

**PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ**

**FACULTAD DE CIENCIAS E INGENIERÍA**



**ELABORACIÓN DE UNA METODOLOGÍA DE GESTIÓN DE  
RIESGOS INTEGRAL PARA UNA EMPRESA LOGÍSTICA DEL  
SECTOR AÉREO**

**Tesis para obtener el título profesional de Ingeniera Industrial**

**AUTORA:**

Andrea Liliana Quiroz Cárdenas

**ASESOR:**

Cesar Augusto Corrales Riveros

Lima, Febrero, 2022

## RESUMEN

Ante el importante crecimiento de las operaciones aeroportuarias en América Latina, se suman importantes retos para la aviación. Por lo que se presenta la conveniencia de esta investigación, ya que la gestión de riesgos está cada vez más presente en las empresas para acompañarlas y ser un soporte que permita aumentar su valor. Los gastos que las compañías del presente sector asumen ante la materialización de los riesgos operacionales son bastante altos, lo cual genera una disminución considerable en los ingresos totales al finalizar el año.

En la presente tesis se implementará un sistema de gestión de riesgos en una empresa del sector aeroportuario con el objetivo de contar con un marco teórico para la implementación y mejora en su sistema. En primer lugar, se definirá el marco teórico considerado para la presente investigación. Ello incluirá la definición de riesgo, qué significa gestionarlos, antecedentes y cómo se de la gestión integral de los mismos. Luego se procederá a explicar la normativa considerada como parte de la investigación, la cual será la ISO 31000:2018 Gestión del Riesgo y el COSO ERM, comité de patrocinio de empresas.

Posterior a ello, se describirá la empresa, incluyendo de dicha forma el sector, actividad económica, concepción del cliente, perfil organizacional, unidades de negocio y entidades participantes en su gestión. También, se explicará los procesos de la organización, el organigrama de la organización y, por último, las referencias normativas que aplican a la organización.

En tercer lugar, se esquematizará la metodología elegida incluyendo los puntos a considerar en la investigación. Para ello, se especificará los requerimientos y recomendaciones solicitados por la normativa incluyendo los objetivos, iniciadores, entradas, actividades y salidas, detallando cada punto para un mayor control y seguimiento.

En cuarto lugar, se procederá a realizar el análisis de brechas entre la situación actual y la indicada por la normativa. Se debe tener en cuenta, que a su vez se indicará la aplicabilidad de dichos faltantes, según la madurez de gestión de riesgos a implementar en la organización. Asimismo, se aplicarán los puntos observados en el análisis de brechas, generando una política, registros de los riesgos relevantes para la organización y el análisis de software como apoyo para la Gestión del Riesgo. Para la elección del presente software, se compararán las opciones y se elegirá las más conveniente de acuerdo a los requerimientos de la organización.

En quinto lugar, se realizará un análisis de costo beneficio para la compañía, tomando en consideración las primas de los seguros adquiridos por la compañía.

Por último, se brindarán las conclusiones y recomendaciones aplicables según análisis. Como conclusión se generará un ahorro de S/. 468,177.20, el mismo que deberá ser acompañado con la implementación de una política de Gestión de Riesgos, un portafolio de riesgos y un software que mejore la gestión de los mismos.



# INDICE

<b>INTRODUCCIÓN .....</b>	<b>1</b>
<b>1. MARCO TEÓRICO .....</b>	<b>3</b>
1.1. RIESGOS .....	3
1.2. GESTIÓN DE RIESGOS .....	3
1.3. ANTECEDENTES.....	3
1.4. GESTIÓN DE RIESGOS SEGÚN ERM: DEFINICIÓN Y FASES .....	5
1.5. NORMAS APLICADAS A LA GESTIÓN DEL RIESGO .....	7
1.5.1. Serie ISO 31000.....	7
1.5.2. Committee of Sponsoring Organizations of the Treadway Commission (COSO).....	25
1.6. PRINCIPALES SIMILITUDES Y DIFERENCIAS EN LAS NORMATIVAS USADAS .....	29
<b>2. DESCRIPCIÓN DE LA EMPRESA .....</b>	<b>32</b>
2.1. DESCRIPCIÓN DE LA EMPRESA DE SERVICIOS AEROPORTUARIOS .....	32
2.1.1. Sector y actividad económica. ....	32
2.1.2. Concepción de cliente y de producto o servicio.....	32
2.1.3. Perfil organizacional y principios empresariales.....	34
2.1.4. Unidades de negocio.....	34
2.1.5. Entidades participantes en el modelo de negocio.....	35
2.2. LOS PROCESOS Y LA ORGANIZACIÓN .....	35
2.2.1. Modelo de procesos. ....	35
2.2.2. Recursos humanos. ....	38
2.3. REFERENCIAS NORMATIVAS:.....	45
2.4. CONTEXTO DE LA ORGANIZACIÓN .....	50
2.4.1. Comprensión de la organización y su contexto .....	50
2.4.2. Ubicación Geográfica.....	51
2.4.3. Análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) .....	51
2.4.4. Análisis de requerimientos de las partes interesadas .....	52
<b>3. ESQUEMA TEÓRICO METODOLÓGICO PARA IMPLEMENTAR LA GESTIÓN DE RIESGOS ..53</b>	
3.1. ANÁLISIS PARA LA IMPLEMENTACIÓN DE LOS PRINCIPIOS .....	53
3.2. ANÁLISIS PARA LA IMPLEMENTACIÓN DEL MARCO DE REFERENCIA .....	57
3.2.1. Liderazgo y compromiso en la organización.....	57
3.2.2. Diseño del marco de referencia.....	60
3.2.3. Implementación del marco de referencia.....	61
3.2.4. Evaluación del marco de referencia .....	62
3.2.5. Mejora del marco de referencia .....	63
3.3. ANÁLISIS PARA LA IMPLEMENTACIÓN DEL PROCESO .....	63
3.3.1. Comunicación y Consulta.....	63
3.3.2. Establecimiento del contexto .....	65
3.3.3. Identificación de riesgos.....	66
3.3.4. Análisis de riesgos.....	68
3.3.5. Evaluación de riesgos.....	70
3.3.6. Tratamiento del riesgo.....	71
3.3.7. Monitoreo y revisión.....	73
3.3.8. Grabación e informes .....	75
3.4. APLICACIÓN DE LAS ACTIVIDADES PENDIENTES .....	76
<b>4. ANÁLISIS DE BRECHAS DE LA ORGANIZACIÓN CONTRA LA NORMATIVA .....</b>	<b>77</b>
4.1. ANÁLISIS PARA LA IMPLEMENTACIÓN DE LOS PRINCIPIOS .....	77
4.2. ANÁLISIS PARA LA IMPLEMENTACIÓN DEL MARCO DE REFERENCIA .....	83
4.2.1. Liderazgo y compromiso.....	83
4.2.2. Diseño del marco de referencia.....	84
4.2.3. Implementación del marco de referencia.....	84
4.2.4. Evaluación del marco de referencia.....	85
4.2.5. Mejora del marco de referencia .....	85
4.3. ANÁLISIS PARA LA IMPLEMENTACIÓN DEL PROCESO .....	85
4.3.1. Liderazgo y compromiso de la organización.....	85

4.3.2.	<i>Comunicación y consulta</i> .....	86
4.3.3.	<i>Establecimiento del Contexto</i> .....	87
4.3.4.	<i>Identificación de riesgos</i> .....	89
4.3.5.	<i>Análisis de riesgo</i> .....	91
4.3.6.	<i>Evaluación de riesgos</i> .....	93
4.3.7.	<i>Tratamiento del riesgo</i> .....	95
4.3.8.	<i>Monitoreo y Revisión</i> .....	98
4.3.9.	<i>Grabación e informes</i> .....	101
4.4.	<b>APLICACIÓN DE LAS ACTIVIDADES PENDIENTES</b> .....	102
4.4.1.	<i>Política de gestión de riesgos</i> .....	102
4.4.2.	<i>Registro de riesgos – Portafolio</i> .....	104
4.4.3.	<i>Softwares para la evaluación de riesgos</i> .....	115
<b>5.</b>	<b>ANÁLISIS COSTO – BENEFICIO</b> .....	<b>141</b>
<b>6.</b>	<b>CONCLUSIONES Y RECOMENDACIONES</b> .....	<b>148</b>
6.1	CONCLUSIONES .....	148
6.2	RECOMENDACIONES.....	148
<b>7.</b>	<b>BIBLIOGRAFIA</b> .....	<b>149</b>



## INDICE DE FIGURAS

Figura 1 Relación entre principios, marco de referencia y procesos .....	22
Figura 3 Resumen del COSO ERM 2017 .....	29
Figura 4 Mapa de procesos - Parte 1 .....	37
Figura 5 Procesos operaciones de la organización .....	38
Figura 6 Procesos de Soporte de la organización .....	38
Figura 7 Premisas organizacionales .....	39
Figura 8 Estructura Matricial .....	1
Figura 9 Estructura ejecutiva .....	1
Figura 10 Equipo Auditoría Interna .....	1
Figura 11 Gerencia SIG .....	1
Figura 12 Gerencia de Mantenimiento Aeronáutico .....	45
Figura 13 Conceptos para la evaluación de gestión de riesgos .....	62
Figura 14 KRI de riesgo: Configuración global de categorías de riesgo .....	118
Figura 15 Divisiones de riesgo, riesgo G.O.P.A.D., categorías de riesgo y gestores de riesgo .....	119
Figura 16 Mapeo de riesgos: Creación y vinculación de categorías de riesgos a una o más G.O.P.A.D. y a una o más divisiones .....	119
Figura 17 Creación de múltiples registros de riesgo .....	120
Figura 18 Paneles de riesgo: elementos de riesgo (visualización de KRI's y gráficos de Pareto) .....	120
Figura 19 Panel de riesgos: mapa de riesgos (mapa de calor de riesgos de recuento de KRI's) .....	121
Figura 20 Panel de riesgos: grupos de riesgos (acumulación de riesgos por G.O.P.A.D.) .....	121
Figura 21 Panel de riesgos: exposición al riesgo (categoría seleccionada versus la empresa) .....	122
Figura 22 Dashboard - Taxonomía del riesgo .....	122
Figura 23 Panel de riesgo - inventario (SQL Queries) .....	123
Figura 24 Panel de riesgos - probabilidad .....	123
Figura 25 Riesgos previos al compromiso .....	124
Figura 26 Compromiso de riesgo .....	124
Figura 27 Compromiso de riesgo - lecciones aprendidas .....	125
Figura 28 Diagramas de riesgo - espina de pescado .....	125
Figura 29 Control de riesgos .....	126
Figura 30 Pronósticos de riesgos .....	126
Figura 31 Mitigación de riesgos .....	127
Figura 32 Sensibilidad de riesgo - análisis tornado .....	127
Figura 33 Escenarios de riesgo - análisis de escenarios múltiples .....	128
Figura 34 Simulación de riesgos - sensibilidad dinámica .....	128
Figura 35 Ejemplo de Matriz de Riesgos .....	129
Figura 36 Filtros por encabezados .....	130
Figura 37 Segmentación por nivel de riesgo .....	130
Figura 38 Evaluación de Riesgos Residuales .....	131
Figura 39 Ejemplo de mapa de calor .....	131
Figura 40 Identificación y calificación del riesgo .....	133
Figura 41 Tratamiento y efectos relacionados .....	134
Figura 42 Mapa de calor de los riesgos TOP identificados .....	135
Figura 43 Descripción del impacto en los riesgos .....	136
Figura 44 Niveles de riesgo planteados .....	137

Figura 45 Mapa de nivel de riesgos planteado..... 138  
Figura 46 Calificación del tratamiento del riesgo..... 139  
Figura 47 Gráfica de línea ajustada ..... 145



## INDICE DE TABLAS

Tabla 1: Tabla comparativa del ERM vs la gestión de riesgos tradicional.....	5
Tabla 2 Herramientas y técnicas de evaluación de riesgos.....	24
Tabla 3 Diferencias conceptuales en las normativas .....	30
Tabla 4 Estructura normativa y representación en la organización .....	30
Tabla 5 Contexto general de la organización.....	53
Tabla 6 Principio integrador .....	54
Tabla 7 Principio estructurado y exhaustivo.....	55
Tabla 8 Principio de adaptabilidad .....	55
Tabla 9 Principio de gestión de riesgos inclusiva.....	56
Tabla 10 Principio de gestión de riesgos dinámica.....	56
Tabla 11 Principio de Mejor información disponible .....	56
Tabla 12 Principio: Factores humanos y culturales .....	57
Tabla 13 Principio de mejora continua .....	57
Tabla 14 Liderazgo y compromiso .....	58
Tabla 15 Elementos críticos del marco de referencia .....	58
Tabla 16 Actividades - Comunicación y consulta .....	64
Tabla 17 Actividades - establecimiento del contexto .....	65
Tabla 18 Actividades - Identificación de riesgos.....	67
Tabla 19 Actividades - análisis de riesgos .....	68
Tabla 20 Actividades - evaluación de riesgos.....	70
Tabla 21 Actividades - tratamiento del riesgo .....	72
Tabla 22 Actividades - monitoreo y revisión.....	74
Tabla 23 Actividades - Grabación e informes .....	76
Tabla 24 Contexto general de la organización.....	77
Tabla 25 Principio integrador .....	78
Tabla 26 Principio estructurado y exhaustivo.....	79
Tabla 27 Principio de adaptabilidad .....	80
Tabla 28 Principio de Gestión de Riesgos Inclusiva .....	80
Tabla 29 Principio de Gestión de Riesgos Dinámica.....	81
Tabla 30 Principio de Mejor Información Disponible.....	82
Tabla 31 Principio Factores Humanos y Culturales .....	82
Tabla 32 Principio de Mejora Continua.....	83
Tabla 33 Liderazgo y compromiso de la organización .....	83
Tabla 34 Análisis de brechas - comunicación y consulta .....	86
Tabla 35 Análisis de brechas - establecimiento del contexto .....	88
Tabla 36 Análisis de brechas - identificación de riesgos.....	90
Tabla 37 Análisis de brechas - análisis de riesgos .....	91
Tabla 38 Análisis de brechas - Evaluación de riesgos.....	94
Tabla 39 Análisis de brechas - tratamiento del riesgo .....	95
Tabla 40 Análisis de brechas - Monitoreo y revisión .....	98
Tabla 41 Análisis de brechas - Grabación e informes .....	101
Tabla 42 Registro de Peligros y Riesgos de SST.....	104
Tabla 43 Lista de Peligros y Riesgos Ambientales.....	115
Tabla 44 Proceso a seguir en el Excel .....	132
Tabla 45 Rango de probabilidades planteado .....	137
Tabla 46 Ponderación de alternativas de software.....	139
Tabla 47 Variación porcentual del seguro de Responsabilidad Civil .....	144
Tabla 48 Porcentaje de siniestralidad por año .....	145
Tabla 49 Proyección de Costos de Prima Neta.....	146



## ***INTRODUCCIÓN***

El sector aeronáutico, en especial la aviación, se encuentra en constante crecimiento en América Latina desde los últimos años. Esto se ve reflejado en el aumento del número de pasajeros en el tráfico aéreo, el número de aeronaves y la cantidad de carga transportada en éstas. Según un estudio realizado por CAF, Banco de desarrollo de América Latina, en el 2015, la oferta aérea de pasajeros ha experimentado una tasa de crecimiento importante de 5.1% anual en el periodo de años de 2006 a 2015 en América Latina y el Caribe, siendo éstos el tercer mercado con mayor crecimiento a escala mundial. Según dicho análisis, Perú, específicamente el aeropuerto de Lima, pasaría de contar con un tráfico de 17.6 millones de pasajeros al año en el 2015 a 67.1 millones de pasajeros para el año 2040. Actualmente, éste crecimiento se ve reflejado en el Perú, ya que se registró, hasta finales del 2018, 192,695 movimientos de aeronaves con un total de 22'127,752 pasajeros y una carga total transportada de 285,636 miles de toneladas en el aeropuerto de Lima, según el informe de Lima-Airport Partners, concesionario del Aeropuerto Internacional Jorge Chávez. Asimismo, según IATA - Asociación Internacional de Transporte Aéreo (2021, p.1), la pandemia COVID-19 ha generado retos emergentes para el sector, los cuales van desde promover la seguridad y salud hacia los pasajeros, hacia los nuevos retos en la logística y transporte de vacunas para dicho virus.

