UNIVERSIDAD CATÓLICA ANDRÉS BELLO
FACULTAD DE CIENCIAS ECONÓMICAS Y SOCIALES
ESCUELA DE ECONOMÍA

APLICACIÓN DE UN MODELO DE GESTIÓN DE RIESGOS BAJO UN ENFOQUE DE ADMINISTRACIÓN DEL VALOR DE LOS ACTIVOS PARA LA EMPRESA DE SERVICIOS CIAP

Trabajo de grado presentado como requisito para optar al título de Economista

Tutor: **Evaristo Diz**
Realizado por: **Sebastian Alchacoa**
CI: **25.964.099**

Caracas, junio de 2020

DEDICATORIA

A mi madre, quien ha sido padre y madre a la vez, y es gracias a ella que nunca nos ha faltado nada a mi hermana y a mí.

A mi padre, que sé que desde el cielo estará orgulloso de mí.

A mis tíos Luis y Julia, por siempre darnos su apoyo incondicional

AGRADECIMIENTO

A la Universidad Católica Andrés Bello, el programa beca-trabajo y al CIAP, ya que no solo me brindaron mi primer trabajo, sino que me dieron la oportunidad de continuar estudiando.

ÍNDICE DE CONTENIDO

ÍNDICE DE CUADROS

ÍNDICE DE FIGURAS

ANEXOS

APLICACIÓN DE UN MODELO DE GESTIÓN DE RIESGOS BAJO UN ENFOQUE DE ADMINISTRACIÓN DEL VALOR DE LOS ACTIVOS PARA LA EMPRESA DE SERVICIOS CIAP

Tutor: **Evaristo Diz**
Realizado por: **Sebastian Alchacoa**
Junio de 2020

RESUMEN

El trabajo de investigación aplica un modelo de gestión de riesgos enfocándose en cómo administrar y proteger el valor de los activos frente a las amenazas y vulnerabilidades a los que está expuestos. Los objetivos que se persiguen con esta investigación son el determinar el nivel de exposición de riesgo de los activos y cómo este nivel de riesgo puede ser gestionado para lograr su respectiva minimización. El modelo fue aplicado en la empresa de servicios CIAP (Centro Internacional de Actualización Profesional) de la UCAB, que es una empresa que se dedica a la formación académica. Al ser una empresa que no contaba con una cultura de riesgos, la recolección de información fue realizada a través de un cuestionario aplicado a los coordinadores y a la directora de la empresa, quienes son considerados como los expertos para recabar la información pertinente. Entre los hallazgos más relevantes destaca el hecho de que los controles establecidos por la empresa son efectivos para reducir la probabilidad de ocurrencia de las amenazas identificas, esto derivó en que la mayoría de las mismas se ubiquen en una zona de riesgo moderada, la cual puede ser considerada como tolerable. A pesar de esto, se identificó una amenaza que requiere atención crítica por parte de la empresa, ya que podría afectar la continuidad las actividades diarias. Además de esto, el modelo permitió identificar, caracterizar y categorizar los activos, amenazas, vulnerabilidades más importantes.

INTRODUCCIÓN

El riesgo es un término que ha acompañado a la humanidad desde sus orígenes, ya que, si nos ceñimos a una definición básica del mismo, encontramos que el riesgo no es más que la posibilidad de que ocurra un resultado o evento no deseado, no esperado y negativo. Por lo que el ser humano a lo largo de la historia se ha enfrentado constantemente al riesgo, y si lo analizamos más profundamente, las personas a la hora de tomar decisiones evalúan las diversas opciones que poseen (en base a la información disponible) y comparan los distintos costos-beneficios que cada una posee, y al realizar este proceso están evaluando los posibles riesgos asociados a su decisión y los pros y los contras que esta les pueda brindar.

En la medida que se fueron desarrollando las sociedades, el entorno en el que se desenvolvían los individuos se fue complejizando, lo que genera un mayor grado de incertidumbre y de riesgo, que este a su vez se iba ramificando en los distintos sectores de la economía, llegando a encontrar en las economías modernas diversos riesgos como: riesgo financiero, riesgo sistemático, riesgo estratégico, riesgo operacional, etc.

Es por esto que a lo largo de los años, el concepto de riesgo y su administración han ido adquiriendo mayor relevancia, ya que la gestión de riesgos y su pertinente minimización permiten en términos financieros el control de las rentabilidades al ser conscientes de los riesgos asociados a los activos, y en términos de organizaciones, una gestión de riesgo efectivo permite conocer las vulnerabilidades y amenazas a las que se está expuesto y saber cómo trabajarlas para mejorar el desempeño de la organización.

El entorno macroeconómico de un país juega un papel fundamental en la creación y gestión de los riesgos, entendiendo el entorno macroeconómico como las condiciones que genera el estado de la economía sobre los individuos, ya que en la

medida que este entorno sea más complejo, el nivel de incertidumbre será mayor y la gestión de riesgos será más compleja.

El caso venezolano, presenta uno de los entornos macroeconómicos más complejos, ya que actualmente se encuentra atravesado una de las peores crisis de su historia, con los mayores índices de inflación registrados, una inestabilidad política tal que llega a afectar a todo el continente, índices de pobreza y desnutrición en récords históricos, etc. Lo que plantea un ambiente lleno de incertidumbre para el desarrollo y toma de decisiones de los individuos, pero por sobre todo, genera un ambiente en el que están expuestos a diversos riesgos y es aquí en donde se hace menester el saber cómo gestionarlos, ya que a los largo de los últimos años el tema de riesgo ha adquirido una mayor importancia, en un ambiente macroeconómico como el de Venezuela se hace aún más importante el tener conocimiento sobre cómo lograr minimizar las vulnerabilidades y amenazas a fin de lograr minimizar el riesgo y el impacto que todos estos factores puedan tener sobre una organización o individuo.

Es por esto que el presente trabajo de investigación buscará estudiar a través de la aplicación de un modelo de gestión de riesgos, cual es el nivel de riesgo al que los activos del Centro Internacional de Actualización profesional (CIAP) están expuestos bajo un entorno macroeconómico tan inestable como el de Venezuela, pero haciendo énfasis en cómo el riesgo afecta el valor de los activos, ya que una de las finalidades de toda empresa es mantener dicho valor y más aún en situaciones como esta. Todo esto con la finalidad de determinar las amenazas, vulnerabilidades y por ende el nivel de riesgo al que están expuestos los activos y una vez obtenidas todas estas variables, cómo podrían ser gestionadas para lograr un control efectivo y lograr una reducción de riesgos y generar un plan de contingencias para futuros imprevistos.

Para lograr dicho proceso el trabajo de investigación presentará de forma esquemática las teorías y metodología necesarias que sustentan el problema previamente enunciado. Para ello se ha dividido su desarrollo en 5 capítulos.

En el primero de ellos se plantea el problema a estudiar, los objetivos que se persiguen y cerrará con la importancia, justificación y factibilidad de la investigación. El segundo capítulo desarrollará el marco teórico sobre el cual estará sustentado el

trabajo, así como los antecedentes de autores claves en relación a la gestión de riesgos y las definiciones necesarias para el entendimiento total del tema. El tercer capítulo plasma el marco metodológico a emplear, donde se especificará el paso a paso a seguir para la definición del objeto de estudio, objeto de análisis, procesamiento y análisis de los resultados obtenidos.

El cuarto capítulo presentará el análisis e interpretación de los resultados obtenidos a través del modelo de gestión de riesgo. Y con base a dichos resultados, será elaborado el quinto capítulo, donde serán plasmadas las conclusiones pertinentes que se obtuvieron en base al desarrollo del trabajo de investigación y la elaboración de las recomendaciones.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Planteamiento del problema

En un entorno volátil como el que vivimos hoy en día, donde existen muchas amenazas y oportunidades, un escenario donde la toma de decisiones y las consecuencias que de ella derivan se vuelven más complejas. Un escenario así obliga a las organizaciones a contar con estrategias que permitan conocer los efectos tanto negativos como positivos que pudiera tener la incertidumbre sobre los objetivos que esta se plantea.

Este entorno tan volátil en el que se desarrollan las empresas plantea una serie de retos a la hora de la toma de decisiones, pero, por sobre todo, este ambiente genera riesgos que deben ser gestionados con el fin de evitar incurrir en pérdidas dentro de la organización “ya que la naturaleza persistente y a largo plazo del riesgo es claramente indeseable” (Walker, 2013, pág. 37).

Y queda claro que bajo estas condiciones es importante tener clara una metodología de gestión de riesgos, pero esta problemática nos lleva a preguntarnos ¿En Latinoamérica existe esta ‘’cultura del riesgo’’? ¿Existe la gestión de riesgos en el ámbito empresarial en Latinoamérica?

Estas preguntas pueden ser clarificadas por el tercer informe realizado por Marsh (2018) y la Asociación Global de Gerentes de Riesgos (RIMS por sus siglas en inglés), donde señalan que solo el 25% de las empresas latinoamericanas cuentan con niveles de madurez avanzados en gestión de riesgo:

> De acuerdo con los resultados de este estudio, las organizaciones en Latinoamérica están en términos generales en las etapas iniciales de madurez, pero con un claro y determinado camino en la búsqueda de resiliencia organizacional. Según los resultados, un grupo reducido de organizaciones se ubica en los segmentos superiores (25% agrupado en los niveles 4 y 5) y un gran grupo de empresas se

> encuentra distribuido en los niveles iniciales (75% disperso entre los niveles 1, 2 y 3). Sin embargo, puntualmente, dos de cada cinco organizaciones latinoamericanas se encuentran en el nivel de madurez 3, donde la gestión de riesgos, si bien ya se encuentra implementada dentro de los procesos rutinarios, las prácticas de gestión de riesgos están establecidas y se aplican de manera consistente a lo largo de la organización, aún requiere esfuerzo en integración y homogenización en todas las áreas de la empresa, así como un camino importante por recorrer frente la adopción de una perspectiva proactiva y modelos de mejora continua. (p.10)

Siendo en la gestión de riesgos del informe el nivel 1: no desarrollado, el nivel 2: formalizado, el nivel 3: establecido, el nivel 4: implantado e interiorizado y el nivel 5: optimizado.

Lo que nos demuestra que si existe en cierto grado una “cultura de riesgo” en el ámbito empresarial latinoamericano. Pero esto nos lleva a la siguiente pregunta: ¿Cómo puede llevarse a cabo metodologías de gestión de riesgo en un entorno macroeconómico tan complejo como el de Venezuela?

Y esta es una pregunta vital para el trabajo de investigación, ya que la grave crisis que plantea la economía venezolana genera un entorno de mucha incertidumbre, pero, sobre todo, de mucho riesgo, lo que queda plasmado por el índice de riesgo país EMBI+ realizado por J.P Morgan que le atribuye una calificación histórica de 12.581 puntos básicos para finales de 2019, siendo uno de los países más riesgosos del mundo.

Además de esto, en Venezuela no está tan desarrollada la llamada “cultura de gestión de riesgos”, es un tema en el que se ha profundizado poco, y en medio de la crisis que atraviesa el país, se ha reducido considerablemente el aparato productivo y empresarial y nos lleva a preguntarnos si ¿la falta de gestión de riesgos podría haberse sumado a la situación país para dar como resultado el cierre de muchas de las empresas del país? esta pregunta escapa del alcance de este trabajo de investigación, pero hay que destacar que este podría ser otro factor más a considerar en las causas de cierre de una empresa.

Por lo tanto, el interés de esta investigación se encuentra en aplicar un modelo de gestión de riesgos para conocer el nivel de exposición asociado a los activos que

posee una empresa en un entorno tan complejo como el venezolano, y como en esta situación el riesgo puede ser gestionado.

1.2 Formulación del problema

El presente trabajo se enfoca en la aplicación de un modelo de gestión de riesgos bajo un enfoque de administración del valor de los activos para la empresa de servicios CIAP. Por tanto, el estudio busca responder las siguientes preguntas:

- ¿Cuál es el nivel de riesgo al que están expuestos los activos de la empresa?
- ¿Cuáles son las amenazas y vulnerabilidades de la que deriva el riesgo de la organización?
- ¿Cómo podría ser gestionado el riesgo?

1.3 Hipótesis

Los activos que posee el Centro Internacional de Actualización Profesional (CIAP) están expuestos a un nivel de riesgo que es originado por la presencia de amenazas y vulnerabilidades que pueden ser mitigados a través del modelo de gestión de riesgos aplicado.

1.4 Objetivos de investigación

1.4.1 Objetivo general

Aplicar un modelo de gestión de riesgos bajo un enfoque de administración del valor de los activos para determinar el riesgo al que está expuesta la empresa.

1.4.2 Objetivos específicos

- Revisar de manera integral el riesgo: identificación y valoración.
- Mostrar como el valor de los activos se ve afectado por las siguientes variables: Amenazas, vulnerabilidades, probabilidades, frecuencias y severidad.
- Calcular el nivel de riesgo revisado y tomar las medidas necesarias (pertinentes) para reducir el riesgo al que está expuesta la empresa.

1.5 Justificación e importancia

Es importante tener clara una metodología de riesgos, y más cuando la toma de decisiones y gerencia se desenvuelven en una economía como la venezolana. Como queda reflejado en el Benchmark de riesgos de Latinoamérica elaborado por (Marsh, 2018):

> En un mundo cada vez más complejo, volátil e interconectado, una de las claves para capturar oportunidades radica en nuestra capacidad de anticipación. Una gestión de riesgos integral e innovadora, no solo crea valor para la organización, sino que le permitirá transformar sus riesgos en ventajas competitivas reales y sostenibles (p.8).

Si además de esto, le agregamos la poca profundización que existe en la aplicación de la gerencia de riesgos en Venezuela, esta investigación aportará una metodología clara y precisa para ser aplicada, ya que una característica esencial del modelo a aplicar, es que será perfectamente replicable a cualquier organización sin importar en el sector de la economía en la que se desenvuelve, teniendo en consideración de que no existe una única metodología para la gestión de riesgos ya que, a través de los años se han desarrollado varias métodos para analizar los riesgos. Pero, teniendo en cuenta que “todas las buenas metodologías de evaluación de riesgos incluyen cuatro cosas” Norman (2009, pág.20):

1. **Consideración de la amenaza**
2. **Consideración de probabilidad**
3. **Consideración de vulnerabilidad**
4. **Consideración de consecuencias**

Por lo que la metodología desarrollada podría ser útil para una empresa que no posee conocimientos sobre la gestión de riesgos y quiera emplear un control para ayudar a sopesar las adversidades a las que se pueda enfrentar.

En términos académicos, el trabajo de investigación a través de la aplicación del modelo, reflejará cómo una organización se ve afectada por algunos de los factores que genera una crisis económica y cómo ello genera riesgos en la misma. Además de plasmar el desarrollo de aplicación de un modelo para determinar el nivel de riesgo y cómo ello puede ser gestionado para lograr su minimización.

1.6 Factibilidad

Dentro del problema de investigación es importante tener en cuenta la factibilidad de la investigación; “para ello, debemos tomar en cuenta la disponibilidad de tiempo, recursos financieros, humanos y materiales que determinarán, en última instancia, los alcances de la investigación” (Mertens, 2010 y Rojas, 2001) citado en (Sampieri, Fernández, & Baptista, 2014).

La investigación en una primera etapa desarrollará el modelo de gestión de riesgo que será empleado para determinar el nivel de exposure. La siguiente etapa consistirá en analizar los resultados obtenidos por el modelo, y como el riesgo obtenido puede ser gestionado.

El alcance de este proyecto de investigación será el de aplicar una metodología estándar de riesgo para su evaluación y control.

En cuanto a los recursos necesarios para la investigación, que en su mayoría son de carácter técnico (programa estadístico y equipos necesarios para el desarrollo de la investigación) se encuentran disponibles para llevar a cabo el trabajo.

CAPÍTULO II

MARCO TEÓRICO

2.1 Reseña histórica sobre el Centro Internacional de Actualización Profesional (CIAP) de la UCAB

La Universidad Católica Andrés Bello inició su programa de formación post universitaria con la fundación del Programa de Formación Continua (PFC) alrededor de los años 1990. Cinco años después, el programa se siguió desarrollando hasta llegar a convertirse en la Dirección de Formación Continua (DFC). En el año 2005 la DFC es renombrada como Centro Internacional de Actualización Profesional (CIAP).

El CIAP es una dependencia del Vicerrectorado Académico de la UCAB que, desde su fundación, tiene como objetivo brindar programas de formación integral que promuevan la innovación, la productividad y el bienestar social, en distintas áreas de conocimiento; donde su público objetivo son los profesionales o estudiantes universitarios que se encuentren cursando los últimos semestres de la carrera.

La oferta del CIAP es bastante variada y es ofrecida tanto de manera presencial como virtual. Entre las distintas modalidades de formación se encuentra:

- Cursos
- Programas
- Diplomados
- Eventos corporativos

2.2 Antecedentes de la investigación

El estudio del riesgo y su gestión ha llevado a muchos investigadores a realizar análisis de su comportamiento en la economía, pero sobre todo las implicaciones que tienen en las empresas debido al impacto que tienen en las mismas. Diversidad de trabajos se han desarrollado obteniendo resultados que influyeron en la conformación de esta investigación y le dan una base importante a nivel metodológico.

2.2.1 Evaluación del nivel de riesgo, amenazas y vulnerabilidades en el Centro Educativo Infantil El Mundo de los Genios del Distrito Metropolitano de Quito

El autor Móran Quelal (2019) en su tesis de grado evalúa el nivel de riesgo al que está expuesto un centro educativo de Quito; en el que el riesgo es el resultado de multiplicación de la valoración de las amenazas por la valoración de las vulnerabilidades a las que la institución está expuesta. Además de identificar las amenazas y vulnerabilidades, el autor también evalúa la capacidad que posee el centro educativo para responder ante la ocurrencia de efectos adversos. Los principales hallazgos de la investigación se centran en que el nivel de riesgo de la institución se encuentra focalizados en las zonas de riesgo moderado (con un 61% de las amenazas identificadas en esta zona) y en la zona de riesgo bajo (con un 38% de las amenazas identificadas en esta zona). En cuanto a la capacidad de la institución para afrontar eventos adversos (medidos como estado de infraestructura, recursos y capacitación del personal), se determinó que la infraestructura y los recursos disponibles poseen deficiencias para afrontar las adversidades a las que se está expuesto, pero que el personal si está capacitado para dichos eventos.

A continuación, son presentados otros antecedentes de investigación en los que son aplicadas metodologías de riesgo basadas en certificaciones internacionales. A pesar de que las empresas objeto de estudio de dichas investigaciones no guardan relación directa con una empresa como el CIAP (debido a que se dedican a otras ramas de la economía), esto nos demuestra que las metodologías de riesgo son muy

amplias y pueden ser abordadas bajo diferentes enfoques para así aplicarlas a empresas de diversos indoles (en cuanto a estructura y especialización). Lo importante es que el modelo de gestión de riesgo que se aplique se ajuste a las necesidades de la empresa y den solución al problema identificado.

2.2.2 Evaluación de los riesgos operativos para los procesos de prestación de servicios de Fuller mantenimiento, C.A basada en la norma ISO 31020:2009, para fomentar la mejora continua

El Lic. Geraldo Escalona (2017) en su trabajo especial de grado del tipo "investigación y desarrollo" o "investigación aplicada" para la empresa de servicios Fuller, que es una empresa reconocida de prestación de servicios de mantenimiento. Desarrolla un modelo de gestión de riesgos operativos para le empresa mencionada, debido a que la empresa manifestó que estaba viendo socavada la calidad de prestación de sus servicios y productos por el agravamiento del entorno económico que atraviesa Venezuela. Para el desarrollo de dicho modelo, el autor se basó en las normas internacionales ISO 31020:2009[1], que es un reconocido estándar internacional en el que se plasma una metodología de análisis y gestión de riesgos operativos. El investigador encontró que la empresa no contaba con "una correcta cultura de gestión de riesgo operacional" y que los principales riesgos a los que estaba expuesta era el deterioro de sus maquinarias y equipos y el de fallas en la prestación de servicio por parte del personal.

2.2.3 Diseño de un sistema de gestión de riesgos bajo el enfoque del modelo COSO y la norma ISO 31000 para la cadena logística de una empresa comercializadora de repuestos automotores

Garcia Bustamante & Jimenez Varón (2018) en su trabajo de grado desarrollan un modelo de riesgos basados en la norma internacional de gestión de riesgos ISO 31000 y el informe COSO, que es un manual de control interno desarrollado por el Comité

[1] La ISO 31000 es una serie de normas sobre la gestión de riesgos en donde se establecen principios y directrices para que las empresas puedan realizar el análisis y evaluación de riesgos.

de Organizaciones Patrocinadoras de la Comisión Treadway[2]. Con base a estas dos metodologías de riesgo el trabajo de investigación desarrolla una metodología para ser aplicada a la empresa dedicada al ramo automotriz. Se encontró que la empresa poseía buenos estándares en los componentes analizados en el informe COSO (ambiente de control, gestión de riesgos, actividades de control, información y comunicación, monitoreo) pero a pesar de esto, la empresa no estaba gestionando de manera efectiva los riesgos a los que estaba expuesto, por fallas en los procesos internos. Además de realizar un análisis de riesgo y establecer los controles necesarios para su gestión, los autores desarrollaron en base al trabajo de investigación un esquema de gestión de riesgos para que la empresa gestionara por si misma todo el proceso de análisis de riesgo.

2.2.4 Desarrollo de un modelo de gestión de riesgo operativo para una empresa ecuatoriana de comercialización e importación de productos de cocina y purificación de agua

En su trabajo de maestría de Finanzas la autora León Ruiz (2017), desarrolla un modelo de gestión de riesgos operativos para una empresa de servicios, donde los riegos a analizar estuvieron enfocados principalmente en procesos, personas, tecnología y eventos cotidianos de la empresa. Los principales hallazgos encontrados por la autora es que la empresa no tenía ningún tipo de conocimiento sobre la gestión de riesgos, lo que implicó que al realizar el estudio se descubrieran diversos riesgos a los que estaba expuesta la empresa, y que nunca habían sido considerados por la directiva de la misma. Además, destaca que, al no poseer una cultura de riesgos, esto planteaba un reto para la cuantificación de los riesgos, al respecto León Ruiz (2017) comenta que:

> Ya que no existían mediciones o indicadores de gestión, por tanto, la opinión de los expertos fue uno de los medios más importantes para la recolección de datos, para

[2] El Comité de Organizaciones Patrocinadoras de Treadway (COSO, por sus siglas en inglés) es una Comisión voluntaria constituida por representantes de cinco organizaciones del sector privado en EEUU: La Asociación Americana de Contabilidad, El Instituto Americano de Contadores Públicos Certificados, Ejecutivos de Finanzas Internacional, el Instituto de Auditores Interno, La Asociación Nacional de Contadores. Dedicada a la orientación en temas de gestión de riesgos y control interno.

> lo cual se debieron considerar medios matemáticos de cálculo como la metodología PERT[3] para poder llegar a un valor específico en cuanto al nivel de pérdida como a la cantidad de eventos posibles (impacto – frecuencia). (pág.89).

2.3 Bases teóricas

2.3.1 Teoría de riesgo

2.3.1.1 Riesgo

El riesgo es comúnmente definido como la posibilidad de que un evento ocurra, es decir, “es la posibilidad de pérdida o daño” (Diz Cruz, 2013). Pero detrás de esta definición hay mayores implicaciones sobre lo que el riesgo conlleva.

El riesgo es definido por el Departamento de salud y servicios humanos de Estados Unidos (HHS, 2007) cómo:

> El impacto neto de la misión teniendo en cuenta (1) la probabilidad de que una **[amenaza]** particular ejecute (se dispare accidentalmente o explote intencionalmente) una **[vulnerabilidad**] particular y (2) el impacto resultante si esto ocurriera. … [R] los riesgos surgen de responsabilidad legal o pérdida de misión debido a:
>
> - Divulgación, modificación o modificación no autorizada (maliciosa o accidental)
> - destrucción de información
> - Errores y omisiones no intencionales
> - Interrupciones informáticas debido a desastres naturales o provocados por el hombre.
> - No ejercer el debido cuidado y diligencia en la implementación y
> - operación del sistema de IT
>
> (pág. 4-5).

