionadas en la ilustración anterior es posible citar, entre otros; la información, en cualquier soporte, que la entidad genera o procesa; el hardware y software con los que se realiza el procesamiento, envío o salvaguarda de la información; los servicios para la ejecución de transferencia y control de la información; los utilitarios y sistemas de información; el capital humano; el conocimiento que genera exclusividad para utilizar y mantener la propiedad sobre algún proceso u objeto y, en consecuencia, también una ventaja competitiva.

Teniendo en cuenta esto, la cantidad de elementos a considerar, clasificar, y analizar es de un volumen considerable, por lo cual es aconsejable hacer uso de softwares especializados para esta labor, los cuales cuentan con una diversa gama de activos definidos.

Para identificar los activos es recomendable hacer uso de lineamientos apropiados. Como ejemplo es posible considerar los propuestos por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MINTIC), que se comentan a continuación:

- Inventario de Activos: Cada activo debe estar identificado, clasificado y registrado a un nivel de detalle razonable y justificable para la gestión de riesgos. Con las diversas iteraciones de esta labor se va profundizando y encontrando un nivel razonable con el cual se puede establecer un estándar de inventario de activos.
- Propiedad de los Activos: Cada activo debe tener asociado un dueño o propietario. Éste será responsable de la gestión del activo durante todo su ciclo de vida, así como de la implementación de los controles necesarios, acorde a la clasificación del activo.
- Clasificación de Activos: La clasificación debe indicar el valor del activo respecto de su sensibilidad y criticidad en términos de su confidencialidad, integridad y disponibilidad.
- Tratamiento de Activos: Es la definición de controles acordes a su clasificación, con base en las buenas prácticas de seguridad.

La identificación de activos a través de su inventario proveerá uno de los datos necesarios para el análisis de riesgo. La siguiente gráfica, muestra la relación de las actividades del proceso de gestión de activos de la información:

Ilustración 4: Metodologías para la Gestión de Activos de información. Fuente: [12]

La cantidad de activos relevados, clasificados y tratados impacta directamente en el análisis de riesgos. Cuanto mayor sea el detalle y la cantidad de información relevada, el proceso de análisis tomará más tiempo, sin embargo optimizará las posteriores actividades del proceso. Su límite está dado por las definiciones previas como, alcance, área de aplicación, procesos y procedimientos, enfoque de seguridad de la información, legislación, normativas que la entidad necesite aplicar.

Es importante mencionar que la norma ISO/IEC 27005 tiene una serie de anexos como información adicional de apoyo y referencia. Puntualmente, el Anexo B[6], en donde se encuentra información como ayuda y guía para identificar los activos y llevar a cabo su valoración.

2.2.4.3 - Identificación de Amenazas

Una amenaza tiene el potencial de causar daños a los activos de información y, por lo tanto, a las organizaciones. Las amenazas pueden ser de origen natural, técnico o humano y podrían ser accidentales o deliberadas

[6] Annex B, Identification and valuation of assets and impact assessment ISO/IEC 27005:2018

y pueden quebrantar la seguridad de un activo de información explotando una vulnerabilidad.

Algunos ejemplos de amenaza son los ataques informáticos; eventos de hurto o fraude; eventos físicos como terremotos, inundaciones o incendios; la falta de disposiciones corporativas y técnicas como ausencia de certificados digitales o de cifrado de canales de comunicación; así como también la gestión de los recursos tecnológicos. Como se puede deducir de los ejemplos anteriores, las fuentes pueden ser tanto internas como externas, siendo necesario identificar correctamente sus consecuencias. Ello debido a que una sola amenaza puede afectar de manera transversal a más de un activo y la consecuencia podría ser diferente para cada uno de ellos.

El relevamiento de las amenazas y de las vulnerabilidades debe ser una labor conjunta y preferiblemente realizada por personas con diversos ámbitos de conocimiento. Una fuente clara de esta información es el usuario o el dueño del activo de información, los cuales conocen su naturaleza y los diversos procesos que interactúan con él, así como los incidentes de seguridad reportados. Otro recurso importante para llevar a cabo esta labor es el Anexo C[7] de la norma ISO/IEC 27005 o los catálogos de amenazas producidos por diferentes entidades. Asimismo, las herramientas informáticas dedicadas al análisis de riesgos brindan una serie de amenazas generalmente asociadas a los activos que pueden sufrirlas.

2.2.4.4 - Identificación de Controles Existentes

Previamente al análisis de riesgos es necesario identificar los controles ya implementados, conocer los activos a los que protegen, validar la documentación relacionada y garantizar su correcto funcionamiento. La inadecuada implementación de los mismos puede derivar en la generación de vulnerabilidades. Este relevamiento evitará generar esfuerzo, trabajo y costos adicionales por redundancia en la implementación de controles ya existentes.

Las actividades necesarias para determinar la eficacia del control pueden ser las siguientes:

[7] Annex C, Examples of typical threats - ISO/IEC 27005:2018

- Validación de la documentación pertinente y relacionada al control existente. Usualmente se puede encontrar la información en reportes, pruebas de funcionamiento realizadas anteriormente y métricas de seguimiento.
- Revisión en conjunto con el personal responsable de la seguridad de la información y los usuarios que interactúan con el activo de información.
- Realización de las pruebas y verificaciones necesarias para garantizar la existencia y su correcto funcionamiento e implementación.
- Revisar los informes de las auditorías, tanto internas como externas.

A partir de esta valoración, si el control es ineficaz o insuficiente, se deberá decidir el uso de controles complementarios o bien de modificar el control, una vez realizada la evaluación de riesgos.

2.2.4.5 - Identificación de Vulnerabilidades

Una vulnerabilidad es una debilidad de un activo, que puede ser explotada por una amenaza. Es necesario identificar las vulnerabilidades asociadas a los activos informáticos. Cabe aclarar que la presencia de una debilidad no asegura que se generará un daño. Es necesario que exista una amenaza para explotarla y de no existir dicha amenaza, puede no ser requerida la implementación de controles para la mitigación del riesgo. Sin embargo la norma recomienda el seguimiento y monitoreo de la misma.

Algunas fuentes para la identificación de vulnerabilidades pueden ser las siguientes:

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión.
- Personal.
- Ambiente físico.
- Configuración del sistema de información.
- Hardware, software y equipos de comunicaciones.
- Dependencia de partes externas.

La norma ISO/IEC 27005 en su anexo D[8], cuenta con los métodos de valoración y ejemplos de vulnerabilidades. Asimismo, existen herramientas específicas en el mercado que pueden ayudar con el relevamiento de esta información.

2.2.4.6 - Identificación de Consecuencias

Ente concepto hace referencia a los efectos, a partir de la materialización de un riesgo, que se producen sobre uno o varios activos. La norma ISO/IEC 27005 cita algunos ejemplos como la pérdida de la eficacia, generación de condiciones adversas de operación, pérdidas del negocio, afectación de la reputación, daños físicos y lógicos sobre los activos. Las consecuencias pueden ser temporales o permanentes, como por ejemplo, en el caso de destrucción de un activo.

Esta actividad identifica las consecuencias para la organización que pueden ser resultado de un escenario de incidente. Éste se puede describir como la amenaza que explota una vulnerabilidad determinada o un conjunto de vulnerabilidades en un incidente de seguridad de la información. Todo escenario de incidente, que puede afectar a uno o varios activos, deriva en una o varias consecuencias, que pueden ser de distinto tipos, desde monetarias hasta degradación de credibilidad. Esta consecuencia se determina acorde a especificaciones definidas en los criterio al establecer el contexto, tal como se explicó previamente.

La ISO/IEC 27005 brinda una serie de recomendaciones para poder evaluar las consecuencias operativas, a saber:

- Tiempo de investigación y reparación.
- Pérdida de tiempo.
- Pérdida de oportunidad.
- Pérdida de salud y seguridad.
- Costos financieros asociados a la reparación del perjuicio.
- Daños en imagen, reputación y buen nombre.

[8] Annex D, Vulnerabilities and methods - ISO/IEC 27005:2018

Cabe mencionar que éstos no son los únicos conceptos de los que puede hacer uso la organización, ya que dependen de los criterios de cada entidad.

El siguiente gráfico muestra la relación entre los elementos a identificar:

Ilustración 5: Relación entre conceptos que hacen al riesgo. Fuente: [17]

2.2.5- Análisis del Riesgo

2.2.5.1 – Métodos para el análisis de riesgo

La norma ISO/IEC 27005 sugiere aplicar ciertos métodos de trabajo y hacer uso de herramientas tecnológicas que permitan el rápido procesamiento de información obtenida en los pasos previos. Estos métodos se aplican para obtener un valor cuantitativo, cualitativo o también, una combinación de ellos.

- **Método Cualitativo:** Hace uso de técnicas como encuestas, formularios, entrevistas, lluvia de ideas, evaluación de especialistas y expertos, análisis y valoración, haciendo uso de grupos multidisciplinarios entre otras técnicas.

Se basa en el conocimiento, la percepción y la experiencia para la toma de decisiones, dada la imposibilidad de realizar cálculos numéricos y un análisis cuantitativo, o la razón más usual, porque no es justificable la asignación de recursos para un análisis detallado.

Se utilizan escalas de calificación tales como alto, medio o bajo.

- **Método Cuantitativo:** A partir de una escala numérica definida y de cálculos matemáticos, genera un resultado con base en valores de la probabilidad de ocurrencia del riesgo, los cuales surgen de múltiples fuentes. Puede hacer uso de técnicas como el análisis de probabilidad, simulación computacional o análisis de consecuencias, sin embargo la calidad de estos resultados depende del modelo numérico usado y las consecuencias ante la materialización de un riesgo.

- **Método Semi-Cuantitativo:** Se aplican las técnicas referidas en la definición del método cualitativo pero el valor de las escalas es numérico. Al igual que el método mencionado, éste es fácilmente susceptible a errores debido a que depende de interpretaciones personales.

2.2.5.2 – Valoración de las consecuencias y de la probabilidad de ocurrencia

El siguiente paso en el análisis de riesgos es la evaluación de las consecuencias. La norma recomienda tener en cuenta el valor estimado en el relevamiento de los activos para la valoración de las consecuencias, tomando en cuenta el costo de tener el activo comprometido, la pérdida o la necesidad de remplazarlo, el tiempo y los costos financieros.

La posibilidad de ocurrencia de un evento se debe analizar a partir de la identificación de los actores que intervienen en la gestión de riesgos. Como se mencionó anteriormente, existen muchas fuentes de información para determinar la probabilidad de ocurrencia. La norma informa algunos parámetros a tener en cuenta y posibles fuentes de información para el cálculo de este valor.

A partir de los conceptos mencionados anteriormente, la valoración del riesgo se obtiene mediante la combinación de la probabilidad de un escenario de incidente y sus consecuencias.

2.2.6- Evaluación del Riesgo

Para realizar la evaluación de riesgos se tendrá en cuenta los criterios definidos al establecer el contexto. Las decisiones generadas en este punto deben tener en cuenta la implementación de métodos adecuados, como lo informa el anexo E[9] de la norma ISO/IEC 27005. Este proceso toma como base el nivel de aceptación del riesgo definido por la organización. La norma recomienda tener en cuenta para la evaluación del riesgo, las propiedades de la seguridad de la información, los requerimientos legales, las normativas aplicables y el grado de importancia del activo para los procesos del negocio.

3-Tratamiento del Riesgo

Las opciones de tratamiento de riesgo son: modificar, aceptar, compartir o evitar los riesgos, las cuales se definen más adelante. A continuación se presenta un gráfico que muestra la relación entre los diferentes niveles de riesgo.