Ante este crecimiento en las operaciones, se suman importantes retos para la aviación. Por lo que se presenta la conveniencia de ésta investigación, ya que la gestión de riesgos está cada vez más presente en las empresas para acompañarlas y ser un soporte que permita aumentar su valor. Según la veintiseisava conferencia científica en economía y evolución social “Building Resilient Society” realizada en diciembre del 2017, las compañías que operan en un ambiente turbulento, complejo y dinámico se encuentran bajo gran presión para lograr resultados positivos en el negocio y satisfacer los requerimientos regulatorios que se le imponen. Los gastos que la compañía asume ante la materialización de los riesgos en operaciones y empresariales son bastante altos, lo cual genera una disminución considerable en los ingresos totales al finalizar el año. Según Paape y Spekle (2012, p.2), las debilidades en las prácticas de gestión de riesgos se han vuelto dolorosamente visibles y las compañías se encuentran actualmente bajo una presión considerable para fortalecer sus sistemas de gestión de riesgos y tomar las medidas adecuadas para mejorar la protección del valor en sus partes interesadas. Es por esto que actualmente la gestión de riesgos en las empresas se brinda desde el enfoque de los stakeholders, para que dicha gestión considere a clientes, proveedores, competidores, comunidad, entre otros actores que permiten generar una gestión integrada fomentando el cumplimiento de los objetivos de la empresa.

Por lo expuesto anteriormente, se propone desarrollar un proyecto que permita adecuar una metodología de gestión de riesgos integrada para una empresa del sector aeronáutico, posterior a ello, poder implementarla en su proceso principal.

En el capítulo 1 “Marco teórico”, se desarrollará la teoría necesaria para el sustento a la recolección y análisis de datos e incluye, entre otros, antecedentes, definiciones y normativa aplicada a la gestión de riesgos.

En el capítulo 2 “Descripción de la empresa”, se presentará la descripción de la empresa, el sistema de organización y el proceso del negocio de la empresa en estudio, también, se detallarán los datos relevantes para el análisis, diagnóstico y se hará el planteamiento de los problemas y determinación de causas de los mismos empleando las herramientas de mejora de la calidad.

En el capítulo 3 “Esquema teórico metodológico para implementar la Gestión de Riesgos”, se presentará el análisis para la implementación del marco teórico y el proceso de gestión de riesgos, en los cuales se detallarán los puntos clave a seguir por las organizaciones con el fin de contar con una gestión de riesgos o mejorar la misma.

En el capítulo 4 “Gestión de Riesgos Actual de la Organización”, se presentará el marco bajo el cual se rige actualmente la empresa del sector logístico. En el capítulo 5 “Análisis de Brechas de la Organización contra la normativa”, se desarrollará el análisis de brechas entre el esquema metodológico planteado en el punto anterior y la gestión actual de la organización.

En el Capítulo 6 “Análisis Costo – Beneficio”, se analizará las ventajas de implementar la metodología planteada, haciendo uso de la disminución de las primas de los seguros.

Por último, en el Capítulo 7 “Conclusiones y Recomendaciones”, se detallarán conclusiones y recomendaciones en base al análisis realizado.

## ***1. MARCO TEÓRICO***

En el presente capítulo se describirán los conceptos principalmente relacionados con los riesgos, tales como Riesgos, Gestión de Riesgos, Antecedentes, ERM, normal aplicadas, etc.

### ***1.1. Riesgos***

Según la norma ISO 31000:2018 (2018, p.1), se define riesgo como el efecto de la incertidumbre sobre los objetivos. En otras palabras, riesgo se entiende como una desviación positiva o negativa de lo previsto, que genera incertidumbre sobre los objetivos de una organización. Muchas veces estos dos conceptos no quedan completamente claros, debido a ello, Mun (2015, p. 39), define que la incertidumbre es la posibilidad de que se produzca un evento y el riesgo es la ramificación de que este evento se produzca. Para entender un poco más esta diferencia, se brinda un ejemplo sencillo: Se lanzan dos dados y usted apuesta S/. 1 a que la suma de los dos es mayor que 6, de esa forma ganaría S/. 2; sin embargo, si es menor o igual a este número, usted pierde todo. El riesgo aquí es que pierda todo, ya que la incertidumbre es que la suma sea menor igual a 6. Por lo tanto, la incertidumbre trae consigo riesgo. Según COSO (2017, p.4), el riesgo se define como la posibilidad de que un acontecimiento ocurra y afecte negativamente a la consecución de los objetivos.

### ***1.2. Gestión de Riesgos***

Según la norma ISO 31000:2018 (2018, p.1), la gestión de riesgos son actividades coordinadas para dirigir y controlar la organización con relación al riesgo, las mismas que van acorde a los objetivos identificados en la planeación estratégica de la organización. Para Bravo (2012, p. 71), se entiende por gestión o administración de riesgo, el proceso mediante el cual se identifican, analiza, evalúan, tratan o manejan, monitorean, y comunican los riesgos generados en una actividad, función o proceso, de tal forma que le sea posible a las empresas u organizaciones minimizar las pérdidas y maximizar las oportunidades. También, es importante resaltar que, en relación a lo definido en la sección anterior, la gestión de riesgos estará relacionada tanto con las oportunidades como con inconvenientes. Es decir, se identificarán y aprovecharán los posibles eventos favorables y también, se prevendrá y mitigarán inconvenientes para el cumplimiento de los objetivos.

### ***1.3. Antecedentes***

Los riesgos son parte de las actividades diarias de las personas, actualmente se convive con ellos y se ven reflejados en cada una de las decisiones que se toman, afrontando de esta forma sus consecuencias. Igualmente, en las empresas también se presentan riesgos en todas las actividades, los

cuales se interponen en el logro de los objetivos; por lo tanto, la organización debe tomar decisiones respecto a estos.

Según Dickinson (2001, pp. 360-366), a finales de los años 40's e inicios de los años 50's, la gestión de riesgos se consideró como parte formal de los procesos de toma de decisiones en las empresas; sin embargo, no fue hasta los años 90's que ésta surgió como concepto y como función en las empresas, ofreciendo un enfoque sistemático e integrado en la gestión de riesgos. Dos de los factores decisivos para la implementación fueron, las grandes pérdidas con riesgos evitables y el enfoque de los accionistas en los conceptos de creación de valor.

Como resultado de todos estos cambios, la gestión de riesgos intentó consolidarse en un proceso continuo que involucra la gestión de riesgos en todas las áreas de la empresa, convirtiéndose en un factor clave en el crecimiento de ésta. El término "Enterprise Risk Management", en adelante ERM, se diferencia del enfoque tradicional debido a que toma en consideración, de forma simultánea, todos los riesgos a los que la compañía se encuentra expuesta (Dvorski, 2017, pp. 364-369).

Dickinson (2001, pp.360-366), indica que las diferencias principales entre el enfoque tradicional de riesgos y el nuevo enfoque ERM son:

- ERM se enfoca en la empresa como un proceso global en donde los riesgos afectan la estrategia del negocio y, por ende, los objetivos de la empresa. Antiguamente, solo se trataban los riesgos y su gestión de estos de una forma individual, sin comprender que estos afectaban a las distintas áreas de la compañía.
- ERM propone disponer de un portafolio de gestión de riesgos aplicable a toda la compañía y para cada una de sus divisiones y/o funciones; por otro lado, la gestión de riesgos tradicional no contempla la predicción de los riesgos, ni la globalización de éstos.
- El ERM presenta un enfoque de riesgos críticos por parte de la alta dirección, debido a la importancia que ellos brindan a las estrategias y objetivos; sin embargo, la gestión tradicional, al no involucrar a la alta dirección, gestiona los riesgos de forma moderada.
- En el nuevo enfoque de ERM, se toma en consideración la creación y/o protección de valor con la gestión de riesgos. Es decir, no siempre la mitigación de éstos hará que la compañía genere mayores ganancias financieramente.
- Para ERM, la Junta Directiva supervisa los riesgos principales y el programa general de gestión de riesgos, mientras que el comité ejecutivo de gestión de riesgos, discute los riesgos estratégicos y emergentes. Para el enfoque tradicional, las responsabilidades no se encontraban definidas.

Se presenta un resumen, de lo expuesto en líneas anteriores, en la Tabla 1.

Tabla 1: Tabla comparativa del ERM vs la gestión de riesgos tradicional

Gestión del riesgo tradicional	Enterprise Risk Management (ERM)
Riesgos individuales	Riesgos en el contexto de la estrategia del negocio
Identificación y evaluación del riesgo	Desarrollo del portafolio del riesgo
Enfoque de riesgos moderados	Enfoque en riesgos críticos
Mitigación del riesgo	Optimización del riesgo
Riesgos sin dueño	Definidas las responsabilidades del riesgo
Cuantificación del riesgo sin metodologías	Seguimiento y medición de los riesgos

Fuente: Dickinson (2001, pp. 360-366)

#### ***1.4. Gestión de riesgos según ERM: definición y fases***

En el presente subcapítulo, se definirán los riesgos y las 4 fases que conlleva su gestión según el ERM (Enterprise Risk Management).

##### **1.4.1. Definición de riesgos**

Para la investigación, el riesgo es el efecto de incertidumbre en los objetivos, se define como la probabilidad de que un evento ocurra y afecte o impida el logro de los objetivos de la empresa. Según Pfohl (2011, p. 2), cada actividad del negocio está conectada con riesgos y estos no pueden ser eliminados, por lo que las organizaciones necesitan administrar y/o gestionar todos los factores que incrementan y reducen la probabilidad de ocurrencia de los riesgos.

Por lo tanto, se define la gestión de riesgos como la acción de “tratar” con los riesgos antes de que éstos se vuelvan problemas, preocuparnos anticipadamente por ellos. Esto incluye planificar la forma en que se gestionarán, identificarlos, documentarlos y analizarlos, planificar cómo enfrentarlos, implementar los planes y luego supervisarlos. Existen fases que nos apoyan en la gestión de los riesgos, si bien existen variaciones según los diferentes autores, la mayoría de ellos (Berenji y Anantharaman, 2011; El salmi y Hachicha, 2013, Giannakis y Louis, 2011; Mand et al, 2013; Olson y Wu, 2010) coinciden en estas cuatro fases que se presentan a continuación:

- Fase 1: Identificación de riesgos

En esta fase se encuentran, reconocen y describen los riesgos. Bravo (2012, p. 137), nos indica que se trata de un proceso consciente de análisis permanente y participativo, en el cual se busca responder como empresa a los riesgos que puedan afectarla. Para ello se debe identificar la fuente de riesgo de cada actividad, los riesgos, sus causas y sus potenciales consecuencias. Para ello, involucra la obtención y documentación de datos históricos, análisis teóricos, opiniones de expertos y la obtención de las necesidades de las partes interesadas, etc. Es uno de los beneficios más importantes ya que es la base para la calificación, evaluación y tratamiento de los mismos, por lo que Velásquez (2012), considera a ésta, la fase más importante en la gestión de riesgos.

Según Bravo (2012), los responsables de esta fase, son dos: Los responsables directos o dueños de los procesos y el personal independiente, de apoyo o externo a la organización. El primero puede encontrarse en la gerencia, en junta directiva, alta dirección, líderes de procesos, proyectos, etc.; para el segundo pueden ser auditores internos o externos, los cuales evalúan la exposición de la organización ante estos y la eficiencia de su gestión. Normalmente se utilizan técnicas tales como el mapeo de la cadena de suministros, listas de chequeo, análisis de árboles de eventos, análisis de fallas y modos de defectos, diagrama causa-efecto de Ishikawa, estas herramientas serán detalladas en la sección 1.5.1 Serie ISO 31000.

- Fase 2: Evaluación de riesgos

En esta fase se busca estudiar cada uno de los riesgos encontrados en la etapa anterior de acuerdo con su probabilidad de ocurrencia y con el impacto o severidad que pudieran tener sobre el cumplimiento de los objetivos. Para Bravo (2012, pp. 17- 49), un paso previo a la valoración de los riesgos, es la revisión de los controles existentes. En muchos casos se deberá realizar el análisis al riesgo puro, y, posteriormente, con los controles actuales, llegando a obtener un análisis de efectividad de los mismos.

Se puede determinar la probabilidad de cada factor de riesgo mediante información subjetiva y/o objetiva. Para el primer tipo de información, se pueden utilizar técnicas tales como el método de Delphi, matrices de riesgo, paneles de expertos; para el segundo, Multicriterio, AHP o AHP difuso y otras. El análisis subjetivo de los riesgos, podrá ayudar separando los riesgos relevantes para la organización, para los cuales se deberá implementar controles, y a su vez, se recomienda que se realice un análisis cuantitativo para un mejor control y seguimiento de los mismos.

- Fase 3: Gestión de los riesgos

Esta fase facilita la comprensión de las variables que impactan dichos riesgos. De acuerdo con los riesgos resultantes de las etapas anteriores, se identifican, evalúan, seleccionan y ejecutan los esquemas apropiados para manejar cada riesgo. Dentro de ellos existen 2 grandes grupos: riesgos considerados como amenazas y los considerados como oportunidades. En los dos casos, los mismos generan incertidumbres, las cuales se pueden traducir en impactos positivos o negativos frente al cumplimiento de objetivos de la organización.

Según Bravo (2012), se puede hacer uso de los siguientes facilitadores para optimizar la gestión de riesgos: Compartir información, agilidad, confianza en los stakeholders, seguridad de la información, responsabilidad social y corporativa, planeación estratégica del riesgo, relaciones de colaboración, compartir el riesgo en la cadena, análisis continuo y evaluación constante de los riesgos.

- Fase 4: Monitoreo de riesgos

En esta fase se busca monitorear los procesos de manera que se identifiquen nuevos riesgos y se continúe con el desarrollo de acciones encaminadas hacia la correcta gestión de los riesgos. Se deberá contar con indicadores de desempeño, para de esa forma revisar el estado de las metas trazadas, y de acuerdo con los resultados, realizar correctivos oportunos si es que el caso lo amerita. También, se deberá evaluar la efectividad del sistema de gestión de riesgos, para garantizar el logro de los objetivos organizacionales.

## ***1.5. Normas aplicadas a la gestión del riesgo***

En esta sección definiremos las normas internacionales que aplican a la presente investigación y que proveen un importante soporte en la gestión de riesgos para las empresas que deciden adoptarlas:

### ***1.5.1. Serie ISO 31000***

Según el prólogo brindado por la misma organización, ISO es una federación mundial de organismos nacionales de normalización, es independiente y no gubernamental. Para la investigación, se tomará en cuenta la ISO 31000:2018 Gestión del riesgo – directrices y la ISO 31010:2019 Gestión del riesgo – técnicas de apreciación.

#### **1.5.1.1. ISO 31000:2018 Gestión del Riesgo – Directrices**

Esta norma obtuvo una última revisión en el año 2018, asegurando de esta forma que su información se mantenga relevante y con herramientas útiles para el mercado. Este es un documento dirigido a las personas que crean y protegen el valor en las organizaciones gestionando riesgos, tomando decisiones y mejorando el desempeño.

Según un estudio realizado a esta última actualización de la norma, Sandrine Tranchard (2018, pp. 180-182), establece que el riesgo es definido como el efecto de incertidumbre en los objetivos de la empresa. Este se enfoca en el conocimiento incompleto de eventos o circunstancias en las decisiones de la organización. Esta norma ayuda a las organizaciones a desarrollar estrategias para la gestión de riesgos para identificar y mitigar éstos de manera efectiva, apoyando el logro de los objetivos y la protección de las ganancias.