Donde la amenaza es “la circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. En la evolución de las normas este concepto se amplía para denominarse «suceso»” según el Instituto Nacional de Ciberseguridad (INCIBE, 2015, pág. 4). Y es a través de una fuente o un actor potencial de amenaza, que esta es ejecutada de manera intencional (o no) a través de una vulnerabilidad.

[3] El método PERT (Project Evaluation and Review Techniques), es un algoritmo basado en la teoría de redes diseñado para analizar y representar las tareas involucradas en un proyecto.

Las amenazas pueden ser originadas por tres tipos de fuentes o agentes de amenaza:

1. **Amenazas naturales**: Que hace referencia a los desastres naturales.

2. **Por el accionar humano directo:** Que pueden ser intencionales (por ejemplo: ataques basados en la red y la computadora, carga de software malicioso información comprometida por robo de equipos, desvelado de secretos, espionaje, etc.) o no intencionales (por ejemplo: entrada de datos involuntaria acciones no autorizadas como uso de software o hardware no autorizados, acciones de eliminación y entrada de datos inexactas, etc.).

3. **Causadas por fallas en infraestructuras:** Pueden incluir fallas de energía, contaminación, productos químicos, fuga de líquido, etc.

La vulnerabilidad, es considerada como una falla o debilidad en los procedimientos de seguridad del sistema, diseño, implementación o controles internos que podrían realizarse (ya se de manera accidental o intencional) y que dan lugar a una violación de seguridad o una violación de la política de seguridad interna. En el caso de los activos, es la debilidad asociada a la naturaleza de los mismos y que facilita la materialización de las amenazas; podemos decir que es un factor intrínseco a nuestros activos. Estas pueden depender del hardware, del software, las redes, el personal, el edificio o las infraestructuras o la organización" (INCIBE, 2015, pág.15).

Las vulnerabilidades pueden ser de dos tipos:

1. **Las vulnerabilidades técnicas:** pueden incluir: agujeros, fallas o debilidades en el desarrollo de sistemas de información; o sistemas de información incorrectamente implementados y / o configurados.

2. **Las vulnerabilidades no técnicas**: pueden incluir políticas, procedimientos, estándares o pautas ineficaces o inexistentes.

Por lo que todo riesgo es función de:

1. La probabilidad de que una amenaza dada desencadene o explote una vulnerabilidad particular.

2. El impacto resultante en la organización.

Esto significa que el riesgo no es un factor o evento único, sino que es una combinación de factores o eventos (amenazas y vulnerabilidades) que, si ocurren, pueden tener un impacto adverso en la organización.

La siguiente figura muestra la relación entre las relaciones de estos conceptos:

Figura 1. ***Relación entre riesgo, amenaza, vulnerabilidad e impacto***

Fuente: INCIBE, Gestión de riesgos. Una aproximación para el empresario, 2005.

El hecho de que no sea un factor único implica que a la hora de gestionar el riesgo tengamos que considerar todas las variables que lo componen y que inciden sobre él. "Ya que gran parte de estos factores son difíciles o muy caros de erradicar y las organizaciones tienen que convivir con ellos tomando medidas que reduzcan el impacto de sus amenazas" INCIBE (2015, pág.15). Al respecto Gheorghe & Mock (1999) plantean que:

> La importancia del riesgo reside tanto en la probabilidad como en la gravedad de los efectos adversos. A veces es probable que el riesgo se malinterprete en gran medida y, por lo tanto, lleve a malas decisiones de gestión.
>
> Sin embargo, al hacer comparaciones, se deben considerar tanto la probabilidad como las consecuencias. Es una práctica común concentrarse en los riesgos con las mayores consecuencias. (p.11)

Y la relación existente entre las vulnerabilidades y las amenazas con el riesgo es la siguiente:

- Una Vulnerabilidad desencadenada o explotada por una Amenaza es igual a un Riesgo.
- Una amenaza debe tener la capacidad de desencadenar o explotar una vulnerabilidad para crear riesgos.

2.3.1.2 Clasificación de riesgos

"Los riesgos pueden surgir por diversas fuentes, internas o externas, y pueden agruparse en diversas categorías o tipos" Superintendencia de Banco, Seguros y pensiones de Perú (SBS, 2008, pág.6). Por lo que a continuación serán plasmadas cuatro clasificaciones que son vitales para el desarrollo de la teoría de riesgos.

1. **Según la percepción**

- **Riesgo objetivo:** "Es el riesgo que resulta de la variación relativa entre la pérdida real y la pérdida probable" (Greene, 1974, pág. 3), es decir, es la pérdida neta cuando ocurre un evento que se genera un impacto y consecuencia.

- **Riesgo subjetivo:** "Es el riesgo que deriva de la incertidumbre psicológica que proviene de la actitud o estado del individuo" (Greene, 1974, pág. 4). Por lo general, este tipo de riesgo no es posible medirlo de manera precisa.

2. **Según el grado de especulación**

- **Riesgo especulativo:** "Describen una situación en la que hay incertidumbre respecto al propio suceso en cuestión" (Greene, 1974, pág. 14) y existe posibilidad tanto de una pérdida como de una ganancia. "Las actividades relacionadas con este tipo de riesgos suelen realizarse con la esperanza de una ganancia, por lo que la apuesta es un claro ejemplo donde yacen este tipo de riesgos" (Outreville, 1997, pág. 3).

- **Riesgo puro:** "Son aquellos que solo ofrecen la posibilidad de pérdida" (Outreville, 1997, pág. 3); en un "riesgo puro" solo se produce pérdida si ocurre el peligro (Greene, 1974, pág. 13).

3. **Según los cambios que ocurren en la economía**

- **Riesgo dinámico:** “Son aquellos que están envueltos en la posibilidad de cambios dinámicos. Son el resultado de los cambios en las condiciones económicas como precios, gusto de consumidores, tecnología” (Outreville, 1997, pág. 3).

- **Riesgo estático:** Son aquellos que están relacionados con la pérdida aún si no suceden cambios en las condiciones de la economía.

4. **Según la naturaleza del causante de la pérdida**

- **Riesgo de crédito:** “Es la posibilidad de sufrir pérdidas si los clientes y contrapartidas, con las que la entidad tiene contratadas operaciones, incumplen los compromisos contractuales que han adquirido, por falta de solvencia” Banco Interamericano de Desarrollo (1999, pág.99).

- **Riesgo estratégico:** La posibilidad de pérdidas por decisiones que toma la alta gerencia de una empresa para la creación de ventajas competitivas. Algunos ejemplos son reflejados por la (SBS, 2008, pág.6): Se encuentra relacionado a fallas o debilidades en el análisis del mercado, tendencias e incertidumbre del entorno, competencias claves de la empresa y en el proceso de generación e innovación de valor.

- **Riesgo de liquidez:** Surgen de la posibilidad de pérdidas por incumplir con los requerimientos de financiamiento, así como por no poder liquidar posiciones abiertas en un plazo conveniente, en la cantidad suficiente y a un precio razonable, es decir, la incapacidad de cumplir con las obligaciones de corto plazo.

- **Riesgo de mercado:** “La posibilidad de pérdidas derivadas de movimientos adversos de las variables del mercado que determinan el valor de la compañía” (BID, 1999, pág. 203). Algunas de estas variables podrían ser: tipo de interés, tipo de cambio, precios de mercancías, etc.

- **Riesgo técnico:** La posibilidad de pérdidas o modificación adversa del valor de los compromisos contraídos en virtud de los contratos de seguros, de reaseguros y de coaseguros.

- **Riesgo de reputación:** La posibilidad de pérdidas por la disminución en la confianza en la integridad de la institución que surge cuando el buen nombre de la empresa es afectado. “El riesgo de reputación puede presentarse a partir de otros riesgos inherentes en las actividades de una organización” (SBS, 2008, pág.6).

Hay que destacar que en las definiciones de todos estos tipos de riesgos hay un factor común, que es el de la posibilidad de pérdida en caso de que efectivamente se materialice el riesgo, y cuando se habla de pérdida se hace referencia a pérdida económica o reparto de valor involuntario.

Al respecto Greene (1974) comenta sobre el riesgo de pérdida:

> El riesgo de pérdida es la incertidumbre de que en un período de tiempo determinado las pérdidas reales se igualen a las probables. Aun cuando las pérdidas probables se reduzcan, el riesgo puede estar todavía presente, pues aún existe la posibilidad de que haya desviaciones importantes en la probabilidad de ocurrencia. (pág.17).

“Por todo ello no es sorprendente que la mayoría de las personas trate de evitar el riesgo lo más posible o reducir sus consecuencias negativas, pero desgraciadamente no todo riesgo puede disminuirse o evitarse” (Greene, 1974, pág. 2).

Ahora, debido a que el trabajo de investigación está enfocado en el riesgo operativo, se le dedicará un apartado exclusivo a su definición y las implicaciones que conlleva.

2.3.1.3 Riesgo operativo

Según Venegas Martínez (2008, pág. 861): “El riesgo operativo también llamado riesgo operacional, es el riesgo de que se presenten pérdidas por fallas en los sistemas administrativos y procedimientos internos, así como errores humanos intencionales o no”. También podría ser ocasionado según la SBS (2008) por: procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación. “Por lo que Los riesgos operativos son un grupo de riesgos que

impactan en la forma en que una empresa lleva a cabo sus negocios" (Sweeting, 2011, pág. 102).

"Muchas de las mayores pérdidas en la industria financiera y el ámbito corporativo pueden atribuirse, de una forma u otra, a fallas de riesgo operacional" (Sheedy, 2004, pág. 1153). Al respecto de las pérdidas que derivan del riesgo operativo Sweeting (2011) comenta que:

> Si no se gestiona correctamente, estos riesgos pueden ser los mayores riesgos que enfrenta cualquier organización. Las fallas operativas han llevado a la desaparición final de más de una empresa. Esto se debe a que un control deficiente del riesgo operativo permite que otros tipos de riesgos, como el riesgo de mercado o de crédito, sean excesivos. En un nivel menos extremo, las fallas operativas o las deficiencias pueden dar lugar a errores e ineficiencias que resultan en multas o pérdida de negocios. (pág. 102).

Sobre la definición de riesgo operativo Sheedy (2004) comenta que:

> Esta definición temprana de la industria identifica las pérdidas esperadas e inesperadas atribuibles a percances operacionales. En términos simples, las pérdidas esperadas son aquellas pérdidas incurridas durante el curso natural de los negocios, y las pérdidas inesperadas generalmente se asocian con grandes sorpresas como resultado de fallas en la administración y la falla en los controles. El alcance del riesgo operacional en esta definición inicial es bastante amplio y se extiende a todas las facetas y aspectos del riesgo asociados con eventos internos y externos, recursos tangibles como tecnología y sistemas de información e intangibles como personas y procesos. (pág. 1157).

Algunos de los ejemplos más representativos de riesgo operativo que Venegas Martínez (2008) desarrolla en su libro son:

> Fallas en hardware, software y telecomunicaciones: errores de captura, ejecución y mantenimiento de operaciones con clientes; fallas en sistemas de seguridad: pérdida total o parcial de bases de dato; robo; daños a los activos fijos (por vandalismo, terrorismo, desastres naturales, etc.); documentación incompleta de clientes; restricciones impuestas por las autoridades financieras para participar en ciertos mercados. (p. 861).

Tabla 1. Dimensiones del riesgo operativo

Dimensión	Definición
Causas	En varios casos, el evento se debió a una falla o falta de uno o más procedimientos de control. El riesgo operativo puede desencadenarse en cualquiera de las siguientes situaciones: falta de segregación de funciones, debilidad en la supervisión de la gestión, error de entrada de datos, etc.
Eventos de riesgo	El evento de riesgo operacional puede definirse como un incidente específico que ocurrió debido a una o más causas que caen dentro de la definición de riesgo operacional y resultaron en uno o más efectos de riesgo operacional. Los eventos de riesgo operacional se agrupan en siete tipos de categorías de eventos: Fraude interno, fraude externo,relaciones laborales y seguridad del trabajo, prácticas con clientes y productos, daños a los activos, interrupción de negocios por fallas tecnológicas y deficiencias en la ejecución de los procesos. Un evento compartido es un evento de riesgo operativo que ocurre a través de múltiples líneas de negocios que pueden conducir a pérdidas de riesgo operativo.
Efectos del riesgo operativo	Un efecto de riesgo operativo es un efecto directo o indirecto de un evento de riesgo operativo que puede causar pérdidas financieras o interrupciones parciales o completas en los procesos de la empresa.

Fuente: Abdul Rahim, et al. Internal Control System and Perceived Operational Risk Management in Malaysian Conventional Banking Industry, 2018
Elaboración propia

2.3.1.3.1 Tipos de riesgo operativo

Los tipos de riesgo operativo que se encuentran dentro de una empresa son bastante diversos y abundantes. “Incluyen una gran cantidad de riesgos diferentes, que a menudo se superponen entre sí en un grado significativo” (Sweeting, 2011, pág. 102). Pero al ser tan diversos, ¿Cuál debe ser el criterio para clasificarlos? Al respecto Sheedy (2004) comenta que:

> El RMG[4] (tuvo problemas con este mismo problema cuando se embarcó en su ejercicio de recopilación de datos de pérdida por evento en junio de 2002. En su

[4] El Grupo de Gestión de Riesgos (RMG, por sus siglas en inglés), es un grupo del Comité de Basilea que se encargó de la recopilación de datos de pérdida de riesgo operacional en instituciones financieras en el año 2002.

> comunicado de prensa, el Comité de Supervisión Bancaria de Basilea (2002) describió los objetivos de este ejercicio: 'El propósito principal de esta encuesta es recolectar datos granulares (evento por evento) de pérdida de riesgo operacional para ayudar al Comité a determinar la forma y estructura apropiadas del AMA (Enfoque de Medición Avanzada). Para facilitar la recopilación de datos de pérdidas comparables tanto a nivel granular como agregado a través de los bancos, el Comité está utilizando nuevamente su marco detallado para clasificar las pérdidas. (pág. 1159).

Las pérdidas se clasifican y se agrupan en una tabla compuesta por ocho líneas de negocio estándar y siete categorías de eventos de pérdida. Estas siete categorías de eventos se dividen en 20 subcategorías. Las ocho líneas de negocios estándar son: finanzas corporativas, comercio y ventas, banca minorista, banca comercial, pago y liquidación, servicios de agencia, gestión de activos y corretaje minorista**.**

Tabla 2. Clasificación del riesgo operativo

Unidad de negocios	Línea de negocios		Grupo de actividades
	Nivel 1	Nivel 2	
Banca de inversión	Finanzas coporativas	Finanzas coporativas	Fusiones y adquisiciones, suscripción, privatizaciones, titulizaciones, investigación, capital de deuda (gobierno, alto rendimiento), sindicaciones, OPI, colocaciones privadas secundarias
		Finanzas Municipales / Gubernamentales	
		banca de negocios	
		Servicios de asesoramiento	
	Trading y ventas	Ventas	Renta fija, patrimonio, divisas, materias primas, crédito, financiación, títulos de posición propios, préstamos y repos, deuda de corretaje, corretaje principal
		Creación de mercado	
		Posiciones propietarias	
		Tesorería	
Banca	Banca minorista	Banca minorista	Préstamos minoristas y depósitos, servicios bancarios, fideicomisos y propiedades.
		Banca privada	Préstamos y depósitos privados, servicios bancarios, fondos fiduciarios, asesoramiento de inversión.
		servicios de tarjeta	Tarjetas comerciales / comerciales / corporativas,
	Banca comercial	Banca comercial	Financiación de proyectos, bienes raíces, financiación de exportaciones, financiación del comercio, factoring, leasing, préstamos, garantías, letras de cambio
	Pago y liquidación	Clientes externos	Pagos y cobros, transferencia de fondos, compensación y liquidación
	Agencia de servicios	Custodia	Fideicomiso, recibos de depósito, préstamos de valores (clientes), acciones corporativas
		Agencia corporativa	Emisor y agentes pagadores
		Confianza corporativa	
Otros	Gestión de activos	Gestión discrecional de fondos	Fondo común agrupado, segregado, minorista, institucional, dosificado, abierto, privado
		Gestión no discrecional de fondos	Agrupado, segregado, minorista, institucional, dosificado, abierto
	Corretaje minorista	Corretaje minorista	Ejecución y servicio completo.

Fuente: Sheedy, El manual del administrador de riesgos profesionales, 2004
Elaboración propia

A pesar de que la clasificación ofrecida en la tabla 2 no guarda relación directa con una empresa como el CIAP (ya que está asociada más a instituciones de corte financiero) nos demuestra que el riesgo operativo posee diversos matices, ya que, por lo general es asociado a: procesos, personas y sistemas internos; el riesgo operativo también puede ser analizado y evaluado desde un enfoque financiero y más específicamente bajo el enfoque de esta investigación, en la que el riesgo operativo está focalizado en los activos que posee la empresa.

2.3.1.3.2 Frecuencia y severidad de eventos de riesgo

Los diferentes eventos de riesgo operativo pueden ser estudiados en términos de su frecuencia (el número de eventos que producen pérdidas en un cierto intervalo de tiempo) y su severidad (el impacto del evento en términos de pérdidas económicas).

2.3.1.4 Gestión de riesgos

Puede considerarse que la misión de una empresa consiste en ofrecer a la sociedad un producto o servicio, para lo cual ha de utilizar una serie de recursos y asumir un conjunto de riesgos, gestionar estos eficazmente y obtener así un beneficio. Desde este punto de vista, la gestión de riesgos es parte fundamental de la estrategia y del proceso de toma de decisiones en la empresa y, por tanto, ha de contribuir a la creación de valor en todos los niveles, especialmente para los accionistas, pero también para aquellos a los que destinan los bienes o servicios (clientes), para otros tenedores de derechos sobre la compañía (prestamistas y otro acreedores, dirección y empleados en general, Estado, etc.). Normalmente, a medio plazo, la creación de valor para estos grupos distintos de los accionistas actuales se traduce a su vez en valor para estos, haciendo crecer los beneficios y la cotización de las acciones.

“La gestión de riesgos incluye los mecanismos, políticas, herramientas, procesos y procedimientos, incluida la supervisión de la gestión para determinar, evaluar, supervisar, describir y controlar el riesgo” (Abdul Rahim, Ahmed, & Faeeq, 2018, pág. 3).

A grandes rasgos el proceso de gestión de riesgo queda plasmado por la siguiente figura:

Figura *2. Composición de la gestión de riesgos*

Fuente: INCIBE, Gestión de riesgos. Una aproximación para el empresario, 2005.

Hay que destacar que no existe una metodología única para la gestión y análisis de riesgos, ya que varían según los autores y las certificaciones internacionales, pero una estructura común sobre el proceso de gestión de riesgos será plasmada a continuación:

1. Establecer el contexto
2. Identificar riesgos
3. Analizar riesgos
4. Evaluación y calificación de riesgos
5. Tratar riesgos
6. Monitorear y revisar
7. Comunicar y consultar

1. Establecer el contexto

Según la ISO 31000 (2009) este paso consiste en:

> Al establecer el contexto, la organización articula sus objetivos, define los parámetros externos e internos a tener en cuenta al gestionar el riesgo, y establece el alcance y los criterios de riesgo para el proceso restante. Al establecer el contexto para el proceso de gestión de riesgos, deben considerarse con mayor detalle y particularmente cómo se relacionan con el alcance del proceso particular de gestión de riesgos. (pág.24).

Además, es importante considerar:

- Identificar una persona con el conocimiento (control interno y riesgos) a nivel operativo
- ¿La organización está basada en la gestión por procesos? ¿Tiene metas y resultados esperados?
- Identificar los objetivos institucionales – grupal
- Se puede comenzar por riesgos de la entidad y luego bajar a nivel de cada proceso, comenzando por los más críticos
- Es importante la participación de todas las partes interesadas

Posteriormente se pueden clasificar y definir los tipos de riesgos.

2. Identificar riesgos

La organización debe identificar las fuentes de riesgo, las áreas de impacto, los eventos y sus causas y sus posibles consecuencias. El objetivo de este paso es generar una lista completa de riesgos basada en los eventos que podrían crear, mejorar, prevenir, degradar, acelerar o retrasar el logro de los objetivos. Además, etapa busca identificar los riesgos que deben ser gestionados, riesgo que no sea identificado, es excluido en cualquier análisis posterior. ¿Qué puede suceder? Puede impedir el logro de los objetivos o responsabilidades asignadas, afecte la eficiencia de mis funciones, genere pérdidas (tiempo, imagen, recursos, etc.). Los riesgos se identifican independientemente de que estén bajo el control de la entidad o no.

Al respecto Lanas (2017) comenta que:

> La identificación de riesgos es el punto de partida de la etapa de valoración del riesgo en general, por lo que en esta metodología se sugiere que en primera instancia se puedan identificar claramente los siguientes elementos en la empresa:
>
> - Los procesos de la empresa
> - Las personas en la empresa con el conocimiento adecuado (expertos)
>
> Estos dos primeros elementos permitirán desarrollar la capacidad de identificar: las fuentes de riesgo, las áreas de impacto, los eventos, las causas y consecuencias potenciales. (pág. 32).

Las técnicas y herramientas de identificación de riesgos son:

- Técnicas de recolección de información:
  - Tormenta de Ideas
  - Técnica Delphi
  - Cuestionarios y encuesta
  - Análisis FODA
  - Entrevistas
  - Diagrama

- Técnicas de diagramación:
  - Diagrama causa/efecto
  - Diagrama flujo de proceso
  - Inventario de Riesgo

Tabla 3. Identificación del riesgo

Nivel de riesgo			Criterios fundamentales	Equivalente Nivel de riesgo / Madurez
Nivel	Criterio	Descripción		
4	Extremo	Requiere de atención urgente de la Alta Dirección	Afectación al cumplimiento de los objetivos estratégicos	1 (Inexistencia / Incial)
			Afectación de la imagen institucional (trascendencia pública a nivel nacional)	
			Interrupción de las operaciones que afecten la prestación de los servicios y que generen un efecto económico negativo.	
			Fraudes, robos e irregularidades intencionales	
			Pérdidas y/o multas por incumplimiento de normatividad interna y externa (> al 50% porciento de la materialidad)	
			Omisión en la aplicación de controles críticos en los procesos estratégicos, operativos y soporte.	
3	Alto	Requiere atención urgente de las Gerencias responsables	Afectación al cumplimiento de los objetivos operativos	2 (En Proceso)
			Atención y servicio al cliente (trascendencia publica local)	
			Pérdidas y/o multas por incumplimiento de normatividad interna y externa (<o=al50%porcientode la materialidad).	
			Omisión en la aplicación de controles críticos en los procesos operativos y de soporte.	
			Carencia de normas y procedimientos internos relacionados con la administración activos y recursos.	
			Omisión en la implantación de recomendaciones en dos periodos consecutivos.	
2	Moderado	Requiere atención de la Gerencia	Incumplimiento reiterativo de procedimientos internos dentro del periodo evaluado.	3 (Implementado)
			Desactualización de normas y procedimientos internos relacionados con la administración de activos, recursos entre otros.	
1	Bajo	Requiere monitoreo periódico fin de mantener los riesgos en este nivel	Incumplimiento parcial de normas y procedimientos internos dentro del periodo evaluado (no repetitivo).	4 (Optimo)

Fuente: Diz Cruz, Gestión de riesgos, 2015
Elaboración propia

3. Analizar riesgos

El análisis de riesgos implica desarrollar una comprensión del riesgo ya que proporciona un aporte a la evaluación de riesgos y a las decisiones sobre si los riesgos deben tratarse, y sobre las estrategias y métodos de tratamiento de riesgos más apropiados (ISO 31000, 2009, pág. 18).

Este paso involucra determinar: fuentes de riesgo, posibilidad, consecuencias, responsables y los controles y acciones que sean necesarias para minimizar el riesgo. La lista que se derive de este análisis debe ser excluyente.

El análisis de riesgos puede ser:

- **Cualitativo:** Este análisis utiliza formatos de palabras o escalas descriptivas para describir la magnitud de las consecuencias potenciales y la probabilidad de que esas consecuencias ocurran.
- **Semicuantitativos:** El numero asignado a cada descripción no tiene que guardar una relación precisa con la magnitud real de las consecuencias y probabilidades
- **Cuantitativo:** Uso de datos numéricos para la determinación de riesgos.