Ilustración 6: Tratamiento del riesgo en Sistemas de Gestión de la Seguridad de la Información, Fuente: [40]

[9] Annex E, Information Security Risk assessment Approaches - ISO/IEC 27005:2018

La norma ISO/IEC 27001, a partir de los informes generados en la evaluación de riesgos, solicita se desarrolle el documento denominado Declaración de Aplicabilidad. Éste indica el perfil de seguridad de organización detallando los controles actuales y las razones de su existencia. En comparación con la evaluación de riesgos realizada, se definirán los controles faltantes, generando así el plan de tratamiento de riesgos, que expresa cómo se van a abordar los cambios a realizar para llegar al nivel de riesgo deseado. En este documento se debe indicar todos los detalles necesarios para la implementación de cada control. Este plan de acción debe ser aprobado por la dirección e impulsado por la alta gerencia para garantizar su cumplimiento. Se requiere cumplir con los siguientes apartados en el plan de tratamiento del riesgo:

- Una operatoria eficaz y eficiente de la organización.
- Controles internos efectivos.
- Conformidad con las normativas, leyes y reglamentos aplicables.

Cabe señalar que mediante las acciones previamente explicadas se deben tratar todos los riesgos cuyo nivel exceda el apetito de riesgo definido por la organización y de acuerdo a la prioridad establecida.

3.1- Estrategia del tratamiento de riesgos

En este punto se explican las opciones de tratamiento mencionadas previamente.

La ISO/IEC 27005 hace referencia al tratamiento de riesgos en la unidad 9, donde indica mediante un diagrama de flujo cuáles son sus opciones riesgo.

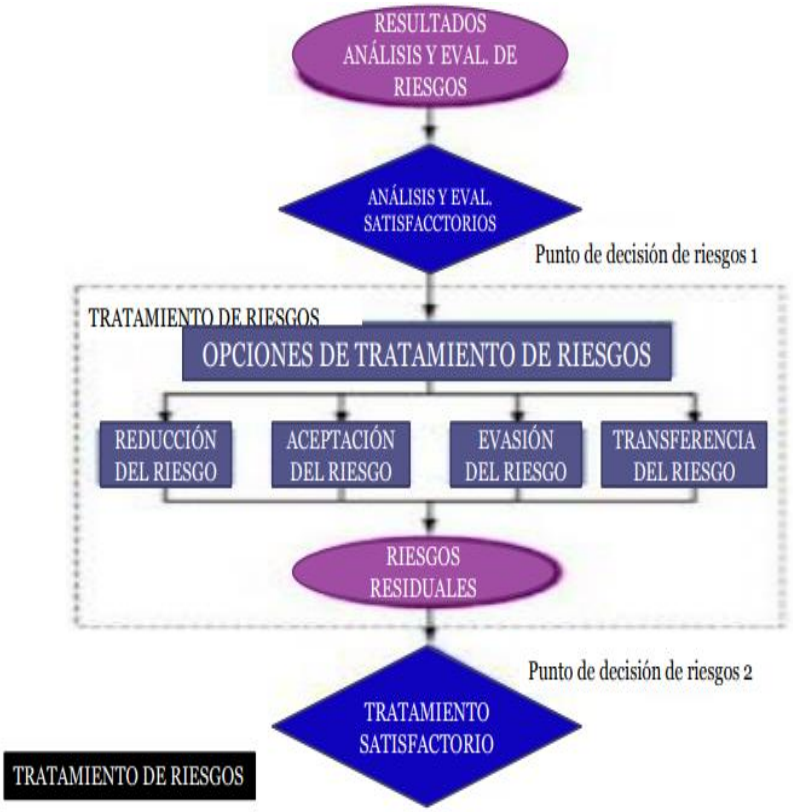

Ilustración 8: Actividades para el tratamiento del riesgo ISO/IEC 27005:2018. Fuente: [9]

Como se puede observar, una vez realizado el análisis y evaluación de los riesgos, se procede al tratamiento, esto equivale a adoptar alguna de las siguientes opciones.

- **Modificación:** Mediante la implementación de controles técnicos o de gestión se trata de disminuir la posibilidad de ocurrencia o la consecuencia de un escenario de riesgo. Se debe tener en cuenta que es necesario monitorear constantemente la implementación y asegurar que todas las medidas utilizadas sean efectivas y se ejecuten acorde al plan de tratamiento de riesgos.
- **Transferencia del Riesgo (Compartir el Riesgo):** Un claro ejemplo es la tercerización de servicios en distintas modalidades tales como, por ejemplo, Software as a Service (SaaS), Platform as a Service (PaaS) y Infrastructure as a Service (IaaS). Es decir, se realiza la transferencia de riesgo tercerizando su tratamiento. Cabe aclarar que esta opción no

disminuye la responsabilidad organizacional sobre los resultados del servicio.

- **Eliminación del Riesgo:** No es posible eliminar el riesgo a menos que se elimine la acción que lo genera. Tal vez sea posible encontrar una acción que reemplace a la original y cuyo riesgo puede ser tratado.
- **Retención del Riesgo:** Esta opción refiere a la convivencia con el riesgo. Ya sea, porque se encuentra dentro de los niveles permitidos para su aceptación o por la imposibilidad de tomar acción para su mitigación. Esto puede generarse por diferentes razones como por ejemplo, altos costos o imposibilidad tecnológica o física. Se debe considerar que se está asumiendo la responsabilidad por las pérdidas, o la carga financiera de las pérdidas o sus consecuencias dentro de la organización.

3.2- Plan de tratamiento del riesgo

El plan de tratamiento de riesgos, debe ser documentado de manera clara y concisa y debe contener los siguientes elementos

- La manera de implementar los controles.
- Responsables.
- Programa de trabajo.
- Resultados esperados.
- Presupuesto.
- Indicadores de desempeño.
- Definición del proceso de revisión.

Para este último punto, se debe definir un mecanismo para evaluar las salvaguardas contra los criterios de desempeño, objetivos y las responsabilidades individuales necesarias, en pro de la realización del plan, acorde a lo proyectado.

4- Aceptación del riesgo

El objetivo general siempre debe ser la mitigación de los riesgos como sea posible, esto puede desencadenar nuevas oportunidades que pueden hacer a un riesgo atractivo para la organización. La adopción de nuevas tecnologías para el tratamiento de los riesgos puede generar un diferencial importante a nivel competitivo a pesar del costo de su implementación. Esto genera nuevas variables para el análisis del riesgo, como se indicó anteriormente, temas como el costo versus la oportunidad son objeto de análisis y mediante un estudio riguroso puede hacer que el criterio de la aceptación del riesgo varíe y sea necesario realizar excepciones. Cuando por el contrario, el riesgo residual después de su tratamiento evidencie que no se encuentra sobre los niveles de aceptación y esto genere implementaciones y toma de decisiones que conlleven a que financieramente sea inviable su tratamiento, igualmente la norma ISO/IEC 27005 exige que deben ser generadas las excepciones específicas y claras del porqué de la excepción.

Como se indica, ya sean por sus efectos positivos o negativos, el criterio de aceptación del riesgo puede variar después del análisis gestión del riesgo, por lo cual los criterios de aceptación del riesgo no es simplemente validar si el riesgo está dentro del apetito de riesgo de la entidad. En la práctica se evidencia que en varios casos no es posible la opción de tratamiento indicada o que cumpla con todo lo necesario para la reducción del riesgo, y de igual forma, se generaran beneficios que conlleven a nuevas oportunidades para la entidad. Por lo cual es importante hacer la revisión de los criterios de aceptación del riesgo para que mediante una mezcla del tratamiento del riesgo y la aceptación de los riesgos residuales.

Lo anterior conlleva a que se debe documentar de manera rigurosa cada decisión y su justificación, aún más cuando se deba aplicar excepciones por cualquier razón. Usualmente, una muestra clara de estas excepciones refiere directamente al presupuesto. Dado que éste siempre

tiene limitaciones es adecuado priorizar los riesgos para atender primero los más importantes. A posteriori, deberá quedar documentado que fue necesario asumir riesgos por falta de presupuesto.

5- Consulta y Comunicación del Riesgo

Ésta es una actividad que tiene como objetivo lograr acuerdo, en la alta dirección y entre las partes interesadas, respecto de la manera de tratar los riesgos intercambiando opiniones y compartiendo información.

Una efectiva comunicación entre las partes interesadas es importante porque asegurará que los responsables de implementar la gestión de riesgos entenderán el motivo de la toma de determinadas decisiones, así como la razón de ejercer acciones particulares.

Como se ha visto a lo largo de este documento, la labor de la gestión de riesgos no refiere exclusivamente a los analistas de riesgos, sino es una labor mancomunada y colaborativa de todas las personas que interactúan en la entidad, lo cual hace que la comunicación sea un pilar de todo el proceso. Una vez se han evaluado los riesgos, el siguiente paso a considerar es la comunicación de los resultados obtenidos y del plan de tratamiento. Es importante considerar en las diversas soluciones para la mitigación del riesgo la percepción de las personas involucradas debido a que ello puede impactar tanto en la evaluación como en los planes de tratamiento.

Se recomienda crear un plan de comunicación para todas las personas involucradas, ya sean internas o externas a la entidad, en donde se informen los temas más relevantes del riesgo, el cómo se verán afectados y los procesos, procedimientos y responsabilidades de cada uno en su mitigación. Esto pretende generar el consenso necesario entre los interesados para la gestión del riesgo. La comprensión del porqué de las decisiones y el apoyo y colaboración del personal para llevar a cabo el plan de tratamiento de riesgos permitirá la retroalimentación de todas las partes y la colaboración mutua para el alcance de los objetivos trazados.

Como se informa en apartados anteriores, la comunicación del riesgo es un proceso que se realiza en cada etapa de la gestión, ya que es necesaria en si misma desde la recolección de la información, hasta la puesta en marcha del plan de tratamiento, lo cual la convierte en punto clave

de todo el proceso. Por lo cual se debe documentar e identificar las apreciaciones de todas las partes interesadas y asegurar que sean comprendidas y tenidas en cuenta, ya que generan consecuencias sobre todo el proceso, las decisiones y la implementación de las mismas.

El alcance de resultados depende en gran medida de la comunicación efectiva, desde el inicio al fin. Esto brindará garantías para el cumplimiento de objetivos, toma de decisiones, implementación del plan de tratamiento de riesgos, concientización, coordinación del personal y apoyo de las diversas áreas a partir de los cambios a realizar.

La organización puede valerse de métodos comunicacionales para la difusión efectiva de la gestión de riesgos, así como un comité de comunicación que pueda evaluar la información emitida por las partes interesadas con respecto a la gestión del riesgo.

6- Monitoreo y revisión del riesgo

Nada puede mejorarse sin conocer su estado a través del tiempo. Esto solo puede darse a partir del seguimiento y la supervisión de la puesta en marcha de los controles, lo cual generará las correcciones que fueran necesarias para su mejoramiento. La evaluación y la verificación del alcance de los objetivos propuestos no solo para la gestión de los riesgos sino para todo el sistema de gestión de la seguridad de la información, mediante el monitoreo y la revisión busca encontrar las carencias y problemas que podría tener el plan de tratamiento. Así como cambios que se presenten en el contexto, nuevas vulnerabilidades, cambios en la probabilidad de ocurrencia, consecuencias y amenazas en el transcurrir del tiempo. El seguimiento permite controlar la eficiencia y efectividad de las medidas tomadas para la mitigación del riesgo, el contexto del riesgo y la vigencia de los controles implementados.

Llevar a cabo el monitoreo generará nueva información valiosa para el ciclo de mejora continua del sistema de gestión de riesgo, y es parte integral de todo el modelo de trabajo. Es aplicable en todas las etapas y su intervención es esencial para prevenir, advertir y retroalimentar cada proceso. La dinámica propia de la entidad influye en este punto. El cambio de los objetivos o estrategia corporativa, la adquisición de nuevas compañías, la adopción de nuevas tecnologías, la adquisición y generación de nuevos activos, el cambio en las normativas y leyes amerita a que el monitoreo sea una labor continua.

De la mano del monitoreo y la revisión se encuentra la mejora continua. Es usual que el enfoque o los criterios de evaluación sean afectados por los cambios en los riesgos, haciendo necesario generar otro ciclo de análisis con los cambios necesarios, o bien cambios en la metodología de análisis, cambios en las herramientas y demás, aplicables al ciclo de gestión de riesgos. Un ratio de tiempo usual para la revisión es de un año.