La norma ISO 31000:2018 es una norma descriptiva, no presenta parámetros establecidos claramente. Gracias a lo especificado anteriormente, las organizaciones pueden adaptar sus componentes a su contexto y requerimientos específicos. Dentro de sus beneficios de la norma, los siguientes presentados, son los de mayor relevancia (Hutchins, 2018, pp. 13-15):

- Es un estándar internacional que ha sido adoptado por más de 60 países para la gestión de sus riesgos nacionales.
- Puede ser aplicado e integrado fácilmente en los sistemas de gestión ISO.
- Puede ser aplicable en casi todos los sectores, nivel de madurez y capacidad en relación con la gestión de riesgos.
- Alienta la toma de decisiones proactiva, preventiva y predictiva, en lugar de una gestión de riesgos reactiva.
- Identifica y trata riesgos en toda la empresa.
- Mejora la identificación de los riesgos que generan oportunidades y las amenazas.
- Cumple con los requerimientos legales y regulatorios.
- Mejora el gobierno corporativo, el riesgo y el cumplimiento. También, mejora la confianza de las partes interesadas.
- Mejora el liderazgo y compromiso de la gerencia hacia la apertura, la integridad, la honestidad y el comportamiento ético.
- Establece una base confiable para la solución de riesgos basado en problemas, en adelante RBP<sup>1</sup> por sus siglas en inglés, y para la toma de decisiones.
- Mejora los controles de riesgos operacionales.
- Asigna recursos de manera efectiva y eficiente para la gestión de riesgos, su tratamiento y mitigación.

- Mejora la gestión de incidentes y su prevención.
- Identifica y minimiza posibles pérdidas.

La norma se divide en 6 partes: Objetivo y campo de aplicación, referencias normativas, términos y definiciones, principios, marco de referencia y proceso. Las primeras 3 partes no cobran mayor relevancia en la investigación debido a que ya fueron explicadas anteriormente. Debido a ello, se pasará a describir desde la cuarta parte, principios.

Principios: Esta se basa en 8 principios básicos para la gestión de riesgos. Estos son la base para el diseño, implementación, monitoreo y mejora continua del marco de referencia, el cual será tratado posteriormente. Estos proporcionan orientación sobre las características de una gestión de riesgos eficaz y eficiente, comunicando su valor y explicando su intención y propósito. La normativa explica que estos principios son el fundamento de la gestión de riesgos y deberían habilitar a la organización para gestionar los efectos de la incertidumbre sobre sus objetivos.

Según la ISO 31000:2018 Gestión del Riesgo, la creación y protección del valor es el impulsor clave para la gestión de riesgos, para poder cumplir con dicho propósito, se busca mejorar el desempeño, fomentar la innovación y contribuir con el logro de objetivos. Según Hutchins (2018, p. 102), valor en el contexto de gestión de riesgos significa:

1. Rentabilidad, crecimiento, inversión o riesgo de valor.
2. Cumplir y superar necesidades, expectativas y requisitos de los clientes o partes interesadas.
3. La ética y la equidad, los cuales son elementos de la cultura organizacional.

Junto con este propósito central (creación y protección del valor), se encuentra 8 principios más, los cuales se detallan a continuación:

- La gestión del riesgo como parte integral de los procesos organizacionales: La gestión de riesgos se convierte integrada cuando se encuentra presente en el gobierno organizacional, riesgos en los procesos y cumplimiento normativo. La gestión de riesgos es una parte esencial en los procesos de gestión, incluyendo planeamiento estratégico, modelo de negocio, fusiones y adquisiciones; por lo tanto, la integración comienza en el nivel superior de la empresa y desciende progresivamente a las demás áreas tales como proyectos, procesos, y nivel operativo.
- La gestión del riesgo es estructurada y exhaustiva: Según la metodología ISO 31000, se busca obtener resultados coherentes y comparables, es por este motivo que la gestión de riesgos debe ser sistemática, estructurada y oportuna. Sistemática hace referencia a que trabaja en base a un plan o método ya que en la norma ISO busca un marco metodológico bien definido y exhaustivo ya que permite que ésta estructura se use para toda la organización.

- La gestión de riesgos debe ser adaptada a cada empresa: La gestión de riesgos necesita ser adaptada y diseñada para la organización y su contexto, por lo que los expertos en gestión de riesgos y los dueños de proceso deben trabajar juntos para diseñar, implementar y asegurar el marco de gestión de riesgos de la norma ISO 31000. La gestión del riesgo requiere una adaptación experta.
- La gestión de riesgos debe ser inclusiva: La transparencia y la inclusividad son atributos clave en la gestión de riesgos, ya que gracias a ellos los clientes, stakeholders y partes interesadas saben cómo se toman las decisiones. Esto crea alineación entre el propósito, misión, visión y asegura que se cumplan los objetivos. Como parte de estos atributos, todos deberían de entrenarse en el marco de la gestión de riesgos, principios, prácticas y en el proceso de toma de decisiones.
- La gestión del riesgo es dinámica, reiterativa y receptiva al cambio: La gestión del riesgo siente y responde continuamente al cambio. A medida los contextos externos e internos cambian, la gestión de riesgos varía, tienen lugar el monitoreo y la revisión de los riesgos, implementación de controles o la modificación de los existentes.
- La gestión de riesgo se basa en la mejor información disponible: La gestión del riesgo se encuentra basada en la mejor información disponible; por lo tanto, ésta debe ser acertada, confiable, suficiente y adecuada de acuerdo al contexto, eventos, riesgos y fuentes de riesgo. Consultas a expertos para evaluar entradas, desarrollo de un procedimiento estándar, evaluación de suposiciones y un profundo entendimiento del problema a solucionar son elementos para la toma de decisiones.
- La gestión del riesgo toma en consideración los factores humanos y culturales: Estos envuelven factores conductuales que son esenciales para la correcta implementación de la ISO 31000 ERM. El elemento humano es uno de los principales retos debido a que los colaboradores necesitan adoptar y adaptar la gestión, el control y otros cambios conductuales en su operación, pero estos pueden resistirse a dicha adaptación.
- La gestión de riesgos facilita la mejora continua: Las organizaciones deben desarrollar e implementar estrategias para mejorar la madurez de su gestión de riesgos junto con todos los otros aspectos de su organización buscando aumentar la competitividad y garantizando la sostenibilidad organizacional.

La norma continúa explicando el “Marco de Referencia”. Este se encuentra basado en un ciclo, que consiste en la integración, diseño, implementación y mejora del mismo. De acuerdo con Hutchins (2018, p.119), el propósito del marco de referencia es:

- Describir el gobierno y supervisión de las actividades de gestión de riesgos.

- Capturar cómo la empresa ofrece valor, incluyendo las claves para el éxito futuro.
- Iniciar el proceso de gestión de riesgos.
- Describir un marco de referencia común que puede usarse para identificar y manejar eventos potenciales que puedan impactar en la empresa.
- Proporcionar responsabilidad por el diseño, implementación y mejora de la ISO 31000:2018.

Según la ISO en mención, el marco de referencia cuenta con los siguientes elementos:

- Liderazgo y compromiso: La gestión de riesgos es efectiva solamente si es apoyada por la gerencia y la junta directiva, debido a que involucra planeamiento estratégico en la organización y la cadena de suministro, requiriendo dirección ejecutiva, autoridades y recursos (Sidorenko, 2019, p. 121). También, se explica que, para poder llevar a cabo la implementación de la gestión de riesgo, se debe un modelo de negocio en el cual se incluya el costo beneficio de la implementación, de esta forma el proyecto será aprobado.

Los roles y responsabilidades de las partes deben estar claras:

- Director ejecutivo: CEO por sus siglas en inglés, es el último responsable de la gestión de riesgos organizacionales emitiendo directivas para la gestión y controles adicionales. Este también autoriza el plan estratégico, las políticas y la estructura de control interno en la organización.
- Director de riesgos: CRO por sus siglas en inglés, es el principal consejero del director ejecutivo, unidades de negocio y colaboradores críticos en la gestión del riesgo. También, es responsable de la arquitectura, diseño, implementación y aseguramiento del programa ERM, este guía a la organización en todos los aspectos del riesgo y realiza evaluaciones de procesos de negocio, programas, proyectos, proveedores, seguridad de la información, cumplimiento, salud, seguridad, amenazas y otras actividades críticas. Este trabaja de cerca con el comité de riesgos identificando, evaluando, priorizando, tratando, monitoreando, comunicando y asegurando los riesgos en todos los niveles de la organización. También, lidera el planeamiento estratégico y la integración de RBPS (Seguridad de Procesos Basada en Riesgo) y RBDM (Toma de Decisiones Basada en Riesgo) en toda la organización.
- Dueños de riesgos: Las unidades de negocio, funciones críticas y los jefes son los dueños de proceso, estos pueden delegar la autoridad; sin embargo, la última responsabilidad les pertenece. Ellos deberán adoptar y adaptar el marco de referencia a sus funciones, operaciones, procesos y programas, en alineación con la política de

riesgos y directivas. A su vez, deberán participar en la gestión de riesgos y desarrollar controles y tratamientos apropiados.

- Comité directivo de riesgos: El director de riesgos preside el comité directivo de gestión de riesgos empresarial, este se encuentra compuesto por los jefes de las unidades de negocio, jefes de ingeniería, finanzas, administración, TI y recursos humanos. La función de este comité es dirigir el desarrollo e implementación de los planes, principios y procesos que priorizan y abordan el riesgo de la empresa. También, identifican, evalúan y tratan los riesgos que impiden alcanzar los objetivos de la empresa; por otro lado, son responsables de asegurar que los riesgos sean manejados para crear valor en la empresa y la priorización consistente con el apetito del riesgo.
  - Equipo de gestión de riesgos de proyectos y procesos: El equipo se encuentra encargado de desarrollar y mantener la política de gestión de riesgos, desarrollar planes de riesgo, diseñar controles en los procesos, desarrollar procedimientos y herramientas para procesos críticos. Este equipo también apoya los esfuerzos para identificar, evaluar, tratar y reportar riesgos. Por último, este equipo puede recopilar datos de riesgo y desarrollar informes de riesgo, a su vez, garantizar que los controles de riesgo sean apropiados para la tolerancia de la organización.
  - Equipo de evaluación de riesgos: Equipo compuesto por expertos en distintas materias, expertos en riesgos, y dueños de procesos. Su responsabilidad es definir y tratar riesgos que incluyan diferentes funciones, también, evaluar los riesgos en el sistema, su dependencia e interdependencia usando técnicas y metodologías apropiadas. Trabajarán con los dueños de proceso en el desarrollo de herramientas de evaluación tales como los árboles de decisiones, análisis de costo-beneficio, identificación de KRI's y KPI's, y el desarrollo de las recomendaciones correspondientes.
- Diseño del marco de referencia: Para diseñar el marco de referencia, es crítico contar con el contexto interno y externo de la organización. Con ello se refiere al ambiente en el cual la organización opera y compete, se cuentan con las siguientes 3 definiciones (Hutchins, 2018, p. 36 - 38):
    - ✓ Definición del entorno físico, ambiente, circunstancias, personas, lugar, partes interesadas, tiempo y otros elementos críticos.
    - ✓ Descripción de la capacidad de riesgos de la organización y la madurez del modelo actual.

- ✓ Contexto interno y externo. Dentro del contexto externo, se evalúan los siguientes puntos: Geografía en dónde se conduce el negocio, cultura, competidores y colaboradores, servicio externo y proveedores, reguladores globales y nacionales, bancos y recursos financieros. Por otro lado, dentro del contexto interno, se evalúa lo siguiente: gobierno, riesgo y cumplimiento, políticas, procedimientos e instructivos, planes estratégicos de riesgo, capacidad de proyectos y procesos, ética de las partes interesadas internas, cultura en la organización, información, modelo de negocio, estándares, requerimientos del sector y regulatorios, etc.

Asimismo, se debe considerar establecer los requerimientos para resolver el problema central y satisfacer las necesidades, asegurar que sea de fácil entendimiento, asegurar que sea simple, claro y consistente, incluir riesgos técnicos y conductas de colaboradores, asegurar que facilite RBPS y RBDM y definir el alcance del mismo. Por otro lado, dentro del diseño del marco de referencia, se solicita la elaboración de una política de gestión de riesgos, la cual incluye su estrategia para la gestión de riesgos, la comunicación de la misma a partes interesadas y clientes, apetito de riesgo, responsabilidad de la junta directiva y gerencia en el manejo de riesgos, métodos para juzgar conflictos derivados de la evaluación de riesgos y el tratamiento de riesgos, compromisos para la gestión adecuada de recursos para asegurar que los riesgos sean manejados dentro del apetito de la organización, identificación de KRI's (Indicadores claves de riesgo) y KPI's (Indicadores clave de performance) y su monitoreo, medición y reporte a los stakeholders claves. Por último, la revisión de cambios en las estrategias, políticas, planes y marco basados en nuevos contextos, condiciones y circunstancias.

Asimismo, Hutchins (2018, pp. 133 – 135) indica que, debemos tener en cuenta que la gestión de riesgos debe ser integrada a todos los procesos de la organización, también que la empresa requiere los recursos necesarios para poder diseñar, implementar y monitorear los riesgos; por último, se deberá establecer un proceso de comunicación interno y externo para asegurar que esta sea adecuada, precisa y confiable.

- Implementación del marco de referencia: Esta se encuentra basada en el entendimiento del contexto organizacional, ambiente y condiciones en las cuales la organización compite y opera, adaptando los principios establecidos en la normal al contexto antes mencionado. La norma no prescribe estrategias ni tácticas para diseñar e implementar el marco de referencia en una organización. Por el contrario, American Society of Safety Engineers, ASSE, formó un comité que desarrolló un reporte técnico llamado “Technical Report (TR) 31004”, el cual sí ofrece pautas a considerar para la implementación del marco de referencia; sin embargo,

dicha guía no es completa. Por lo tanto, para implementar el mismo, se tienen las siguientes sugerencias (Hutchins, 2018, pp. 137 - 139):

- ✓ Asegurar que la junta directiva y los ejecutivos que supervisan la gestión de riesgos se comprometan en garantizar la resolución de problemas.
- ✓ Entender cómo manejar la incertidumbre para lograr los objetivos de negocio.
- ✓ Integrar el buen gobierno a las estrategias, política y plan de la ISO 31000:2018.
- ✓ Desarrollar una estrategia para implementar el marco de referencia.
- ✓ Identificar y cumplir con los requerimientos legales, de los clientes y de las partes interesadas. También, asegurar que estos estén entrenados en la gestión de riesgos, ERM y en el marco de referencia de la norma.
- ✓ Asegurar que RBPS y RBDM se encuentren alineados con las estrategias de dirección de la organización.
- ✓ Centrarse en resultados compatibles y asegurar el cumplimiento de los objetivos del negocio.
- ✓ Monitorear el diseño, implementación y aseguramiento del marco de referencia hacia el cumplimiento de las expectativas, necesidades y requerimientos.
- ✓ Realizar un análisis para identificar brechas entre lo que la organización se encuentra realizando, los principios de la norma y las cláusulas específicas. También para asegurar el entendimiento de los riesgos organizacionales y desarrollo apropiado del tratamiento para asegurar el cumplimiento de los objetivos.
- ✓ Desarrollar y seguir un enfoque de madurez y capacidad en el diseño e implementación de la gestión de riesgos.
- ✓ Integrar reportes operaciones de riesgos significantes en reportes financieros.
- ✓ Integrar la gestión y objetivos de riesgos en operaciones, cadena de suministro y otros tipos de reportes para asegurar que los objetivos sean alcanzados.

Para una organización larga, como la actual, requiere un plan de implementación detallado, con una estructura de desglose de trabajo, que incluya hitos, derivables, recursos, línea crítica y alcance. Asimismo, el compromiso de las cabezas de la organización. Esta implementación, a su vez, busca pasar de un nivel ad hoc de gestión de riesgos a un nivel alto de capacidad y madurez, siguiente el moderado RCMM.

- Evaluación del marco de referencia: Dentro de este concepto se busca alcanzar los objetivos del negocio, para esto es necesario tener en cuenta lo siguiente:

- ✓ Medición continua con KPI's y KRI's evaluando el performance de los objetivos. Revisar la efectividad, eficiencia y economía de la implementación del marco de referencia.
- ✓ Medir la performance de la gestión de riesgos en contraposición con el plan de gestión de riesgos propuesto, para poder corregir las desviaciones durante la ejecución del mismo.
- ✓ Revisar la arquitectura, diseño, implementación y aseguramiento del marco de referencia, las estrategias, tácticas, políticas y planes basados en los cambios externos e internos del contexto de la organización.
- ✓ Comunicar la performance y políticas de riesgos a los patrocinadores, stakeholders, y partes interesadas.