4. Evaluación y calificación de riesgos

La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente. El propósito de la evaluación de riesgos es tomar decisiones basadas en resultados del análisis de riesgos (tratamiento de riesgo y la prioridad).

Al respecto se comenta en la ISO 31000 (2009) que:

> En algunas circunstancias, la evaluación de riesgos puede llevar a la decisión de realizar un análisis más detallado. La evaluación de riesgos también puede llevar a una decisión de no tratar el riesgo de otra manera que no sea mantener los controles existentes. Esta decisión estará influenciada por la actitud de riesgo de la organización y los criterios de riesgo establecidos. (pág.18).

La entidad debe evaluar cada uno de los Riesgos identificados, estableciendo el impacto de los mismos frente al logro de los objetivos del Proceso de Contratación y su probabilidad de ocurrencia. Esta evaluación tiene como fin asignar a cada Riesgo una calificación en términos de impacto y de probabilidad, la cual permite establecer la valoración de los Riesgos identificados y las acciones que se deban efectuar.

Posteriormente con toda esta información recolectada, se procede a construir el mapa de calor o mapa de riesgos.

Según García (1994), el objetivo del Mapa de Riesgos es sintetizar la información relativa a las indeterminaciones que afronta la empresa y colaborar en las estrategias destinadas a mitigar la exposición y los daños potenciales citado en (Rodríguez López, Piñeiro Sánchez, & de Llano Monelos, 2013, pág. 6)

“El mapa contribuye al objetivo general de supervivencia de la empresa aportando la información precisa para medir y controlar esa exposición, y poner en práctica un

modelo de gestión proactiva del riesgo" (Rodríguez López et al., 2013, pág. 8). Además, ayuda a identificar y medir los riesgos a los que se está expuesto, proporcionar una visión analítica de las relaciones de causalidad subyacentes y aportar una visión total de la exposición que posee la empresa.

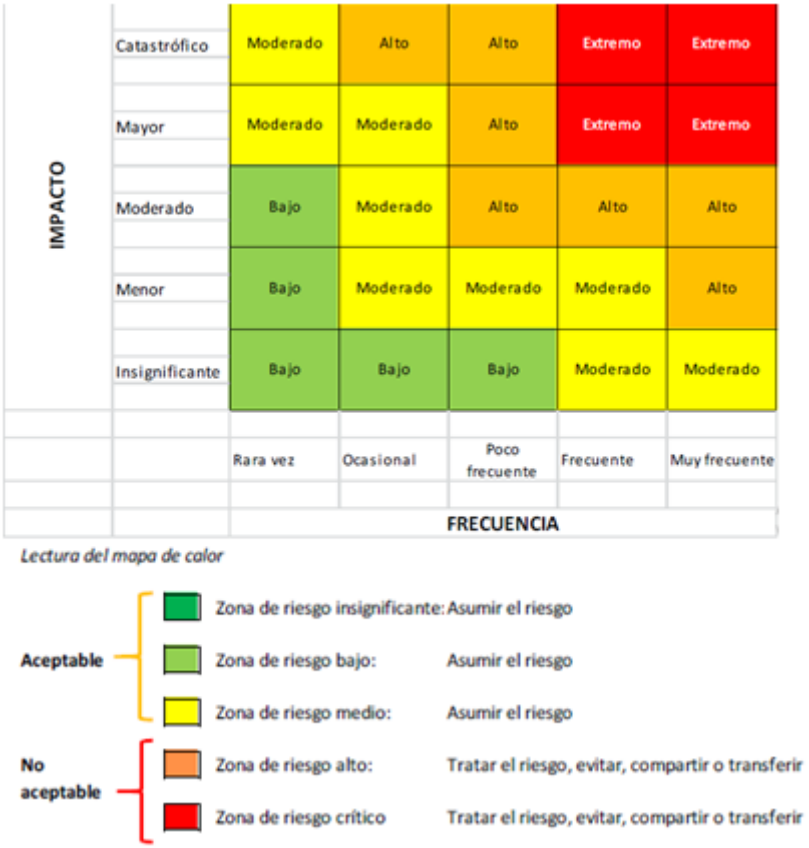


Figura *3. Mapa de calor*

Fuente: León Ruiz, Desarrollo de un modelo de gestión de riesgos, 2017

5. Tratamiento de los riesgos

Al respecto la ISO 31000 (2009) nos dice que:

> El tratamiento del riesgo implica seleccionar una o más opciones para modificar los riesgos e implementar esas opciones. Una vez implementados, los tratamientos proporcionan o modifican los controles.
>
> El tratamiento del riesgo implica un proceso cíclico de:
>
> - Evaluar un tratamiento de riesgo;
> - Decidir si los niveles de riesgo residual son tolerables;
> - Si no es tolerable, generar un nuevo tratamiento de riesgo; y
> - Evaluar la efectividad de ese tratamiento
>
> (pág. 19).

Algunos de los tratamientos que pueden ser aplicados a la gestión de riesgos son:

- Asunción del riesgo.
- Evitar el riesgo o eliminar el riesgo
- Cesión o transferencia del riesgo.
- Reducirlo o mitigarlo

- **Asunción del riesgo**

También conocida como no aseguramiento o aceptación del riesgo. Este método consiste según INCIBE:

> Se asume el riesgo, bien porque está debajo del umbral aceptable de riesgo bien en situaciones en las que los costes de su tratamiento son elevados y aun siendo riesgos de impacto alto su probabilidad de ocurrencia es baja o porque aun a pesar del riesgo la empresa no quiere dejar de aprovechar la oportunidad que para su negocio supone esa actividad arriesgada (pág.7).

"En este caso se recomiendan medidas para reducir el Riesgo o mitigar su impacto, así como el monitoreo" (Colombia compra eficiente, 2013, pág. 14).

- **Evitar el riesgo o eliminar el riesgo**

"Evitar el Riesgo, para lo cual debe decidir no proceder con la actividad que causa el Riesgo o buscar alternativas para obtener el beneficio del Proceso de Contratación" (Colombia compra eficiente, 2013, pág. 14). Siguiendo a INCIBE (2015), en el caso de los activos, se podría sustituir el activo que se está viendo afectado por la amenaza o eliminando la actividad que la produce. Aunque hay que tener en cuenta que el riesgo no siempre puede ser eliminado, esto dependerá de: las condiciones en las que se desarrolla, sus causas y el control que tenga la empresa sobre los anteriores elementos.

- **Cesión y transferencia del riesgo**

"Transferir el Riesgo haciendo responsable a otra entidad quien asume las consecuencias de la materialización del Riesgo, típicamente se transfiere el Riesgo a través de las garantías previstas en un contrato estableciendo con claridad quien es el responsable" (Colombia compra eficiente, 2013, pág. 14).

Al respecto (Greene, 1974) comenta que:

> El riesgo de pérdida es a menudo el mismo para el cesionario que para el cedente. El que acepta el riesgo puede, no obstante, tener mayor conocimiento de la probabilidad de pérdida y estar de esa forma en mejor situación financiera para asumirla que el cedente. Sim embargo el riesgo aún existe. (pág.18).

- **Reducirlo o mitigarlo**

Este método consiste en tomar las medidas oportunas para reducir el nivel de riesgo. Algunas de las medidas recomendadas por INCIBE (2015) son:

- Reducir la probabilidad o frecuencia de ocurrencia: tomando, por ejemplo, medidas preventivas.
- Reducir el impacto de la amenaza o acotar el impacto, estableciendo por ejemplo controles y revisando el funcionamiento de las medidas preventivas.

Todos estos métodos para tratar el riesgo quedan reflejados en la matriz de riesgos, ya que el objetivo de toda empresa debe ser construir su matriz para tener claro los riesgos a los que está expuesto, y trabajar para reducir los riesgos desde el punto A hasta el punto D.

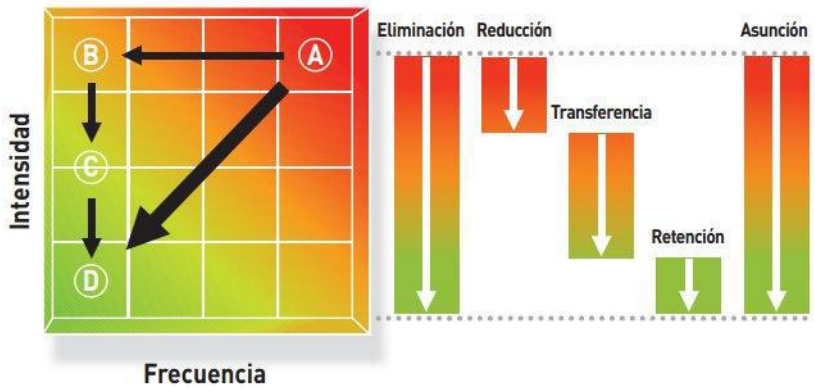


Figura 4*. Tratamiento de riesgos en el mapa de calor*

Fuente: Gestión de riesgos (Diz Cruz, 2015)

6. Monitorear y revisar

La Entidad debe realizar un monitoreo constante a los riesgos, pues las circunstancias cambian rápidamente y los riesgos no suelen ser estáticos. La matriz y el plan de tratamiento deben ser revisadas constantemente y revisar si es necesario

hacer ajustes al plan de tratamiento de acuerdo con las circunstancias. Un monitoreo periódico de los riesgos asegurará que estos estén actualizados y la empresa no quede expuesta a las pérdidas asociadas al riesgo.

En el Manual Colombia compra eficiente (2013) refleja cual debería ser el monitoreo a aplicarse:

> - Garantizar que los controles son eficaces y eficientes en el diseño y en la operación.
> - Obtener información adicional para mejorar la valoración del riesgo.
> - Analizar y aprender lecciones a partir de los eventos, los cambios, las tendencias, los éxitos y los fracasos.
> - Detectar cambios en el contexto externo e interno que puedan exigir revisión de los tratamientos del riesgo y establecer un orden de prioridades de acciones para el tratamiento del riesgo.
> - Identificar nuevos riesgos que pueden surgir.
>
> (pág.15).

7. Comunicar y consultar

La comunicación y consulta con las partes interesadas externas e internas debe tener lugar durante todas las etapas del proceso de gestión de riesgos.

Al respecto, la ISO 31000 (2009) establece que:

> Los planes de comunicación y consulta deben desarrollarse en una etapa temprana. Estos deberían abordar cuestiones relacionadas con el riesgo en sí, sus causas, sus consecuencias (si se conocen) y las medidas tomado para tratarlo. Deben realizarse comunicaciones y consultas externas e internas efectivas para garantizar que los responsables de implementar el proceso de gestión de riesgos y las partes interesadas entiendan la base sobre qué decisiones se toman y las razones por las cuales se requieren acciones particulares.
>
> Un enfoque de equipo consultivo puede:
>
> - Ayudar a establecer el contexto adecuadamente.
> - Garantizar que se entiendan y consideren los intereses de las partes interesadas.
> - Ayudar a garantizar que los riesgos se identifiquen adecuadamente.
> - Reunir diferentes áreas de especialización para analizar los riesgos.
> - Garantizar que se tengan en cuenta las diferentes opiniones al definir los criterios de riesgo y al evaluar los riesgos.
> - Respaldo y apoyos seguros para un plan de tratamiento.
> - Mejorar la gestión de cambios adecuada durante el proceso de gestión de riesgos.
> - Desarrollar un plan apropiado de comunicación y consulta externa e interna.
>
> (pág. 14).

Todo este proceso de gestión de riesgos puede ser resumido en la siguiente gráfica:

Figura 5*. Proceso de gestión de riesgos*

Fuente: INCIBE, Gestión de riesgos. Una aproximación para el empresario, 2005.

2.3.1.5 Riesgo, incertidumbre y beneficio

Esta teoría fue desarrollada por el economista Frank Knight en 1921 cuando publicó su libro titulado “riesgo, incertidumbre y beneficio”, donde expuso su teoría del empresario y las implicaciones de su gestión en la economía.

Knight (1921) fue de los primeros economistas en hacer la distinción de entre riesgo e incertidumbre mientras desarrollaba su teoría del empresario, ya que sus predecesores consideraban que no existía dicha diferencia o simplemente era irrelevante y no era desarrollado este tema. Hacía un especial énfasis en que el riesgo y la incertidumbre son dos conceptos totalmente distintos, el definía el riesgo como la

aleatoriedad que tenía probabilidades conocidas, mientras que la incertidumbre era la aleatoriedad con probabilidades desconocidas.

También destaca que existen dos tipos de riesgos, el riesgo técnico y el riesgo económico:

- **Riesgo técnico:** Medida de la incertidumbre asociada a que se produzcan los productos en las condiciones y características previstas.
- **Riesgo económico:** Medida de la incertidumbre asociada a que los ingresos por ventas superen a los costes.

Y la relación entre el riesgo y la incertidumbre subyace en que el riesgo es la medida de la incertidumbre del sistema económico.

Sobre estos dos conceptos es que Knight desarrolla su teoría del empresario, ya que para él tenía un papel fundamental en la economía. Considera que su función es la de asegurar las rentas de los factores productivos asumiendo el riesgo asociado a la actividad económica de la empresa. El empresario adquiere los factores de producción a un precio (que es conocido) y tiene que hacer previsiones futuras sobre la demanda (que es incierta, tanto en la cantidad que podrá vender como en el precio final de venta). Por tanto, el empresario es quien se encarga de asumir el riesgo que deriva de la actividad económica que realiza su empresa y el beneficio es la recompensa por asumir ese riesgo. Knight (1921) describe al beneficio como un beneficio residual que es incierto (no se conoce con seguridad) porque este se ve expuesto por las variaciones de las condiciones económicas.

Ya que el empresario es quien se encarga de hacer las previsiones sobre la demanda, es quien asume el riesgo de equivocarse en dichas previsiones, y que estas afecten negativamente a su empresa y se incurra en pérdidas. Lo único que conoce con exactitud el empresario, son sus costes, ya que sus ingresos son inciertos debido a que estos dependen de las previsiones que ha realizado anteriormente. Y es aquí donde juega un papel fundamental la incertidumbre, ya que el empresario no puede saber con exactitud lo que sucederá en el futuro y según la información y conocimientos de las que dispone, la incertidumbre será mayor o menor, lo que hará que las predicciones sean más o menos acertadas.

En resumen, el empresario es quien asume el riesgo en situaciones de incertidumbre y es recompensado por ello a través del beneficio que obtiene.

2.4 Conceptos básicos

A continuación, se presenta una variedad de términos que se deben manejar para entender la investigación dado que estos serán empleados de manera continua en el trabajo:

- *Activo*: Según INCIBE (2015):

  > Cualquier recurso de la empresa necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste. La naturaleza de los activos dependerá de la empresa, pero su protección es el fin último de la gestión de riesgos (pág.4).

- *Actitud de riesgo:* ISO 31000 (2009): “enfoque de la organización para evaluar y eventualmente perseguir, retener, tomar o alejarse del riesgo”.

- *Consecuencia del riesgo:* Es el resultado del evento, que tiene como efecto un impacto sobre los objetivos de la organización.

- *Contexto Externo:* Según la ISO 31000 (2009): “entorno externo en el que la organización busca alcanzar sus objetivos”.

- *Contexto interno:* Según la ISO 31000 (2009): “entorno interno en el que la organización busca alcanzar sus objetivos”.

- *Control interno:* Según la SBS (2008):

  > Un proceso, realizado por el Directorio, la Gerencia y el personal, diseñado para proveer un aseguramiento razonable en el logro de objetivos referidos a la eficacia y eficiencia de las operaciones, confiabilidad de la información financiera, y cumplimiento de las leyes aplicables y regulaciones. (pág.3).

- *Empresa:* Es una organización o institución dedicada a actividades o persecución de fines económicos o comerciales, lográndolo a través de satisfacer las necesidades de bienes y/o servicios de la sociedad.

- *Entorno macroeconómico:* Condiciones que genera el estado de la economía sobre los individuos. Donde dicho estado depende de diversas variables económicas que evolucionan de manera dinámica.

- *Evaluación de riesgos:* Proceso de identificación, análisis y evaluación de riesgos.

- *Evento de riesgo:* Según la ISO 31000 (2009): “ocurrencia o cambio de un conjunto particular de circunstancias”.

- *Exposición:* Es la condición de desventaja debido a la ubicación, posición o localización de un sujeto, objeto o sistema expuesto al riesgo CIIFEN (s.f).

- Frecuencia: Es el número de repeticiones por unidad de tiempo de cualquier evento periódico.

- *Gestión de riesgos:* Según la ISO 31000 (2009): “actividades coordinadas para dirigir y controlar una organización con respecto al riesgo”.

- *Impacto:* Según la SBS (2008): “La consecuencia o consecuencias de un evento, expresado ya sea en términos cualitativos o cuantitativos. Usualmente se expresará en términos monetarios, como pérdidas financieras. También es llamado severidad” (pág.9).

- *Incertidumbre:* Es el grado de desconocimiento de lo que ocurrirá en el futuro.

- *Probabilidad:* Según Greene (1974) la probabilidad puede ser definida como: “se refiere a la posibilidad de acontecimiento de largo plazo, o frecuencia relativa, de algún suceso”.

- *Probabilidad de pérdida:* Es la posibilidad de incurrir en una pérdida económica o reparto de valor involuntario cuando se materializa el riesgo.

- *Resiliencia:* Según CIIFEN (s.f) puede ser definido como:

  > Es la capacidad de un sistema, comunidad o sociedad expuestos a una amenaza para resistir, absorber, adaptarse y recuperarse de sus efectos de manera oportuna y eficaz, lo que incluye la preservación y la restauración de sus estructuras y funciones básicas.

- *Riesgo:* Es la probabilidad de que una amenaza particular ejecute (se dispare accidentalmente o explote intencionalmente) una vulnerabilidad y genere pérdidas y afecte adversamente a la consecución de los objetivos de una organización.

- *Riesgo de pérdida: “*El riesgo de pérdida es la incertidumbre de que en un período de tiempo determinado las pérdidas reales se igualen a las probables” (Greene, 1974, pág. 17).
  .
- *Riesgo país:* Es el riesgo asociado a un país que es resultado de las operaciones que mantiene con el resto del mundo. Específicamente es el “riesgo que asumen las entidades financieras, las empresas o el estado, por

el posible impago por operaciones comerciales o prestamos que realizan con el sector público o privado de otro país" (Olarte, 2006, pág. 348).

- *Riesgo residual:* Es el riesgo que existe aun cuando después del proceso de tratamiento de riesgos.

- *Susceptibilidad: "*Es el grado de fragilidad interna de un sujeto, objeto o sistema para enfrentar una amenaza y recibir un posible impacto debido a la ocurrencia de un evento adverso" CIIFEN (s.f).

- *Tolerancia al riesgo:* Según la (SBS, 2008, pág. 9): "El nivel de variación que la empresa está dispuesta a asumir en caso de desviación a los objetivos empresariales trazados".

- *Volatilidad:* Es una medida de la intensidad y frecuencia de los cambios que el precio de un activo o de un tipo definido como la desviación estándar de dicho cambio en un horizonte temporal específico.

CAPÍTULO III

MARCO METODOLÓGICO

Ya que ha sido desarrollado el marco teórico sobre el cual se sustenta el trabajo de investigación, el siguiente paso será desarrollar la metodología que será utilizada en el trabajo. Por lo que el siguiente capítulo desarrollará los principales apartados relacionados a la estructura metodológica, en donde el primero de ellos será especificar cuál será el tipo de investigación a realizar en el trabajo y partiendo de esta base será definido el diseño, la muestra a utilizar y cómo será procesada dicha muestra a fines de obtener la información pertinente.

3.1 Tipo de investigación

Son varios los enfoques que pueden ser utilizados para catalogar las tipologías a ser empleadas, por lo que este trabajo utilizará como referencia la establecida por Sampieri, Fernández y Baptista (2014) quienes definen la tipología como: “La tipología se refiere al alcance que puede tener una investigación científica. La tipología considera cuatro clases de investigaciones: exploratorias, descriptivas, correlaciónales y explicativas” (p 104).

Para este trabajo de investigación será llevado a cabo un estudio de alcance descriptivo, que según Sampieri, Fernández y Baptista (2014):

> Con frecuencia, la meta del investigador consiste en describir fenómenos, situaciones, contextos y sucesos; esto es, detallar cómo son y se manifiestan. Con los estudios descriptivos se busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es decir, únicamente pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren, esto es, su objetivo no es indicar cómo se relacionan éstas. (p.92).

El trabajo corresponde con dicha tipología porque se pretende estudiar como el riesgo que puede estar asociado a los activos de la empresa, pueden afectar el valor

de los mismos y por ende terminen afectando a la empresa. Y para entender como son los riesgos asociados a los activos de la empresa, es necesario estudiar y describir las características de la empresa de servicios CIAP. Siguiendo la premisa establecida por Sampieri et al., (2014), sólo se recogerá información de manera independiente o conjunta sobre los activos y los riesgos asociados a ellos.

De acuerdo a la finalidad de la investigación, será de carácter aplicado, ya que tiene como propósito la solución de problemas, que en este caso es cómo gestionar los riesgos asociados a los activos de la empresa.

De acuerdo a su alcance será de carácter seccional o transversal, ya que no serán usadas series de tiempo en ningún momento.

Y, por último, de acuerdo a su amplitud, la investigación será microsociológica (se estudian variables y sus relaciones limitándose a grupos pequeños y medianos).

3.2 Diseño de investigación

"El diseño de investigación es la estrategia general que adopta el investigador para responder al problema planteado. En atención al diseño, la investigación se clasifica en: documental, de campo y experimental" (Arias, 2012, pág. 27). Además, el diseño de investigación también es utilizado según Sampieri et al., (2014) con el propósito de responder a las preguntas de investigación planteadas y cumplir con los objetivos del estudio.

El diseño de investigación a utilizar corresponde al diseño de campo o investigación de campo, que es definida según Arias (2012) como:

> Aquella que consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna, es decir, el investigador obtiene la información, pero no altera las condiciones existentes. De allí su carácter de investigación no experimental. (pág. 31).

Esta definición es complementada con la ofrecida por Universidad Pedagógica Experimental Libertador (2003):

> Se entiende por investigación de campo, el análisis sistemático de problemas en la realidad, con el propósito bien sea de describirlos, interpretarlos, entender su

> naturaleza y factores constituyentes, explicar sus causas y efectos, o predecir su ocurrencia, haciendo uso de métodos característicos de cualquiera de los paradigmas o enfoques de investigación conocidos o en desarrollo. Los daos de interés son recogidos en forma directa de la realidad; en este sentido se trata de investigaciones a partir de datos originales o primarios. (pág. 14).

Pero esto no resulta excluyente que se tengan matices propios de un diseño de investigación del tipo documental. Al respecto Arias (2012) comenta que:

> En una investigación de campo también se emplean datos secundarios, sobre todo los provenientes de fuentes bibliográficas, a partir de los cuales se elabora el marco teórico. No obstante, son los datos primarios obtenidos a través del diseño de campo, los esenciales para el logro de los objetivos y la solución del problema planteado. (pág. 31).

Además de que parte de la información necesaria para llevar a cabo la investigación será recabada de material documental ofrecido por la empresa.

Siguiendo a Ramírez (2010) citado en Arias (2012), la investigación a su vez será de carácter intensivo, debido a que se concentra en un caso particular, sin la posibilidad de generalizar los resultados.

Sabino (2002) citado en Arias (2012), incluye en los diseños de campo, los siguientes tipos:

- Encuesta
- Panel
- Estudio de casos
- Ex post facto

Donde nos centraremos en el estudio de caso debido a que es el que se ajusta a la investigación que se está desarrollando. Es definido por Arias (2012) como:

> **Estudio de casos**
>
> En principio, se entiende por caso, cualquier objeto que se considera como una totalidad para ser estudiado intensivamente. Un caso puede ser una familia, una institución, una empresa, uno o pocos individuos.
>
> Debido a que un caso representa una unidad relativamente pequeña, este diseño indaga de manera exhaustiva, buscando la máxima profundidad del mismo. (pág. 33).