7- Comparación de las Metodologías de Análisis de Riesgos CRAMM, MAGERIT y OCTAVE

A continuación se realizará una comparativa de las características más relevantes de las metodologías CRAMM, MAGERIT y OCTAVE, las cuales se encuentran descritas en el Anexo A de este documento, con el fin de validar la viabilidad de la aplicación a la gestión de riesgos de la seguridad de la información según la ISO/IEC 27005. En esta comparación se desea determinar a nivel general, la metodología con el enfoque más inclusivo y que permita un análisis y evaluación de los riesgos más fácil, eficiente y eficaz, a la hora de la aplicación en cualquier entidad. Se tendrán en cuenta temas como:

- Inventario de activos de información.
- Listado de amenazas y vulnerabilidades.
- Análisis de probabilidad de ocurrencia y consecuencia.
- Método de evaluación de riesgos.
- Lista de recomendaciones de controles y salvaguardas.
- Generación de plan de tratamiento de riesgo.

Para esta labor de análisis se realizará la validación del grado de compatibilidad entre los diferentes métodos de evaluación de riesgos y la ISO/IEC 27005, a partir de los siguientes parámetros:

Caracterización del sistema: Generación del inventario de los activos que van a ser objeto de análisis, su correspondiente valoración y el nivel de riesgo aceptable para dicho activo.

Evaluación de amenazas y vulnerabilidades: Listado de amenazas y vulnerabilidades referentes a los activos relevados.

Evaluación del riesgo: Cómputo del nivel de riesgo, ya sea cualitativo o cuantitativo a partir de la información relevada para poder determinar la consecuencia.

Generación de controles: Listado de controles acordes a los riesgos evaluados y que cumplan con la mitigación de los mismos para reducir su nivel y puedan ser aceptados por la organización.

Evaluación de controles sugeridos: Priorización de los controles acorde al análisis realizado y a la necesidad de la entidad que resulten de mayor beneficio para la entidad.

La siguiente tabla muestra de manera comparativa las tres metodologías descritas acorde a los parámetros establecidos anteriormente.

Metodología	CRAMM	MAGERIT	OCTAVE
Caracterización del sistema	Genera un listado de Activos.	Determina los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.	Determina cuáles son los activos críticos de la entidad y los controles o salvaguardas asociados a éstos. Posteriormente realiza un análisis y una evaluación organizacional
Evaluación de amenazas y vulnerabilidades	Realiza la evaluación de amenazas y vulnerabilidades relevadas.	Evalúa las amenazas y vulnerabilidades que exponen a los activos	Se realiza una valoración del estado actual de la infraestructura que soporta la información, empezando por el análisis de los principales componentes operacionales y las vulnerabilidades asociadas que puedan afectar a los activos
Evaluación del riesgo	Realiza la evaluación del riesgo en base a la información generada anteriormente	Realiza la evaluación de riesgos en todas las aristas que contextualizan al sistema, determina la probabilidad de ocurrencia y la consecuencia sobre los activos y generación del riesgo. Adicionalmente,	Realiza los cálculos referentes a la consecuencia en relación con las amenazas relevadas sobre los activos

Metodología	CRAMM	MAGERIT	OCTAVE
		brinda una serie de ejemplos de los errores más repetitivos y típicos en la implementación del análisis de riesgos.	
Generación de controles	Genera listado de salvaguardas	Provee la información necesaria para la toma de decisiones en pro de la mitigación de los riesgos por parte de la alta dirección a partir de la implementación de medidas de seguridad	Planes de implementación de controles y salvaguardas para la mitigación de los riesgos analizados
Evaluación de controles sugeridos	Genera recomendaciones de los controles a implementar en base a los datos evaluados	Genera un plan de establecimiento de salvaguardas acordes manteniendo el nivel de riesgo aceptable por la organización. Prioriza mediante los costos económicos, que facilita la toma de decisiones, y asegura la creación de una base fiable y verídica del porqué de la toma de decisión	Genera un plan de protección alineado al catálogo de prácticas relevadas y que deban mejorarse o las que se deberían implementar, genera acciones de corto, medio y largo plazo y prioriza la resolución de las vulnerabilidades que necesiten un tratamiento inmediato.

Tabla 1 - Fuente: Elaboración propia en base a información de las metodologías expuestas[1]

La siguiente tabla expone las ventajas y desventajas de las metodologías CRAMM, MAGERIT y OCTAVE.

Metodología	Ventajas	Desventajas
CRAMM	• Aplicable para cualquier entidad. • Corresponde correctamente con lo necesario para el análisis de riesgos. • Cuenta con un catálogo de activos, vulnerabilidades y amenazas. • Cuenta con una base amplia de salvaguardas y contramedidas sugeridas.	• Se limita únicamente a los elementos básicos para el análisis de riesgo. • No cuenta con la visibilidad suficiente para un análisis integral del riesgo en la seguridad de la información
MAGERIT	• Es clara en su formato y están fácilmente diferenciadas sus diversas etapas. • Describe actividades básicas del análisis y gestión de riesgos. • Diferencia y prioriza claramente todos los elementos que intervienen en el análisis de riesgos. • Cuenta con documentación suficiente y casos de éxito de la implementación de la metodología. • Cuenta con herramientas y software para la facilidad de la implementación de la metodología.	• No cuenta con la visibilidad suficiente para un análisis integral del riesgo en la seguridad de la información. • Su implementación es de un costo alto, a pesar de que la metodología es gratuita.

Metodología	Ventajas	Desventajas
OCTAVE	• Aplicable a cualquier entidad y de uso interno gratuito. • Clara categorización de los activos y fuertemente alineada con los objetivos estratégicos de la organización. • Genera concientización del personal sobre la seguridad de la información. • Análisis en detalle de los riesgos ocultos. • Amplia documentación para su implementación. • Generación de planes de tratamiento de riesgos a medida. • Brinda un estado de riesgo a partir de las vulnerabilidades relevadas. • Correlaciona todo los procesos y sus elementos.	• Depende de la disponibilidad de todo el personal. • Demandante de tiempo y conocimiento técnico. • Generación de carga laboral para los empleados a partir del proceso de la metodología

Tabla 2 - Fuente: Elaboración propia en base a información de las metodologías expuestas [2]

Cabe aclarar que este análisis es netamente descriptivo y basado en la documentación en la cual se sustenta este documento, por lo cual, un análisis más riguroso necesitará de métodos que puedan brindar resultados objetivos.

7- Implementación de las metodologías de riesgo según el estándar ISO/IEC 27005:2018

A partir de lo realizado en los capítulos anteriores, el haber descrito la norma ISO/IEC 27005 y las metodologías CRAMM, MAGERIT y OCTAVE, nos brinda el contexto y la información suficiente para poder seguir al próximo paso, ver la viabilidad y los retos que representa la implementación de las metodologías siguiendo el marco normativo de la ISO/IEC 27005.

Este estándar de buenas prácticas es muy claro y fácil de seguir y de acoplar con diversas metodologías. Al ser un proceso secuencial y claro en las definiciones de cada etapa, permite anticipar fácilmente el mapeo de la norma con las diferentes fases, procesos y procedimientos de cada metodología, en este aspecto lo primero que se debe tener en cuenta son los 7 aspectos de la ISO/IEC 27005 para la gestión del riesgo:

1. Establecimiento del contexto.
2. Identificación del riesgo.
3. Estimación del riesgo.
4. Evaluación del riesgo.
5. Tratamiento del riesgo.
6. Aceptación del riesgo.
7. Comunicación del riesgo.

Es fácil deducir cómo cada proceso de cada metodología se ubica en cada paso descrito por la norma, ya que cada metodología utiliza los conceptos y los términos definidos en ella. La diferencia radica en cómo lleva a cabo cada paso, a partir del enfoque que tiene cada metodología. Es decir, la metodología permite realizar un análisis de riesgos de seguridad de la información que, entre otras cosas, abarca toda la empresa, brinda más herramientas y métodos para las labores a ejecutar. Es posible ejecutar de manera más efectiva acciones tales como:

- Establecer la lista de activos relevantes.
- Identificación de amenazas.

- Identificación de vulnerabilidades.
- Cálculo del nivel de riesgo en base a las variables que lo determinan.
- Análisis de consecuencia si se produce la amenaza.
- Niveles de riesgo acordes al análisis realizado.
- Relevamiento de los controles y salvaguardas actuales.
- Listado de nuevas salvaguardas y controles a implementar a partir de lo relevado.
- Creación de plan de acción para mitigar el riesgo.

Cada metodología se vale de las normas ISO para marcar las pautas de su ejecución y estructura, estableciendo el ciclo de gestión de riesgos de la información. Sin embargo son fácilmente identificables ciertas etapas que componen el proceso.

Relevamiento de los activos de información: Esto refiere al proceso de identificación, categorización y valoración considerando los criterios asentados en las normativas ISO como los son la Disponibilidad, Integridad y Confidencialidad. Un claro ejemplo de esto fue descrito para las tres metodologías analizadas, CRAMM, MAGERIT y OCTAVE, así mismo analizan el proceso correcto de no repudio, gestión correcta de la autenticación y autorización.

Relevamiento de las amenazas: Para OCTAVE, se contempla este punto en el proceso número cuatro, llamado Creación de los Perfiles de Amenaza; CRAMM lo realiza en el proceso número dos, Clasificación de las amenazas y las vulnerabilidades y MAGERIT en su modelo de trabajo, descrito en el libro I - Método, donde hace referencia a la manera en que esta metodología determina a qué amenazas están expuestos los activos. Es decir, cada una de ellas procede de una forma diferente en este paso, sin embargo cumplen con la identificación de las amenazas existentes en el contexto de riesgo. Una de las diferencias más marcadas refiere a los criterios de valoración, ya sean cualitativos o cuantitativos.

Evaluación del Riesgo: El cómputo referente a la evaluación del riesgo puede ser uno de los ítems más marcados como diferencia. Sin embargo, cada método cumple con la valoración de la consecuencia en un activo

generado por una amenaza que explota las vulnerabilidades relevadas. Proceso usualmente apoyado en las herramientas y software de uso de cada metodología.

Lista de Salvaguardas: Como se vio anteriormente, cada metodología genera un listado de mecanismos de mitigación de los riesgos relevados. Estas salvaguardas y contramedidas están en línea con el anexo F de la ISO/IEC 27005, el cual especifica las restricciones para definir la modificación de los riesgos entre las que se encuentran las operativas, técnicas, culturales, éticas y legales.

Análisis del Riesgo Residual: Una vez aplicadas las contramedidas y salvaguardas sugeridas, se procede a la evaluación de riesgo remanente después de la mitigación. Se valida si se encuentra por debajo del nivel de riesgo aceptado, calculando la nueva consecuencia contra su mitigación. Como refiere la norma en el proceso de gestión de riesgo visto en el capítulo dos de este documento, cada metodología presenta un ciclo iterativo que se realiza hasta que el riesgo disminuya y sea aceptable para la organización.

En términos generales, la automatización de las metodologías permite reducir los tiempos de ejecución de las actividades requeridas para la gestión de riesgos y quizás lo más importante, minimizar los errores. Muchas metodologías hacen uso de software específico para esto, por ejemplo, CRAMM que es en sí mismo un software o MAGERIT que hace uso del software PILAR, acrónimo de “Procedimiento Informático-Lógico para el Análisis de Riesgos”. PILAR es una herramienta desarrollada por el Centro Criptológico Nacional (CCN) de España para realizar los procesos de gestión de riesgos aplicando la metodología MAGERIT.

Asimismo, cuentan con una serie de catálogos similares a los anexos que comprende el estándar, lo cual permite la correlación entre el estándar y las metodologías. Los catálogos más comunes son los de tipos de activos, vulnerabilidades y amenazas. Adicionalmente, permiten la actualización de estos catálogos y usualmente la adición manual de datos que no se encuentren definidos en ellos, así pueden ser usados acorde al contexto y al paso del tiempo.

Las fases o procesos de las metodologías mencionadas cumplen con la iteración continua del análisis del riesgo, la evaluación de los riesgos residuales después de la implementación de salvaguardas para poder asegurar la correcta mitigación, así como la mejora continua a partir de la evolución de la entidad, como lo especifica la norma.

Otro punto importante, entre los contemplados por la norma, es la generación de informes de tratamiento de riesgos, tema en el que las metodologías presentan la información de manera priorizada, lo cual facilita la toma de decisiones.