Según Hutchins (2018, pp. 143 – 144), dentro de la evaluación del marco, se utilizan distintos conceptos explicados a continuación:

- ✓ Vigilancia: Observación de proyectos, procesos y/o sistema para asegurar que estos continúen en control y capaces de cumplir requerimientos y objetivos.
- ✓ Monitoreo: Se verifica la performance con los KRI's y KPI's contra los objetivos.
- ✓ Revisión: Evaluación periódica de cambios en el entorno, la situación o el contexto.
- ✓ Auditorías: Objetivas y/o evaluaciones independientes de sistemas, políticas, procedimiento para determinar que estos satisfacen los estándares.

El propósito de implementar estos conceptos en la empresa es proveer un nivel de aseguramiento del riesgo a los clientes, autoridades relacionadas y a las partes interesadas. Este nivel de aseguramiento estará determinado por el contexto de la organización y las necesidades de los entes antes mencionados. Para completar la idea, el monitoreo externo apoya a la organizacional informando de los eventos potenciales tales como político, ambiental, proveedores que puedan impactar en la continuidad del negocio.

Dentro de la evaluación, se debe tomar en cuenta que la junta directiva de las organizaciones, desea que se cumpla con los estándares, estatutos del gobierno, que los controles operen según lo requeridos, cumplimiento de objetivos, que los riesgos residuales sean identificados, controles efectivos y que mitiguen el riesgo según el apetito de la organización, si es que algún “cisne negro” está por ocurrir, y tratamientos adicionales que se puedan presentar.

- Mejora del marco de referencia, en la cual la idea central es la adaptabilidad y mejora del marco de referencia, esto debido a los cambios que se puedan presentar en el contexto. Para

esto, es necesario las revisiones periódicas, también, se debe tener en cuenta que los cambios realizados deberán incluir la satisfacción de stakeholders, requerimientos regulatorios, asegurar la efectividad del control y alcanzar los objetivos del negocio.

Hutchins (2018, pp. 148 – 149), nos dice que hay múltiples iniciadores para evaluar la mejora en el marco de referencia, tales como cambios disruptores en el ambiente competitivo, modelo de negocio, contexto y/o requerimientos del cliente. También, cambios en los reportes, riesgos crónicos y sistémicos, cambios en la organización, cambios en los productos o servicios u otras innovaciones, nuevos riesgos, pérdida de estructura interna, tratamiento inadecuado o inapropiado, etc.

- Integración del marco de referencia: En esta sección se discute acerca de la importancia de integrar el marco de referencia de la ISO 31000:2018, con los otros marcos existentes en la organización, tales como calidad, seguridad, medio ambiente, seguridad de la información, etc., de esta forma se contribuye con la solución de problemas basado en riesgo y la toma de decisiones basadas en riesgos. Para ello, se deben responder las siguientes preguntas:
  - ¿Los marcos de referencia serán integrados independientemente en la organización?
  - ¿Los marcos de referencia se integrarán en uno general?
  - ¿Alguno de los marcos será el dominante?

La respuesta ante estas preguntas vendrá en conformidad con el contexto de la organización. La alineación del marco de referencia planteado por la norma de referencia, podrá ser alcanzada mediante lo siguiente (Hutchins, 2018, pp. 151 - 153):

- Discutiendo los requerimientos en la gestión de riesgos y objetivos con la Junta Directiva y ejecutivos claves.
- Entendiendo el contexto organizacional, ambiente y criterios de riesgo.
- Entendiendo la capacidad y madurez actual en la gestión de riesgos.
- Entendiendo el apetito de riesgo y los criterios.
- Desarrollando una política general de gestión de riesgos.
- Discutiendo con los stakeholders la satisfacción con la gestión de riesgos actual.
- Determinando si las actividades de gestión de riesgos se pueden alinear con los principios.
- Integrando los principios de la normativa con los marcos de referencia existentes.

- Realizando un análisis de brechas entre el modelo existente y los requerimientos de la norma.
- Determinando las brechas y elaborando un plan para el cierre de las mismas.
- Revisando los planes, procesos, políticas y estándares de la gestión de riesgos actual.
- Revisando el conocimiento de riesgos, habilidades y destrezas del personal.

Como conclusión se tiene que la integración y el alineamiento de dos marcos de referencia puede ser un reto debido a la diferencia en principios, prácticas y requerimientos que pueden tener cada uno de ellos. Estas deben ser identificadas, especialmente las variaciones en políticas, procedimientos, alcance, recursos, reportes, calidad, comunicación y escalamiento de los problemas.

La sexta parte es el proceso de gestión de riesgos. Esta, según la norma, de acuerdo con Hutchins (2018, p. 155), cuenta con los siguientes atributos:

- Es integral a toda la organización, ya que involucra gobierno, reporte a la junta directiva, alcance de objetivos, satisfacción de clientes y cumplimiento regulatorio.
- Está alineada con la estrategia de la organización y el plan de gestión de riesgos.
- Está adaptada al modelo de la organización, cultura, clima de la organización y su ética.

A su vez, se encuentra compuesta por 8 pasos, los cuales se procederá a detallar:

- Comunicación y consulta: Ayuda a entender las necesidades de los stakeholders, clientes y partes interesadas para que el propósito, intención, alcance, objetivos y el proceso puedan ser diseñados, implementados y mejorados. Según Hutchins (2018, pp. 157 – 158), se debe tener en cuenta ciertas acciones claves, tales como identificar el ambiente, la ética, modelo de negocio y otros factores que se consideren claves, también, asegurar que se tomen en cuenta los puntos de vista de los stakeholders, clientes y partes interesadas cuando se define el criterio de riesgo, atributos y apetito del riesgo. También, debemos asegurar que los ejecutivos apoyen la gestión de riesgos, el marco de referencia, proceso, controles y tratamiento de los riesgos, identificar a los stakeholders, clientes y partes interesadas envueltas en la gestión de riesgos y en la implementación de los procesos. Adicional a ello, asegurar que los riesgos, necesidades requerimientos y expectativas de los stakeholders, clientes y partes interesadas sean identificados y sean alcanzados, asegurar KPI's, KRI's y objetivos sean identificados adecuadamente, asegurar que la organización cuente con el conocimiento, habilidades para identificar, analizar, controlar y tratar riesgos. Por último, es

importante desarrollar una comunicación efectiva y un plan de consulta para los stakeholders, clientes y partes interesadas, y asegurar un cambio efectivo en la gestión a través de la aplicación del proceso de gestión de riesgos.

Un punto importante de la comunicación y consulta, es que, en base a ella, se puede definir cuándo la organización toma o evita un riesgo, por ello este proceso debe encontrarse documentado. Este plan de comunicación y consulta, debe responder las siguientes preguntas:

- ¿Quiénes son los stakeholders, clientes y partes interesadas?
- ¿Cuáles son los requerimientos de información en relación a riesgos?
- ¿Qué es el proceso de comunicación y reporte?
- ¿Cuándo quieren ser notificados y con qué frecuencia?
- ¿Cómo las comunicaciones serían monitoreadas y evaluadas?

Los canales de comunicación y protocolos son esenciales para integrar el plan de gestión de riesgos, políticas, procedimientos y otros protocolos en los 3 niveles de la empresa (empresarial, proyectos y procesos, y operacional).

- Establecimiento del contexto: Según Hutchins (2018, p. 164), este podría ser el paso más importante de acuerdo a la normativa, ya que, durante la realización del mismo, se define cuales procesos deberían ser enfatizados según el perfil empresarial. Para ello, se deberá definir el contexto externo e interno de la organización. Para el primero se debe tomar en cuenta el ambiente externo el cual incluye los requerimientos, preocupaciones históricas, geopolíticas, económicas y de ambiente que puedan impactar a los objetivos y dirección, también los factores políticos, legales, financieros, competitivos, etc.; asimismo, la geografía, tendencias globales, históricas y culturales; valores, ética, gobiernos internacionales y la estructura de estándares de riesgo nacionales e internacionales. Por otro lado, el contexto interno abarca la definición del gobierno, riesgo y cumplimiento, la identificación del ambiente competitivo, el modelo de negocio, la ética en la organización, los valores y la estructura de la misma. También, la identificación de los stakeholders internos, el establecimiento de estrategias, tácticas, requerimientos y planes para alcanzar objetivos, la identificación de estrategias de dirección, los objetivos y metas del marco de referencia, procedimiento y procesos, etc.
- Identificación de riesgos: Este, es a su vez, es el primer paso de la evaluación de riesgos. Los procesos de riesgo incluyen descubrir y describir posibles riesgos, estos se encuentran

basados en factores tales como la madurez, capacidad, controles operacionales, madurez técnica, KRI's y KPI's, dependencias internas y externas, habilidades y soporte. En este paso, la organización identifica los posibles eventos de riesgo, amenazas, oportunidades que puedan mejorar, impedir, retrasar, prevenir, degradar o acelerar el logro de objetivos. La fuente de dichos riesgos puede ser conocida o desconocida y puede estar dentro o fuera de la organización. También, se deben considerar la cascada, dependiente, interdependencia, acumulación e interacción de los riesgos. Una vez identificada esta fuente, se pueden obtener posibles escenarios y causas y consecuencias son identificadas.

Hutchins (2018, pp. 175 – 177), explica que la identificación de riesgos debe realizarse en todos los niveles de la organización usando un proceso estructurado y sistemático para el desarrollo de un registro de riesgos. Este registro es una lista de riesgos conocidos y se debe especificar qué, cuándo, por qué y cómo pueden ocurrir dichos eventos. Dentro de las fuentes de información, se puede tomar en cuenta los registros y reportes de riesgo, registros internos de problemas, registros de auditorías, análisis BIA, comentarios externos e internos, FODA, PESTEL, lluvia de ideas, análisis de escenarios, encuestas, cuestionarios, entrevistas, análisis de stakeholders, grupos de trabajo, conocimiento corporativo, análisis de proceso y otros.

- **Análisis del riesgo:** Es el segundo componente de la evaluación de riesgos, comprende el entendimiento del tipo de riesgo, grado y naturaleza de las amenazas y riesgos identificados. Es importante para determinar si el riesgo debe ser tratado o manejado, también, determina la estrategia y métodos adecuados. Este a su vez involucra que este sea basado en necesidades organizacionales, en el contexto, propósito, requerimientos para fiabilidad y precisión. También, se debe analizar el tipo, nivel, y naturaleza de los riesgos, las causas, amenazas, peligros de cada uno de ellos.

Según Hutchins (2018, pp. 185 – 187), el análisis de riesgo cuenta con factores críticos, se mencionan los siguientes:

- **Objetivos múltiples:** los riesgos, amenazas o peligros pueden tener varias consecuencias que afecten a más de un objetivo, por lo que es crítico de que los controles y su efectividad sean analizados para cada uno de los riesgos que mitigan.
- **Tipos de análisis de riesgo:** Se pueden usar técnicas cualitativas y cuantitativas, la decisión de optar por ella dependerá del contexto, ambiente, aplicación y disponibilidad de información.

- Evaluación cualitativa de riesgos: Se puede usar un mapa de riesgos o mapa de calor para evaluar y analizar riesgos. Para la consecuencia y probabilidad de los riesgos, se indica que pueden ser definidos por niveles que vayan del 1 al 5 para cada caso.
  - Evaluación cuantitativa de riesgos: Esta se encuentra basada en probabilidades para determinar la probabilidad y las medidas económicas para determinar la consecuencia. Son basados en su mayoría por data histórica, tendencias u otro análisis. Este nivel de evaluación muchas veces es costoso o no se cuenta con la información necesaria, por ello, se debe analizar el costo beneficio de su aplicación.
  - Factores múltiples: Múltiples factores pueden resultar en una consecuencia o situación en la cual un solo evento puede que no sea identificado. Para este caso, el análisis de riesgo se puede enfocar en sub componentes, sub partes o componentes.
  - Controles existentes: El análisis del riesgo comprende el desarrollo de un entendimiento de los controles existentes que pueden estar mitigando el riesgo. Estos controles pueden ser personas, tecnología, o procesos. Estos a su vez se pueden ver identificados en el diagrama de Ishikawa (métodos, máquinas, personas, materiales, medición, ambiente).
- Valoración del riesgo: El propósito de la valoración del riesgo es prepararse para tomar decisiones basadas en riesgo, RBDM. Este paso nos ayuda a priorizar riesgos en cada uno de los niveles de la empresa (empresarial, proyectos y procesos, y operativo). La valoración del riesgo compara la consecuencia estimada y probabilidad del riesgo con el criterio definido cuando el contexto fue determinado. También, ayuda a determinar la aplicación de un tratamiento o gestión de los riesgos. Si este se encuentra dentro del apetito, no se requerirá controles adicionales; por el contrario, si el riesgo se encuentra fuera del apetito de riesgo, se definirán controles adicionales. La evaluación de riesgos no abarca todos los riesgos identificados, sino que se centra en los riesgos que pueden tener consecuencias a nivel empresarial. Por lo que, en esta etapa, el liderazgo ejecutivo deberá estar preparado para revisar estos riesgos y sus posibles controles y tratamiento. A su vez, dedicará recursos para la minimización de los mismos.
  - Tratamiento del riesgo: Apoya en el control de riesgos dentro del apetito de riesgo de la organización., se mira el rango de las opciones para el tratamiento y se preparan planes de control para estos. El propósito es asegurar una decisión apropiada para los riesgos. Normalmente los tratamientos de riesgos consisten en las siguientes decisiones estratégicas: Evitar, aceptar, reducir y transferir. Evitar riesgos incluye descontinuar operaciones, proyectos o actividades de un área específica, cancelar productos o transacciones, remover el

core del proceso, prohibir las actividades con riesgos altos, eliminar el riesgo de la fuente mediante procesos preventivos y desarrollando controles adicionales. Aceptar riesgos incluye aceptar riesgos en su nivel presente el cual se encuentra dentro del apetito de la compañía y no se toman acciones extras. Reducir el riesgo incluye desarrollar controles internos adicionales para reducir la probabilidad o consecuencia de un evento no deseable, también, responder a las contingencias mediante un plan de continuidad de negocio efectivo, empoderar al personal para que puedan tomar decisiones independientes basadas en el riesgo, testear y asegurar que los controles sean adecuados y se sostengan en el tiempo, disminuir la probabilidad y consecuencia de la actividad que te lleva a riesgos, desarrollar controles para la seguridad de la información, etc. Transferir el riesgo incluye tercerizar el riesgo, obtener niveles apropiados de aseguramiento incluyendo auditorías de partes terceras, delegar riesgos a autoridades capaces mediante arreglos especiales y/u obtener niveles apropiados de seguros.

- **Monitoreo y revisión:** Esta es una parte crítica en la gestión de riesgos, debido a que es un monitoreo de evaluación de riesgos continuo, que determina si los controles son efectivos, eficientes y económicos. Nos provee de un importante análisis de brechas de la gestión de riesgos busca contra los resultados, objetivos del negocio riesgos residuales, presupuesto y niveles de performance, por ello es necesario que las responsabilidades, autoridades de encuentren definidas y claramente documentadas.
- **Registro e informe:** En esta etapa se registran e informan documentos e información relevante en el marco de referencia, procesos y sistemas, también se reportan cambios a los stakeholder y las partes interesadas. Los reportes son importantes debido a que provee de información a las partes interesadas y asegura la gestión de riesgos presentada en una organización, también la data es importante para el planeamiento y evaluación ya que contiene históricos, por último, brinda de manera visual indicadores de medición de riesgos. Dentro de los ejemplos se pueden incluir: mapas de calor, controles de procesos, políticas, procedimientos, instructivos, registro de evaluaciones, identificación de riesgos, mapas de decisión, acciones correctivas, determinación de tratamientos, etc.

En la Figura 1, se muestra la interrelación entre los principios, el marco de referencia y los procesos.