Por todos estos sustentos teóricos que fueron presentados podemos decir que, la investigación que se está desarrollando corresponde a un diseño de investigación de campo de carácter intensivo del tipo: estudio de caso. Esto debido a que el objetivo que se persigue es analizar el riesgo asociado a los activos para una empresa en

particular, en el que la información es obtenida directamente de la institución sin que se altere de alguna manera el ambiente en el que se desarrolla la misma.

3.3 Unidad de estudio y unidad de análisis

En esta sección se debería describir a la población, así como el tamaño y forma de selección de la muestra, es decir, el tipo de muestreo.

Pero, siguiendo a Arias (2012), este punto se omite en:

> a) Investigaciones documentales monográficas, debido a que el universo equivale al tema de estudio.
>
> b) Estudios de caso único, los cuales se concentran en uno o pocos elementos que se asumen, no como un conjunto sino como una sola unidad. (pág. 111).

La unidad de estudio es la unidad de la cual se requiere la información; la unidad de estudio corresponde a la entidad que va a ser objeto de medición y se refiere al qué o quién es sujeto de interés en una investigación. Para este trabajo de investigación, la unidad de estudio corresponde a la empresa de servicios CIAP.

La unidad de análisis es la unidad que define el investigador para realizar mediciones. Teniendo en consideración el objetivo general de la investigación es **aplicar un modelo de gestión de riesgos bajo un enfoque de administración del valor de los activos para determinar el riesgo al que está expuesto la empresa**; la unidad de análisis estará constituida por los activos que pertenecen a la organización en estudio; Esto “le permitirá al investigador, limitar y dar un alcance claro y definido al caso de estudio, el cual contribuirá a dar respuesta al problema planteado” (Escalona, 2017)

3.4 Técnicas e instrumentos de recolección de datos

Sampieri, Fernández y Baptista (2014) detallan cual sería el procedimiento a seguir a una vez llegado a este punto en un trabajo de investigación:

> La siguiente etapa consiste en recolectar los datos pertinentes sobre los atributos, conceptos o variables de las unidades de muestreo/ análisis o casos (participantes, grupos, fenómenos, procesos, organizaciones, etcétera).

> Recolectar los datos implica elaborar un plan detallado de procedimientos que nos conduzcan a reunir datos con un propósito específico
> Este plan incluye determinar:
>
> ¿Cuáles son las fuentes de las que se obtendrán los datos?
> ¿En dónde se localizan tales fuentes?
> ¿A través de qué medio o método vamos a recolectar los datos?
> Una vez recolectados, ¿de qué forma vamos a prepararlos para que puedan analizarse y respondamos al planteamiento del problema?
> (p.198).

"Para ello es necesario utilizar las técnicas e instrumentos de recolección de datos. Se entenderá por técnica de investigación, el procedimiento o forma particular de obtener datos o información" (Arias, 2012, pág. 67), por lo que dicha técnica precede al instrumento de recolección a utilizar. Mientras que, el instrumento de recolección de datos "es cualquier recurso, dispositivo o formato (en papel o digital), que se utiliza para obtener, registrar o almacenar información" (Arias, 2012, pág. 68)

Para llevar a cabo el trabajo de investigación es vital conocer cuáles son los activos de la empresa y el valor de los mismos. Para obtener dicha información las técnicas e instrumentos que se utilizaran son:

1. **Análisis documental:** Revisión de los estados financieros de la empresa y cualquier otro material que sea pertinente para la investigación.

2. **Encuesta:** "Constituye una técnica de investigación dirigida al estudio, para recoger datos cuantitativos" Morales (1994) citado en Castro Márquez (2003, pág.71) mediante la aplicación de procesos de interrogación y registro de datos.

   La encuesta a emplear será del tipo escrita, la cual recibe el nombre de cuestionario, que "consiste en un conjunto de preguntas respecto de una o más variables a medir" (Chasteauneuf, 2009) citado en Sampieri et al., (2014, pág.217). El cuestionario realizará preguntas de tipo cerrada con opciones múltiples de respuesta.

Las encuestas serán empleadas debido a que la empresa no posee información estadística sobre las amenazas (probabilidades, frecuencia, impacto). Las personas a encuestar serán los denominamos "expertos".

Es importante que en esta encuesta participen las personas que conozcan a profundidad los procesos y los sucesos diarios de la empresa. Mientras mayor

cantidad de expertos participen es más robusto el cálculo, sin embargo, la prioridad en este punto es que quienes participen puedan ser considerados realmente expertos. En este sentido, se define como experto a un empleado de la empresa que tenga al menos un año como empleado del CIAP y que además tenga asignado el cargo de "coordinador", ya que son ellos quienes dirigen los procesos medulares de la empresa. También será incluido dentro de los expertos a la directora de la empresa.

3.5 Técnicas de procesamiento y análisis de datos

Las técnicas de procesamiento y análisis de datos son las herramientas necesarias para poder transformar la información recabada. A partir de ella es que se podrán realizar conclusiones y en base a eso dar respuesta a las incógnitas creadas en el trabajo de investigación.

Sobre este proceso Arias (2012) comenta que:

> En este punto se describen las distintas operaciones a las que serán sometidos los datos que se obtengan: clasificación, registro, tabulación y codificación si fuere el caso. En lo referente al análisis, se definirán las técnicas lógicas (inducción, deducción, análisis-síntesis), o estadísticas (descriptivas o inferenciales), que serán empleadas para descifrar lo que revelan los datos recolectados. (pág. 111).

Las técnicas de procesamiento a emplear son:

1. **Registro**: Técnica para indicar la frecuencia con que ocurre un suceso (Castro Márquez, 2003). En nuestro caso, esto se realiza en el cuestionario cuando se les pregunta a los expertos sobre la frecuencia de las amenazas.
2. **Codificación:** Técnica que consiste en categorizar los datos obtenidos para transformarlos en símbolos numéricos Castro Márquez (2003). Esta técnica se utiliza para procesar los procesos de caracterización de los activos, las amenazas y las vulnerabilidades.
3. **Tabulación:** Técnica que consiste en el ordenamiento de la información que al ser procesada y cuantificada por ítems y agrupada por variable permite la presentación de tablas Méndez (2001) citado en Castro Márquez (2003, pág. 78). Esta técnica será empleada para la información recaba en el cuestionario sobre las variables en estudio, para así poder realizar el análisis y Graficación pertinente de cada una.

Las técnicas de análisis de datos a emplear son:

1. **Descriptivas:** Se emplea para comprender el tratamiento y análisis de datos que tienen por objeto resumir y describir los hechos que han proporcionado la información, y que por lo general toman la forma de tablas, cuadros e índices Tamayo (2001) citado en Castro Márquez (2003, pág. 80).

Toda esta información obtenida será procesada a de los programas de Office: **Word y Excel**.

3.6 Metodología

3.6.1 Fase 1: Determinar el contexto

Es esencial que la gestión de riesgos se integre tanto con el resto de áreas de la empresa como con su entorno externo. Por tanto, hay que determinar las condiciones tanto internas como externas que definen el marco de trabajo en el que se desenvuelve la empresa “lo que determinará el análisis de riesgos y la aplicación de la metodología en general” Departamento administrativo de la función pública de Colombia – DAFP (2018, pág.11). A nivel interno se tendrán en cuenta: misión, valores, estructura organizacional, organigrama de procesos. A nivel externo se consideran diferentes aspectos relativos al entorno: políticos, económicos y financieros, sociales, culturales y competitivos.

3.6.2 Fase 2: identificación y caracterización de los activos de la empresa

En esta fase se determinarán cuáles son los activos que posee la empresa. Para ello se podría trabajar con un inventario de activos elaborado por la empresa o por los reflejados en el balance general. En nuestro caso usaremos el balance general de la empresa para determinar los activos y su valor por la ausencia de un inventario.

La caracterización se realizará en base a los dos factores críticos asociados a un activo: El primer factor es la importancia crítica del activo para la misión de la organización, y el segundo es: el tiempo perdido, la productividad, y el costo de recuperar el activo si se daña o se pierde (consecuencias) (Norman, 2009). Pero haciendo la aclaratoria de que las consecuencias que son medidas en esta fase no guardan relación con el impacto (severidad) que será determinado en una fase superior. Este tipo de consecuencias son estudiadas para entender la importancia que tienen los activos identificados en las operaciones diarias de la empresa.

La importancia de un activo para la misión de la organización se mide por la gravedad de las operaciones de la organización que se afectarían si el activo se pierde o sufre daños graves. Si un activo (persona, propiedad, información o reputación comercial) es esencial para la misión de la organización, se puede decir que es crítico.

Tabla 4. Nivel crítico de los activos

Leyenda	
Nivel crítico	
Valor	**Descripción**
0	absolutamente no crítico para la misión
1	no es crítico, pero es útil para las operaciones
3	algo crítico pero las operaciones se verían seriamente afectadas
5	crítico, pero las operaciones podrían continuar a una capacidad disminuida
7	muy crítico, pero las operaciones podrían continuar por varios días
10	Absolutamente crítico para las operaciones diarias

Fuente: L. Norman, Análisis de riesgos y contramedidas de seguridad, 2009
Elaboración propia

Tabla 5. Consecuencias en caso de daño parcial o pérdida total del activo

Leyenda
Anális de consecuancias en caso pérdida total o daño parcial Posibles consecuencias
Bajas Masivas
Pérdida de la propiedad
Pérdida de producción
Pérdida de información
Impacto medio ambiental
Pérdida de reputación comercial (confianza en la organización por parte del público)

Fuente: L. Norman, Análisis de riesgos y contramedidas de seguridad, 2009
Elaboración propia

Tabla 6. Costo de reemplazo en caso de daño parcial o pérdida total del activo

Leyenda	
Análisis de consecuencias en caso pérdida total o daño parcial	
Costo de reemplazo	
Categoría	**Descripción**
Absolutamente crítico	El costo de reemplazar sería imposible de soportar
Muy crítico	Reemplazable a un costo muy alto en dólares o pérdida de producción
Crítico	Reemplazable a un costo significativo dólares o pérdida de producción
Algo crítico	El costo afectaría a otras operaciones o desarrollo de planes
No crítico	Fácilmente reemplazable

Fuente: L. Norman, Análisis de riesgos y contramedidas de seguridad, 2009
Elaboración propia

3.6.3 Fase 3: Identificar / seleccionar las amenazas y sus fuentes / actores

Una vez que se han determinado cuales son los activos de la empresa, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos. Tal y como imaginamos, el conjunto de amenazas es amplio y diverso por lo que se debe hacer un esfuerzo en mantener un enfoque práctico y aplicado.

A su vez, también serán identificados los distintos actores de amenaza a los que está expuesto la empresa en base a las características internas y externas en las que se desenvuelve.

3.6.4 Fase 4: Identificar vulnerabilidades

La siguiente fase consiste en estudiar las características de nuestros activos para identificar puntos débiles o vulnerabilidades. Además de aquellas vulnerabilidades que se presentan en las labores cotidianas de la empresa que podría afectar a los activos.

3.6.5 Fase 5: Análisis de riesgos

Se busca establecer la probabilidad de ocurrencia de las amenazas y su impacto o severidad, con el fin de estimar la zona de riesgo inicial. Una vez recolectada toda la información pertinente se podrá proceder al cálculo del riesgo inherente (riesgo total antes del estudio de los controles).

- **Probabilidad, impacto y frecuencia de las amenazas:**

La probabilidad, impacto y frecuencia asociado a las amenazas será determinada a partir del cuestionario realizado a los coordinadores de la empresa. Una vez hayan sido tabuladas todas las respuestas de los coordinadores (expertos) se procederá a calcular el promedio aritmético para cada una de ellas, con la finalidad de obtener un valor final de probabilidad de ocurrencia e impacto para cada amenaza.

Se utilizarán los criterios establecidos en la **tabla 7** (impacto de las amenazas), en donde la calificación monetaria (pérdida de valor) corresponde al criterio utilizado en el trabajo de investigación de León Ruiz (2017) (que corresponde al antecedente número **4** de este trabajo de investigación). Y los criterios establecidos en la **tabla 8** (probabilidad de ocurrencia) para categorizar los resultados obtenidos en las encuestas.

Tabla 7. Impacto (severidad) de las amenazas

Nivel	Descripción	Concepto	Calificación monetaria (Pérdida de valor)
1	Insignificante	El riesgo tiene un efecto nulo o pequeño, en el desarrollo del proceso - Baja pérdida financiera	El activo pierde hasta un 1% del valor
2	Menor	El desarrollo del proceso sufre un daño menor - Con pérdida financiera menor	El activo pierde hasta un 5% del valor
3	Moderado	El desarrollo del proceso sufre un deterioro, dificultando o retrasando su cumplimiento - Con afectación financiera	El activo pierde hasta un 10% del valor
4	Mayor	El desarrollo del proceso es afectado significativamente - Pérdida financiera mayor	El activo pierde hasta un 30% del valor
5	Catastrófico	El proceso es gravemente dañado - Enorme pérdida financiera	El activo pierde hasta un 100% del valor

Fuente: Diz Cruz, Gestión de riesgos, 2015
Elaboración propia

Tabla 8. Probabilidad de ocurrencia de las amenazas

Nivel	Descripción	Concepto	Desde	Hasta
1	**Casi improbable**	Puede ocurrir en algún momento	**0%**	**9%**
2	**Poco probable / Raro**	Puede ocurrir en circunstancias excepcionales	**10%**	**25%**
3	**Probable**	Probablemente ocurrirá en la mayoría de las circunstancias	**26%**	**50%**
4	**Potencial**	Puede ocurrir en la mayoría de circunstancias	**51%**	**75%**
5	**Casi cierto**	Se espera que ocurra en la mayoría de las circunstancias	**76%**	**100%**

Fuente: Diz Cruz, Gestión de riesgos, 2015
Elaboración propia

Llegado a este punto disponemos de los siguientes elementos para cada amenaza:

- Frecuencia
- Impacto / severidad
- Probabilidad de ocurrencia

Por lo que podremos proceder a calcular el riesgo total. Además de esto, con esta información también es posible elaborar la matriz de riesgo (mapa de calor).

Modelo matemático:

- La empresa cuenta con activos que poseen un valor determinado. Dicho valor de los activos lo denominaremos $\boldsymbol{v_j}$, donde $\boldsymbol{j = 1 \ldots M}$.
- Existen amenazas que explotan las vulnerabilidades e impactan los activos, tal que el impacto de la amenaza $\boldsymbol{i}$ sobre el activo $\boldsymbol{j}$ la denominaremos $\boldsymbol{c_{ij}}$.
- Si llamamos $\boldsymbol{p_i}$, a la probabilidad de ocurrencia de la amenaza $\boldsymbol{i}$, entonces el riesgo inherente o riesgo total viene dado por la ecuación 1:

Ecuación 1. Nivel de riesgo

$$R = \sum_{i=1}^{i=N} \sum_{j=1}^{M} p_i \times c_{ij} \times v_j$$

Que corresponde al **nivel de exposure de riesgo**.

3.6.6 Fase 6: Evaluación de riesgo

Se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (riesgo residual).

El primer paso corresponde a analizar los controles existentes para cada amenaza identificada. La existencia de los controles y el grado de implementación y eficiencia serán determinados a través del cuestionario realizado a los “expertos”. Además, el de determinar el factor de reducción (**μ**), que es la reducción de la probabilidad de ocurrencia de la amenaza gracias al control establecido.

Tabla 9. Criterios de evaluación de los controles de la empresa

Evaluación de controles existentes		
tipo de control	**descripción**	**valoración**
a) determinar si los controles son documentados		
documentado	Es posible conocer cómo se lleva a cabo el control, quien es el responsable, periodicidad y reportes de gestión. Existen manuales, instructivos o procedimientos para el control de riesgos	**15**
	Están definidos los responsables para el control	**5**
no documentado	No existe evidencia escrita del control	**0**

b) Establecer si el control que se implementa es automático o manual		
Automático	Utilizan herramientas tecnológicas para hacer seguimiento, aprobaciones a ejecuciones, control de aprobación, sistemas de grabación, entre otros	**15**
Manual	Políticas de operación aplicables, controles duales, firmas conjuntas, firmas de autorización, confirmaciones vía correo o telefónicas, listas de chequeo, controles con personal de seguridad	**10**
c) Determinar si los controles se están aplicando en la actualidad		
Se aplican en la actualidad	La frecuencia del control es adecuada	**15**
	Se cuenta con evidencias de control efectuado	**10**
	En el tiempo que lleva la herramienta demuestra ser efectiva	**30**
No se aplica en la actualidad	Existen en conocimiento del personal, pero no son aplicables por que no están documentados o no forman parte de un proceso.	**0**
Fuente:		
Valor total obtenido en base a los controles establecidos		**100**

León Ruiz, Desarrollo de un modelo de gestión de riesgos, 2017
Elaboración propia

Una vez se obtenga toda la información pertinente sobre los controles, se procederá a valorar cada uno de ellos, para así determinar el grado de eficiencia que posee cada uno.

Tabla 10. Valoración de controles de la empresa

Valoración de controles		
Rango de clasificaciones	**Descripción del control**	**Valoración**
Entre 0 y 5	No existe control	0%
Entre 6 y 50	Control deficiente	25%
Entre 51 y 75	Control medio	50%
Entre 76 y 100	Control efectivo	100%

Fuente: León Ruiz, Desarrollo de un modelo de gestión de riesgos, 2017
Elaboración propia

Con base a esta información se puede proceder a calcular el riesgo residual y la matriz de riesgo definitiva, ya que en esta fase se cuenta con las amenazas ajustadas por los controles y el riesgo calculado es el definitivo.

Modelo de control:

- Si la empresa dispone de $\boldsymbol{Q}$ controles con un costo de $\propto_{\boldsymbol{k}}$, donde el control $\boldsymbol{k}$ reduce la probabilidad de la amenaza $\boldsymbol{i}$ por un factor **μ**, entonces la **probabilidad de ocurrencia revisada** es:

Ecuación 2. Probabilidad ajustada por control

$$p_i^* = \prod_{k=1}^{Q}(1 - \mu_{ki}) \times p_i$$

- Si introducimos la ecuación de probabilidad de ocurrencia revisada en la formula original, obtendremos el **nivel revisado de exposure al riesgo ($\boldsymbol{R}^*$)**:

Ecuación 3. Nivel de riesgo revisado

$$R^* = \sum_{i=1}^{i=N}\sum_{j=1}^{M}\left(\prod_{k=1}^{Q}(1 - \mu_{ki}) \times p_i\right) \times c_{ij} \times v_j$$

- Si $\boldsymbol{\gamma}$ es el presupuesto máximo asignado para controles, entonces el problema de optimización viene dado por:

$$Minimizar\colon\ R^* + \sum_{k=1}^{k=Q} \propto_j \ tal\ que \sum_{j=1}^{k=Q} \propto_j \ \leq \ \gamma$$

3.6.7 Fase 7: tratamiento del riesgo

A continuación, se identifican y evalúan las opciones existentes de tratamiento de cada una de las amenazas que sea necesario tratar según se determinó en la fase anterior.

Todo el proceso del modelo de gestión de riesgo aplicado queda resumido en la figura 6.

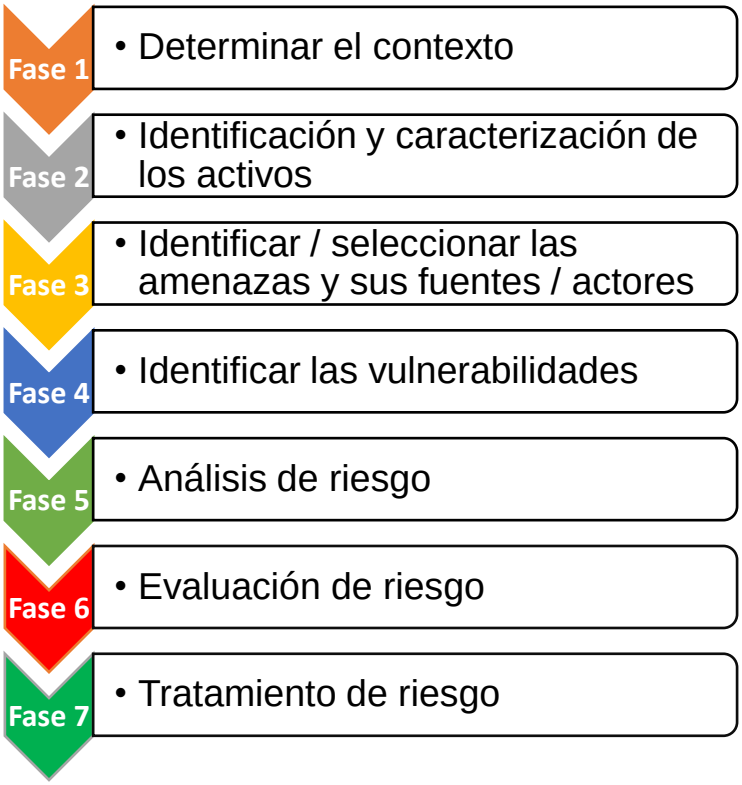


Figura 6. Modelo de gestión de riesgo aplicado

Fuente: Elaboración propia

CAPÍTULO IV

ANÁLISIS DE RESULTADOS

En el presente capítulo se realiza la exposición de los resultados obtenidos en la ejecución de las distintas fases de la metodología de gestión de riesgos empleada.

4.1 Fase 1: Establecimiento del contexto de la empresa

4.1.1 Contexto interno

Descripción de la empresa: El Centro Internacional de Actualización Profesional (CIAP) es una empresa que cuenta aproximadamente con 22 empleados. Dicha empresa se dedica a la formación académica para aquellas personas que se encuentren culminando la carrera universitaria o que ya la han culminado.

En los últimos cinco años ha contado con 18.474 participantes, 1145 actividades y 294 adiestramientos corporativos.

Misión: “Ofrecer a los técnicos y profesionales la actualización que requieren para incrementar su potencial, maximizar su desempeño laboral, transformar su entorno personal y organizacional, y generar bienestar social” CIAP (2018).

Visión: “Desarrollar y producir la oferta nacional e internacional de actualización técnico-profesional en las diferentes áreas del conocimiento, con criterios de pertinencia y excelencia académica, así como con altos niveles de calidad de servicio, a través de Diplomados, Programas, Cursos y Eventos, sustentados en los modelos presenciales, semipresenciales y en línea” CIAP (2018).

Valores: “Responsabilidad, Innovación, Empatía y Compromiso” CIAP (2018).

Estructura organizacional y diagrama de procesos: A continuación, es presentado el organigrama de la empresa. Para ver el diagrama de procesos deberá acudir al **anexo A**.

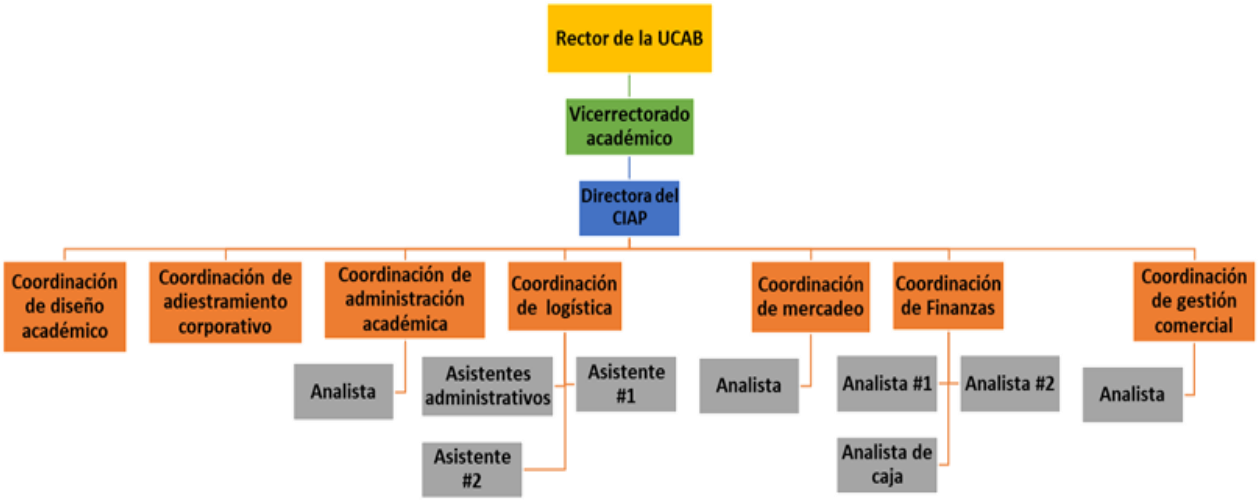


Figura 7*. Estructura organizacional*

Fuente: CIAP
Elaboración propia

4.1.2 Contexto externo

Entorno político: El entorno político en Venezuela cada año se vuelve más complejo, hasta el punto de estar viviendo la peor crisis política en la historia del país. Una crisis que ha llegado a afectar a los países vecinos de la región y que ha calado en el debate de la política internacional. Esto queda reflejado por la ruptura del sistema político y democrático del país, que ha generado en todos los ámbitos de la economía distorsiones de tal magnitud, que no solo se vean afectadas las libertades civiles, sino, que la legislación económica hace muy complejo que una empresa logre mantenerse operando durante esta crisis.