Después del análisis realizado sobre los modelos descritos se puede ver que las metodologías se encuentran altamente relacionadas con el proceso de gestión de riesgos, por lo cual su implementación encajada sobre el proceso de análisis y evaluación del riesgo cumple con lo requerido por la norma ISO/IEC 27005. Cada uno de los capítulos de la norma se asemeja a las diferentes fases o procedimientos de las metodologías, cumpliendo en diverso grado con los requerimientos propuestos y las salidas o resultados esperados.

La agrupación de los capítulos de la norma sobre cada metodología no impide el cumplimiento de la misma, por lo contrarío automatiza y optimiza las labores a desempeñar, los procedimientos que hacen al análisis de riesgos tienen un orden lógico y secuencial que caracteriza a la metodología.

Por último, se muestra un análisis comparativo entre la relación de las diferentes metodologías y los diferentes capítulos de la norma ISO/IEC 27005 para la gestión de riesgos. Se utiliza una convención de completo, alto, medio, bajo y nulo para expresar el grado de completitud con el que la metodología cumple con las pautas propuestas por la norma en cada uno de sus apartados:

		Metodología CRAMM						
ISO 27005: 2018		Caracterización del sistema	Evaluación de amenazas y vulnerabilidades	Evaluación del riesgo	Generación de controles	Evaluación de controles sugeridos	Seguimiento y Revision	Comunicación
	Establecer el contexto	Medio						
	Identificar los riesgos		Medio					
	Estimación del riesgo			Alto				
	Evaluacion del riesgo			Alto				
	Tratamiento del riesgo				Alto	Medio		
	Aceptación del riesgo				Alto	Medio		
	Seguimiento del riesgo						Bajo	
	Comunicación del riesgo							Bajo

Tabla 3 - Fuente: Elaboración propia, Relación de CRAMM con la ISO/IEC 27005:2018[3]

		Metodología MAGERIT						
ISO 27005: 2018		Caracterización del sistema	Evaluación de amenazas y vulnerabilidades	Evaluación del riesgo	Generación de controles	Evaluación de controles sugeridos	Seguimiento y Revision	Comunicación
	Establecer el contexto	Medio						
	Identificar los riesgos		Alto					
	Estimación del riesgo			Alto				
	Evaluacion del riesgo			Alto				
	Tratamiento del riesgo				Alto	Alto		
	Aceptación del riesgo				Alto	Alto		
	Seguimiento del riesgo						Medio	
	Comunicación del riesgo							Medio

Tabla 4 - Fuente: Elaboración propia, Relación de MAGERIT con la ISO/IEC 27005:2018[4]

		Metodología OCTAVE						
ISO 27005: 2018		Caracterización del sistema	Evaluación de amenazas y vulnerabilidades	Evaluación del riesgo	Generación de controles	Evaluación de controles sugeridos	Seguimiento y Revision	Comunicación
	Establecer el contexto	Completo						
	Identificar los riesgos		Completo					
	Estimación del riesgo			Alto				
	Evaluacion del riesgo			Alto				
	Tratamiento del riesgo				Alto	Alto		
	Aceptación del riesgo				Alto	Alto		
	Seguimiento del riesgo						Alto	
	Comunicación del riesgo							Medio

Tabla 5 - Fuente: Elaboración propia, Relación de OCTAVE con la ISO/IEC 27005:2018 [5]

Como se puede ver en las tablas anteriores, la que a consideración del análisis descriptivo de este documento tiene mayor compatibilidad con la

ISO/IEC 27005:2018 es la metodología OCTAVE, dado su método altamente alineado con las pautas de la norma y la gestión de cada una de sus fases para el alcance de los objetivos del análisis de riesgos.

8- Relación de la Norma ISO/IEC 27005:2018 con la norma ISO/IEC 27001:2013

La ISO/IEC 27001 brinda las definiciones básicas para el proceso del análisis de riesgos, lineamientos que se encuentran sugeridos en la familia de las normas ISO/IEC 27000. Es notable y evidente la importancia de llevar a cabo esta labor de manera consciente y detallada, ya que a partir de los resultados entregados por el análisis de riesgos se generará la plataforma del sistema de gestión de seguridad de la información. La validación de la probabilidad de fallas o incidentes que se puedan presentar en una compañía, ya sean internos o externos, genera un resultado que está orientado a definir a la correcta priorización de los hallazgos encontrados para su posterior tratamiento y obtener los medios adecuados para hacer frente a estos eventos.

En una manera resumida de simplificar el proceso de gestión de riesgos que cita la ISO/IEC 27001 brinda seis pasos para la evaluación del riesgo. A continuación se describen de forma breve cada una de estas etapas:

- **Metodología de evaluación de riesgos:** Como se ha expuesto en los apartados anteriores, en esta etapa se definen los tópicos necesarios para realizar y estandarizar dentro de la entidad la evaluación del riesgo, independientemente de cuál sea el objetivo a cubrir.

- **Implementación de evaluación del riesgo:** En esta parte se realiza el relevamiento de todos los eventos que pueden llegar a presentar a partir de las vulnerabilidades y amenazas relacionadas con los activos de información a evaluar, posteriormente se lleva a cabo el análisis de la relación entre la probabilidad de que suceda el evento descrito y la consecuencia que pueda tener sobre cada activo de información. Esta evaluación dará como resultado el nivel de riesgo para cada activo.

- **Implementación del tratamiento del riesgo:** A partir de los resultados obtenidos en el paso anterior y de la priorización de los riesgos encontrados, se inicia su tratamiento. La norma brinda cuatro posibilidades para la mitigación del riesgo, y brinda una serie de controles en sus diversos anexos. En un apartado posterior se ampliará esta información.

- **Reporte de evaluación del riesgo del Sistema de Gestión de Seguridad de la Información:** En este punto la norma enfoca sus esfuerzos en la correcta documentación de lo realizado anteriormente, buscando garantizar la correcta trazabilidad del proceso y los pasos siguientes a partir de los resultados obtenidos. Así mismo, esta información es un soporte para posibles auditorias y nuevos procesos de evaluación de riesgos.

- **Declaración de aplicabilidad:** La información aquí reportada es quizás lo que define la filosofía y postura de las organizaciones con respecto a sus riesgos, ya que en este documento se evidencia los controles implementados y exclusiones realizadas del anexo A de la ISO/IEC 27001 brindando la bitácora del tratamiento del riesgo. Como en el anterior ítem, este documento es una usual solicitud a la hora de afrontar una auditoria.

- **Plan para el tratamiento de riesgos:** A partir de aquí se procede con la implementación de los controles definidos anteriormente teniendo en cuenta ciertos puntos clave como el presupuesto con el que se cuenta, roles y responsables de la implementación, tiempos de ejecución, procesos de seguimiento a dicha implementación y más aplicables.

Como se puede deducir, la ISO/IEC 27005 es la base y sustentación de la ISO/IEC 27001, ya que los seis pasos señalados están especificados por el estándar. Cabe aclarar que la correlación entre estos estándares

permite llevar a cabo un proceso integral y transversal de la gestión de la seguridad de la información en cualquier entidad.

9- Conclusiones

En el desarrollo de este documento se muestra que el proceso de gestión de riesgos en general es tan complejo como la entidad en sí misma, por lo cual es imperativo hacer uso de metodologías que logren encausar y simplificar la labor. Las metodologías brindan un mayor cubrimiento del riesgo, asociado a la seguridad de la información, al hacer visible relaciones entre los diversos activos de la organización permitiendo así incrementar su protección. Asimismo, conforman una fuente de información para la definir acciones de mitigación de los riesgos a los que está expuesta la organización, lo cual redunda en aseguramiento de la información.

Conocer las características, fases, ventajas y desventajas asociadas a las metodologías de gestión de riesgos brinda la capacidad de seleccionar la que mejor se adecue a las necesidades de la entidad, para poder obtener el mayor éxito posible a la hora de su implementación.

Los costos relacionados, tanto de de implementación, software, personal a contratar para esta labor, mantenimiento del proceso y demás son menores, comparados con los beneficios otorgados. La gestión de riesgos para las organizaciones de hoy en día es una necesidad primaria para conocer no solo sus riesgos sino sus oportunidades, lo cual les permite ser más competitivos.

El creciente mundo corporativo y la propia globalización generan facilidades que conllevan riesgos con complejidades no vistas en otros tiempos. Por ello, el uso de una metodología de evaluación de riesgos, dado que permiten contar con pasos definidos en detalle, con documentación precisa, con softwares alineados, con listas de amenazas así como de controles, entre otras herramientas, facilitan el accionar de las organizaciones en cuanto a la toma de decisiones frente a entornos sumamente cambiantes.

El estándar ISO/IEC 27005:2018 establece un proceso de análisis y gestión de riesgo integral, sin dejar de lado los aspectos como la

comunicación, seguimiento y mejora continua. También permite la ampliación de su alcance en cada nueva iteración, la adición de otras áreas y procesos, transformándose así en una herramienta esencial para el sistema de gestión de riesgos de la entidad.

Es importante tener en cuenta que si bien el estándar es claro y específico y que además cuenta con una guía de implementación y resultados esperados, es más difícil llevar a cabo la gestión de riesgos sin hacer uso de las metodologías. Ello en razón de que el estándar se limita a describir los pasos y no brinda procedimientos específicos para las acciones a ejecutar. Esto le da sentido al uso de las metodologías analizadas, y a las demás que existen en el mercado, así como hace a la razón de ser de este trabajo de especialización.

10- Anexos

Anexo A

En este anexo se desarrollaran las metodologías para el análisis, evaluación y/o gestión de riesgos, comparadas en el documento principal. A continuación se describen y se detallan las metodologías usadas para este documento.

Hacer uso de una metodología para el análisis de riesgos permite llevar a cabo el procesamiento del gran volumen de información generado, de una manera ordenada y sistemática, buscando satisfacer los requerimientos, necesidades y limitaciones de la entidad en esta materia, y de que sus resultados conlleven a la preservación de la seguridad de manera integral. Asimismo, sugieren los controles que podrían mitigar los riesgos que deben ser tratados.

Mediante el uso de una metodología para el análisis de riesgo se brinda una perspectiva enfocada al alcance de los objetivos corporativos y los compromisos que afronta a nivel de seguridad de la información. El proceso sistemático que aporta una metodología evita pérdida de esfuerzo y optimización de recursos.

En el mercado existen varias metodologías para efectuar el análisis, evaluación y/o gestión de riesgos. A continuación se mencionarán las más notables en el área de la seguridad informática y por motivos de alcance de este documento, se analizaran en detalle solo tres de ellas. A continuación, un breve resumen de las herramientas y metodologías más relevantes:

- **CORAS:** Conocida como “Construct a Platformfor Risk Analysis of Security Critical System”, creada en el 2001 por el SINTEF, un grupo de investigación noruego financiado por organizaciones del sector público y privado. Iniciando en la confección de modelos, que consta de siete pasos, apoyados primordialmente en la realización de entrevistas con los expertos. Proporciona herramientas como un lenguaje de modelado

unificado, una gama de casos base reutilizables y otras herramientas más para la implementación de la metodología.

- **CiticusOne:** Herramienta de software comercial de la entidad Citicus, la cual hace uso de la metodología FIRM del Foro de Seguridad de la Información.
- **EBIOS:** Diseñada para la gestión de riesgos de seguridad de los sistemas de información, cuenta con cinco fases que responden a la necesidad del tratamiento de riesgos dando información relevante para la toma de decisiones que encausen la mitigación del riesgo, mediante la consideración de las salvaguardas existentes e integra la seguridad a los sistemas en funcionamiento. Por su flexibilidad, puede usarse en diversos procesos de seguridad de la información.
- **NIST SP 800-30: E**s una publicación del NIST y brinda las guías y criterios para realizar la evaluación del riesgo de la seguridad de la información en los sistemas y organizaciones del ámbito federal. Mediante tres niveles de la jerarquía de gestión de riesgos, la preparación de la evaluación, la generación y mantenimiento de la evaluación proporciona a las partes interesadas, directivos y ejecutivos, la información suficiente para la toma de decisiones y la ejecución de acciones necesarias para la mitigación de los riesgos identificados.
- **Mehari:** Creada por el CLUSIF (Club de la Sécurité de l'Information Français), proporciona una metodología para la evaluación de riesgos en el ámbito de la seguridad de la información acorde a la norma ISO/IEC 27005, brindando una serie de herramientas y elementos creados para la gestión de la seguridad en diferentes segmentos de tiempo y parametrizables según el nivel de madurez de la entidad.