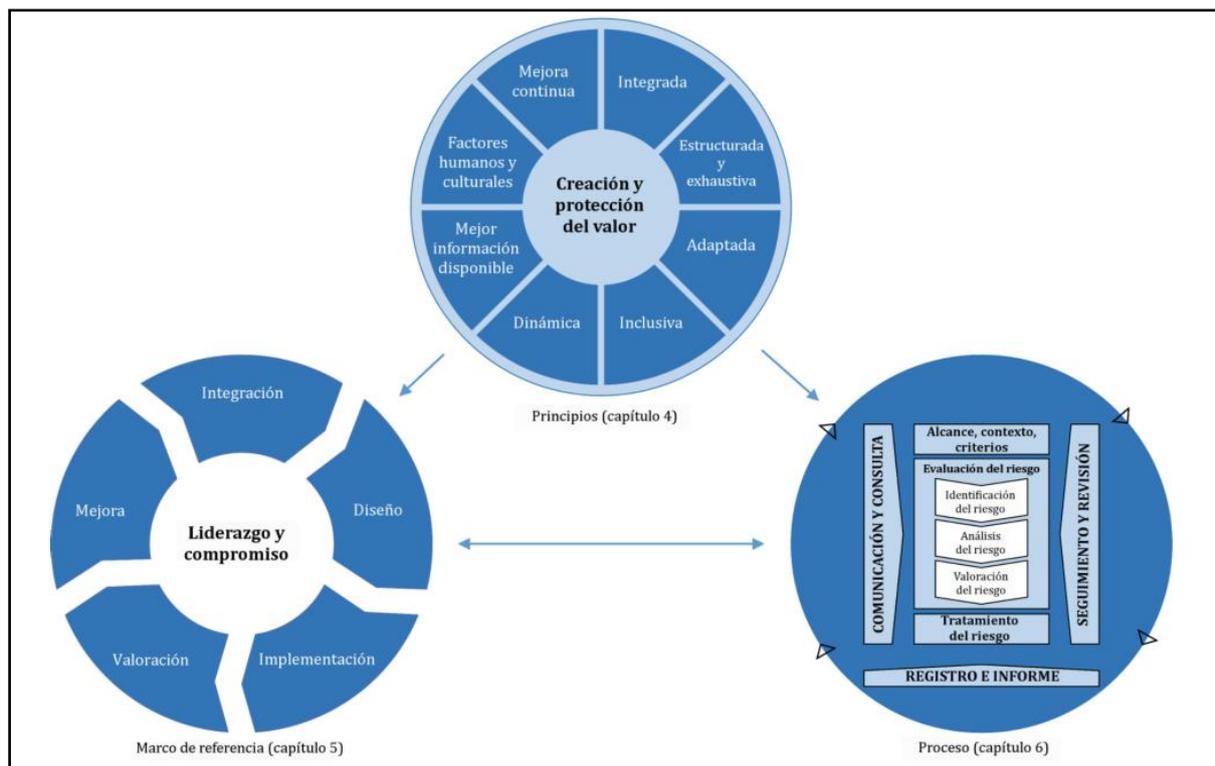


Figura 1 Relación entre principios, marco de referencia y procesos

Fuente: ISO 31000:2018 Gestión de riesgos

### 1.5.1.2. ISO 31010:2019 Gestión del riesgo – Técnicas de apreciación del riesgo

Esta normativa fue desarrollada como soporte de la ISO 31000, ya que provee técnicas para la gestión de riesgos, por lo que su función es la proporción de directrices para la selección y aplicación de dichas técnicas. Es importante mencionar que la norma no pretende que la organización aplique exactamente alguna de estas técnicas, sino que invita a la organización a que identifique sus requerimientos y, según ellos, seleccione la técnica más adecuada basada en su contexto y en otros factores que considere relevantes.

Esta norma se divide en seis partes: Objeto y campo de aplicación, normas para consulta, términos y definiciones, conceptos de apreciación del riesgo, uso de técnicas de gestión de riesgos e implementación de las mismas. Las primeras cuatro partes no serán de mayor relevancia para la investigación ya que son conceptos generales, por lo que se pasará a analizar las siguientes.

En la quinta parte, se explican que los beneficios en el uso de las técnicas tanto para los riesgos comunes como para los riesgos nuevos, complejos, o en los cuales los stakeholders tienen distintos puntos de vista.

En la sexta parte, se menciona en la norma su alineación con la ISO 31000, ya que, con el marco de referencia definido, la organización debería disponer de una política o estrategia para deducir cómo y cuándo se debería realizar la apreciación de los riesgos. Se indica, también, la importancia de la

comunicación y consulta eficaces entre las partes interesadas. De esta forma se logrará asegurar que los intereses de los mismos se comprendan y se tomen en consideración y, a la vez, permitirá reunir a las diferentes áreas de conocimiento técnico para la identificación y análisis de riesgo.

Asimismo, describe el proceso de apreciación del riesgo. Lo divide en la identificación del riesgo, el análisis del mismo, la evaluación, documentación, seguimiento y revisión de la apreciación del riesgo y la aplicación de la misma durante las fases de ciclo de vida. La norma indica que en la identificación del riesgo se pueden usar métodos basados en evidencias, los enfoques sistemáticos del equipo, las técnicas de razonamiento inductivo, y para mejorar la precisión y exhaustividad se puede utilizar la lluvia de ideas y la metodología Delphi. También, se menciona que el análisis del riesgo implica desarrollar una comprensión de ellos, a su vez, proporciona un elemento de entrada para la apreciación del riesgo y apoya en la toma de decisiones acerca del tratamiento de los mismos, así como las estrategias y métodos más apropiados para el tratamiento. Los métodos utilizados para esta etapa pueden ser cualitativos, semi-cuantitativos o cuantitativos. El detalle requerido depende de cada organización, o en todo caso por la legislación. También, se hace énfasis en la apreciación de controles, ya que de aquello dependerá el nivel del riesgo, por lo que la norma propone evaluar las siguientes preguntas:

1. ¿Cuáles son los controles existentes para un riesgo en particular?
2. ¿pueden estos controles tratar adecuadamente el riesgo, de manera que pueda controlarlo hasta un nivel que se considere tolerable?
3. ¿en la práctica funcionan los controles de la manera prevista y pueden demostrar que son eficaces cuando se requiere la aplicación de los mismos?

Otro punto importante, son los 3 enfoques generales utilizados en el análisis y la estimación de la probabilidad, estos son los siguientes:

1. La utilización de datos históricos importantes para identificar sucesos ocurridos en el pasado y poder extrapolar la probabilidad de que puedan volver a ocurrir. El fallo del presente enfoque se da en el caso de que la probabilidad extrapolada de que el suceso ocurra es bastante pequeña o cero, ya que intuye que el suceso no podrá ocurrir en un futuro.
2. Los pronósticos de probabilidad, en los cuales se utilizan técnicas de predicción tales como el análisis del árbol de fallos y el análisis del árbol de sucesos.
3. La opinión de un experto para estimar la probabilidad en procesos sistemáticos o estructurados. Los métodos disponibles son el enfoque Delphi, las comparaciones pareadas, la clasificación en categorías y los dictámenes de probabilidad absoluta.

Posterior a ello, en la evaluación de riesgos, se toma la decisión de si se debe tratar el riesgo y de cómo tratarlo. Esta decisión puede depender, entre otras cosas, de los costes y de los beneficios de aceptar el riesgo y de los costes y beneficios de implementar controles mejorados.

En la parte 6, selección de técnicas para la apreciación del riesgo, se clasifican las técnicas en cada etapa del proceso de apreciación del riesgo (identificación, análisis y evaluación), en la Tabla 2. se presenta una lista de 31 técnicas, las cuales son las más usadas comúnmente en la evaluación de riesgos. Se tiene las siguientes siglas para dichas técnicas: MA: Muy aplicable, A: Aplicable, NA: No aplicable.

**Tabla 2 Herramientas y técnicas de evaluación de riesgos**

Herramientas y técnicas	Proceso de apreciación del riesgo				
	Identificación del riesgo	Análisis del riesgo			Evaluación del riesgo
		Consecuencia	Probabilidad	Nivel de riesgo	
Tormenta de ideas	MA <sup>1)</sup>	NA <sup>2)</sup>	NA	NA	NA
Entrevistas estructuradas o semiestructuradas	MA	NA	NA	NA	NA
Delphi	MA	NA	NA	NA	NA
Listas de verificación	MA	NA	NA	NA	NA
Análisis preliminar de peligros	MA	NA	NA	NA	NA
Estudios de peligros y de operatividad (HAZOP)	MA	MA	3)	A	A
Análisis de peligros y puntos de control críticos (HACCP)	MA	MA	NA	NA	MA
Apreciación de riesgos ambientales	MA	MA	MA	MA	MA
Estructura «y si...» (SWIFT)	MA	MA	MA	MA	MA
Análisis de escenario	MA	MA	A	A	A
Análisis del impacto económico	A	MA	A	A	A
Análisis de la causa primordial	NA	MA	MA	MA	MA
Análisis de los modos de fallo y de los efectos	MA	MA	MA	MA	MA
Análisis del árbol de fallos	A	NA	MA	A	A
Análisis del árbol de sucesos	A	MA	A	A	NA
Análisis de causa-consecuencia	A	MA	MA	A	A
Análisis de causa-y-efecto	MA	MA	NA	NA	NA
Análisis de capas de protección (LOPA)	A	MA	A	A	NA
Diagrama de decisiones	NA	MA	MA	A	A
Análisis de fiabilidad humana	MA	MA	MA	MA	A
Análisis de pajarita	NA	A	MA	MA	A
Mantenimiento centrado en la fiabilidad	MA	MA	MA	MA	MA
Análisis del circuito de fuga	A	NA	NA	NA	NA
Análisis Markov	A	MA	NA	NA	NA
Simulación Monte-Carlo	NA	NA	NA	NA	MA
Estadísticas Bayesianas y redes Bayes	NA	MA	NA	NA	MA
Curvas FN	A	MA	MA	A	MA
Índices de riesgo	A	MA	MA	A	MA
Matriz de consecuencia/probabilidad	MA	MA	MA	MA	A
Análisis de costes/beneficios	A	MA	A	A	A
Análisis de decisión multicriterios (MCDA)	A	MA	A	MA	A

Fuente: ISO 31010:2019 Gestión del riesgo

Estas herramientas y técnicas pueden ser clasificadas en seis grandes grupos, Hutchins (2018, p.):

- Métodos de búsqueda: tales como los checklist y análisis de peligros.
- Métodos de soporte, tales como entrevistas estructuradas, lluvias de ideas, método Delphi, etc.
- Análisis de escenarios, para técnicas tales como el análisis de la causa principal, evaluación de riesgos ambientales, análisis de impacto de negocio, análisis de árbol de fallas, etc.
- Análisis de funciones, para técnicas como FMEA, mantenimiento centrado en la fiabilidad, análisis de peligros y puntos críticos de control, etc.
- Evaluación de controles, tales como análisis de capas de protección.
- Métodos estadísticos, como el análisis de Markov, Monte Carlo y Bayes.

La selección de las técnicas depende del nivel organizacional, madurez y capacidades y deberían de contener las siguientes características:

- Deberían ser justificables y apropiadas a la situación u organización que se está considerando.
- Deberían proporcionar resultados de una forma que mejoren la comprensión de la naturaleza del riesgo y de cómo se puede tratar.
- Deberían poder utilizarse de una forma que sea trazable, reproducible y verificable.

### ***1.5.2. Committee of Sponsoring Organizations of the Treadway Commission (COSO)***

COSO que es el Comité de Organizaciones Patrocinadoras de la Comisión Treadway, explica que el mismo se dedica a proporcionar liderazgo de pensamiento mediante el desarrollo de marcos y orientaciones generales sobre control interno, gestión del riesgo empresarial y la disuasión del fraude. Dentro de esta iniciativa participan 5 empresas: Asociación de Consultoría Americana, Instituto Americano de Certificadores Públicos de Contaduría, Ejecutivos Financieros Internacionales, Instituto de gestión de contaduría y el Instituto de Auditores Internos.

El comité antes mencionado ha publicado su última actualización en el marco de referencia sobre la gestión de riesgos empresariales en el 2017. Según un estudio realizado por la consultora EY (2017), indica las siguientes características fundamentales de la gestión del riesgo son:

- Debe estar orientada al logro de los objetivos estratégicos, operacionales, de información y de cumplimiento.
- Debe decantar en tareas y actividades continuas, alineadas a la estrategia.
- Debe ser un proceso continuo, efectuado por personas. Es decir, no se trata solamente de la definición de manuales, políticas, sistemas y formularios, sino de acciones ejecutadas por el

personal de cada nivel de la organización para llevar a cabo actividades de control que mitiguen riesgos de negocio.

- Debe ser capaz de proporcionar una seguridad razonable al Directorio y a la Alta Gerencia sobre el logro de objetivos, al tener identificados y gestionados los principales riesgos que enfrenta la organización.
- Debe ser adaptable a la estructura de la entidad y aplicable a los diversos niveles que ésta tenga, así como a las regiones geográficas donde opera.

Según el paper Understanding the New ISO and COSO Updates (2018, p.2), el COSO ERM del 2017, reconoce la dinámica y la naturaleza integrada que comienza con la misión, visión y valores de la organización hacia la creación de un mejor rendimiento. Establece que el propósito de una gestión eficaz del riesgo empresarial es ayudar a las juntas y a la gestión a optimizar los resultados. También, explora la gestión de riesgos empresariales al evaluar una estrategia en particular, considerando la posibilidad de que ésta se encuentre desalineada con los objetivos.

Según un estudio realizado por Deloitte en el 2017, el comité trata de responder la siguiente pregunta, ¿Cómo tomar mejores decisiones acerca de las incertidumbres que afectan nuestro futuro?, para lo cual se tiene como actividad clave, establecer el marco general para la gestión de los riesgos más significativos de la organización.

El objetivo central de la metodología es mejorar el logro de los objetivos estratégicos y la supervisión de riesgos en la junta directiva.

El comité plantea que existen oportunidades y riesgos. Dentro de las oportunidades se encuentran el desarrollo de nuevos productos o servicios, nuevos modelos de precios y nuevos mercados objetivos; por el otro lado, dentro de los riesgos se pueden encontrar las sanciones y multas, el fraude, desastres, entre otros.

El COSO se basa en la premisa subyacente del ERM, cada entidad existe para proveer valor para sus stakeholders, por lo que cada organización deberá determinar que tanta incertidumbre aceptar en su búsqueda del crecimiento de ese valor, Estupiñán (2006, p. ).

El valor se maximiza cuando la administración define estrategias y objetivos orientados a conseguir un balance óptimo entre las metas de crecimiento y retorno, así como los riesgos relacionados, a la vez que despliega recursos eficientes y efectivos para el cumplimiento de dichos objetivos.

COSO hace énfasis en 5 componentes: Gobierno y cultura, estrategias y objetivos, performance, revisión, e información, comunicación y reporte. Cada uno de ellos cuenta con principios, en total 20. Se hará una descripción de los mismos.

- Gobierno y Cultura: Un gobierno efectivo de riesgos establece el tono de una organización y refuerza la importancia del mismo, estableciendo responsabilidades de vigilancia en la gestión del riesgo, NACD (2018). En este contexto establecido, la cultura hace referencia a los

valores éticos y a un comportamiento responsable especialmente en la toma de decisiones. Esto lleva a la empresa a fomentar la supervisión efectiva de la junta directiva, reconocer el perfil de riesgo introducido en el modelo operativo, fomentar la conciencia del riesgo, demostrar un compromiso con la integridad y ética, establecer el ERM como una responsabilidad, y atraer, desarrollar y retener talento individual. Una organización alineada con los principios planteados por COSO, es caracterizada por un fuerte liderazgo, estilo participativo, responsable por sus acciones y resultados, cuenta con una toma de decisiones basada en riesgos y con diálogos abiertos y positivos acerca de la gestión del riesgo. También, cuenta con los siguientes principios: Consejo proporciona supervisión a los riesgos, organización establece estructura operativa, organización establece cultura deseada, organización demuestra compromiso con los valores fundamentales, y atraer, desarrolla, capacitar el talento.