A todo esto, se le suma la persecución del gobierno a las distintas facciones políticas opositoras, lo cual es una arista importante a considerar en el entorno del CIAP, debido a que en la sede se dan encuentros de diversas personalidades políticas y universitarias. A su vez, este tipo de encuentros tienen lugar en el Centro de Estudios Políticos y de Gobierno de la UCAB, que se ubica en el mismo edificio en el que se encuentra el CIAP.

Entorno económico y financiero: Sumado a la grave crisis política del país, Venezuela también está atravesando la peor crisis económica de su historia, alcanzando niveles históricos de: inflación, caída del PIB, pobreza, desigualdad social, corrupción, etc.

Si la situación de Venezuela no era lo suficientemente grave, ahora se le suma la crisis económica mundial generada por el COVID-19, que ha paralizado al mundo por meses, generando que se disparen las tasas de desempleo e incertidumbre sobre el futuro de las economías. Lo más preocupante de esta situación es el impacto que tuvo sobre el mercado petrolero, que desde principios de 2019 entró en un declive y no pudo superar la barrera de los 65$, pero con la crisis sanitaria, el precio del barril de petróleo de la OPEP ha sido fuertemente castigado por la paralización de la economía mundial y la consecuente caída de la demanda de petróleo. Es a mediados de mayo que ha empezado la recuperación del precio del barril de petróleo (aun así, oscilando alrededor de los 35$, lo cual es un precio que no beneficia a los países petroleros).

Hoy más que nuca Venezuela es dependiente de los ingresos petroleros, pero la destrucción de la industria petrolera y la situación que atraviesa el gobierno, generan que este no tenga capacidad de respuesta ante la crisis. Esto plantea un entorno en el que es cada día más complejo para las empresas y las personas, que al ver socavado su poder adquisitivo y nivel de vida, dedican sus ingresos a bienes de primera necesidad, lo que deja a empresas como el CIAP en una situación crítica, ya que cada vez dedican menos dinero a educación superior.

Entorno social y cultural: La crisis política y económica ha afectado brutalmente a la sociedad venezolana, esto ha quedado reflejado en los índices de desnutrición, deserción del sistema educativo, criminalidad, migración, etc. Siendo la migración uno de los factores más importantes en la crisis venezolana, ya que la migración ha alcanzado niveles de países que están en guerra, y el movimiento migratorio ha sido tal, que los países de la región se han visto desbordados de la cantidad de venezolanos que han llegado, y esto a su vez ha traído problemas de xenofobia contra los migrantes del país. Por lo que cada vez son más los venezolanos que deciden emprender rumbo al exterior y desarrollar sus estudios y carreras en otros países, y así como se mencionaba antes, todos estos factores generan que las personas que

se dedican a continuar sus estudios después del bachillerato o la universidad sean cada vez menos, lo que plantea una fuerte disminución de la demanda de formación post universitaria de empresas como el CIAP. Este hecho queda contrastado con un artículo publicado en marzo de 2020 por el portal venezolano “Descifrado”, en el que se entrevistó a Benjamín Scharifker (rector de la Universidad Metropolitana y coordinador del Plan País), que aseveró que “la deserción estudiantil y profesoral ronda en promedio el 40%”.

Entorno competitivo: La empresa CIAP ofrece formación en distintas áreas para profesionales y lo hace bajo distintos niveles de formación, que van desde cursos y diplomados, hasta acreditaciones internacionales; son impartidos tanto en modalidad presencial como virtual. Esto implica que sus principales competidores son sus homólogos de otras universidades como los centros de formación de las Universidades: Simón Bolívar, Central de Venezuela y la Metropolitana. Pero al ofrecer diversas modalidades de formación en diversas áreas genera que la competencia del CIAP vaya desde instituciones muy bien valoradas como el IESA, hasta instituciones más modestas de menor envergadura. Por lo que el CIAP se desenvuelve en un mercado muy competitivo que cada vez tiene menos demanda por parte del público.

4.2 Fase 2: Identificación y caracterización de los activos

Los activos identificados (con su respectivo valor) quedan reflejados en la tabla 11:

Tabla 11. Activos identificados y valor reflejado en el balance general al 31 de julio de 2019

Activo	Valor en Bolívares	Valor en dólares
Efectivo en cajas y bancos	Bs.S 690.540.298	$ 64.350
Cuentas por cobrar	Bs.S 19.197.020	$ 1.789
Equipo y mobiliario neto	Bs.S 324.000.000	$ 30.193
Valor total activos	Bs.S 1.033.737.318	$ 96.332

Fuente: Elaboración propia

El valor de los activos expresado en bolívares (constantes) fue obtenido del Balance General proporcionado por la empresa, que corresponde a un informe financiero al 31 de julio de 2019. Y la tasa utilizada para calcular el valor en dólares, fue la tasa oficial publicada por el Banco Central de Venezuela al 31 de julio de 2019, que corresponde a una tasa de cambio de 10.731 Bs.S por dólar.

Debido a la situación de hiperinflación que vive Venezuela, el valor de los activos reflejados en el balance general para julio 2020, ya están desfasados. Pero al no poseer la información financiera necesaria por parte de la empresa para actualizar los valores de dichos activos, una actualización de los mismos considerando las tasas de inflación de julio 2019 a julio 2020 causaría la sobrevaloración de los activos, ya que, hay que recordar que los valores reflejados en el balance general son el resultado de normas y procedimientos contables que deben ser respetados.

Para haber realizado una correcta actualización de su valor, se tienen que aplicar las normas establecidas por la VEN-NIF (Normas de Información Financiera de Venezuela), en la que se contemplan la actualización de los estados financieros por el efecto de la inflación en los mismos. Para realizar dicha actualización, la norma establece que se debe contar con información financiera sobre: depreciación de activos, costo de adquisición, valor en uso, rendimiento esperado del activo en caso de que la característica del mismo atribuya un rédito futuro por su utilización, etc. Ya que la empresa no posee toda la información necesaria para realizar la actualización correcta, se usará el valor de los activos reflejados en el balance general al 31 de julio de 2019 como el valor actual de los activos.

El valor de los activos será reflejado en dólares por ser la moneda más representativa actualmente en la economía venezolana.

A continuación, se presentan los resultados y el análisis de los datos sobre los activos obtenidos a través de la encuesta aplicada a los expertos.

4.2.1 Nivel crítico de los activos

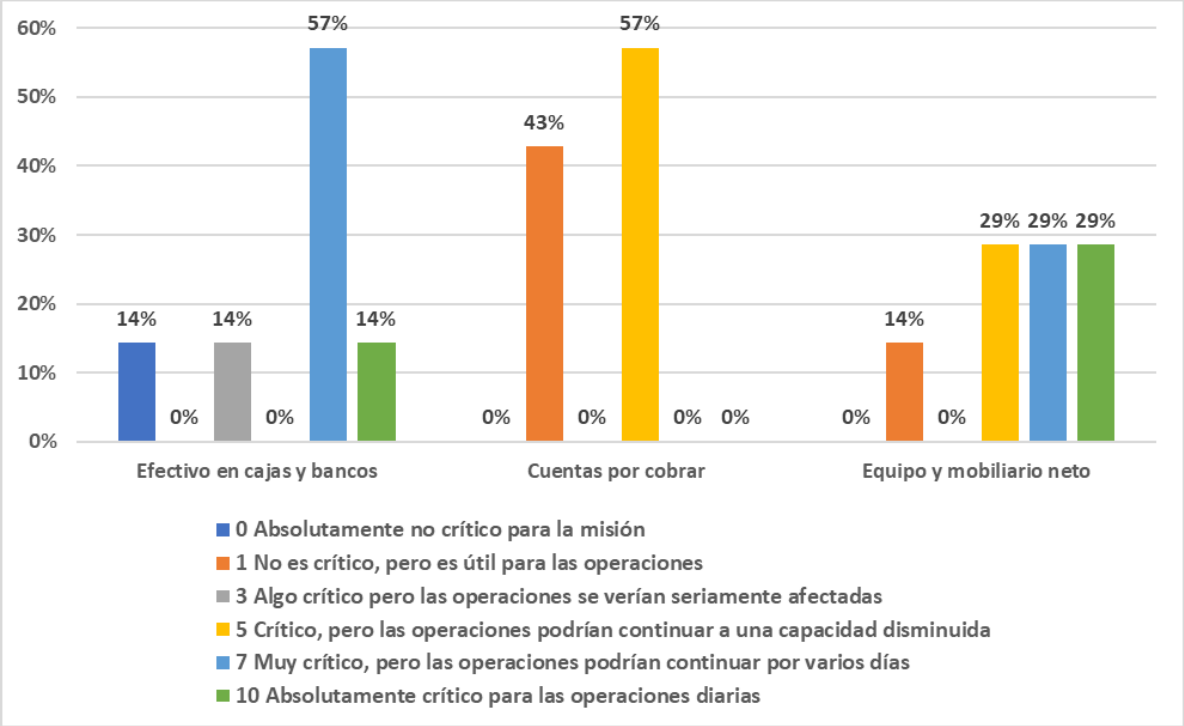


Figura 8. Nivel crítico de los activos de la empresa

Fuente: Elaboración propia

El nivel crítico para el activo “efectivo en cajas y bancos” se encuentra concentrado con un 57% en la categoría de “muy crítico”, mientras que, el resto de las opiniones se encuentran disperso con un 14% entre las opciones de “absolutamente no crítico” y “absolutamente crítico”. Lo que nos deja en claro que este es un activo importante, pero no paralizaría las operaciones en caso de sufrir una situación adversa.

En el caso del activo “cuentas por cobrar” se puede apreciar con claridad que no existe consenso claro en el nivel crítico que posee el activo. Ya que el 57% de los expertos lo clasifica como crítico para las operaciones, mientras que, el 43% lo clasifica como un activo que no es crítico para las operaciones. Esta disparidad puede deberse a que parte de los participantes del CIAP son admitidos bajo la modalidad de adiestramiento corporativo, y en este tipo de admisión, las empresas suelen pagar bajo cartas de compromiso. Por lo que, a pesar de ser un activo importante para la empresa y su continuidad a largo plazo, no es un activo del que dependen la cotidianidad de las actividades que desempeña.

El activo “equipos y mobiliario” tampoco posee un consenso claro sobre el nivel crítico, ya que las respuestas se encuentran repartidas con un 29% entre tres categorías. Lo que es destacable es que, en las tres categorías en las que se encuentran concentradas, son las clasificaciones más altas para el nivel crítico. Lo que nos da a entender que a pesar de que no exista una respuesta definitiva, este activo es vital para las operaciones diarias de la empresa. Y si lo analizamos con detenimiento, la única unidad de negocio que posee el CIAP (la prestación de servicios educativos), es lógico que este activo sea el más importante de los tres analizados, ya que es a través de él, es que se presta el servicio de formación académica.

4.2.2 Consecuencias en caso de daño parcial o pérdida total del activo

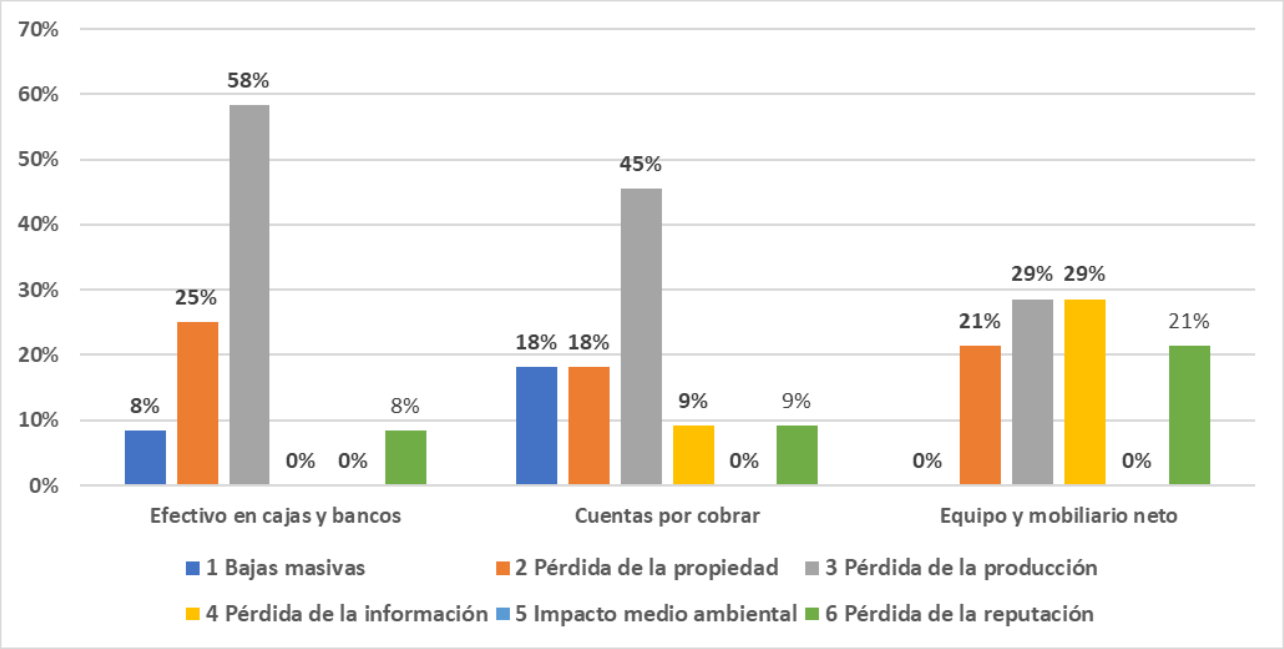


Figura 9. Consecuencias en caso de daño parcial o pérdida total del activo

Fuente: Elaboración propia

Las posibles consecuencias que generaría el daño o pérdida en el caso del activo “Efectivo en cajas y bancos” tiene una clara tendencia/respuesta. El 58% de los coordinadores concuerda que se generaría una pérdida de la producción. Mientras que el 25% considera que se generaría pérdida de la propiedad, que se refiere a la pérdida de la posesión del activo. Otro 8% considera que, si el activo sufriera una situación adversa, esto podría llegar a generar pérdida de la reputación del CIAP. Esto

puede estar ligado al hecho de que ocurra una situación como, por ejemplo: el robo de las divisas en efectivo (ya sea por parte de un agente externo o de algún personal del CIAP), podría generar pérdida de la confianza en la seguridad de la institución por parte del público y que sea catalogada como un lugar inseguro.

En el caso del activo “cuentas por cobrar”, también existe una clara tendencia/respuesta. El 45% de los coordinadores considera que el daño o pérdida de este activo generaría pérdida de la producción para la empresa. Mientras que el resto de las respuestas se encuentran bastante dispersas entre las distintas categorías. En segundo lugar, con 18% para cada una, se encuentra repartido entre bajas masivas y pérdida de propiedad. En tercer lugar, con 9% para cada una, se encuentra repartido entre pérdida de información y pérdida de reputación. A pesar de que no es un activo tangible, este activo es importante en las operaciones de la empresa, ya que contiene parte de los ingresos que genera la empresa bajo una de las dos modalidades de admisión (siendo las modalidades de admisión: ingreso para el público en general e ingreso a través de una empresa, que son quienes suelen pagar bajo cartas de compromiso).

Las respuestas para el activo “equipo y mobiliario” no posee un conceso, ya que las respuestas se encuentran dispersas de manera bastante pareja entre las distintas categorías. El primer escalón donde se concentran la mayoría de las respuestas, se encuentra con un 29% para cada una entre las categorías de pérdida de producción y de información. En el segundo escalón donde se concentran las respuestas, se encuentra con un 21% para cada una, entre las categorías pérdida de propiedad y de reputación. Esto nos habla de la importancia del activo, ya que, al ser tan importante, las consecuencias de daño o pérdida total, serían muy variadas.

Un punto importante a destacar en los activos “Efectivo en cajas y bancos” y “cuentas por cobrar”, es que algunos de los coordinadores encuestados respondieron que una de las posibles consecuencias que generaría el daño o pérdida del activo sería “bajas masivas”. Por lo que podemos concluir que existió un mal entendimiento de esta consecuencia, ya que esta hace referencia a la pérdida numerosa de vidas humanas, y el daño o pérdida de estos activos no poseen la capacidad de generar tal consecuencia.

4.2.3 Costo de reemplazo en caso de daño parcial o pérdida total del activo

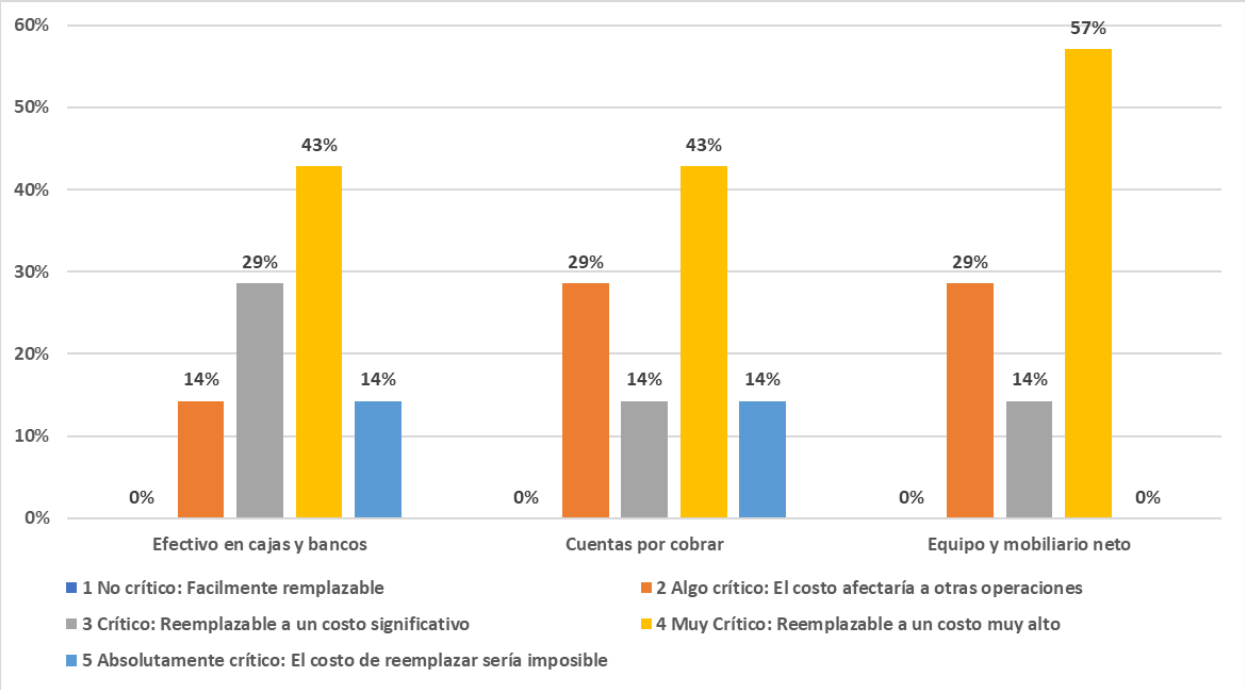


Figura 10. Consecuencias en caso de daño parcial o pérdida total del activo

Fuente: Elaboración propia

Para los 3 activos queda claro que existe una clara tendencia/respuesta del costo de reemplazo en caso de daño o pérdida del activo. Las categorías donde se concentran la mayoría de las respuestas se encuentran en la categoría “4. Muy crítico: El costo de reemplazo sería muy alto”. Mientras que el resto de las respuestas se encuentran entre las categorías 2 y 3. Lo cual tiene sentido cuando se tiene en consideración en el análisis que Venezuela está atravesando la peor crisis económica de su historia, por lo que es claro que esta situación con una hiperinflación, genera que reemplazar cualquier activo sea muy costoso y es aquí donde reside la importancia de proteger los activos de la empresa. Otro punto a destacar es que el hecho de que ningún activo sea categorizado como “imposible de reemplazar”, habla de la salud y capacidad financiera de la empresa, lo cual es un punto importante a considerar en la gestión de los activos de la empresa.

4.3 Fase 3: Identificación de las amenazas y sus fuentes/actores

En base a las condiciones de la empresa, las condiciones del entorno en el que se desenvuelven sus operaciones y las características de los activos, se identificaron las siguientes amenazas:

Tabla 12. Lista de amenazas identificadas

Amenaza	Variable
Operaciones no registradas intencionalmente	A1
Destrucción maliciosa de activos	A2
Robo de divisas en efectivo	A3
Robo de mobiliario	A4
Robo de equipos	A5
Robo de componentes de computadoras	A6
Robo de información (física o digital)	A7
Violación de normas de salud o seguridad	A8
Fallas en el software de los equipos	A9
Fallas en el Hardware de los equipos	A10
Carga de software malicioso (intencional o no)	A11
Cortes/Fallas en los servicios públicos	A12
Intrusión de cuerpos de seguridad y/o inteligencia del estado	A13
Terremotos	A14
Incendios	A15
Acceso no autorizado a las instalaciones	A16
Vandalismo	A17
Uso inadecuado del mobiliario por parte de los visitantes de la sede	A18

Fuente: Elaboración propia

Debemos recordar que la amenazas pueden ser originados por tres fuentes: naturales, ambientales y humanas. En el caso de las fuentes naturales se encuentran los terremotos e incendios. En el caso de la fuente ambiental: las fallas en los servicios públicos. El caso de las fuentes humanas, requiere un mayor nivel de caracterización por las características de la empresa, ya que es lugar de encuentro de personalidades políticas y universitarias. Además de que al ser un centro de formación educativo posee un flujo constante de entrada y salida de personas, por lo que la fuente de amenaza humana es la que tiene mayor capacidad de afectar los activos de la empresa. Es por esto que se hace menester el caracterizar los posibles actores de amenaza humana que podrían afectar a la empresa. Esta caracterización queda plasmada en la tabla 13.

Tabla 13. Actores potenciales de amenazas de origen humano

Grupo	Subgrupos
Delincuentes económicos	Delincuentes económicos poco soficticados
	Criminales callejeros (pandillas)
Criminales violentos no terroristas	Visitantes enojados
	Asalto / Violencia en el estacionamiento
	Desorden civil (evento de vionecia)
Subversivos	Subversivos orientados a la causa
	Espías políticos e industriales
	Saboteadores (Subversivos no alineados)
	Cultos / grupos activistas dedicados
	Violadores de reglas persistentes
Pequeños delincuentes	Vándalos

Fuente: L. Norman, Análisis de riesgo y contramedidas de seguridad, 2009.
Elaboración propia

Siguiendo la caracterización de amenazas humanas desarrollada por L. Norman se profundizará en la definición de los subgrupos cuya categoría no deje en claro su estructura e implicaciones:

- **Delincuentes económicos poco sofisticados:** Los delincuentes económicos poco sofisticados no tienen experiencia en el uso de armas y herramientas y no tienen una organización formal. Sus objetivos son aquellos artículos que satisfacen sus necesidades inmediatas. Los delincuentes poco sofisticados están interesados en objetivos oportunos que presentan poco o ningún riesgo.

- **Subversivos orientados a la causa:** Los subversivos orientados a la causa pueden incluir grupos de activistas con una agenda opuesta a un gobierno, religión, causa o industria.

A su vez, es importante definir las características de los actores potenciales de amenaza. La elaboración del cuadro antes presentado se basó en los planteamientos de actores potenciales de amenaza humana de Norman (2009).