A continuación se describirán en detalle, las metodologías comparadas en este trabajo, a saber: CRAMM, MAGERIT y OCTAVE.

Metodología CRAMM

El nombre de esta metodología es el acrónimo de “CCTA Risk Assessment and Management Methodology”. Fue adoptada por Siemens y desarrollada por el Central Communication and Telecommunication Agency

(CCTA) del Reino Unido. En su versión actual, la 5.2, esta metodología está orientada al aseguramiento de la triada de seguridad: integridad, confidencialidad y disponibilidad, mediante un proceso de tres fases en las cuales se establecen los objetivos, se realiza el relevamiento y valoración de los activos, el análisis de riesgos y la generación de controles efectivos. Se ejecutan en base a un proceso disciplinado y estructurado. Su proceso de evaluación es mixto, es decir, cuantitativo y cualitativo *[1]*. Una de sus grandes cualidades es la compatibilidad de muchas de sus herramientas con la ISO/IEC 27001 al tener por ejemplo, activos de modelado de dependencia, evaluación de las consecuencias a nivel empresarial, identificación y evaluación flexible de amenazas y vulnerabilidades, cálculo del nivel de riesgo e identificación y justificación de las salvaguardas y controles necesarios.

En su alcance de evaluación, este software no se limita solo a los aspectos técnicos de la entidad, sino también abarca aspectos de seguridad provenientes de fuentes físicas y humanas, brindando una evaluación cualitativa de estos temas. Debido a su concepto y bases, CRAMM puede aplicarse en cualquier momento dentro del ciclo de vida de los sistemas de información o avance de cualquier sistema de gestión de la seguridad de la información. Asimismo, a diversos entornos tecnológicos y entidades, comenzando con la necesidad de asegurar una infraestructura tecnológica hasta evaluar el nivel de madurez de la seguridad de la información de la entidad.

De una manera resumida, a partir de la definición de activos, amenazas, vulnerabilidades y consecuencias, esta metodología establece un valor a cada par de activo versus consecuencia. Posteriormente se correlacionan las tripletas amenazas-consecuencias-activos y se procede a la evaluación de las amenazas y vulnerabilidades generando un valor cualitativo, es decir bajo, medio o alto. Luego se computa y se genera el requerimiento de seguridad a partir del riesgo de cada una de las tripletas ya mencionadas.

El siguiente gráfico muestra la división del análisis y la gestión de riesgos:

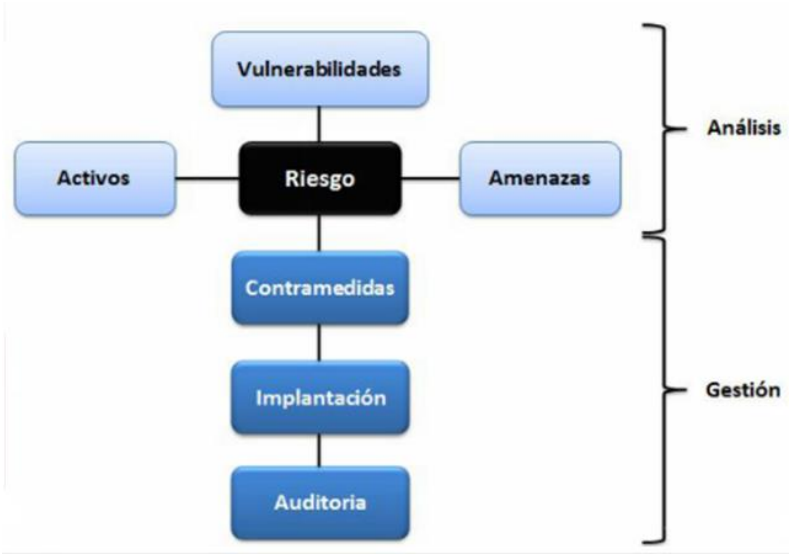

Ilustración 6: Modelo de Análisis Metodología CRAMM, Fuente: [15]

Para llevar a cabo esta labor, hace uso de tres fases de trabajo, las que se describen a continuación *[48]*.

Fase 1 – Evaluación del alcance de la seguridad - Esta fase consta de 3 etapas en las cuales se realiza el relevamiento y delimitación del alcance de la evaluación de riesgo.

Proceso1 – Preparación del Marco de Proyecto - Se realiza el relevamiento de las necesidades y objetivos del proyecto. Se hace uso de herramientas como entrevistas y reuniones con personal seleccionado previamente, para adquirir información relevante para el análisis a realizar. Se lleva a cabo la reunión de inicio del proyecto, donde se trabaja en la elaboración del detalle funcional de los sistemas de información que serán evaluados. Se acuerda el alcance y se relevan y documentan los activos físicos (hardware, comunicaciones, medio ambiente, software, documentación) y de datos (datos organizados interrelacionados); la estructura organizacional, la definición de roles y se identifican los usuarios de los datos. Se genera la documentación inicial y necesaria para el cronograma del proyecto.

Proceso 2 – Identificación y valoración de activos - En esta etapa, se realiza la categorización y valoración de los activos físicos así como de los datos comprendidos en el alcance. La valoración de los datos es más compleja que la de los activos físicos, ya que pueden tener diferente tipo de valor a partir del usuario que interactúa con ellos o de un periodo de tiempo específico. Una forma simplificada para conocer el valor de los datos es a partir de cuestionarios, en los cuales se definen los escenarios más adversos, y sin tener en cuenta los controles y salvaguardas existentes, el usuario realiza una valoración numérica a partir de una correlación de valor. En este paso se toma en cuenta temas como la transgresión de la privacidad personal, incumplimiento legal, pérdida económica, perdida de disponibilidad, la confidencialidad comercial, pérdida de imagen o problemas de seguridad personal. El resultado de este proceso es la generación de un resumen del valor de los activos. A posteriori se genera un informe para la gerencia en la cual se identifica la contextualización de la entidad, conocimiento de la misma y el inventario de activos con su respectivo valor.

Proceso 3 – Revisión de la valoración de los datos - Este paso se realiza solo si los resultados obtenidos en el paso anterior no se corresponden con la realidad

En esta primera fase se generan los siguientes resultados:

- Definición de objetivos, alcance, roles y conocimiento de la entidad.
- Inventario de activos y su valoración.
- Informe CRAMM para la dirección con la recopilación de la información.

Fase 2 – Evaluación de riesgos - En esta fase, se procede con el relevamiento de amenazas y vulnerabilidades para cada activo, así como con la definición de la relación entre amenazas, activos y consecuencias.

Proceso1 – Identificación de amenazas, activos y consecuencias - Se identifican amenazas en relación a los activos y se definen las consecuencias que se pueden presentar. CRAMM cuenta con treinta y un

amenazas genéricas que cubren todas las que podrían surgir de eventos por conducta maliciosa.

Proceso 2 – Clasificación de amenazas y vulnerabilidades - La clasificación de amenaza refleja la probabilidad de que ocurra una amenaza y tiene en cuenta si la amenaza ha sucedido en el pasado y quién está interesado en los activos involucrados. Para la clasificación de vulnerabilidad evalúa si el sistema de información aumenta la probabilidad de ocurrencia de amenaza dada y si su propia arquitectura y diseño permiten un daño mayor.

Proceso 3 – Generación de los requerimientos de seguridad - Mediante una matriz de búsqueda tridimensional, se generan los requerimientos de seguridad a partir de las diversas combinaciones dadas por los ejes de clasificación definidos anteriormente. Dicha matriz maneja un sistema de valoración que comprende una escala del 1 al 5 y generan los requisitos para cada combinación de amenaza-consecuencia-activo donde 1 refiere a la línea valor mínimo de exigencia de seguridad y el 5 genera un requisito de seguridad muy alto.

Proceso 4 – Verificación de los requisitos de seguridad - una vez generados los requisitos de seguridad con su respectivo valor, se verifican para evitar errores, los cuales se traducirían en costos innecesarios o por lo contrario, dejarían el sistema sin controles acordes al valor de sus activos, siempre teniendo en cuenta la relación costo y el apetito de riesgo de la entidad.

Una vez culminada esta fase, los resultados obtenidos serán:

- Lista de las amenazas, activos y consecuencias.
- Clasificación de las amenazas y las vulnerabilidades.
- Lista de los requerimientos de seguridad.

Fase 3 – Generación de controles y salvaguardas - A partir del análisis de riesgos, CRAMM genera las salvaguardas correspondientes a cada sistema en los que se necesite satisfacer los requisitos de seguridad y

los riesgos relevados. Estos resultados se comparan con los controles actuales.

Proceso 1 – Identificación de las salvaguardas necesarias - Haciendo uso del requerimiento de seguridad, se generan las contramedidas aplicables y un perfil de seguridad recomendado para poder elegir los controles que mitiguen el nivel de riesgo. Este software cuenta con cincuenta y tres grupos de salvaguardas, agrupados por su potencia, costo, aspecto de seguridad (hardware, software, comunicaciones, procedimiento, físico, personal, medio ambiente) y tipo de subgrupo (para reducir la amenaza, reducir la vulnerabilidad, reducir la consecuencia, detectar y recuperar), cuenta con aproximadamente 3000 salvaguardas.

Proceso 2 – Comparación de los controles existentes versus los sugeridos - Se realiza la comparación entre los existentes y los sugeridos por la herramienta como consecuencia del análisis realizado, permitiendo así identificar los controles que es necesario implementar.

Proceso 3 – Generación del informe - En este último paso, se generan las recomendaciones y se analiza con la dirección los resultados obtenidos y las nuevas salvaguardas sugeridas.

Los resultados de esta tercera fase son:

- Lista de salvaguardas necesarias.
- Comparativo entre las salvaguardas existentes y los sugeridas.
- Informe de análisis de riesgos.
- Evaluación de resultados con la dirección.

En una vista procedimental, CRAMM realiza las siguientes actividades para el análisis y gestión de riesgos:

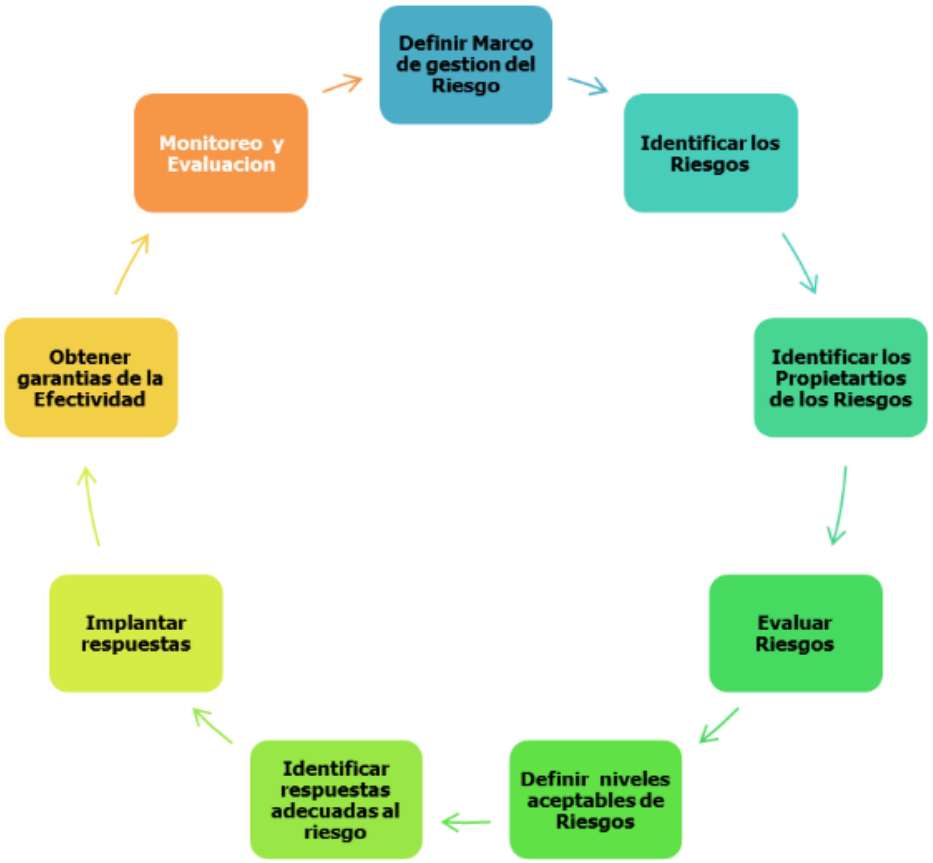

Ilustración 7: Ciclo de actividades de CRAMM. Fuente: [15]

Al relacionar la metodología con lo expresado por la ISO/IEC 27005 es posible observar que contempla todas las etapas indicadas por el estándar, por lo cual hace muy fácil su mapeo e implementación. Al hacer uso de un proceso simple y sistematizado, facilita la labor de los analistas a la hora de llevar a cabo cada una de las actividades.