- Ajustes en estrategias y objetivos: La estrategia, los objetivos y ERM trabajan juntos en el proceso de planeamiento estratégico. El apetito del riesgo es establecido y alineado con la estrategia. Los objetivos del negocio ponen la estrategia en práctica mientras sirven como base para identificar, asesorar y responder a los riesgos, Anderson (2017, pp. 40). Este componente cuenta con los siguientes principios: analiza contexto de negocio, define apetito de riesgo, evalúa estrategias alternativas, y formula objetivos de negocio.
- Performance: El riesgo que puede impactar en la estrategia y los objetivos necesita ser identificado y gestionado. Los riesgos son priorizados por severidad en el contexto de apetito de riesgo definido por la organización. Posteriormente, la organización selecciona respuestas a estos riesgos y revisa el portafolio de riesgos asumidos por la organización, siendo reportado a las partes interesadas claves. Este componente cuenta con los siguientes principios: Identifica riesgo, evalúa severidad de riesgo, prioriza riesgo, implementa respuesta de riesgo y desarrolla portafolio.
- Revisión: Al revisar el performance de la gestión de riesgos, la organización puede considerar que tan bien se encuentran funcionando los componentes del ERM en el tiempo y, a la vez, tomar en cuenta las revisiones necesarias debido a cambios importantes. Los principios asociados son: evaluar cambio sustancial, revisar riesgo y desempeño, y perseguir el mejoramiento de la gestión de riesgos.
- Información, comunicación y reporte: ERM requiere un proceso continuo de obtención e intercambio de información necesaria, de fuentes internas y externas. El reporte se enfoca en riesgos empresariales de áreas limitadas y especializadas, conteniendo recomendaciones para la mejora del ambiente de riesgo en dicha áreas. Este componente cuenta con los siguientes principios: Apalanca información y tecnología, comunica información de riesgo e informa sobre riesgo, cultura y desempeño.

COSO también define la gestión de riesgos en 4 fases: Identificación del riesgo, evaluación cuantitativa o cualitativa de riesgos documentados, priorización de riesgos y plan de respuesta, y monitoreo del riesgo. Estas fases ya fueron explicadas previamente en el punto 1.4.1. Definición de Riesgos.

Dentro de la primera fase, se definen 4 tipos de riesgos: Estratégicos, Operacionales, financieros, información y tecnología. Se pasará a realizar una breve descripción de cada uno de ellos:

- Riesgos estratégicos: Riesgos de industria, de economía, de competidores, cambios legales y regulatorios, riesgo en las necesidades del cliente, riesgo reputacional, etc.
- Riesgos operacionales: Riesgos en la cadena de suministro, satisfacción del cliente, riesgo en la ejecución del proceso, riesgo ambiental, riesgo de cumplimientos regulatorios, riesgos de recursos humanos, riesgos en la capacitación, riesgos en el performance de los incentivos, etc.
- Riesgos financieros: Riesgo en la tasa de interés, riesgo en la disponibilidad de capital, riesgo en la capacidad de crédito, etc.
- Riesgos de tecnología e información: riesgos de tasación financiera, riesgo en reportes regulatorios, riesgos en la seguridad del trabajador, riesgos en la infraestructura, riesgos en el acceso a la información, etc.

Esto es lo importante: Enterprise Risk Management se trata tanto de comprender las implicaciones de la estrategia y la posibilidad de que la esta no se alinee como de gestionar los riesgos para establecer objetivos. La Figura 3, ilustra estas consideraciones en el contexto de la misión, la visión, los valores centrales y como un impulsor de la dirección y el rendimiento general de una entidad. La gestión de riesgos empresariales, como se practica habitualmente, ha ayudado a muchas organizaciones a identificar, evaluar y gestionar los riesgos de la estrategia. Pero las causas más importantes de destrucción de valor en una organización, están integradas en la posibilidad de que la estrategia no respalde la misión y visión de la entidad, y las implicaciones de la estrategia. La gestión de riesgos empresariales mejora la selección de estrategias. Elegir la misma requiere una toma de decisiones estructurada que analice el riesgo y alinee los recursos con la misión y la visión de la organización.

Figura 2 Resumen del COSO ERM 2017



Fuente: COSO ERM 2017

### ***1.6. Principales similitudes y diferencias en las normativas usadas***

En esta sección se brindará un análisis entre las principales similitudes y diferencias en las normativas: ISO 31000:2018 y COSO ERM 2017. El objetivo es encontrar el punto medio para poder implementar una metodología basada en ambas normativas.

Por lo tanto, se presenta a continuación las similitudes más relevantes:

- ✓ Ambas normativas reflejan la evolución de la gestión de riesgos, reconociendo a la misma como una competencia de gestión integrada, Fox (2018, pp. 5). Tal como se mencionaba anteriormente, los riesgos eran analizados individualmente, ya que no se tenía en cuenta la consecuencia de los mismos en los objetivos de la organización.
- ✓ Ambas normativas enfatizan que la gestión del riesgo es parte integral en la toma de decisiones y vital para llevar a cabo su misión y mejorar el desempeño de la organización, por lo que, la gestión de riesgos ya no es considerada solamente como una actividad periódica de evaluación y actualización de los mismos, Fox (2018, pp. 5).
- ✓ Ambas revisiones también reconocen que el riesgo y la incertidumbre son consideraciones importantes a medida que los líderes de la compañía forman una estrategia, ejecutan operaciones y entregan iniciativas de proyectos, Fox (2018, pp.5).
- ✓ Ambas analizan las influencias importantes que la cultura y los prejuicios tienen en las prácticas de toma de decisiones y gestión de riesgos (Fox, 2018, pp. 7).

Por otro lado, en la Tabla 3, se presentan algunas diferencias conceptuales entre las dos normativas. Como se puede ver en la tabla, la ISO 31000:2018 presenta conceptos diferenciadores tales como la

política de gestión de riesgos y el plan de gestión de los mismos. Asimismo, dentro de los conceptos comunes, se puede evidenciar pequeñas diferencias en cuanto a definición; sin embargo, esta no es muy marcada generando similitud entre las mismas.

**Tabla 3 Diferencias conceptuales en las normativas**

<b>Concepto</b>	<b>COSO ERM</b>	<b>ISO 31000</b>
Riesgo	Eventos adversos	Efecto de incertidumbre sobre los objetivos
Gestión de riesgos	Proceso que incluye a los gerentes, la gerencia y el personal de una compañía para formular estrategias, identificar posibles eventos que pueden afectar a la empresa, administrar riesgos y brindar confianza para el logro de los objetivos.	Proceso que incluye el contexto, la estrategia de la compañía, para identificar, analizar, evaluar, tratar y monitorear riesgos.
Marco de referencia	Se trata de un conjunto de 8 componentes que incluyen configuración interna, establecimiento de objetivos, identificación de eventos, evaluación de riesgos, respuesta a riesgos, actividades de control, información y comunicación y actividades de monitoreo.	Es un conjunto de componentes que proporcionan infraestructura y regulaciones para el diseño, implementación, monitoreo, observación y desarrollo continuo de la gestión de riesgos.
Política de gestión de riesgos	No definido	Referida a la gestión de riesgos de una empresa y cumplimiento de sus objetivos
Plan de gestión de riesgos	No definido	Es el plan el que incluye los recursos, los componentes de gestión y el enfoque de la gestión de riesgos.
Proceso de gestión de riesgos	COSO ERM define toda la gestión de riesgos como un proceso con sus componentes	Comunicación, consulta, métodos de identificación de riesgos, análisis, detección, mejora, monitoreo y revisión de controles, implementación sistemática de políticas y procedimientos de gestión

Fuente: Comparación entre ISO 90001 y COSO ERM

En la Tabla 4, se presenta los conceptos relacionados en cada normativa y cómo se encuentran relacionados con la estructura de la organización:

**Tabla 4 Estructura normativa y representación en la organización**

<b>ISO 3100</b>	<b>COSO ERM</b>	<b>CONEXIÓN CON LA ESTRUCTURA DE LA ORGANIZACIÓN</b>
1. Establecimiento del contexto	Riesgo gobierno / cultura - Estrategia del riesgo / establecimiento de objetivos	Alta gerencia - Unidades de negocio
2. Evaluación del riesgo	-	-
2.1. Identificación del riesgo	Estrategia del riesgo	Unidades de negocio
2.2. Análisis del riesgo	Riesgo en ejecución	Nivel funcional

2.3. Valoración del riesgo	Riesgo en ejecución	Nivel funcional
3. Tratamiento del riesgo	-	-
4. Registro e informe	-	-
5. Comunicación y consulta	Información, comunicación y reporte del riesgo	Gestión de sistemas de información y análisis de riesgo
6. Seguimiento y revisión	Monitoreo de la performance del ERM	Todos los procesos dentro y en toda la organización

Fuente: A more effective audit after COSO ERM 2017 or after ISO 31000:2009? (2018, pp.12)

- ✓ Como se observa en el Tabla 3, ISO 31000 considera a la estrategia de riesgos y los objetivos como parte del contexto de la organización, mientras que en COSO ERM estos son conceptos autónomos y se relacionan al concepto de gobernanza y cultura del riesgo, ya que el gobierno organizacional apoya a cubrir a la organización del riesgo y la cultura se relaciona con la percepción de los valores importantes para la actividad de desarrollo de la empresa. Por lo general, dicha información se obtiene de la alta gerencia, De Sena (2018, pp. 12).
- ✓ La evaluación de riesgos es un ítem considerado solamente por la ISO 31000, para el COSO ERM, se realiza al final, midiendo el desempeño o rendimiento de la empresa luego de implementar la gestión de riesgos.
- ✓ El tratamiento del riesgo para la ISO significa ya se llevaron a cabo todos los procedimientos necesarios (controles) para evitar el riesgo. Para COSO, esto puede aparecer en la última fase: monitorear el rendimiento del ERM, De Sena (2018, pp. 13).
- ✓ Mientras que para ISO "Comunicación y consulta" se encuentra presente en cada parte del proceso, para ERM 2017 aparece al final del proceso, De Sena (2018, pp. 13).
- ✓ El monitoreo y la revisión pertenecen a ISO o ERM 2017. Mientras que para ISO es un proceso interactivo aplicable en cada momento de cada etapa del proceso para ERM, se establece después de la gestión de riesgos y se pretende evaluar su desempeño en la empresa.

## **2. DESCRIPCIÓN DE LA EMPRESA**

En el presente capítulo, se describirá brevemente a la empresa, sus procesos y cómo está compuesta la organización. Adicionalmente, se establecerá el contexto de la organización, aplicando el análisis FODA y requerimientos de las partes interesadas.

### **2.1. Descripción de la empresa de servicios aeroportuarios**

En el presente sub capítulo, se describirá el sector y actividad económica, la concepción del cliente y servicio, perfil organizaciones y principios, unidades del negocio y entidades participantes del modelo.

#### **2.1.1. Sector y actividad económica.**

Esta empresa cuenta con más de 25 años en el mercado aeroportuario ofreciendo servicios en el país, como también en Latinoamérica. Es la empresa líder en el sector aeronáutico, la cual brinda servicios aeroportuarios especializados, contando con estándares internacionales los cuales se respaldan con certificaciones como las ISO 9001:2015, ISO14001:2015, ISO 45001:2018, ISO 28000:2008, ISO 37001:2016, BASC e ISAGO. Por otro lado, con relación a la clasificación industrial uniforme (CIU), le corresponde el código 5223, debido a que esta clase comprende las actividades relacionadas con el transporte aéreo de pasajeros, animales o carga: Explotación de instalaciones terminales, como terminales aéreas, etc., actividades aeroportuarias y de control de tráfico aéreo, actividades de servicio en tierra realizadas en aeropuertos, etcétera. Sin embargo, también se incluye, manipulación de carga (CIU 5224).

#### **2.1.2. Concepción de cliente y de producto o servicio**

- ✓ Producto o servicio: A continuación, se muestran los principales servicios brindados por la organización:
  - Operador de base fija (Fixed Base Operator): El servicio FBO está dirigido a operadores de aeronaves privadas que no cuentan con un centro de control de operaciones aeronáuticas en sus destinos. Este servicio cubre la atención integral a la aeronave, tripulación y los pasajeros de vuelos corporativos como agente operador de base fija, desde la llegada, durante la estadía y hasta el despegue. Este servicio también implica comunicaciones con la aeronave, desde su ingreso al territorio hasta su arribo en tierra.
  - Atención de aeronaves: Atención integral a la aeronave mientras permanece en la rampa del aeropuerto, desde las coordinaciones previas con las Líneas Aéreas antes de la llegada del vuelo hasta el remolque final de la aeronave para el próximo despegue. Dicho servicio

- incluye el manejo del equipaje, carga y descarga de bodegas, limpieza de la cabina, remolque de la aeronave y otros servicios de soporte.
- Atención de pasajeros: La atención a los pasajeros y equipaje tanto de salida como de llegada en los vuelos de las Líneas Aéreas:
    - o Atención a Pasajeros de Salida, comprende desde la atención en counter hasta el embarque en la aeronave
    - o Atención a Pasajeros de Llegada, comprende desde el desembarque de la aeronave hasta la entrega final del equipaje.
  - Carga aérea de importación: El servicio de carga aérea de importación incluye el manejo físico y documentario de la carga desde su recepción, en la rampa del aeropuerto, hasta la entrega final al consignatario en nuestros almacenes luego de su desaduanaje.
  - Carga aérea de exportación: El servicio de carga aérea de exportación incluye el manejo físico y documentario de la carga de exportación, desde la recepción de los bultos entregados por los clientes en los almacenes hasta la entrega final en la rampa del aeropuerto para su embarque en la aeronave.
  - Carga aérea nacional: El servicio de carga aérea nacional incluye el manejo físico y documentario de la carga tanto para el flujo de mercadería de salida (desde Lima hacia provincias), como para el flujo de llegada (desde provincias hacia Lima):
    - o El flujo de salida, comprende desde la recepción de la carga entregada por el cliente en almacén, hasta su entrega final en la rampa del aeropuerto para su embarque en la aeronave.
    - o El flujo de llegada, comprende desde la recepción de la carga en la rampa del aeropuerto, hasta su entrega en nuestros almacenes al consignatario.
  - Servicio de agente de asistencia en tierra (GHA): El servicio de Agente de Asistencia en Tierra, está dirigido a líneas aéreas que deseen optimizar el negocio de carga. El objetivo es administrar eficientemente los recursos permitiendo orientar las operaciones a la actividad comercial. Mediante este servicio, la aerolínea designa al servicio especializado a las labores administrativas y operativas del departamento de carga.
  - Actividades de mantenimiento de la línea de vuelo: El servicio está dirigido a los operadores que deseen mantener en un nivel mantenimiento acorde a las exigencias internacionales que incorporan una mayor importancia a los aspectos de seguridad, medio ambiente además de un conocimiento creciente entre la conexión existente de la disponibilidad de la aeronave con la calidad del servicio brindado. Mediante este servicio, la aerolínea designa las labores de recepción y despacho de aeronave que comprenden los chequeos sobre la condición externa e interna de los sistemas del avión. Adicionalmente se provee el servicio de representante técnico para líneas aéreas extranjeras y de depósito de material de uso aeronáutico.

- Servicio de Capacitación Técnica: Es un centro de capacitación del sector aerocomercial orientado a convertir al Perú en una plaza moderna en el mundo del transporte aéreo internacional, a través de la capacitación a personal de líneas aéreas, terminales aeroportuarios, agentes de carga, aeropuertos, agencias de viaje, entre otros.
- ✓ Cliente: Los clientes de la organización pueden ser de dos tipos: Aerolíneas a las cuales se les da el servicio de rampa (atención de aeronaves), mantenimiento y de almacenamiento, transporte y recepción de carga (servicio logístico de carga); y personas naturales brindándoles el servicio de almacenamiento, transporte y recepción de carga.

### ***2.1.3. Perfil organizacional y principios empresariales.***

Al ser una empresa especializada sigue los estándares establecidos para una empresa de su sector, por ello todos los colaboradores conocen y respetan los valores de la empresa, los objetivos de ésta y su política.

Visión: “Liderar el mercado de servicios aeroportuarios en Latinoamérica y ser reconocidos por nuestros altos estándares de seguridad, calidad y excelencia operacional.”

Misión: “Brindar una propuesta de valor integral de servicios aeroportuarios, que garanticen la eficiencia, la seguridad y la calidad requerida tanto para nuestros clientes como para nuestros colaboradores y reguladores.”

Valores: Honradez en todo lo que hacemos, responsabilidad y dedicación por el trabajo, entrega total y dedicación al cliente, nunca conformarnos con lo que somos y hacemos.