En la tabla 14 quedan plasmadas las características de los distintos actores potenciales de amenaza humana identificados. Dicha tabla fue elaborada considerando las características de los grupos y del entorno del CIAP.

Tabla 14. Características de los actores potenciales de amenaza

Amenazas (Humanas)				
Características de los actores potenciales de amenaza				
Características	**Delincuentes económicos**	**Criminales violentos no terroristas**	**Subversivos**	**Pequeños delincuentes**
Profundidad de violencia				
Bajas masivas				
Pocas bajas		X		
Víctimas Individuales	X	X	X	
Lesiones	X	X	X	X
Delitos contra la propiedad				
Destrucción de la propiedad	X		X	
Robo de propiedad	X	X	X	X
Daño de propiedad	X	X	X	X
Delitos de información				
Destrucción de información		X		X
Robo de información		X	X	X
Daño a la información	X	X		X
Acceso no autorizado	X	X	X	X
Carga de software malicioso		X	X	
Delitos contra la reputación				
Daño contra la reputación del negocio	X	X	X	X
Métodos de ataque				
Ataque a plena vista	X	X	X	X
Generalmente ataca en sigilo		X	X	
Sobre la interrupción del ataque				
Probablemente se rendirá ante la interrupción	X	X	X	X
En respuesta forzada			X	
Repelerá la respuesta forzada	X	X	X	
Puede repeler la respuesta forzada	X	X	X	

Fuente: Elaboración propia

4.4 Fase 4: Identificación y caracterización de las vulnerabilidades

Con base a las condiciones de la empresa, las condiciones del entorno en el que se desenvuelven sus operaciones y las características de los activos, se identificaron las siguientes vulnerabilidades:

Tabla 15. Lista de vulnerabilidades identificadas

Vulnerabilidades	Variable
Manejo de divisas en efectivo	VU1
Fácil acceso a equipos	VU2
Falta de inversión en Hardware (Computadores y periféricos)	VU3
Falta de inversión en software para equipos	VU4
Sistemas operativos antiguos / desactualizados	VU5
Sistemas antivirus inexistentes o desactualizados	VU6
Uso de dispositivos externos sin control (pendrive)	VU7
Utilización de software de comunicación susceptible a intrusión	VU8
Fallas de comunicación y respuestas del equipo DTI (Dirección de tecnología e información)	VU9
Reemplazo inadecuado de equipos viejos	VU10
Insuficientes y/o inoperativas guayas de seguridad para las laptops	VU11
Control de inventario de equipos se efectúa esporádicamente	VU12
Mobiliario susceptible a termitas	VU13
Los equipos de computación son susceptibles a variaciones de voltaje	VU14
Ubicación vulnerable a terremotos	VU15
Falta de identificación de las personas que visitan la sede	VU16
Personal corruptible	VU17
Sede de la empresa es lugar de encuentro de personalidades políticas y de autoridades universitarias	VU18
La sede se encuentra abierta hasta la noche	VU19
Mantenimiento inadecuado de los equipos	VU20

Fuente: Elaboración propia

A continuación, se presentan los resultados y análisis obtenido a través de la encuesta para el nivel de importancia de las vulnerabilidades:

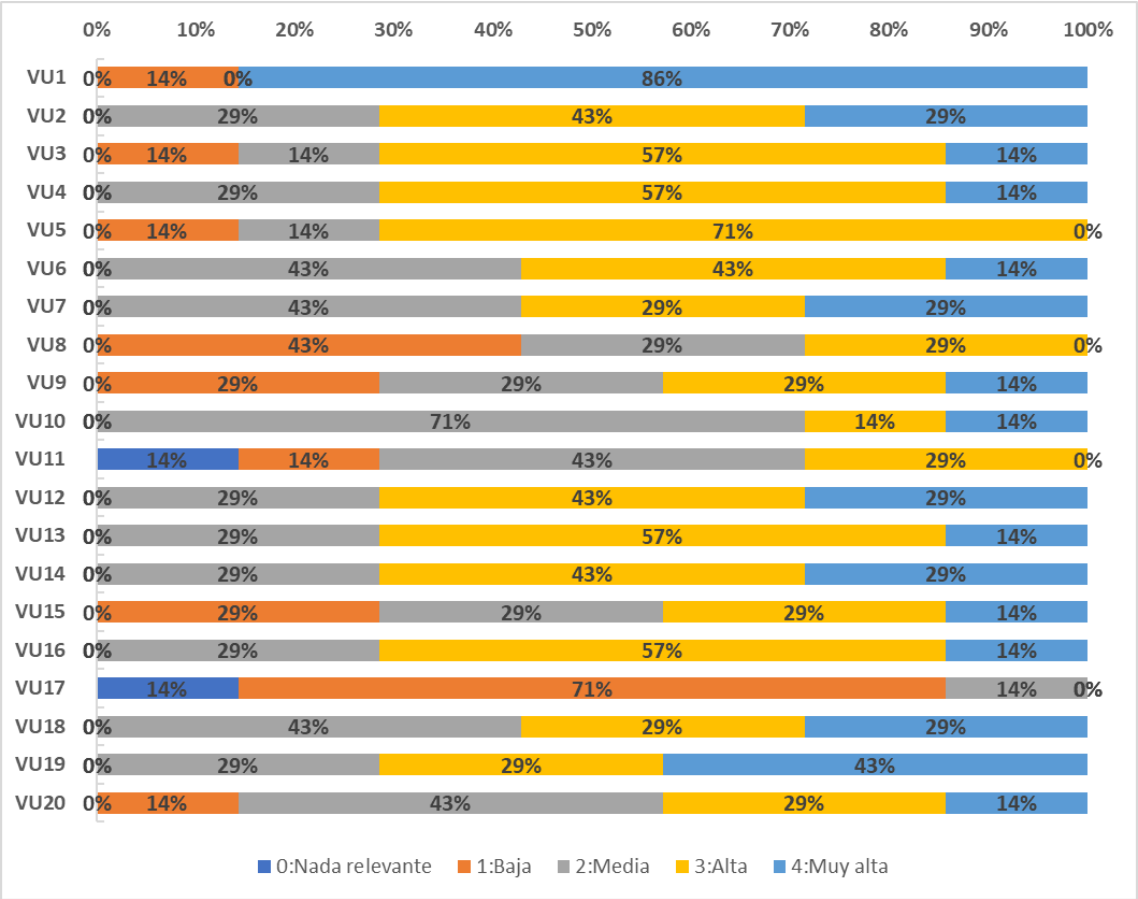


Figura 11. Nivel de importancia de las vulnerabilidades

Fuente: Elaboración propia

Entre las distintas vulnerabilidades identificadas, las más importantes en la categoría **"4: Muy alta"** destacan:

- **Con un 86%:** Manejo de divisas.
- **Con un 43%:** La sede se encuentra abierta hasta la noche.
- **Con un 29%:** fácil acceso a equipos, Uso de dispositivos externos sin control (pendrive), Control de inventario de equipos se efectúa esporádicamente, Los equipos de computación son susceptibles a variaciones de voltaje, Sede de la empresa es lugar de encuentro de personalidades políticas y de autoridades universitarias

Entre las distintas vulnerabilidades identificadas las más importantes en la categoría **"3: Alta"** destacan:

- **Con un 71%:** Sistemas operativos antiguos / desactualizados.
- **Con un 57%:** Falta de inversión en Hardware (Computadores y periféricos), Falta de inversión en software para equipos, Mobiliario susceptible a termitas, Falta de identificación de las personas que visitan la sede.
- **Con un 43%:** Fácil acceso a equipos, Sistemas antivirus inexistentes o desactualizados, Control de inventario de equipos se efectúa esporádicamente, Los equipos de computación son susceptibles a variaciones de voltaje.

Entre las distintas vulnerabilidades identificadas las más importantes en la categoría **"2: Media"** destacan:

- **Con un 71%:** Reemplazo inadecuado de equipos viejos.
- **Con un 43%:** Sistemas antivirus inexistentes o desactualizados, Uso de dispositivos externos sin control (pendrive), Insuficientes y/o inoperativas guayas de seguridad para las laptops, Sede de la empresa es lugar de encuentro de personalidades políticas y de autoridades universitarias, Mantenimiento inadecuado de los equipos.

Entre las distintas vulnerabilidades identificadas las más importantes en la categoría **"1: Baja"** destacan:

- **Con un 71%:** Personal corruptible.
- **Con un 43%:** Utilización de software de comunicación susceptible a intrusión.
- **Con un 29%:** Ubicación vulnerable a terremotos.

En la categoría **"0: Nada relevante":** Solo hay dos vulnerabilidades y solo el 14% de los coordinadores considera como "para nada importante" la vulnerabilidad de Personal corruptible e Insuficientes y/o inoperativas guayas de seguridad para las laptops. Por lo que todas las vulnerabilidades identificadas son en mayor o menor medida importantes y están presentes en la cotidianidad de la empresa.

Pero en términos generales, las vulnerabilidades más importantes son:

Tabla 16. Vulnerabilidades más importantes

Variable	Vulnerabilidad	Importancia
VU1	Manejo de divisas en efectivo	**4: Muy alta**
VU19	La sede se encuentra abierta hasta la noche	**4: Muy alta**
VU6	Sistemas operativos antiguos / desactualizados	**3: Alta**
VU4	Falta de inversión en Hardware (Computadores y periféricos)	**3: Alta**
VU5	Falta de inversión en software para equipos	**3: Alta**
VU14	Mobiliario susceptible a termitas	**3: Alta**
VU17	Falta de identificación de las personas que visitan la sede	**3: Alta**
VU3	Fácil acceso a equipos	**3: Alta**
VU7	Sistemas antivirus inexistentes o desactualizados	**3: Alta**
VU11	Reemplazo inadecuado de equipos viejos	**2: Media**
VU12	Insuficientes y/o inoperativas guayas de seguridad para las laptops	**2: Media**
VU19	Sede de la empresa es lugar de encuentro de personalidades políticas y de autoridades universitarias	**2: Media**
VU20	Mantenimiento inadecuado de los equipos	**2: Media**

Fuente: Elaboración propia

Dicho ranking fue elaborado tomando en cuenta el porcentaje de respuestas de los expertos en cada categoría, es decir, estas son las vulnerabilidades que obtuvieron la mayor cantidad respuestas dentro de cada categoría. Por lo que son las vulnerabilidades más presentes en las actividades cotidianas de la empresa y las más críticas, por eso las categorías 0 y 1 no fueron consideradas.

Además, es importante destacar que en las categorías: “3: Alta” y “4: Muy Alta” (las categorías más altas de importancia), el 65% de las respuestas para cada amenaza son superiores al 50%, lo que quiere decir que, la mayoría de las respuestas están concentradas en estas dos últimas categorías, por lo que vulnerabilidades identificadas se encuentran bastante presentes en la cotidianidad de la empresa y son un punto crítico a considerar en el análisis.

4.5 Fase 5: Análisis de riesgo

En la tabla 17 se puede observar el consolidado de los datos obtenidos a través de la encuesta. En dicha tabla se encuentran los valores finales de: probabilidad de ocurrencia, impacto y frecuencia de cada una de las amenazas identificadas. En base a estos valores finales es que se realizará el cálculo del riesgo total (riesgo antes de los controles).

Tabla 17. Análisis de riesgo. Componentes de la amenaza

	Indicadores							
	Probabilidad		Impacto		Frecuencia		Score de riesgo	
Amenaza	Grado	Categoría	Nivel	Impacto monetario	Promedio	Eventos totales	Valoración	Zona de riesgo
A1	11%	2	4	30%	1,14	8	8	Moderado
A2	10%	2	4	30%	0,14	1	8	Moderado
A3	23%	2	4	30%	0,14	1	8	Moderado
A4	10%	2	3	10%	0,14	1	6	Moderado
A5	29%	3	4	30%	0,86	6	12	Alto
A6	31%	3	4	30%	1,00	7	12	Alto
A7	19%	2	4	30%	0,14	1	8	Moderado
A8	25%	2	3	10%	0,43	3	6	Moderado
A9	54%	4	4	30%	7,14	50	16	Extremo
A10	43%	3	4	30%	5,00	35	12	Alto
A11	24%	2	4	30%	2,29	16	8	Moderado
A12	46%	3	4	30%	9,00	63	12	Alto
A13	25%	2	3	10%	0,14	1	6	Moderado
A14	14%	2	4	30%	0,00	0	8	Moderado
A15	14%	2	4	30%	0,00	0	8	Moderado
A16	44%	3	3	10%	5,43	38	9	Alto
A17	11%	2	4	30%	0,00	0	8	Moderado
A18	29%	3	3	10%	4,29	30	9	Alto

Fuente: Elaboración propia

El score de riesgo es el resultado de multiplicar la categoría de probabilidad de ocurrencia de la amenaza por el nivel de impacto que esta tiene sobre el valor de los activos. El valor que se obtiene nos permitirá ubicar cada amenaza en una matriz de riesgo (mapa de calor). Esto nos ayudará a determinar cuáles son las amenazas más importantes.

Como se puede observar en la matriz de riesgo elaborada con los datos de la tabla 17, las amenazas se encuentran concentradas entre las categorías de probabilidades: **2** y **3,** y entre los niveles de impacto: **3** y **4**; que son zonas de riesgo moderado y alto. Solo una de las amenazas se encuentra en una zona de riesgo crítica, que es la

amenaza 9: Fallas en el software de los equipos. Esto se debe a que posee categorías de probabilidad e impacto elevadas. Lo que, en principio es preocupante, debido a que la totalidad de las amenazas identificas presentan un riesgo importante para los activos de la empresa. Pero hay que recordar que estas son las amenazas sin el efecto de los controles.

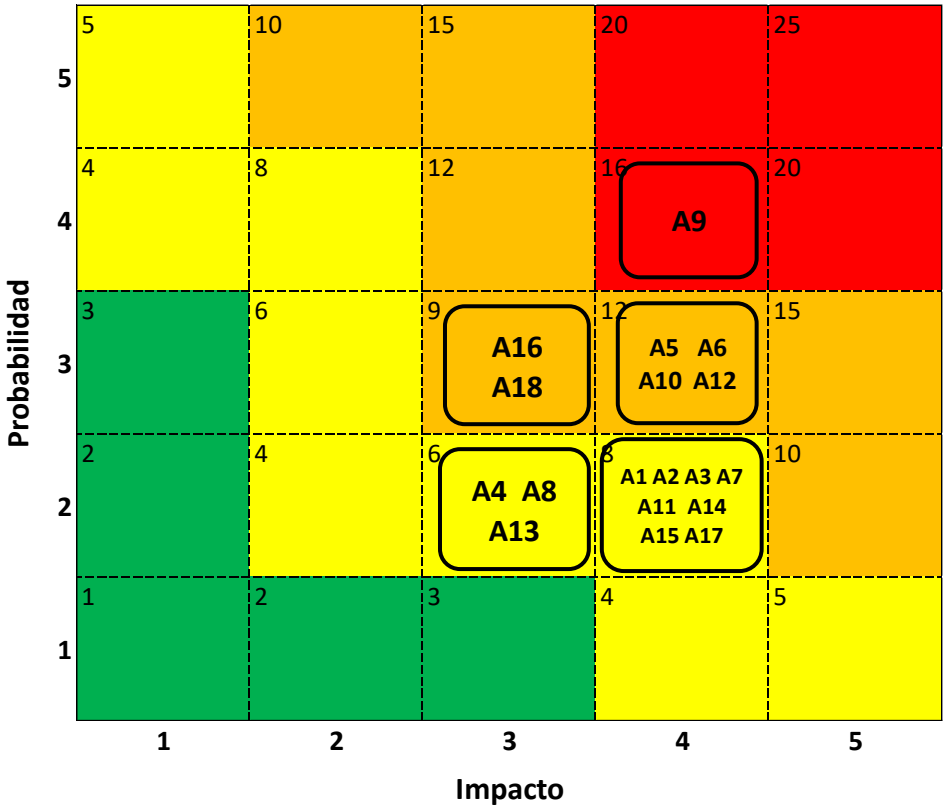


Figura 12. Matriz de riesgo de las amenazas

Fuente: Elaboración propia

4.5.1 Riesgo total

Con todos estos datos presentados se procedió al cálculo de riesgo total (riesgo antes de los controles).

El riesgo al que están expuestos los activos es igual a **$48.748**, lo cual es un nivel de exposición bastante alto. Esto queda plasmado por la proporción de riesgo, que es el valor del riesgo entre el valor total de los activos. La proporción es de 0,51, lo que quiere decir que el **51%** de los activos se encuentra en riesgo, lo cual es un valor

bastante preocupante. Pero hay que tener en cuenta que este riesgo es antes de considerar el efecto que tienen los controles establecidos por la empresa para contrarrestar las amenazas.

En la figura 13 se puede observar el riesgo que genera cada amenaza y el crecimiento acumulado del mismo. Adicionalmente, el cálculo detallado queda reflejado en el **anexo B**.

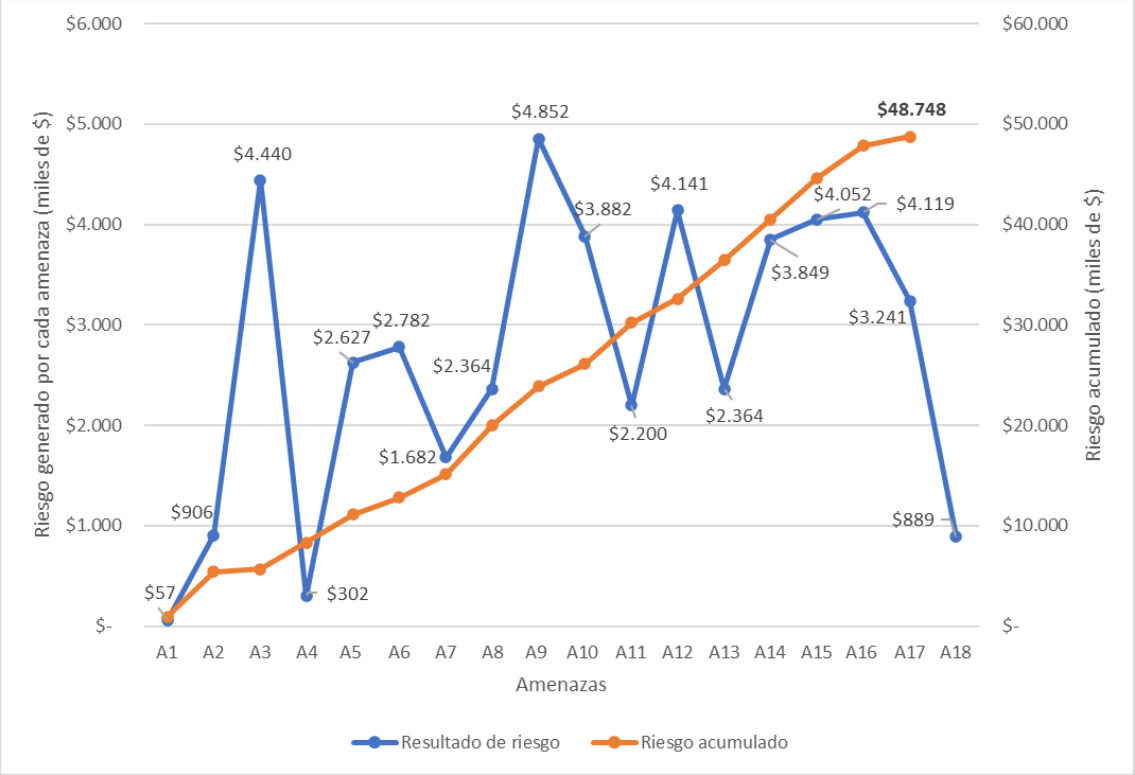


Figura 13. Riesgo inherente (total) de la empresa

Fuente: Elaboración propia

4.6 Fase 6: Evaluación de riesgo

En esta fase es evaluada la eficiencia de los controles existentes para las amenazas identificas anteriormente y el impacto que los mismos generan sobre las amenazas y, por ende, sobre el nivel de riesgo de la empresa.

Tabla 18. Evaluación de controles existentes

Amenaza	Existencia	Grado de documentación	Modo de apliación	Estado de aplicación	Suma de controles	Valoración	Factor de reducción
A1	SI	12,14	12,14	16,43	40,71	control deficiente	66%
A2	SI	10,71	11,43	16,43	38,57	control deficiente	59%
A3	SI	10,71	11,43	22,14	44,29	control deficiente	67%
A4	SI	10,00	11,43	20,00	41,43	control deficiente	50%
A5	SI	10,00	11,43	17,14	38,57	control deficiente	47%
A6	SI	9,29	11,43	17,14	37,86	control deficiente	46%
A7	SI	9,00	10,71	15,00	34,71	control deficiente	43%
A8	SI	11,43	11,43	19,29	42,14	control deficiente	60%
A9	SI	10,00	12,14	17,14	39,29	control deficiente	47%
A10	SI	10,71	12,86	17,14	40,71	control deficiente	46%
A11	SI	10,71	12,86	15,71	39,29	control deficiente	54%
A12	NO	-	-	-	-	no existe control	-
A13	SI	6,43	7,86	8,57	22,86	control deficiente	27%
A14	NO	-	-	-	-	no existe control	-
A15	SI	9,29	9,29	13,57	32,14	control deficiente	26%
A16	SI	10,00	11,43	17,86	39,29	control deficiente	62%
A17	SI	8,57	11,43	17,14	37,14	control deficiente	61%
A18	SI	11,43	11,43	20,00	42,86	control deficiente	63%

Fuente: Elaboración propia

La valoración de los controles fue efectuada según los criterios presentados en la **tabla 10 del capítulo 3**. Y los valores obtenidos en cada una de las categorías de control (grado de documentación, modo de aplicación y estado de aplicación), son el resultado del promedio aritmético de las respuestas de los coordinadores y de la directora (expertos). Los rangos de los posibles valores de cada una de las categorías mencionadas, fueron presentados en la 28**tabla 9 del capítulo 3**.

Como se puede observar en la tabla anterior, para la gran mayoría de las amenazas existe un control por parte de la empresa. Sólo en dos amenazas se catalogó la inexistencia de un control. Pero es importante destacar que para estas dos amenazas (Fallas en los servicios públicos y terremotos) no es posible establecer un control por parte de la empresa; se pueden establecer procedimientos de respuesta para salvaguardar la vida de las personas dentro de la sede, pero esto no corresponde con un control para reducir el efecto adverso que tienen las amenazas.

Ahora, al analizar la valoración obtenida para los controles de las amenazas, es importante destacar que todos los controles obtuvieron una valoración de “control deficiente”, debido a que obtuvieron del total de las categorías un valor entre **6** y **50** (teniendo en cuenta que el rango para la valoración está comprendido entre **0** y **100** según los criterios establecidos en la **tabla 10 del capítulo 3**). Lo que a primera instancia podría dar a pensar que los controles establecidos no son buenos para mitigar los efectos de las amenazas. Pero si analizamos los resultados obtenidos en cada una de las categorías, podemos observar que para las categorías “grado de documentación” y “control automático o manual”, los scores obtenidos se encuentran cercanos a la mayor calificación posible. Mientras que, para la categoría “estado de aplicación”, los scores obtenidos oscilan entre **8,57** y **22,14** (Dentro de un rango de posibles valores comprendido entre **0** y **30**), por lo que son resultados deficientes en cuanto a la aplicación y esto perjudica a la valoración final.

Pero la deficiencia de los controles tiene que ser contrastada contra el factor de reducción de cada uno y la frecuencia con la que suceden cada una de las amenazas. Al analizar estos dos últimos factores, se puede evidenciar que, a pesar de que los factores de reducción oscilan entre **26%** y **67%**; **14** de los **16** controles que existen tienen un factor de reducción superior o igual a **40%**, lo cual puede considerarse como un control eficiente y más aún si observa que las probabilidades y frecuencias de las amenazas son bajas.

Por lo que podemos concluir que la deficiencia en la valoración de los controles viene dada en gran parte por las bajas calificaciones obtenidas en la categoría “estado de aplicación del control”. Pero en cuanto a la eficiencia reduciendo los efectos adversos generados por las amenazas podemos decir que parecen ser efectivos. Esto será efectivamente evaluado cuando se analice el verdadero impacto que tienen los controles en el nivel de exposición de los activos de la empresa.