En resumen, esta metodología en su primera etapa, puede plantear una serie de problemas, como el largo período de tiempo que se tarda en completar. Además, puede producirse una mala agrupación de los datos si los entrevistados o el entrevistador no son los adecuados. La primera etapa también puede estar atascada en detalles inútiles o los períodos de indisponibilidad pueden ser incorrectos.

Los problemas impuestos por la segunda etapa son generados principalmente por el hecho de que hay demasiadas preguntas que hacer (aproximadamente 600). Hace el proceso dispendioso, adicionalmente,

muchas veces las respuestas no son objetivas, por lo cual deben repetirse las entrevistas.

Los problemas que se tienen con la tercera etapa son la dificultad en la identificación de las contramedidas ya instaladas. Esto debido a que el conocimiento de los entrevistados es a veces inadecuado, o las contramedidas no están realmente instaladas.

La escala de tiempo típica para un ciclo CRAMM va de seis días para un sistema pequeño (un ordenador, una aplicación), a diecisiete días para un sistema mediano (un mini ordenador, varias aplicaciones), a treinta días para un sistema grande (un mainframe con sitios en varias ubicaciones geográficas).

Un problema común con CRAMM, es que requiere conocimiento experto, los entrevistados correctos y conseguir el equilibrio correcto entre coste y riesgo. No tiene en cuenta la política de seguridad de una empresa, los productos existentes y el coste de los productos, ni la cultura organizativa de la empresa. Por otro lado, CRAMM es una metodología rigurosa, es aplicable a la mayoría de los sistemas, se actualiza regularmente y cuenta con una base de datos de contramedidas de gran calidad *[1]*.

Metodología MAGERIT

MAGERIT es el acrónimo de Metodología de Análisis y Gestión de Riesgos de la Tecnología de Información, creada por el Consejo Superior de Administración Electrónica del gobierno de España. Dada la necesidad creciente de utilizar las tecnologías de información, busca determinar y minimizar los riesgos a partir de la evaluación de riesgos y de la definición de medidas de seguridad para minimizarlos.

Su primera versión es de 1997 y la última, 3.0, data del 2012, la cual es hoy en día ampliamente usada en diversos campos de la seguridad de la información, debido a su concepto sencillo pero eficaz a la hora de generar los requisitos mínimos para la protección de la información. Esta metodología hace referencia a la seguridad como “la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de

confianza, los accidentes o acciones ilícitas o mal intencionadas que comprometen la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles". Sus objetivos son los siguientes *[23]*:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos.
4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Permite analizar los riesgos que se relacionan con cualquier sistema de información, el ambiente en el cual se desarrolla y las posibles consecuencias a partir de la materialización de los riesgos en estudio. Su resultado es una serie de controles y salvaguardas a medida que brindan conocimiento, prevención, seguimiento, reducción o mitigación de los riesgos investigados. MAGERIT hace uso de los siguientes elementos para la evaluación de los riesgos:

- Activos
- Amenazas
- Vulnerabilidades
- Consecuencias
- Riesgos
- Salvaguardas, ya sean funciones, servicios o mecanismos.

A continuación se muestra la relación entre los mencionados elementos:

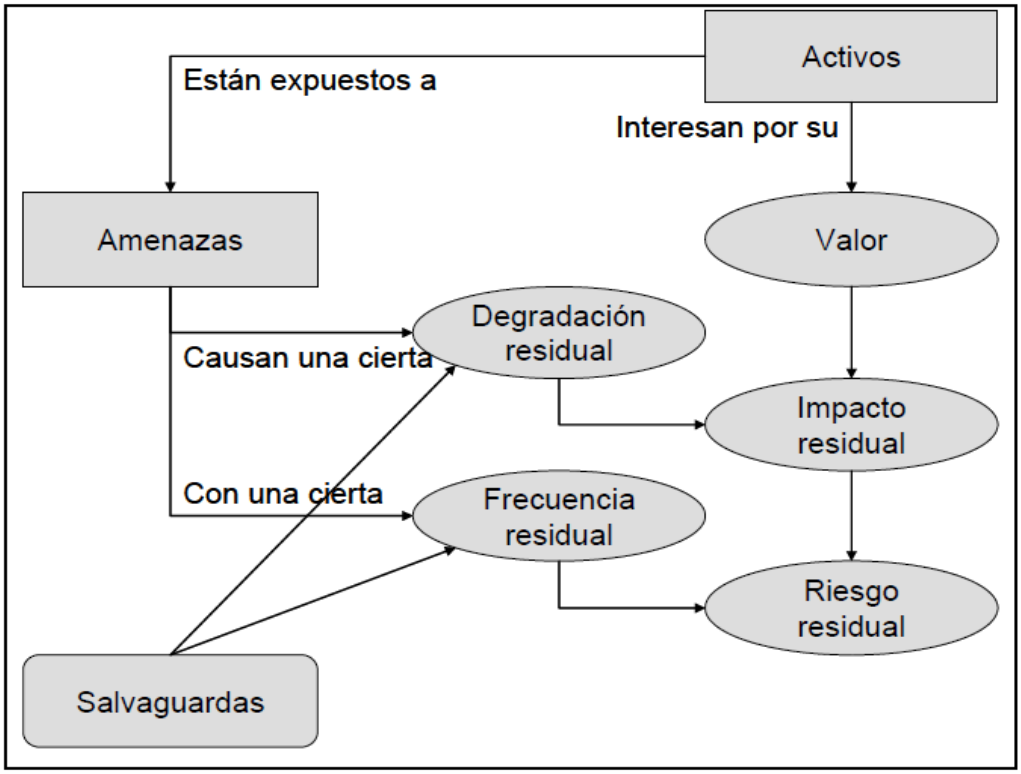

Ilustración 8: Modelo de Análisis Metodología MAGERIT, Fuente: [32]

Como se puede ver en la ilustración anterior, de la correlación de los activos y su valor, su exposición a las amenazas que generan una degradación acorde a la frecuencia de ocurrencia, concibe un riesgo y una consecuencia en el valor del activo. Esto a su vez debe ser minimizado mediante salvaguardas que puedan reducir los mencionados consecuencia y el riesgo.

Dada esta relación, la metodología establece las siguientes etapas para lograr sus objetivos.

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar la consecuencia, definido como el daño sobre el activo derivado de la materialización de la amenaza.

5. Estimar el riesgo, definido como la consecuencia ponderada por la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

En uno de los tres volúmenes que conforman la documentación, denominado MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I - Método (capítulo 7 titulado “Desarrollo de sistemas de información”) describe la metodología para los sistemas de información, teniendo en cuenta a la seguridad como un proceso integral formado por todos los partícipes técnicos, humanos y organizativos, que interactúen con los mencionados sistemas. Se enfoca en la concienciación de las personas y en la definición de los procesos para, mediante esta vía, evitar que el desconocimiento, o falta de organización y coordinación, así como instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

En este capítulo, MAGERIT, sustenta a la gestión de riesgos como la base y parte fundamental del proceso de aseguramiento de cualquier sistema, a partir de un estudio consiente, de alto grado de detalle, con una documentación y actualización continua para lograr el sostenimiento de un ambiente controlado, disminuyendo los riesgos hasta niveles aceptables por la organización. Como Proceso de Gestión de Riesgos, MAGERIT provee la información necesaria para la toma de decisiones por parte de la alta dirección en el marco del uso las tecnologías de información y de manera de hacer posible la reducción de los niveles de riesgo a partir de la implementación de medidas de seguridad, que brinden un equilibrio entre el tipo de datos, los procesos que los manipulan, los riesgos a los que estén expuestos y las salvaguardas existentes. Las medidas de seguridad se revalúan y actualizan periódicamente, para adecuar su eficacia a la constante evolución del entorno, de los riesgos y los nuevos sistemas de protección, y de ser necesario a replantear la seguridad. Este análisis constante provee una serie de información práctica procedente de la experiencia obtenida en el proceso y acumulada en el tiempo para el análisis y gestión del riesgo de manera mucho más efectiva.

Como se citó inicialmente, MAGERIT cuenta con 3 documentos que describen todos los aspectos y herramientas que usa para el análisis de riesgo, de manera detallada y su versión original es en español, lo cual es una ventaja. El contenido de estos documentos esta agrupado por Volúmenes de la siguiente manera:

Volumen I – Método *[23]*: Descripción de la metodología: en sus diferentes capítulos define los actores de la gestión de riesgos, explica los pasos a seguir para una gestión integral de riesgos, brinda una serie de proyectos de análisis de riesgos donde se identifican las diferentes etapas e iteraciones acorde a diferentes escenarios, lo cual conlleva a diferentes tomas de decisiones en todo el ciclo de la gestión de riesgos. Genera la introducción para la creación y gestión del plan estratégico de seguridad, también llamado plan director.

En este volumen se aborda el desarrollo del análisis de riesgos en entornos de sistemas de información en todas las fases del ciclo de vida del desarrollo seguro. Brinda, además, una serie de ejemplos de los errores típicos en la implementación del análisis de riesgos. Contiene información sobre el marco legal que envuelve el análisis y gestión en la Administración Pública Española y sobre las características y funcionalidades que se requieren para las herramientas en las cuales soporta el proceso de análisis y gestión de riesgos.

Volumen II – Catálogo de Elementos *[24]*: Referencia y complementa el volumen anterior a partir del inventario de diversos elementos que usa la metodología como los siguientes:

- Tipos de activos.
- Dimensiones de valoración de los activos.
- Criterios de valoración de los activos.
- Amenazas típicas sobre los sistemas de información.
- Salvaguardas a considerar para proteger los sistemas de información.

Mediante estos catálogos ayuda a la implementación de la metodología en un proyecto dado, ya que define los objetos típicos de análisis que interactúan en un contexto puntual. Asimismo estandariza los

términos, lo cual permite una lectura fácil, así como comparar los resultados entre diferentes análisis realizados. Otra característica que se resalta es la notación XML, lo cual le permite compatibilidad con diversas herramientas de gestión, de manera tal que el catálogo de elementos empleados pueda ser usado por estas herramientas.

Volumen III – Guía de Técnicas *[25]*: Proporciona una lista de técnicas que se pueden usar en las distintas etapas del análisis de riesgos. La idea de esta información es dar una guía para el despliegue del proyecto. Algunas de las técnicas que contiene son las siguientes:

- Técnicas Específicas.
  - ✓ Análisis mediante tablas.
  - ✓ Análisis algorítmico.
  - ✓ Árboles de ataque.

- Técnicas Generales.
  - ✓ Técnicas gráficas.
  - ✓ Sesiones de trabajo: entrevistas, reuniones y presentaciones.
  - ✓ Valoración Delphi.
  - ✓ Diagrama de procesos.
  - ✓ Diagrama de flujos de datos.
  - ✓ Análisis de Coste-Beneficio.
  - ✓ Administración de Proyectos.