### ***2.1.4. Unidades de negocio***

La presente empresa cuenta con cuatro unidades de negocio:

- ✓ Carga: Brinda el servicio logístico para el procesamiento de la carga (Almacenamiento, recepción y entrega) tanto para carga nacional, importación y exportación.
- ✓ Rampa: En esta unidad de negocio, se le brinda servicio a las aeronaves desde que la aeronave ingresa al aeropuerto hasta que se despacha el siguiente vuelo. Dentro de las actividades se encuentra el servicio de atención a pasajeros, también a pasajeros de atención especializada, el llenado de combustible, remolque de aeronave, etc.
- ✓ Escuela de entrenamiento: es una escuela que brinda capacitaciones y cursos establecidos por la DGAC y se encuentra certificada por IATA siendo impartidos por instructores certificados y especializados.

- ✓ Mantenimiento de Aeronaves: Brinda el servicio de mantenimiento preventivo, correctivo y por condición a las aerolíneas clientes.

### **2.1.5. Partes Interesadas**

- ✓ Operadores de aduanas: Aduanas es una entidad pública gubernamental fundamental para el funcionamiento de la organización, su presencia se centraliza en el proceso de carga ya que dentro de éste, ellos fiscalizan el cumplimiento de los derechos de importación y exportación a la introducción o salida de mercancías en el país.
- ✓ Empresas importadoras y exportadoras: Estas empresas trabajan con la organización para movilizar su mercadería dentro y fuera del Perú, gracias al servicio de carga ofrecido por la compañía.
- ✓ Aerolíneas: Son clientes de la empresa ya que a ellos son los que se les brinda servicios en tierra. Son claves para las operaciones debido a que las aerolíneas deciden con qué empresa desean aliarse.
- ✓ Dueños de aeródromos: Debido a que la atención a aeronaves, es decir la unidad de negocio de rampa se da en las instalaciones del aeropuerto, la organización tiene la obligación de cumplir con el correcto uso de ella.

## **2.2. Los procesos y la organización**

En el presente sub capítulo, se describirán los procesos principales llevados a cabo por la organización, el nivel organización y las referencias normativas aplicables a la organización.

### **2.2.1. Modelo de procesos.**

La organización cuenta con nueve procesos de negocio operativos:

- ✓ Atención a pasajeros: Este proceso se encuentra dividido por los siguientes tipos de vuelo:
  - Vuelo de salida: Se cuenta con los siguientes sub procesos: Planificación para el check-in, generación del check-in (mostrador), embarque de pasajeros, verificación de documentos del vuelo y envío de mensajes.
  - Vuelo de llegada: Verificación de los documentos del vuelo y coordinación y desembarque de pasajeros.
  - Vuelo de transferencia o tránsito: Recepción de pasajeros de vuelo de transferencia o tránsito, desembarque y orientación de pasajeros y transferencia o tránsito de pasajeros.

- ✓ Gestión de equipajes: El cual cuenta con los siguientes sub procesos: Aceptación y check-in de equipajes, colocación del bag tag y el embarque de equipajes.
- ✓ Despacho de vuelo: Incluye los siguientes sub procesos: Planificación del vuelo, coordinación del vuelo, atención del vuelo y despacho del mismo.
- ✓ Atención de aeronaves: Cuenta con los siguientes sub procesos: Planificación de recursos para atención de aeronaves, recepción de la aeronave, atención de la aeronave en tierra y despacho de la aeronave. También, cuenta con el sub proceso de mantenimiento de equipos de rampa.
- ✓ Carga Internacional Importaciones: Cuenta con los siguientes sub procesos: Traslado de carga de PEA al almacén, recepción de carga internacional de importación, almacenaje de esta, servicios intermedios y el despacho de la misma.
- ✓ Carga Internacional Exportaciones: Cuenta con los siguientes sub procesos: Recepción de carga internacional de exportación, transmisión a aduanas, almacenaje de la misma, servicios intermedios de la carga, paletizaje de la misma, despacho de la carga.
- ✓ Carga Nacional: cuenta con los siguientes sub procesos: traslado de carga de PEA a almacén, recepción de la carga, almacenaje de la misma, trámites de carga y/o aduana, entrega de carga nacional de llegada, despacho de carga nacional de salida, traslado de carga de almacén a la PEA.
- ✓ Organización de mantenimiento aprobada: Cuenta con los siguientes sub procesos: solicitud de servicio, planificación de actividades, recepción de aeronave, pernocta, mantenimiento de aeronave, mantenimiento del In Flight Entertainment, despacho o entrega de aeronave, administración, depósito de material aeronáutico DMA.
- ✓ Servicio de capacitación técnica: cuenta con los siguientes sub procesos: venta de cursos externos TTS, dictado de cursos externos TTS.

Además, se cuenta con procesos de soporte, que se presentan a continuación:

- ✓ Gestión Comercial
- ✓ Gestión de Atención al Cliente
- ✓ Gestión de la Tecnología e Información
- ✓ Gestión de Seguridad de la Aviación
- ✓ Gestión y Desarrollo del Talento Humano
- ✓ Gestión de Administración y Finanzas
- ✓ Gestión de Mantenimiento e Infraestructura
- ✓ Gestión de logística y compras

Por último, se presentan los procesos direccionales y estratégicos:

- ✓ Gestión de la alta dirección
- ✓ Gestión de desarrollo de nuevos negocios

- ✓ Gestión legal y marco regulatorio
- ✓ Sistemas Integrados de Gestión
- ✓ Gestión de proyectos
- ✓ Gestión de comunicación interna y relaciones institucionales

En la Figura 4, se presenta el mapa de procesos direccionales y estratégicos, asimismo, se muestran los procesos de atención a pasajeros, gestión de equipajes y despacho de vuelos.

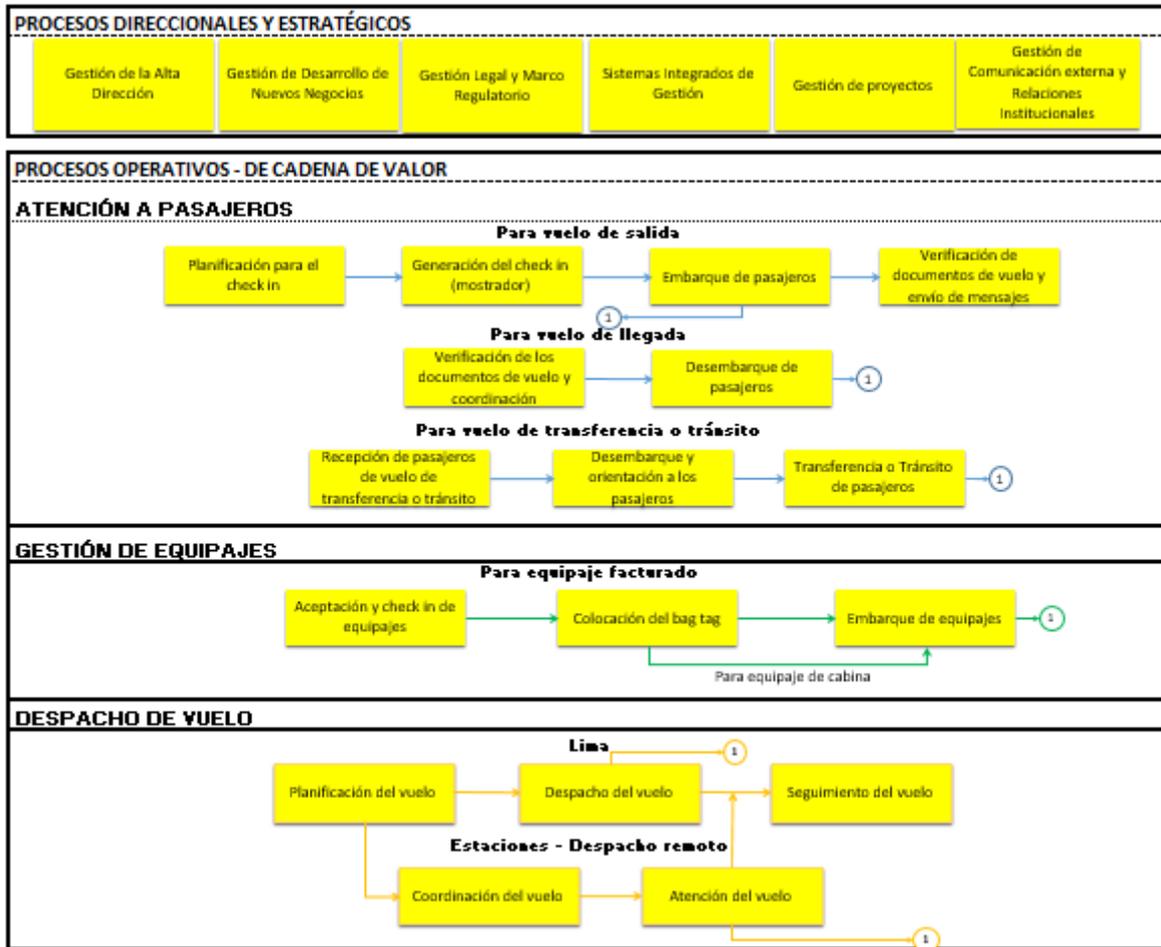
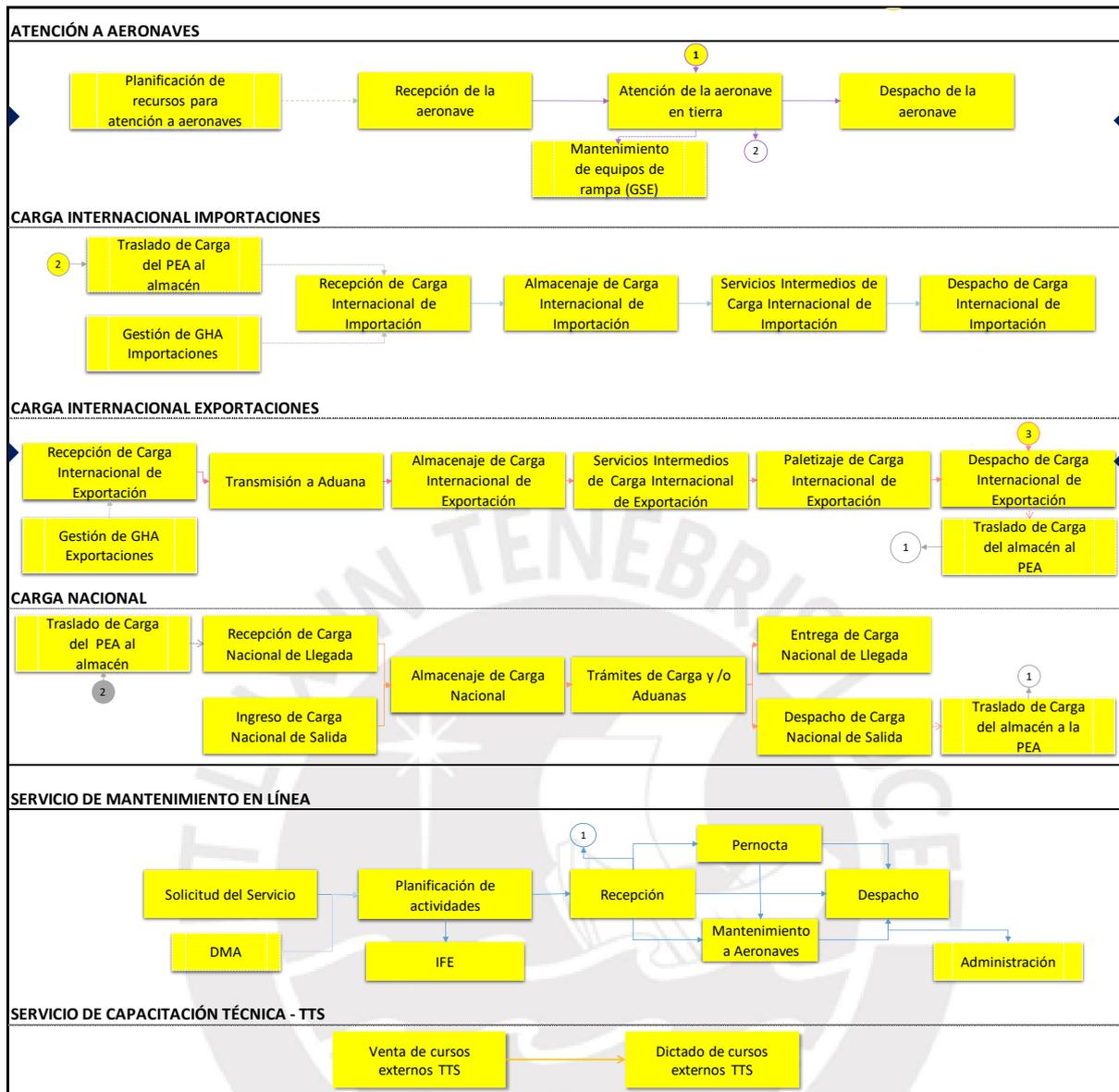


Figura 3 Mapa de procesos - Parte 1

En la Figura 5, se presentan los procesos de atención a aeronaves, carga internacional de importaciones, carga internacional de exportaciones, carga nacional, servicio de mantenimiento en línea y servicio de capacitación técnica TTS.



**Figura 4 Procesos operaciones de la organización**

Por último, se muestra en la figura 6, los procesos de soporte de la organización.



**Figura 5 Procesos de Soporte de la organización**

### 2.2.2. Recursos humanos.

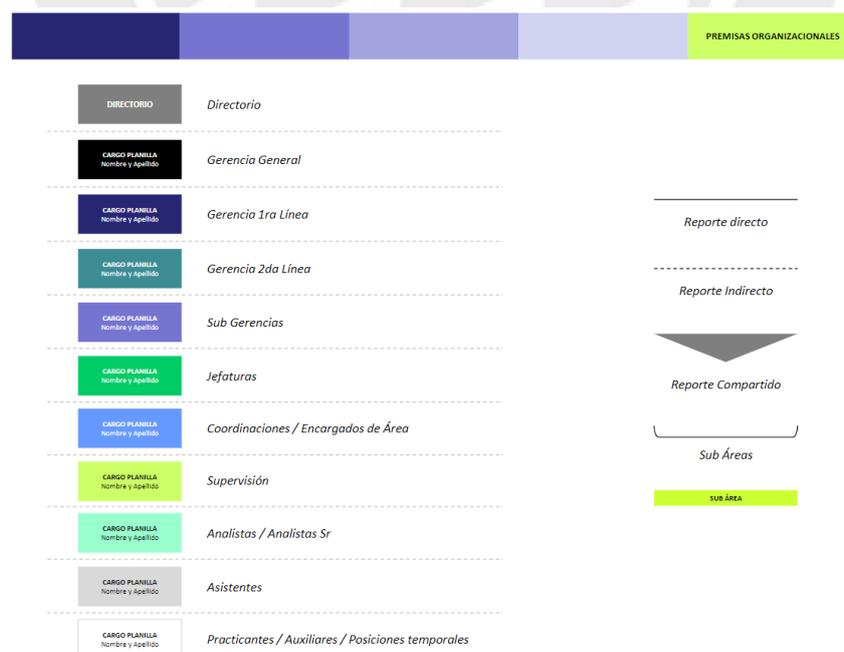
Rol de personal: en la empresa, el rol del personal se divide en los siguientes niveles. En primer lugar, el Nivel Ejecutivo, en el cual se encuentran los gerentes y jefes de áreas. Son los encargados de liderar y brindar soporte al personal a cargo, como también a las diversas áreas que lo necesiten. En segundo

lugar, el Nivel de Mando Medio, en el cual se encuentran los coordinadores, analistas, asistentes, practicantes, supervisores, personal de facturación y counters. Son los encargados de proveer la información y ejecutar proyectos bajo el mando de los gerentes o jefes de áreas según corresponda. Por último, el Nivel Operativo, compuesto por los operarios de carga y rampa. Ellos se encargan de apoyar en la realización de los servicios brindados por dichas unidades y son parte fundamental de la compañía.

Condiciones laborales: Las condiciones laborales que brinda la organización dependen de los niveles de los colaboradores mencionados en el anterior punto. Por ejemplo, el nivel ejecutivo y el nivel de mando medio cuenta con un horario de oficina, el cual es de 9:00 a.m. a 18:00 p.m. Los operarios y jefes del área operativa manejan un horario rotativo y manejan un turno de 2x2 o 5x2 dependiendo de la antigüedad y tipo de contrato con cada uno de ellos.