El efecto de los controles sobre la probabilidad de ocurrencia de la amenaza queda reflejado en la tabla 19. A su vez, se puede observar en las nuevas zonas de riesgo en las que se ubican las amenazas (en base a la probabilidad e impacto).

Tabla 19. Probabilidad ajustada por controles y nuevas zonas de riesgo

Amenaza	Indicadores							
	P	Factor de reducción μ	P*		Impacto	Score de riesgo*		
	Grado	Grado	Grado*	Categoría*	Nivel	Valoración*	Zona de riesgo*	Zona de riesgo
A1	11%	66%	4%	1	4	4	Moderado	Moderado –
A2	10%	59%	4%	1	4	4	Moderado	Moderado –
A3	23%	67%	8%	1	4	4	Moderado	Moderado –
A4	10%	64%	4%	1	3	3	Bajo	Moderado ↓
A5	29%	47%	16%	2	4	8	Moderado	Alto ↓
A6	31%	46%	17%	2	4	8	Moderado	Alto ↓
A7	19%	43%	11%	2	4	8	Moderado	Moderado –
A8	25%	60%	10%	2	3	6	Moderado	Moderado –
A9	54%	47%	28%	3	4	12	Alto	Extremo ↓
A10	43%	46%	23%	2	4	8	Moderado	Alto ↓
A11	24%	54%	11%	2	4	8	Moderado	Moderado –
A12	46%	0%	46%	3	4	12	Alto	Alto –
A13	25%	27%	18%	2	3	6	Moderado	Moderado –
A14	14%	0%	14%	2	4	8	Moderado	Moderado –
A15	14%	26%	11%	2	4	8	Moderado	Moderado –
A16	44%	62%	17%	2	3	6	Moderado	Alto ↓
A17	11%	61%	4%	1	4	4	Moderado	Moderado –
A18	29%	63%	11%	2	3	6	Moderado	Alto ↓

Fuente: Elaboración propia
Nota: Las variables que poseen el símbolo (*****) de superíndice, significa que son valores ajustados por el efecto de los controles

Aquí es donde podemos empezar a ver el impacto que tienen los controles sobre las amenazas y cuál es la importancia relativa de cada una de las mismas.

El primer punto a destacar es que el factor de reducción de cada amenaza tiene un impacto alto, ya que logra reducir en buena medida la probabilidad de ocurrencia. En la última columna se puede apreciar la variación de la zona de riesgo como resultado de los controles. Solo el **39%** de las amenazas sufrió una variación, es decir, solo **7** de las **18** amenazas se trasladó de su zona de riesgo anterior. La poca variación en las zonas de riesgo es debida a que a pesar de que las probabilidades disminuyeron en buena medida, muchas de estas reducciones no fueron suficientes para disminuir

en la categoría de probabilidades en la que son catalogadas cada una. Sumado a esto, el impacto que generan las amenazas sigue siendo el mismo.

A pesar de esto, los resultados pueden considerarse bastante positivos, ya que **5** de las **6** amenazas que estaban catalogadas en una zona de riesgo “Alto”, pasaron a una zona de riesgo de “Moderado”. Incluso, la **amenaza 9**: Fallas en el software de los equipos, que estaba en una zona de riesgo “Crítica”, pasó a una zona de riesgo “Alta”, que aun siendo una zona donde se debe considerar tomar medidas, el control logró desplazar la única amenaza que se encontraba en la zona crítica.

En base a todos estos resultados se construyó la matriz de riesgo para el riesgo revisado. En el que se observa que la gran mayoría de las amenazas se encuentran en la zona de riesgo moderado, que puede ser considerado como una zona tolerable y ya no hay ninguna amenaza en una zona de riesgo crítica.

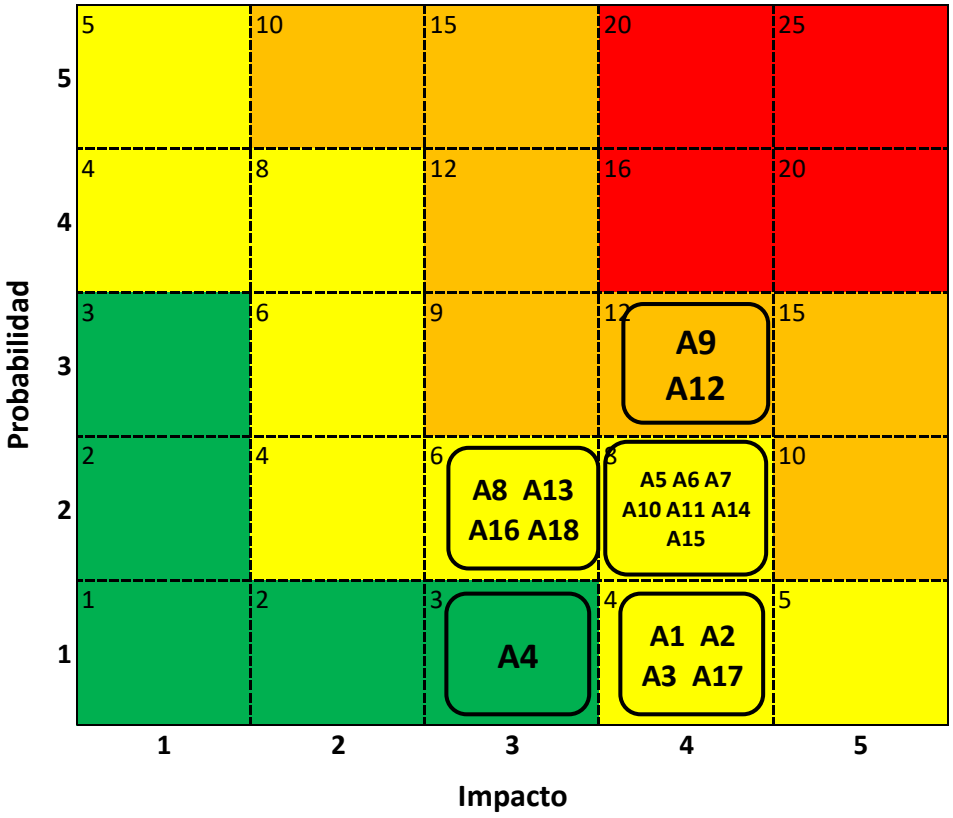


Figura 14. Matriz de riesgo revisado de las amenazas

Fuente: Elaboración propia

4.6.1 Riesgo revisado

En base a los resultados obtenidos en la valoración de los controles, se procedió a calcular el riesgo revisado, que es el riesgo ajustado por el efecto de los controles sobre las amenazas.

El riesgo revisado es igual a **$28.329**, lo cual representa una variación con respecto al riesgo antes de controles del **42%**. Lo cual habla de la eficiencia de los controles sobre el nivel de riesgo al que están expuestos los activos de la empresa. La proporción de riesgo es igual a 0,29, es decir, el **29%** de los activos se encuentran en riesgo. Este resultado queda contrastado con el análisis anterior sobre los scores obtenidos por cada control. Se puede evidenciar que los controles si son eficientes para reducir el nivel de riesgo de la empresa y la valoración deficiente que recibieron es causada en gran parte por el estado de aplicación de los controles. El riesgo revisado queda reflejado en la figura 15. Adicionalmente, el cálculo detallado queda reflejado en el **anexo B**.

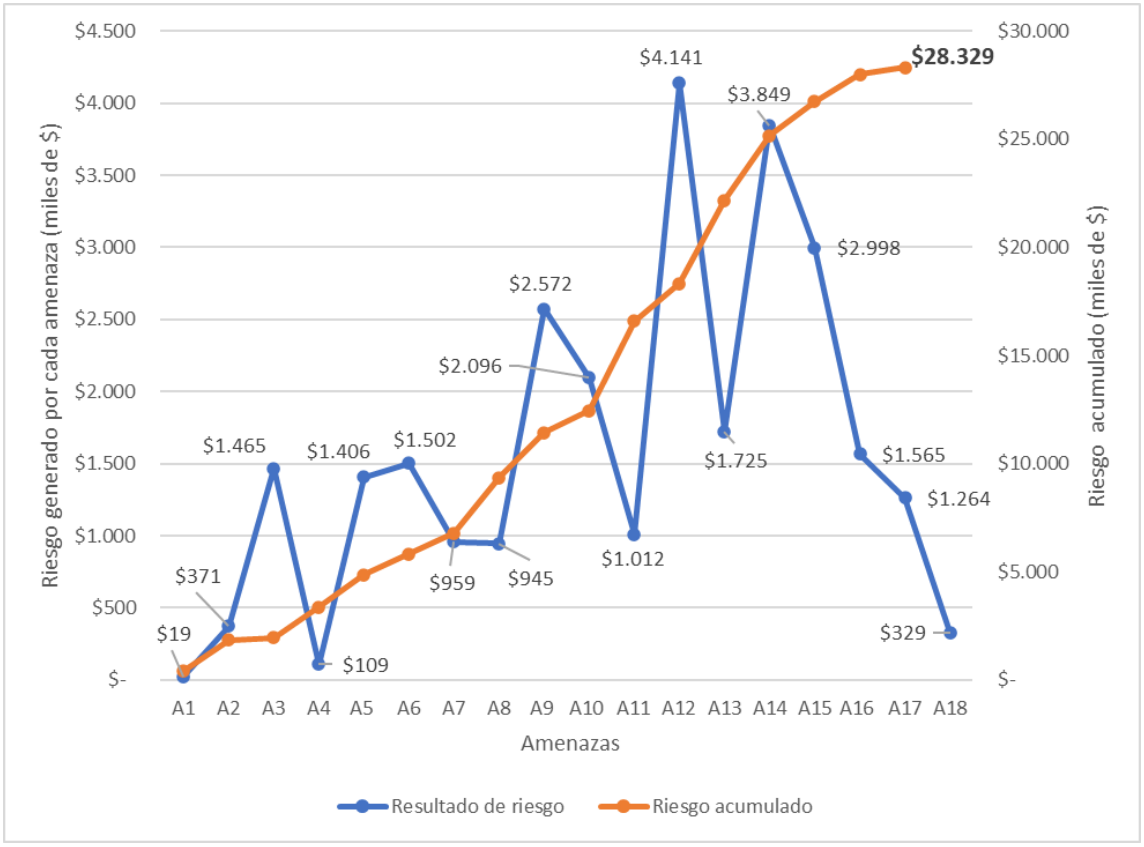


Figura 15. Riesgo revisado de la empresa

Fuente: Elaboración propia

4.7 Fase 7: Tratamiento del riesgo

Hay que recordar que el tratamiento del riesgo dependerá de las zonas de riesgo en la que se encuentran las amenazas. Los criterios para definir las medidas de tratamiento están expuestos en la figura 3 (mapa de calor) del capítulo 2 y en apartado de tratamiento de riesgos.

Zona de riego bajo: En esta zona se encuentra la **amenaza 4** “Robo de mobiliario”. En esta zona de riesgo la medida correctiva correspondiente es **aceptar el riesgo**: no se adopta ninguna medida que afecte la probabilidad o impacto del riesgo.

Es importante destacar que esta medida es totalmente tolerable en esta zona de riesgo debido a que a pesar de que la amenaza 4 pudiera generar un impacto importante sobre los activos (30% del valor del activo), su probabilidad de ocurrencia es muy baja, catalogándose en la categoría de probabilidad 1 (casi improbable).

Zona de riesgo Moderado: En esta zona es donde se concentran la mayoría de las amenazas, tanto así, que en esta zona de riesgo se encuentra el 89% de las mismas. Las amenazas en zona de riesgo moderado son:

- A1: Operaciones no registradas intencionalmente
- A2: Destrucción maliciosa de activos
- A3: Robo de divisas en efectivo
- A5: Robo de equipos
- A6: Robo de componentes de computadoras
- A7: Robo de información (física o digital)
- A8: Violación de normas de salud o seguridad
- A10: Fallas en el Hardware de los equipos
- A11: Carga de software malicioso (intencional o no)
- A13: Intrusión de cuerpos de seguridad y/o inteligencia del estado
- A14: Terremotos
- A15: Incendios
- A16: Acceso no autorizado a las instalaciones
- A17: Vandalismo
- A18: Uso inadecuado del mobiliario por parte de los visitantes de la sede

En esta zona de riesgo la medida correctiva correspondiente es: **aceptar el riesgo**. Pero las amenazas que conforman esta zona poseen diferentes pares de probabilidad e impacto, por lo que profundizaremos en si este tratamiento está justificado:

- 4 amenazas tienen una categoría de impacto de 3 (10% del valor del activo). Por lo que, sumado a la baja probabilidad, representan poco riesgo para los activos.

- 12 de las 16 amenazas que se encuentran en una zona de riesgo moderado poseen una categoría de impacto 4 (30% del valor del activo) que es una severidad importante. Pero el hecho de que estén catalogadas entre las categorías 1 y 2 de probabilidad (las más bajas) genera que el riesgo que representen dichas amenazas sea bajo. Por lo que la medida de aceptar el riesgo puede ser tolerable.

- La naturaleza de las amenazas 14: terremotos y 15: incendios las hacen únicas. Aunque sus probabilidades de ocurrencia son muy bajas el tratamiento correspondiente para amenazas como estas difiere de la medida de “aceptar el riesgo”. Por lo que la medida de tratamiento pertinente será desarrollada junto con la amenaza 12: fallas en los servicios públicos (que es una amenaza que se encuentra en una zona de riesgo alta).

Es importante que a pesar de que la mayoría de las amenazas se encuentran ubicadas en la zona de riesgo moderada, donde la medida de tratamiento de riesgo correspondiente es aceptarlo, es vital que se realice un monitoreo constante de que tan frecuentemente ocurren efectivamente cada amenaza, así como el registro pertinente de este evento adverso, para realizar periódicamente una revisión de la probabilidad e impacto que generan, y a su vez el riesgo al que están expuestos los activos de la empresa. Todo esto con la finalidad evaluar y monitorear que estas amenazas se mantengan (o no) en el tiempo en los cuadrantes identificados.

Zona de riesgo Alta: Gracias a la efectividad de los controles, en esta zona de riesgo solo se encuentran: la **amenaza 9**: “Fallas en el software de los equipos” (que antes se ubicaba en una zona de riesgo crítica) y la **amenaza 12**: “Cortes/Fallas en los servicios públicos”. En esta zona de riesgo las posibles medidas correctivas a tomar son: reducir o mitigar (tratar), evitar, compartir o transferir.

En el caso de la **amenaza 9** la medida correctiva correspondiente es: **Reducir o mitigar (tratar)**. En este caso es necesario tomar acciones para lograr la reducción de la probabilidad y/o impacto de la amenaza; y más aún cuando se considera la tabla de las vulnerabilidades más importantes. Ya que, 6 de las 13 vulnerabilidades más

importantes guardan relación directa con el mantenimiento de los equipos; estas vulnerabilidades son: sistema operativos antiguos y desactualizados (VU6), falta de inversión en hardware (VU4), falta de inversión en software (VU5), sistema antivirus desactualizado o inexistentes (VU7), reemplazo inadecuado de equipos viejos (VU11) y mantenimiento inadecuado de los equipos (VU20). Esto genera que la amenaza pueda suscitarse debido a diferentes vulnerabilidades, incluso, están tan relacionadas que una vulnerabilidad puede desencadenar la ocurrencia o profundización del problema que representan las demás.

Es por esto que es necesario realizar una revisión exhaustiva de todos los equipos que posee el CIAP, tanto a nivel de software como de hardware, para identificar cuáles son los componentes físicos y de software que son necesarios para un mantenimiento adecuado de los equipos e identificar que equipos obsoletos requieren reemplazo.

Es vital que la empresa se enfoque de manera crítica en esta amenaza, ya que es a través de los equipos que se presta el servicio educativo y el medio de trabajo que utilizan, de modo que, si no se realiza el tratamiento adecuado y a tiempo de la amenaza, puede entorpecer y reducir la calidad de prestación del servicio, afectando la imagen del CIAP como una empresa que representa el alto nivel educativo de la UCAB.

Para tratar esta amenaza es necesario que la empresa coordine con la unidad DTI (Dirección de tecnología e información) de la UCAB, ya que son ellos los encargados de realizar el mantenimiento de todos los equipos de la universidad.

En el caso de la **amenaza 12**, su naturaleza la hace única, ya que las características de esta amenaza generan que sean considerada como una externalidad negativa. Por lo cual, el tratamiento requerido para una amenaza como esta es: **transferir el riesgo**. Esta medida puede ser lograda a través de la contratación de un seguro para la empresa contra eventos de estas características, ya que, con esto se logra que sea un tercero quien asuma las consecuencias de un evento adverso. Otras amenazas que pueden ser catalogadas como externalidades negativas son: la amenaza 14: terremotos y la amenaza 15: incendios, y como se mencionaba en el tratamiento de la zona de riesgo moderado, estas amenazas requieren otro tipo de medida. Que, en

este caso, corresponden con la medida adoptada para la amenaza 12 (**transferir el riesgo)**.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Pudimos comprobar que el riesgo no es un evento o factor único, y que este, es determinado por la probabilidad de ocurrencia de las amenazas que aprovechan de manera accidental (o no) la existencia de una vulnerabilidad; esto termina generando un impacto que es medido como la pérdida de valor del activo, que tiene como consecuencia no solo la pérdida en los valores reflejados en el balance general, sino que, entorpecen o imposibilitan las operaciones diarias de la empresa. Es por esto que se hace vital la existencia y aplicación de un modelo de gestión de riesgos en toda empresa, ya que esto permite tener de manera clara y cuantificada cuales son las amenazas y vulnerabilidades presentes en la cotidianidad de la empresa y, por ende, el nivel de exposición que se posee.

A pesar de que no existe una única metodología de gestión de riesgos es importante que la metodología a emplear considere: amenazas, probabilidades, vulnerabilidades y consecuencias, ya que esto permitirá no solo analizar todos los componentes del riesgo, sino que, permitirá que la gestión de riesgo realice el ciclo completo al considerarse causas, efectos y tratamiento.

El modelo de gestión de riesgos empleado considera todos los factores importantes relacionados al riesgo, por esto podemos afirmar que es una buena metodología no solo para la empresa CIAP, sino para cualquier empresa, ya que la metodología planteada es perfectamente aplicable para cualquier empresa sin importar el ramo de la economía en la que se desarrolle, solo que la naturaleza de la empresa generará que el análisis realizado pueda incluir alguna variación. Pero lo más importante de este modelo es que es escalable, esto quiere decir que la recolección de datos sobre amenazas y vulnerabilidades con el tiempo puede ser perfeccionada y ser más precisa, con la finalidad de que los resultados de exposición de riesgo sean más

acertados y esto permita evolucionar el modelo a aplicaciones estadísticas como ajustar las probabilidad de ocurrencia a través de una distribución de probabilidades para una variable discreta, e incluso llegar a realizar con los datos un modelo de simulación.

A través de la aplicación del modelo, pudimos observar que los activos identificados están expuestos a diversas amenazas y vulnerabilidades, que en mayor o menor medida representan un riesgo para la empresa, pero que en general, todas las variables identificadas se encuentran bastante presentes en la cotidianidad de la empresa. Y este análisis solo pudo realizarse gracias a la opinión de los coordinadores y la directora, ya que la empresa no contaba con información relacionada a los eventos adversos a los que están expuestos los activos. De esta manera se realizó el proceso de análisis integral (identificación y valoración), ya que, no solo se cuantifico y analizó el riesgo de la empresa, sino que también se valoró la importancia que tiene cada uno de los activos para la continuidad de las operaciones y como el entorno en el que se desarrolla el CIAP juegan un papel fundamental en el análisis de riesgo.

Un punto importante a destacar del modelo de gestión de riesgos aplicado es el factor de reducción **μ,** debido a que es un factor de transición entre las variables, ya que, es el efecto que tienen los controles sobre la probabilidad de ocurrencia de las amenazas y esto a su vez genera un efecto sobre el valor final de riesgo de los activos. Además, la estructura de esta variable es bastante particular, debido a que el comportamiento que posee hace que se ajuste al comportamiento presentado por las cadenas de Márkov.

Por último, es importante que en toda gestión de riesgos se realice un constante monitoreo y revisión de las variables identificadas y analizadas, ya que este proceso repetitivo de análisis y cuantificación debe ser revisado y ajustado con una cierta periodicidad, con la finalidad de que los las decisiones que toma la alta gerencia en base a la gestión de riesgo, sean acertadas y acordes al momento que atraviesa la empresa.

Las recomendaciones a nivel investigativo son:

- Es importante que el proceso de recolección de datos permita obtener información precisa, ya que es a través de este proceso que se realiza todo el cálculo y análisis del modelo de gestión de riesgos.

- A través de las frecuencias observadas de las amenazas pueden ser calculadas las probabilidades de ocurrencia de las amenazas utilizando una distribución de probabilidades de una variable discreta. Pero esto es un proceso complejo, ya que para ello es necesario establecer:

    - La distribución de probabilidad que mejor se ajuste a los datos, pero determinar esto es complejo, y además conlleva establecer diversos supuestos.
    - Establecer un horizonte de riesgo, es decir, el periodo de análisis de las frecuencias de las amenazas. Pero para hacer esto hay que contar con data certera sobre las frecuencias y poseer una data que abarque un periodo mínimo de un año.

- En un entorno tan volátil y complejo como el de Venezuela, tiene que ser incluido en el análisis las perturbaciones que genera una economía como esta, ya que pudimos apreciar en la fase de determinación del contexto e identificación de activos, que las distintas ramas de un país juegan un papel fundamental en las condiciones en las que opera una empresa y en las que se realiza el análisis.

Las recomendaciones para mejorar la gestión de riesgos en la empresa CIAP son:

- Debido a que es la primera vez que se emplea una metodología de riesgos en la empresa, debe realizarse un adecuado plan de comunicación interno en el que se establezca los procedimientos necesarios para poseer una retroalimentación adecuada entre las distintas coordinaciones, para que la ejecución de la gestión de riesgos sea lo más eficiente posible. Este punto ayudará a crear una cultura de riesgos dentro de la empresa, además de capacitar a todo el personal sobre su rol dentro de la gestión de riesgos

- Es importante, mas no crítico, mejorar el grado de implementación de los controles aplicados en la empresa. Así como mejorar el grado de conocimiento por parte de los coordinadores sobre su existencia y aplicación, ya que esto permitiría mejorar el score obtenido por los controles.

- Es vital que se realice una revisión trimestral de las amenazas y vulnerabilidades, tanto su probabilidad, frecuencia e impacto. Para que las medidas que tengan que ser tomadas sean acertadas y tomadas a tiempo.

- La creación de un inventario de activos es una medida crítica que debe ser realizada en el menor tiempo posible. Además de esto es importante que también sea recopilada toda la información necesaria para la actualización del valor de los activos, ya que esto permitirá que el análisis realizado sea más detallado y preciso.

- Evaluar la propuesta de política de gestión de riesgo plasmada en el **anexo C**. Ya que esto ayudaría a establecer de manera formal en la empresa no solo la cultura de riesgo, sino, los procedimientos y normativas necesarias para llevar a cabo la correcta implementación de la gestión de riesgos.

REFERENCIAS

Abdul Rahim, N. F., Ahmed, E. R., & Faeeq, M. K. (2018). Internal Control System and Perceived Operational Risk Management in Malaysian Conventional Banking Industry. *10(1)*. Global Business and Management Research: An International Journal.

Arias, F. G. (2012). *El proyecto de investigación. Introducción a la metodología científica* (6ta ed.). Caracas, Venezuela: Episteme.

Banco Interamericano de Desarrollo. (1999). *Gestión de riesgos financieros: un enfoque prácticos para países latinoamericanos.*

Castro Márquez, F. (2003). *El proyecto de investigación y su esquema de elaboración* (2da ed.). Venezuela: Uyapar.

CIIFEN. (n.d.). *Centro Internacional para la Investigación del Fenómeno del Niño*. Retrieved Enero 01, 2020, from http://www.ciifen.org/index.php?option=com_content&view=category&layout=blog&id=84&Itemid=336&lang=es

Colombia compra eficiente. (2013). *Manual para la Identificación y cobertura de riesgos en los procesos de contratación.* Manual.