A partir de sus múltiples técnicas de análisis, acoplamiento con la gestión de riesgos e independientemente del grado de madurez que manifieste la organización, MAGERIT permite, mediante la visión global y estratégica del análisis de riesgos, una rápida implementación acorde a los pasos definidos por la metodología, con sus resultados expresados en costos económicos. Su modelo de fácil implementación permite tener resultados confiables y oportunos, priorizando la planificación en el establecimiento de salvaguardas acordes manteniendo el nivel de riesgo aceptable por la organización y cumpliendo con los compromisos normativos de certificación y de auditoría. En este marco se hace sencillo su

incorporación en cualquier sistema de gestión de la seguridad de la información.

Teniendo en cuenta lo anterior, MAGERIT es una metodología apropiada para las entidades que estén iniciando su sistema de gestión de seguridad de la información ya que encamina los recursos y esfuerzos mediante la priorización de la resolución de los riesgos con mayor criticidad y al estar en línea con los estándares de la ISO/IEC 27001, se adecua perfectamente con su ciclo de mejora continua.

Metodología OCTAVE

OCTAVE es un acrónimo de “Operationally Critical Threat, Asset, and Vulnerability Evaluation”. A partir de la evaluación y la gestión de riesgos genera los cimientos para responder a la necesidad de la seguridad de los sistemas de información, teniendo en cuenta los aspectos organizacionales y tecnológicos. Esta metodología fue desarrollada por la Carnegie Mellon University *[42]*.

Cuenta con las siguientes versiones:

- OCTAVE, versión original.
- OCTAVE-S, versión enfocada en las pequeñas empresas.
- OCTAVE-ALLEGRO, versión simplificada.

El enfoque de esta metodología es la priorización de la relación costo – beneficio para la implementación de los planes de gestión de riesgos, la creación de una estrategia de protección, planes de mitigación y diseño de políticas de seguridad. Caracterizada por ser flexible, auto-dirigida y enfocada al estudio de la infraestructura de la información, se diferencia de los tradicionales análisis de riesgos que se enfocan en la tecnología. Sus objetivos son la comprensión de la gestión de los activos, para lo cual plantea un proceso de relevamiento y valoración de los riesgos que afectan la seguridad y que deberá ser realizado por personal relacionado con tecnologías de la información. Hace uso de entrevistas y encuestas para la identificación de los recursos importantes de la compañía. Esta labor inicia con la identificación de los requisitos de seguridad de la información

ponderando un valor del nivel de riesgo de la entidad. Esto se realiza a partir de la identificación y evaluación de los riesgos mediante la tipificación de los activos relevantes para la misión y alcance de los objetivos de la entidad, el relevamiento de las vulnerabilidades y amenazas que impactan a los activos y los criterios cualitativos que permitan describir el riesgo en función del negocio, lo cual permite establecer las posibles consecuencias.

Una de las características más relevantes de OCTAVE, es su enfoque basado no solo en el riesgo tecnológico, sino también en el organizacional. Esto hace que se deba generar un trabajo conjunto con el personal que trabaja en las diferentes áreas de la entidad y se cuente con un conocimiento multidisciplinario.

La metodología define tres fases, las que a su vez tienen una serie de procesos para abarcar no solo los riesgos tecnológicos sino también los de origen organizacional. A continuación, su descripción *[19]*:

- **Visión organizativa:** En este punto se relevan los activos, vulnerabilidades organizativas, amenazas, requerimientos de seguridad y normativas existentes.
- **Visión tecnológica:** Los elementos anteriormente relevados se catalogan en vulnerabilidades técnicas y componentes claves.
- **Estrategia y desarrollo del plan:** En esta fase se realiza la evaluación de los riesgos, se crean los planes y estrategias de protección, valoración de los riesgos y proceso de planificación para mitigación de los riesgos.

Su correlación se puede ver en el siguiente gráfico.

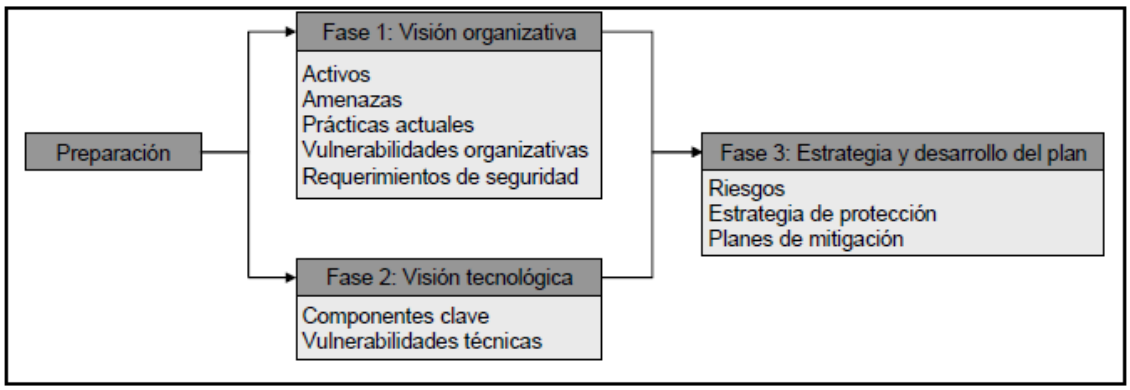

Ilustración 9: Fases de Desarrollo de la Metodología OCTAVE, Fuente: [35]

Estas fases se componen de ocho pasos en total, en los que se detalla el procedimiento a llevar a cabo para cumplir con los objetivos de OCTAVE. Cada una de estas actividades genera resultados que son prerrequisitos de las siguientes, conformando un proceso. A continuación se muestra el modelo de trabajo y sus resultados por fase:

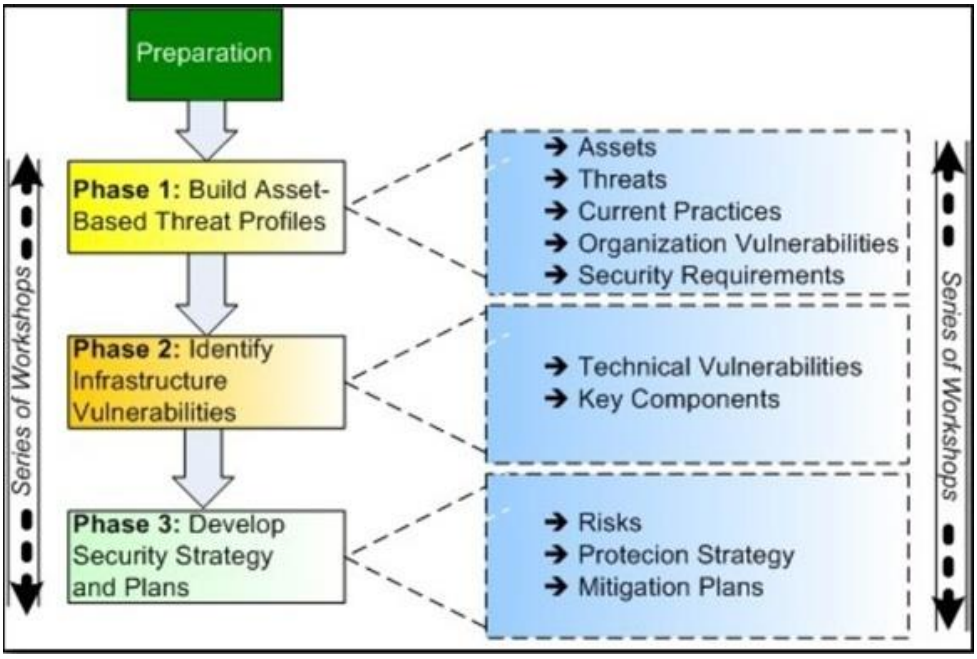

Ilustración 10: Modelo de Trabajo de OCTAVE, Fuente: [33]

A continuación se describen dichas fases y los procesos de OCTAVE *[40]*:

Fase 1 - Creación De Los Perfiles De Activos Basados En La Amenaza - A partir de la recopilación de información en los diversos niveles de la organización, se determina cuáles son los activos críticos de la entidad y los controles o salvaguardas asociados a éstos. Posteriormente se realiza un análisis y una evaluación organizacional. Esta fase está conformado por 4 procesos.

Proceso 1 - Conocimiento de la Dirección - Los gerentes deben identificar y definir los elementos de mayor valor para la organización y realizar la priorización correspondiente, informando los posibles escenarios de amenaza para estos activos. Esto creará una primera definición de los requerimientos de seguridad para su protección, los cuales se contrastarán con la identificación de las vulnerabilidades organizacionales y las

estrategias existentes de protección. Este proceso usualmente se lleva a cabo mediante encuestas y sus resultados se debaten para determinar el estado de la organización a nivel de la seguridad de la información. Su resultado es el alcance operacional que tendrá el análisis de riesgo.

Proceso 2 - Identificación Del Conocimiento De La Gestión Operativa - Para este proceso se evalúa el conocimiento que tienen los líderes de las áreas operacionales acorde al alcance determinado, buscando una visión transversal de la organización. Igual que en el proceso anterior, se determinan los activos más relevantes y su respectiva priorización, los posibles escenarios en los cuales podrían ser afectados y los requerimientos necesarios para asegurar los activos a partir de las amenazas relevadas. Se identifican los métodos actuales de protección y las vulnerabilidades de la organización en el ámbito operativo y las oportunidades de mejora en esta materia.

Proceso 3 – Relevamiento del Conocimiento del Personal de las Áreas Operativas y de las Tecnologías de Información - Identifica los conocimientos del personal operativo y de TI, bajo el mismo proceso de trabajo: identificación de activos, su priorización, descripción de los escenarios en los cuales los activos podrían ser amenazados, generación de los requerimientos de seguridad, relevamiento de las estrategias de protección y vulnerabilidades asociadas a la organización. En este proceso, el personal de Tecnología de Información cumple un rol diferencial e importante al definir los pasos anteriores en el marco de los activos que permiten desarrollar su trabajo, por lo cual el proceso desarrollado es diferente en relación con los demás roles en la organización.

Proceso 4 - Creación de los Perfiles de Amenaza - A partir de la información recopilada en los procesos anteriores, se crean los perfiles de amenaza y se expanden en relación a los activos críticos de la entidad realizando una labor de depuración y afinamiento de la información para definir la estructura de activo, vulnerabilidad, amenaza, escenarios, medidas actuales de protección y requerimientos de seguridad.

A partir de estos cuatro primeros procesos que conforman la fase uno, se generan los siguientes resultados:

- Identificación del conocimiento de la Gerencia
- Identificación del conocimiento de los líderes de las áreas operativas.
- Identificación del conocimiento del personal operativo y de TI.
- Creación de los perfiles de amenaza.

Fase 2 - Identificación de las Vulnerabilidades de la Infraestructura - Se realiza una valoración del estado de la infraestructura que soporta la información, empezando por el análisis de los principales componentes operacionales y las vulnerabilidades asociadas. Cuenta con dos procesos asociados.

Proceso 5 – Identificación de los Componentes Clave - Se realiza el relevamiento de los elementos clave de la infraestructura tecnológica tales como firewalls, servidores físicos y virtualizados, switches, routers, sistemas de respaldo y almacenamiento de información, balanceadores de carga, entre otros. Se analizan los caminos posibles para llegar al activo identificando aquellos que podrían permitir un acceso no autorizado.

Proceso 6 – Evaluación de los Componentes Seleccionados - Una vez relevados todos los componentes, se procede a su evaluación, identificando las vulnerabilidades asociadas. Es una actividad netamente técnica y podría ser subcontratada.

En esta fase se generan los siguientes resultados:

- Identificación de componentes clave.
- Evaluación de los componentes clave.

Fase 3 - Estrategia y Plan de Desarrollo - Con la información recopilada en los pasos anteriores, se procede a identificar los riesgos asociados a los activos críticos y a definir los mecanismos de protección con sus respectivos planes.

Proceso 7 - Análisis de Conducta de Riesgo - Se realiza los cálculos referentes a las consecuencias en relación con las amenazas relevadas sobre los activos. Para esta tarea se establecen los criterios de evaluación y se genera el perfil de riesgo por cada activo. Con base en los perfiles de amenaza, se relevan los riesgos y se calcula la consecuencia acorde al criterio mencionado anteriormente, usualmente de forma cualitativa, es decir, bajo, medio y alto. Los mencionados criterios podrían basarse en aspectos tales como pérdidas económicas, afectación de la producción, daño de la imagen, consecuencias que afecten al personal.

Proceso 8 - Creación de Estrategias de Protección - En este paso se desarrolla los planes de implementación de controles y salvaguardas para la mitigación de los riesgos analizados, los cuales deben ser revisados y aprobados por la alta dirección. Para ello se debe compilar los resultados y el material usado para el relevamiento de la información, revisar lo relevado y los resultados obtenidos en cada una de las etapas anteriores, con especial atención a los activos, vulnerabilidades, amenazas, riesgos y prácticas empleadas. Con esta información se lleva a cabo la creación del plan de protección alineado al catálogo de prácticas relevadas, enfocándose en las que deban ser mejoradas o implementadas. Esto generará una serie de acciones de corto, medio y largo plazo con especial enfoque en la resolución de las vulnerabilidades que necesiten un tratamiento inmediato.

Los resultados obtenidos en esta fase deberán ser los siguientes:

- Análisis de los riesgos.
- Diseño de la estrategia de protección.

La implementación de OCTAVE genera resultados como la identificación de los riesgos de seguridad que atenten contra el objetivo de la entidad, la evaluación de riesgos, la generación de la estrategia para el tratamiento del riesgo estando en línea con los objetivos de la entidad y el cumplimiento de la normativa vigente que aplique para cada organización.

OCTAVE es una metodología que hace partícipe a todo el personal en todos sus niveles, lo cual genera concientización y conocimiento de los riesgos de seguridad de la información que atañen a la entidad y permite

generar resultados a corto plazo sin dejar al lado el grado de detalle necesario para la gestión de riesgos. Su método es sencillo y explicito y se adapta perfectamente para la implementación de la ISO/IEC 27005.

11- Bibliografía Específica

[1] (ENISA), T. E. (2019). *CRAMM (CCTA Risk Analysis and Management Method)*. Recuperado el 14 de Marzo de 2019, de Threat and Risk Management, CRAMM: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html

[2] (ENISA), T. E. (2019). *Inventory of Risk Management / Risk Assessment Methods and Tools.* Recuperado el 11 de Marzo de 2019, de (ENISA), The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory

[3] (ENISA), T. E. (2019). *Octave v2.0 (and Octave-S v1.0 for Small and Medium Businesses), Carnegie Mellon University, SEI (Software Engineering Institute)*. Recuperado el 12 de Marzo de 2019, de (ENISA), The European Union Agency for Cybersecurity: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html

[4] (ICONTEC), I. C. (2009). Compendio, sistema de gestión de seguridad de la información (SGSI). *ICONTEC, Compendio, sistema de gestión de seguridad de la información (SGSI)*. Bogota, Cundinamarca, Colombia: (ICONTEC), Instituto Colombiano de Normas Técnicas y Certificación.

[5] (ISO), O. I. (11 de Febrero de 2019). ISO Guide 73:2009. *Risk management - Vocabulary*.

[6] (ISO), O. I. (6 de Febrero de 2019). ISO/IEC 27000:2018. *Information technology - Security techniques - Information security management systems - Overview and vocabulary*.

[7] (ISO), O. I. (22 de Febrero de 2019). ISO/IEC 27001:2013. *Information technology - Security techniques - Information security management systems - Requirements*.

[8] (ISO), O. I. (20 de Marzo de 2019). ISO/IEC 27002:2013. *Information technology - Security techniques - Code of practice for information security controls*.

[9] (ISO), O. I. (2 de Febrero de 2019). ISO/IEC 27005:2018. *Information Technology - Security Techniques - Information Security Risk Management*.

[10] (ISO), O. I. (3 de Marzo de 2019). ISO/IEC 31000:2018. *Risk management - Guidelines*.

[11] (ITU), I. T. (2014). *Global Cybersecurity Index*. Recuperado el 16 de Agosto de 2019, de www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

[12] (MINTIC), M. d. (15 de Marzo de 2016). *Metodología de Gestión de Activos de Información.* Recuperado el 4 de 02 de 2019, de Ministerio de Tecnologías de la Información y las Comunicaciones: http://ticbogota.gov.co/sites/default/files/documentos/Gestio%CC%81n%20Activos-Riesgos%20Diciembre.pdf

[13] (NIST), N. I. (Marzo de 2011). *SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View.* Recuperado el 14 de Marzo de 2019, de Computer Security Resource Center, Documentations: https://csrc.nist.gov/publications/detail/sp/800-39/final

[14] (NIST), N. I. (Septiembre de 2012). *SP 800-30 Rev. 1, Guide for Conducting Risk Assessments.* Recuperado el 11 de Marzo de 2019, de Computer Security Resource Center, Documentations: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[15] (UNAD), U. N. (22 de Marzo de 2014). *Metodologias De Evaluacion De Riesgos Informaticos*. Recuperado el 19 de Febrero de 2019, de Blog, Riesgos - Universidad Nacional Abierta y a Distancia : http://riesgosunad.blogspot.com/

[16] Agustín López Neira, J. R. (2012). *iso27000.es*. Recuperado el 16 de Febrero de 2019, de El portal de ISO 27001 en Español: http://www.iso27000.es/glosario.html

[17] Agustín López Neira, J. R. (2012). *Sistema de Gestion de Seguridad de la Información*. Recuperado el 14 de Febrero de 2019, de El portal de ISO 27001 en Español: http://www.iso27000.es/sgsi.html

[18] Alliance, C. (2 de Junio de 2014). *Citicus ONE vR.4.0*. Recuperado el 10 de Marzo de 2019, de CyberRisk Alliance: https://www.scmagazine.com/review/citicus-one-vr-4-0/

[19] Christopher J. Alberts, A. J. (Diciembre de 2001). *OCTAVE Criteria, Version 2.0.* Recuperado el 11 de Marzo de 2019, de Software Engineering Institute, Carnegie Mellon University: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2001_005_001_13871.pdf

[20] Colombia, M. d. (15 de 03 de 2016). *Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).* Recuperado el 23 de 02 de 2019, de https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

[21] Colombia, M. d. (1 de Febrero de 2019). *Ministerio de Tecnologías de información y comunicaciones de Colombia*. Recuperado el 2 de Abril de 2019, de https://www.mintic.gov.co/

[22] Deniz Tunçalp, D. o. (2014). *Diffusion and Adoption of Information Security Management Standards.* Istanbul, Turkey: Routledge, Taylor & Francis Group .

[23] Dirección General de Modernización Administrativa, P. e. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de*

los Sistemas de Información. Libro I - Método. Madrid: Ministerio de Hacienda y Administraciones Públicas.

[24] Dirección General de Modernización Administrativa, P. e. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

[25] Dirección General de Modernización Administrativa, P. e. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

[26] Edo, J. (8 de Diciembre de 2016). Integración entre la ISO 27001 y la Certificación en Continuidad de Negocio ISO 22301. Valencia, España: Mobiliza Academy.

[27] Electrónica, C. S. (1 de Noviembre de 2017). *Portal de Administración Electrónica Ministerio de Política Territorial y Función Pública Secretaría General de Administración Digital*. Recuperado el 15 de Marzo de 2019, de MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XcsyuEZKjIU

[28] Eric Lachapelle, F. R. (14 de Octubre de 2015). *Risk Assessment with OCTAVE, Information Security Management*. Recuperado el 11 de Marzo de 2019, de Information Security Management, PECB: https://pecb.com/whitepaper/risk-assessment-with-octave

[29] Francisco Nicolás Javier Solarte Solarte, E. R. (Diciembte de 2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL – RTE, Vol. 28, N. 5, 492-507*. Pasto, Nariño, Colombia: (UNAD), Universidad Nacional Abierta y a Distancia .

[30] Fray, I. (Septiembre de 2012). A Comparative Study of Risk Assessment Methods, MEHARI & CRAMM with a New Formal Model of Risk Assessment (FoMRA) in Information Systems. *11th International Conference on Computer Information Systems and Industrial Management (CISIM)* (págs. 428-442). Venecia: Italia.

[31] Gomez, J. (24 de Abril de 2012). *La Seguridad y la Confidencialidad de la Información es Obligación de Todos*. Recuperado el 12 de Abril de 2019, de Marca 2.0: https://www.merca20.com/la-seguridad-y-confidencialidad-de-la-informacion-es-obligacion-de-todos/

[32] Government, S. S. (Julio de 2005). *HT Transparency Tools.* Recuperado el 10 de Marzo de 2019, de https://ht.transparency.tools/FileServer/FileServer/clienti/Clever%20Consulting/standards/CRAMM%20Version%205.1%20User%20Guide.pdf

[33] Huerta, A. (26 de Abril de 2012). *Análisis De Riesgos Con Magerit en el ENS (II)*. Recuperado el 18 de Marzo de 2019, de Security Art Work:

https://www.securityartwork.es/2012/04/26/analisis-de-riesgos-con-magerit-en-el-ens-ii/

[34] Huerta, A. (2 de Abril de 2012). *Introducción al análisis de riesgos – Metodologías (II).* Recuperado el 11 de Marzo de 2019, de Security Art Work: https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/

[35] ISACA. (10 de Marzo de 2015). *www.isaca.org*. Recuperado el 23 de Abril de 2019, de www.isaca.org

[36] IT, A. S. (11 de Marzo de 2014). *OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)*. Recuperado el 26 de Febrero de 2019, de Metodologías de Análisis de Riesgos: http://apuntesseguridadit.blogspot.com/2014/03/octave-o-perationally-c-ritical-t-hreat.html

[37] Madrid, C. d. (Septiembre de 2014). *Gestión de riesgos, tratamiento.* Recuperado el 21 de Marzo de 2019, de Comunidad de Madrid: http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/5TratamientodelRiesgo%28AR%29_es.pdf

[38] Microsoft. (2019). *Azure Microsoft*. Recuperado el 18 de Marzo de 2019, de Azure Microsoft: https://azure.microsoft.com/es-es/overview/what-is-saas/

[39] OECD (2015), D. S. (2015). *OECD Recommendation and Companion Document, OECD Publishing, Paris.* Recuperado el 3 de Marzo de 2019, de www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf

[40] Office, T. K. (2017). *Octave Method Of Security Assessment*. Recuperado el 11 de Marzo de 2019, de Information Technology, The University of Kansas: https://technology.ku.edu/octave-method-security-assessment

[41] Poveda, I. J. (Septiembre de 2013). *Ing. Jose Manuel Poveda*. Recuperado el 10 de Abril de 2019, de Universidad Nacional de Ingeniería: https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf

[42] Richard A. Caralli, J. F. (Mayo de 2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. *Technical Report, Software Engineering Institute*. Software Engineering Institute.

[43] Riesgos, C. C.-0. (12 de Agosto de 2019). AS/NZS 4360:1999. *Estándar Australiano - Administración de Riesgos AS/NZS 4360:1999*.

[44] S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S. (12 de Mayo de 2015). *Incibe, Instituto Nacional de Ciberseguridad de España*. Recuperado el 3 de Abril de 2019, de https://www.incibe.es/que_es_incibe/que-hacemos.

[45] University, C. M. (Enero de 05 de 2007). *CERT, Software Engineering Institute, Carneige Mellon University*. Recuperado el 22 de Marzo de 2019, de Introducing OCTAVE Allegro: Improving the Information Security Risk

Assessment Process: https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419

[46] Veiga, J. M. (Mayo de 2009). *Análisis de Riesgos de Seguridad de la Información.* Recuperado el 3 de Abril de 2019, de Facultad de Informática, Universidad Politécnica de Madrid: http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

[47] Vieites, Á. G. (2011). *Enciclopedia de la Seguridad Informática. 2ª Edición.* Mexico D.F.: Grupo Editorial RA-MA.

[48] Yazar, Z. (11 de Abril de 2011). *A Qualitative Risk Analysis and Management Tool - CRAMM.* Recuperado el 12 de Marzo de 2019, de SANS Technology Institute: https://www.sans.org/reading-room/whitepapers/auditing/paper/83