Comité de Basilea. (2003). *The New Basel Capital Accord.*

Departamento administrativo de la función pública de Colombia. (2018). *Guía para la administración del riesgo y diseño de controles en entidades públicas.* Ministerio de Tecnologías de la Información y Comunicaciones, Departamento administrativo de la función pública de Colombia, Bogota.

Departamento de salud y servicios humanos de Estados Unidos. (2007). *Basics of Security Risk Analysis and Risk Management.* centro de servicios medicare y medicaid. The security series of papers

Descifrado. (2020, Marzo 8). *Existe un 40% de deserción de profesores y alumnos en las Universidades*. Caracas, Venezuela. Retrieved Julio 25, 2020, from https://www.descifrado.com/2020/03/08/existe-un-40-de-desercion-de-profesores-y-alumnos-en-las-universidades/

Diz Cruz, E. (2013). *Estadística actuarial y financiera.* Caracas: Biosfera.

Escalona, G. (2017, Mayo). Evaluación de los riesgos operativos para los procesos de prestación de servicios de Fuller mantenimiento, C.A Basada en la norma ISO

31010:2009, para fomentar la mejora continua. Caracas, Venezuela.Tesis de grado

Garcia Bustamante, J. J., & Jimenez Varón, J. A. (2018). *Diseño de un sistema de gestión de riesgos bajo el enfoque del modelo COSO y la norma ISO 31000 para la cadena logística de la empresa comercializadora de repuestos automotores.* PONTIFICIA UNIVERSIDAD JAVERIANA CALI, FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS. Tesis de grado

Gheorghe, A. V., & Mock, R. (1999). *Risk Engineering* (Vol. 6). (A. Z. Keller, Ed.) SPRINGER-SCIENCE+BUSINESS MEDIA, B.V.

Greene, M. R. (1974). *Riesgo y Seguro.* Madrid: Mapfre.

Instituto nacional de ciberseguridad. (2015, Julio 06). *Instituto nacional de ciberseguridad.* Retrieved Marzo 13, 2020, from Gestión de riesgos. Una guía de aproximación para el empresario: https://www.incibe.es/protege-tu-empresa/guias/gestion-riesgos-guia-empresario

ISO 31000. (2009). Indian Standard RISK MANAGEMENT — PRINCIPLES AND GUIDELINES. Retrieved Enero 2, 2020, from https://law.resource.org/pub/in/bis/S07/is.iso.31000.2009.pdf

Knight, F. (1921). *Riesgo, incertidumbre y beneficio.* Boston and New York, Estados Unidos: Houghton Mifflin.

Lanas, X. C. (2017, abril). Desarrollo de un modelo de gestión de riesgo operativo para una empresa ecuatoriana de comercialización. Quito, Ecuador.

León Ruiz, K. (2017). *Desarrollo de un modelo de gestión de riesgo operativo para una empresa ecuatoriana de comercialización.* Universidad Andina Simón Bolívar, Programa de Maestría en Finanzas y Gestión de Riesgos, Quito. Tesis de grado

Marsh. (2018). *Reimaginando el riesgo. Capturando oportunidades en un mundo de riesgo. III BENCHMARK DE GESTIÓN DE RIESGOS EN LATINOAMÉRICA* (Vol. 1).

Norman, T. L. (2009). *Risk Analysis and security countermeasure selection.* Florida, Estados Unidos : CRC press.

Olarte, J. C. (2006, Diciembre). *Redalyc*. Retrieved Mayo 15, 2020, from https://www.redalyc.org/pdf/849/84911652061.pdf

Outreville, F. J. (1997). *Theory and practice of insurance.* Kluwer academic publishers.

Pan, Y., Siege, S., & Wang, T. Y. (2017). *Corporate Risk Culture.* JOURNAL OF FINANCIAL AND QUANTITATIVE ANALYSIS.

Rodríguez López, M., Piñeiro Sánchez, C., & de Llano Monelos, P. (2013). *Mapa de riesgos: Identificación y gestión de riesgos.* Universidad de A Coruña, Facultad Economía y Empresa. Atlantic Review of Economics.

Sampieri, R. H., Fernández, C., & Baptista, M. D. (2014). *Metodología de la investigación* (6ta ed.). Ciudad de México: Mc Graw Hill.

Sheedy, E. (2004). *El manual del administrador de riesgos profesionales.* (C. Alexander, Ed.) PRMIA .

Sheedy, E., & Trenor, R. (1999). *Asset-Allocation decision when risk is changing.* The Journal financial research.

Superintendencia de Banca y Seguros del Perú. (2008). *Resolución S.B.S. N° 37.* Resolución, Lima.

Sweeting, P. (2011). *Financial enterprise risk managment.* New York, Estados Unidos: Cambridge university press.

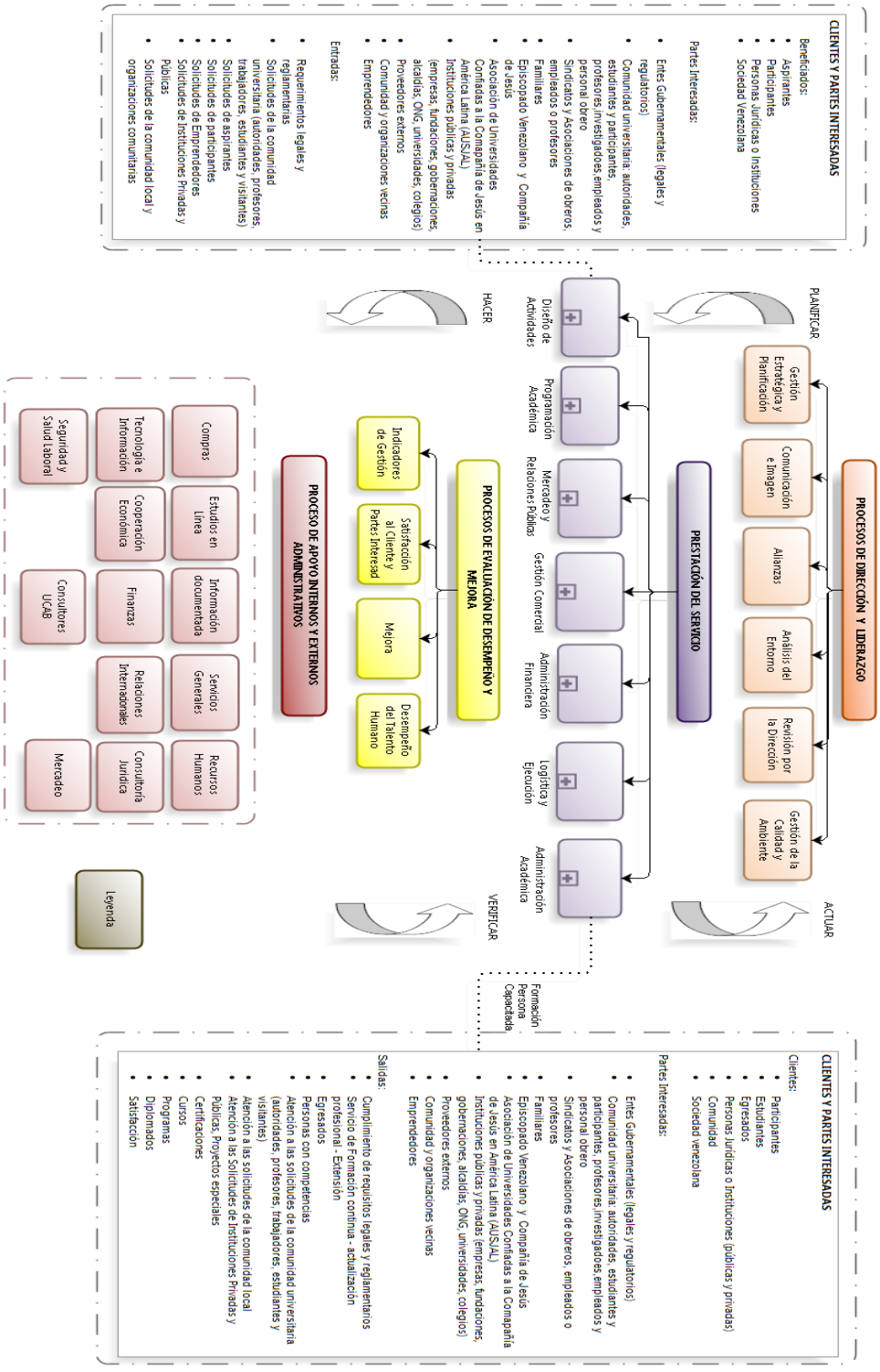
Universidad Pedagógica Experimental Libertador. (2003). *Manual de trabajo de grado de especialización y maestría y tesis doctorales.* Caracas, Venezuela: Fondo editorial de la Universidad Pedagógica Experimental Libertador.

Venegas Martínez, F. (2008). *Riesgos financieros y económicos* (Segunda ed.). México: CENGAGE Lerarning.

Walker, R. (2013). *Winningm with risk managment* (Vol. 3). Estados Unidos: World Scientific .

ANEXO A

DIAGRAMA DE PROCESOS DE LA EMPRESA



ANEXO B

CÁLCULO DEL NIVEL DE RIESGO INICIAL Y REVISADO

Es importante recordar que se identificaron 18 amenazas que explotan las vulnerabilidades e impactan los activos, tal que el impacto de la amenaza $\boldsymbol{i}$ sobre el activo $\boldsymbol{j}$ es denominado $\boldsymbol{C_{ij}}$. Además, fueron identificados **3 activos** que poseen un valor asociado: **Activo 1**: Efectivo en cajas y bancos **(V_1), Activo 2**: Cuentas por cobrar (V_2)**, Activo 3**: Equipo y mobiliario (V_3)**.**

B.1 Cálculo del nivel de riesgo inicial

Descripción del cálculo	Amenaza (Variable)	Probabilidad	Impacto	Valor del activo	Resultado de riesgo	Riesgo acumulado
$P_1 \times C_{12} \times V_2$	**A1**	11%	30%	$ 1.789	$ 57	
$P_2 \times C_{23} \times V_3$	**A2**	10%	30%	$ 30.193	$ 906	$ 963
$P_3 \times C_{31} \times V_1$	**A3**	23%	30%	$ 64.350	$ 4.440	$ 5.403
$P_4 \times C_{43} \times V_3$	**A4**	10%	10%	$ 30.193	$ 302	$ 5.705
$P_5 \times C_{53} \times V_3$	**A5**	29%	30%	$ 30.193	$ 2.627	$ 8.331
$P_6 \times C_{63} \times V_3$	**A6**	31%	30%	$ 30.193	$ 2.782	$ 11.113
$P_7 \times C_{73} \times V_3$	**A7**	19%	30%	$ 30.193	$ 1.682	$ 12.796
$P_8 \times C_{8(1,3)} \times (V_1 + V_3)$	**A8**	25%	10%	$ 94.543	$ 2.364	$ 15.159
$P_9 \times C_{93} \times V_3$	**A9**	54%	30%	$ 30.193	$ 4.852	$ 20.012
$P_{10} \times C_{103} \times V_3$	**A10**	43%	30%	$ 30.193	$ 3.882	$ 23.894
$P_{11} \times C_{113} \times V_3$	**A11**	24%	30%	$ 30.193	$ 2.200	$ 26.093
$P_{12} \times C_{123} \times V_3$	**A12**	46%	30%	$ 30.193	$ 4.141	$ 30.234
$P_{13} \times C_{13(1,3)} \times (V_1 + V_3)$	**A13**	25%	10%	$ 94.543	$ 2.364	$ 32.598
$P_{14} \times C_{14(1,3)} \times (V_1 + V_3)$	**A14**	14%	30%	$ 94.543	$ 3.849	$ 36.447
$P_{15} \times C_{15(1,3)} \times (V_1 + V_3)$	**A15**	14%	30%	$ 94.543	$ 4.052	$ 40.499
$P_{16} \times C_{16(1,3)} \times (V_1 + V_3)$	**A16**	44%	10%	$ 94.543	$ 4.119	$ 44.618
$P_{17} \times C_{17(1,3)} \times (V_1 + V_3)$	**A17**	11%	30%	$ 94.543	$ 3.241	$ 47.860
$P_{18} \times C_{183} \times V_3$	**A18**	29%	10%	$ 30.193	$ 889	$ 48.748

B.2 Cálculo del nivel de riesgo revisado

Descripción del cálculo	Amenaza (Variable)	Probabilidad revisada	Impacto	Valor del activo	Resultado de riesgo	Riesgo acumulado
$P_1^* \times C_{12} \times V_2$	**A1**	4%	30%	$ 1.789	$ 19	
$P_2^* \times C_{22} \times V_2$	**A2**	4%	30%	$ 30.193	$ 371	$ 391
$P_3^* \times C_{31} \times V_1$	**A3**	8%	30%	$ 64.350	$ 1.465	$ 1.856
$P_4^* \times C_{43} \times V_3$	**A4**	4%	10%	$ 30.193	$ 109	$ 1.965
$P_5^* \times C_{53} \times V_3$	**A5**	16%	30%	$ 30.193	$ 1.406	$ 3.371
$P_6^* \times C_{63} \times V_3$	**A6**	17%	30%	$ 30.193	$ 1.502	$ 4.873
$P_7^* \times C_{63} \times V_3$	**A7**	11%	30%	$ 30.193	$ 959	$ 5.832
$P_8^* \times C_{8(1,3)} \times (V_1 + V_3)$	**A8**	10%	10%	$ 94.543	$ 945	$ 6.777
$P_9^* \times C_{93} \times V_3$	**A9**	28%	30%	$ 30.193	$ 2.572	$ 9.349
$P_{10}^* \times C_{103} \times V_3$	**A10**	23%	30%	$ 30.193	$ 2.096	$ 11.445
$P_{11}^* \times C_{113} \times V_3$	**A11**	11%	30%	$ 30.193	$ 1.012	$ 12.457
$P_{12}^* \times C_{123} \times V_3$	**A12**	46%	30%	$ 30.193	$ 4.141	$ 16.598
$P_{13}^* \times C_{13(1,3)} \times (V_1 + V_3)$	**A13**	18%	10%	$ 94.543	$ 1.725	$ 18.323
$P_{14}^* \times C_{14(1,3)} \times (V_1 + V_3)$	**A14**	14%	30%	$ 94.543	$ 3.849	$ 22.172
$P_{15}^* \times C_{15(1,3)} \times (V_1 + V_3)$	**A15**	11%	30%	$ 94.543	$ 2.998	$ 25.171
$P_{16}^* \times C_{16(1,3)} \times (V_1 + V_3)$	**A16**	17%	10%	$ 94.543	$ 1.565	$ 26.736
$P_{17}^* \times C_{17(1,3)} \times (V_1 + V_3)$	**A17**	4%	30%	$ 94.543	$ 1.264	$ 28.000
$P_{18}^* \times C_{183} \times V_3$	**A18**	11%	10%	$ 30.193	$ 329	$ 28.329

ANEXO C

PROPUESTA DE POLÍTICA DE GESTIÓN DE RIESGO

C.1 Objetivo

La política de gestión de riesgo es una propuesta que tiene como finalidad establecer los principios básicos y el marco general de actuación para la gestión de riesgos operativos a los que se enfrenta el CIAP. La política busca, además, establecer los límites de exposición del riesgo operativo, así como la definición del grado de responsabilidad entre las diferentes áreas de la Empresa.

C.2 Alcance

La política de gestión de riesgo propuesta tiene como finalidad preservar el valor de los activos de la empresa ante los efectos adversos que generan las amenazas y vulnerabilidades a los que están expuestos. El alcance y capacidad de acción de la política de riesgo se fundamentan en los principios teóricos y prácticos expuestos en el trabajo de investigación elaborado.

C.3 Principios

- ***Protección y mejora continua*:** Proteger el valor, es decir, contribuir a la consecución de los objetivos y la mejora del desempeño, con la finalidad de facilitar la mejora continua

- ***Integral:*** Ser una parte integral de todos los procesos de la empresa y que formen parte todos los factores humanos y culturales. De modo que pueda ser incluida en la toma de decisiones de la empresa.

- ***Organización:*** Ser sistemática, estructurada y oportuna

- ***Disponibilidad**:* Basarse en la mejor información disponible

- ***Adaptabilidad:*** Alineándose con el contexto interno y externo y con los perfiles del riesgo

- ***Confiabilidad:*** Ser trasparente y participativa

- ***Dinamismo:*** Dinámica, iterativa y capaz de responder a los cambios

C.4 Importancia del establecimiento de una política de riesgo

El establecimiento de la política de gestión de riesgo es la formalización de los lineamientos, procedimientos, recursos y definición de los responsables necesarios para la consecución de las distintas fases del modelo de gestión de riesgo a emplear para lograr la correcta y oportuna prevención de los efectos adversos que puedan generar las amenazas al afectar el valor de los activos de la empresa.

Además, al establecer la política de riesgo se estará estableciendo 3 líneas de defensa:

Primera línea de defensa: Se desarrolla e implementan procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

Segunda línea de defensa: Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.

Tercera línea de defensa: Proporciona información sobre la efectividad del sistema de gestión de riesgo empleado. Se incluye la operación de la primera y segunda línea de defensa.

Por lo que la política propuesta es bastante completa, sobre todo si se considera que las distintas líneas de defensa que establece están sustentadas entre ellas. Pero esto genera que la empresa establezca un total compromiso en su correcta aplicación

(tanto en normativa como uso del modelo de gestión), ya que solo así, se logrará que las tres líneas de defensa establecidas sean efectivas.

C.5 Definición de los responsables

Para llevar a cabo el establecimiento y ejecución de la política de gestión de riesgos es necesario establecer los distintos grupos y responsables que se encargaran de la ejecución y supervisión de procedimientos para el análisis y tratamiento de riesgo.

C.5.1 Directiva

La directiva es el departamento encargado de la administración superior de la empresa, son quienes aprueban y disponen la aplicación de las políticas y procedimientos idóneos que permitan una adecuada gestión de riesgos. Este departamento está a cargo de la directora del CIAP y es supervisado por el vicerrectorado académico de la UCAB.

Entre las responsabilidades relacionadas a la política de gestión de riesgo son:

- Conocer y comprender el nivel de riesgo inherente al que están expuestos los activos de la empresa.

- Establecer la tolerancia de riesgo para la empresa y que este sea compatible con la visión, misión y objetivos de la organización.

- Determinar y actualizar permanentemente las estrategias, políticas, procesos y procedimientos que permitan una adecuada gestión de riesgos, así como el adecuado seguimiento y concienciación del control de riesgo en todos los niveles de la organización.

- Implementar medidas correctivas en caso de que las estrategias, políticas o procesos para la gestión de riesgos no se estén cumpliendo, o que los implementados no demuestren ser efectivos

- Designar al jefe/encargado de la unidad de administración de riesgo

- Aprobar los planes de contingencia

C5.2 Comité de administración de riesgo

Este comité estará compuesto por la directiva del CIAP (directora del CIAP y vicerrector académico de la universidad) y el jefe/encargado de la unidad de administración de riesgos.

Las directrices que deriven de las reuniones del comité deberán ser aprobadas por la directiva, pero resueltas bajo consenso de todas las partes que lo componen. Este comité solo podrá sesionar si todos sus integrantes están presentes.

Entre las responsabilidades relacionadas a la política de gestión de riesgo son:

- Revisar, definir y aprobar las estrategias, políticas y procesos para la administración de riesgo propuesta por la Unidad de Riesgos

- Establecer políticas para la asignación clara de responsabilidades de cada integrante del proceso de gestión de riesgos

- Asegurar que se efectúe de manera adecuada la implementación de las metodologías, políticas, manuales y procesos para la gestión de riesgos

- Conocer el nivel de exposure de riesgo a los cuales está expuestos los activos de la empresa.

- Evaluar el informe del análisis de riesgos elaborado por la unidad de administración de riesgos de manera trimestral, para tomar las medidas pertinentes en base a la información presentada en dicho informe.

- Definir los mecanismos para monitorear y evaluar los cambios que pueden tener lugar en el tiempo y afecten al nivel de exposure de riesgo

- Establecer el presupuesto para llevar a cabo todo el proceso de gestión de riesgos

C5.3 Unidad de administración de riesgos

Esta unidad estará conformada por 3 coordinadores de la empresa. El jefe/encargado de la unidad será determinado por la directiva del CIAP.

Esta unidad tiene como objetivo desarrollar e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

Entre las responsabilidades relacionadas a la política de gestión de riesgo son:

- Registrar toda la información pertinente sobre la ocurrencia de alguna de las amenazas ya identificadas o de alguna nueva.

- Registrar y monitorizar las vulnerabilidades presentes en los activos y los distintos procesos de la empresa

- Realizar el levantamiento y procesamiento de la información pertinente para realizar el proceso de gestión de riesgos. La información necesaria para dicho proceso está compuesta por: amenazas (probabilidad, frecuencia, impacto), vulnerabilidades, controles (eficacia y grado de documentación e implementación)

- Ejecutar las distintas fases del modelo de gestión de riesgo con la finalidad de determinar el nivel de riesgo al que están expuestos los activos

- Elaborar el informe de riesgo en base a la información recaba por la implementación del modelo de gestión de riesgos. Este informe será presentado ante el comité de administración de riesgo para su discusión y determinación de las medidas correspondientes.

- Monitorizar y revisar de manera periódica la información recabada, el cálculo de riesgo (y su pertinente matriz) y el análisis derivado de todo lo anterior, para asegurar que el nivel de exposure y medidas correctivas sean adecuadas ante las variaciones del riesgo

C.5.4 Unidad de apoyo

Esta unidad estará conformada por el resto de coordinadores y por el departamento de logística. Tiene como finalidad prestar apoyo en cualquiera de las

responsabilidades que están a cargo de la unidad de administración de riesgo, pero su función más importante, será la de ayudar a identificar y registrar, cualquier amenaza o vulnerabilidad (ya identificada o nueva) que tenga lugar en actividades diarias de la empresa.

C.5.5 Tolerancia de riesgo

La tolerancia al riesgo será determinada por la directiva tomando en consideración los objetivos estratégicos de la empresa y del informe de riesgo elaborado por la unidad de administración del riesgo. Pero la tolerancia debería tener como límite aquellas amenazas que se ubiquen en la zona de riesgo moderado, donde la medida correctiva es aceptar el riesgo y realizar un monitoreo constante, ya que su impacto en la empresa es bajo.

A su vez, la tolerancia del riesgo estará determinada por los recursos asignados para llevar a cabo la gestión de riesgos. Dentro de dichos recursos se contempla: equipos, personal, tiempo y recursos financieros. Por lo que es una tarea vital del comité de gestión riesgos establecer el presupuesto necesario para llevar a cabo las actividades pertinentes, y que el presupuesto asignado sea lo más optimo posible. Este concepto es conocido como “coste de protección” y se busca que la organización vigile no emplear más recursos de los necesarios para cumplir con la gestión de riesgos.

La relación entre el coste de protección y riesgo queda reflejada en la figura 16.

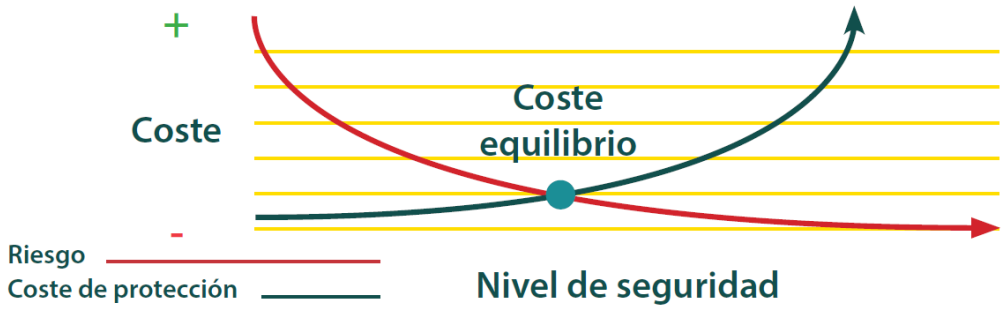


Figura 16. Coste de equilibrio

Fuente: INCIBE, Manual de gestión de riesgos, 2015