La empresa cuenta con comedor, microondas, vestidores (para el área operativa) y sala de lactancia. En muchas ocasiones se realizan campañas manteniendo al personal incentivado para que cumplan con sus labores a su 100%.

Por otro lado, también se cuenta con el organigrama de la organización. Tal como se muestra en la Figura 7, se encuentra compuesto por el Directorio, Gerencia General, Gerencia 1ra Línea, Gerencia 2da Línea, Sub Gerencia, Jefaturas, Coordinaciones, Supervisión, Analistas, Asistentes y Practicantes. En las Figura 8, se presenta una estructura matricial de la organización, en la Figura 9, una estructura ejecutiva, en la Figura 10, se desagrega al área de Auditoría Interna, en la Figura 11 al área de Sistemas Integrados de Gestión (SIG) y en la Figura 12 al área de mantenimiento de aeronaves.



**Figura 6 Premisas organizacionales**  
**Fuente: Empresa del Sector Aeroportuario**

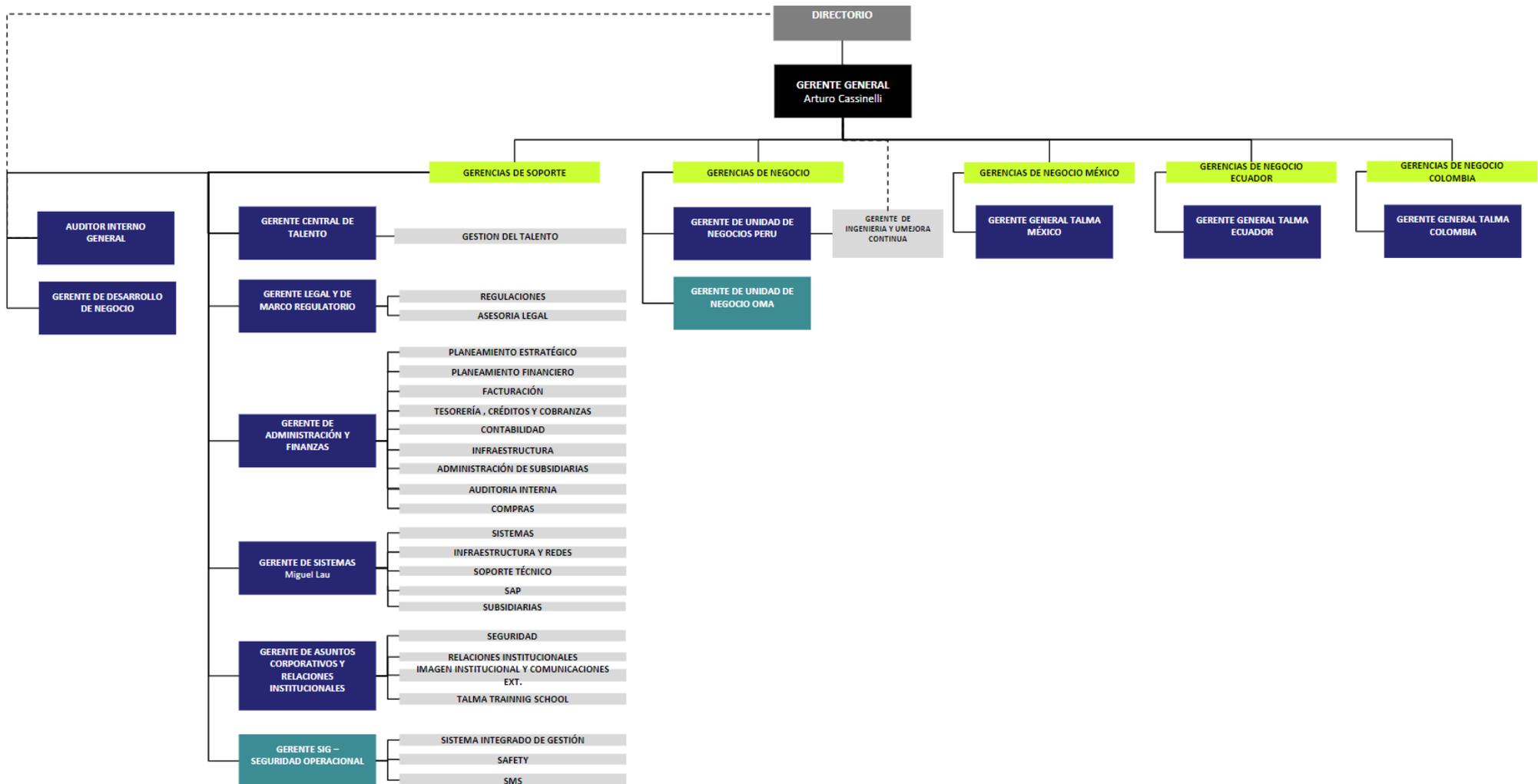
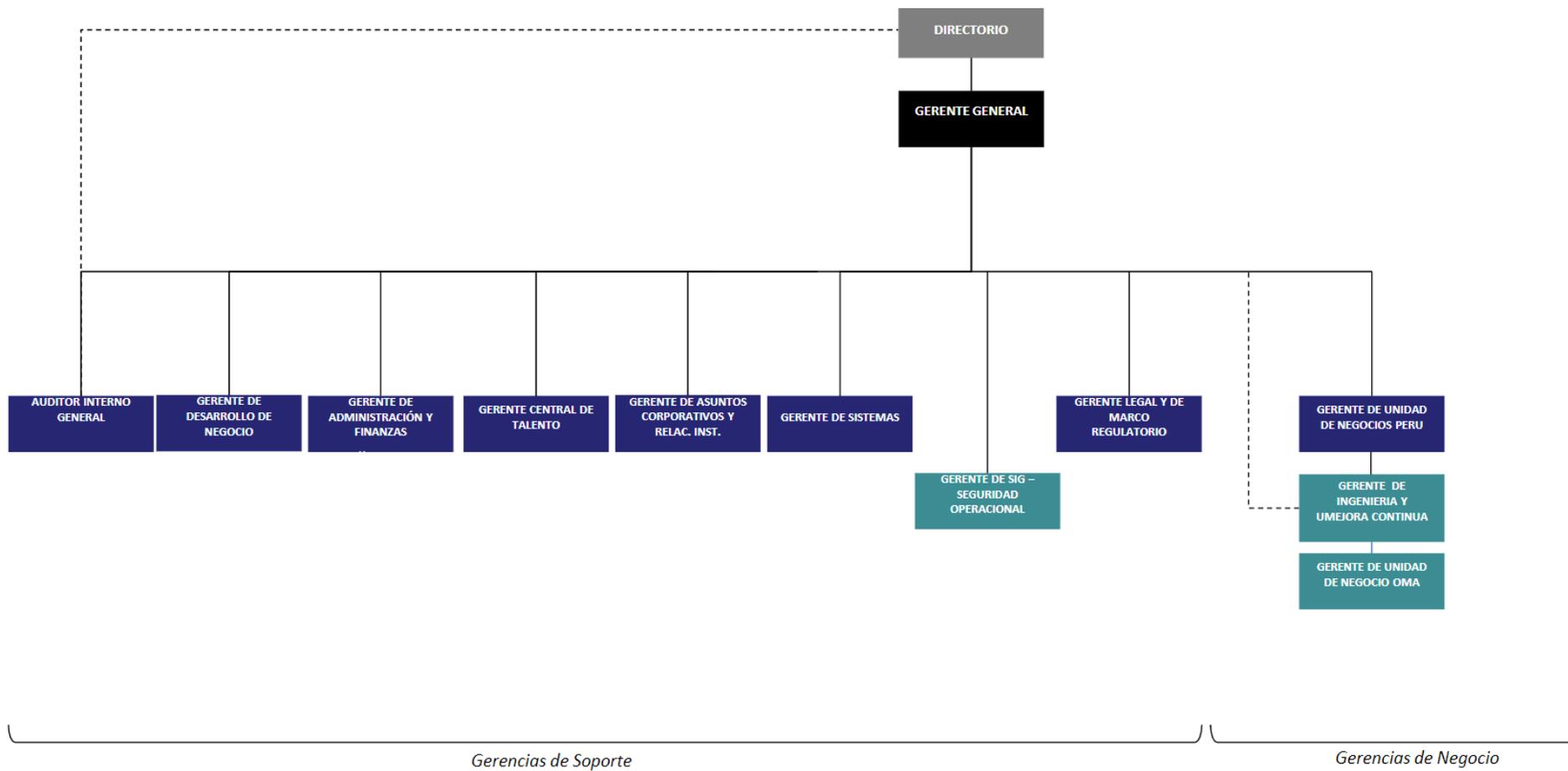
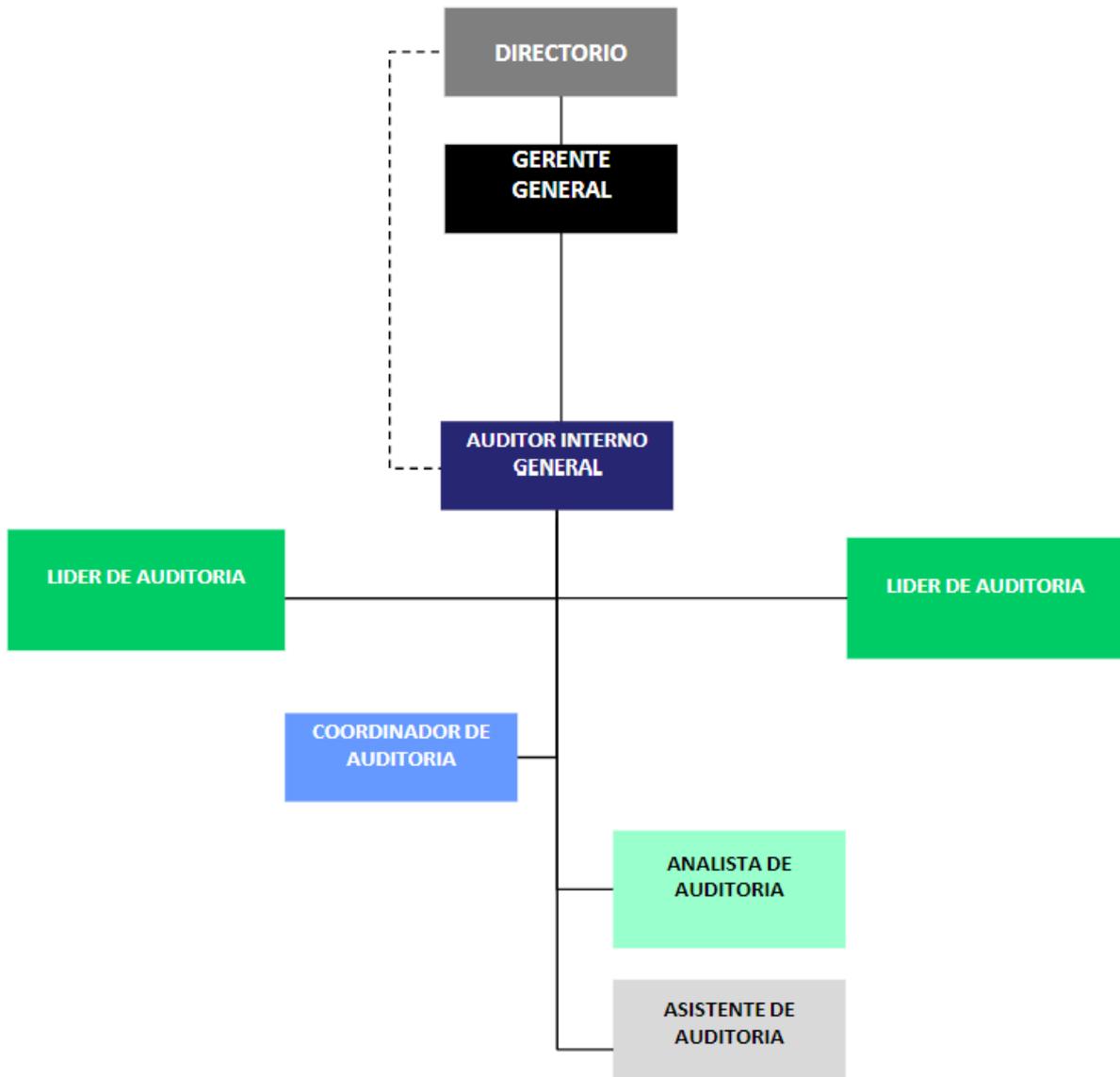


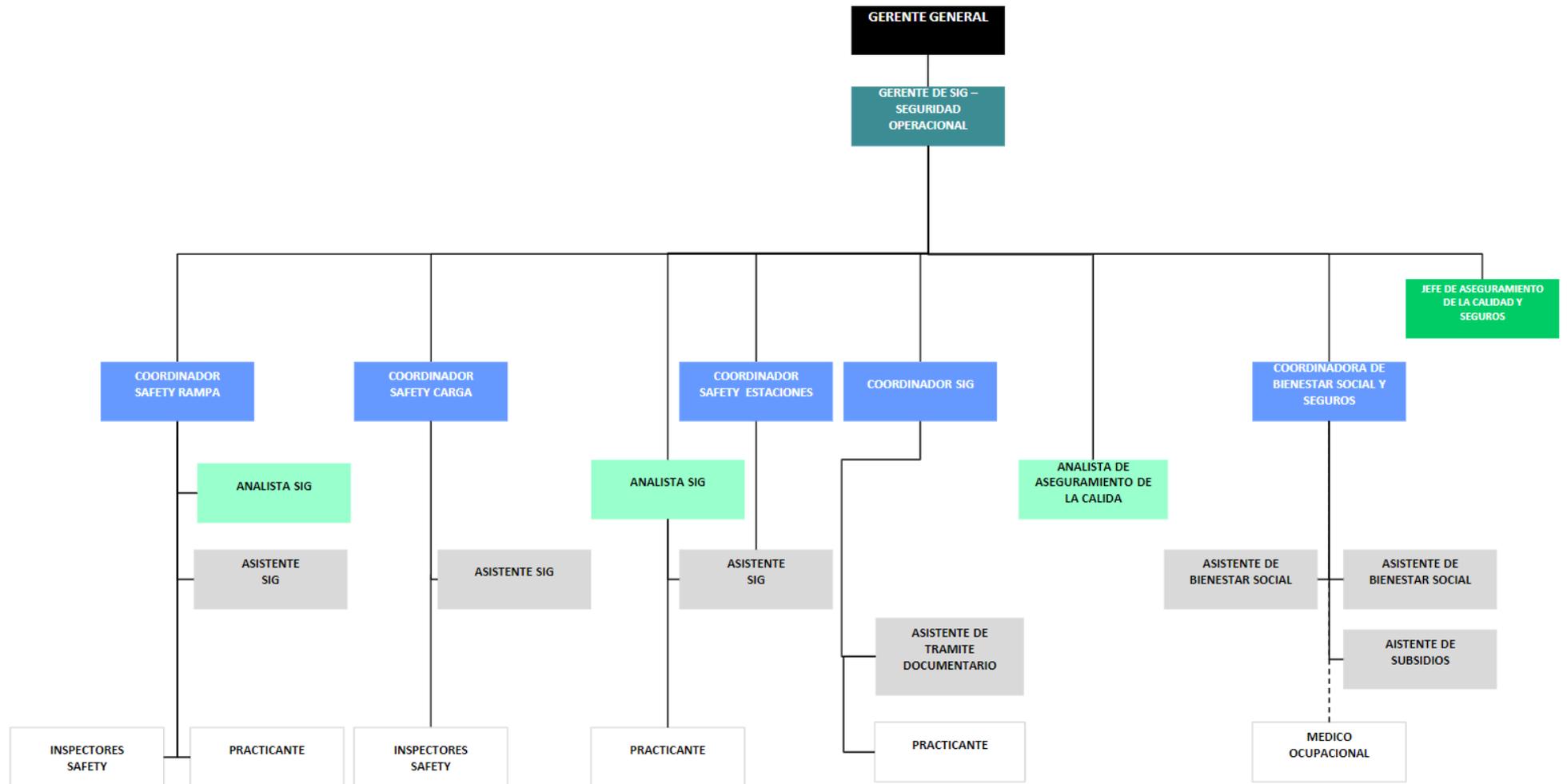
Figura 7 Estructura Matricial



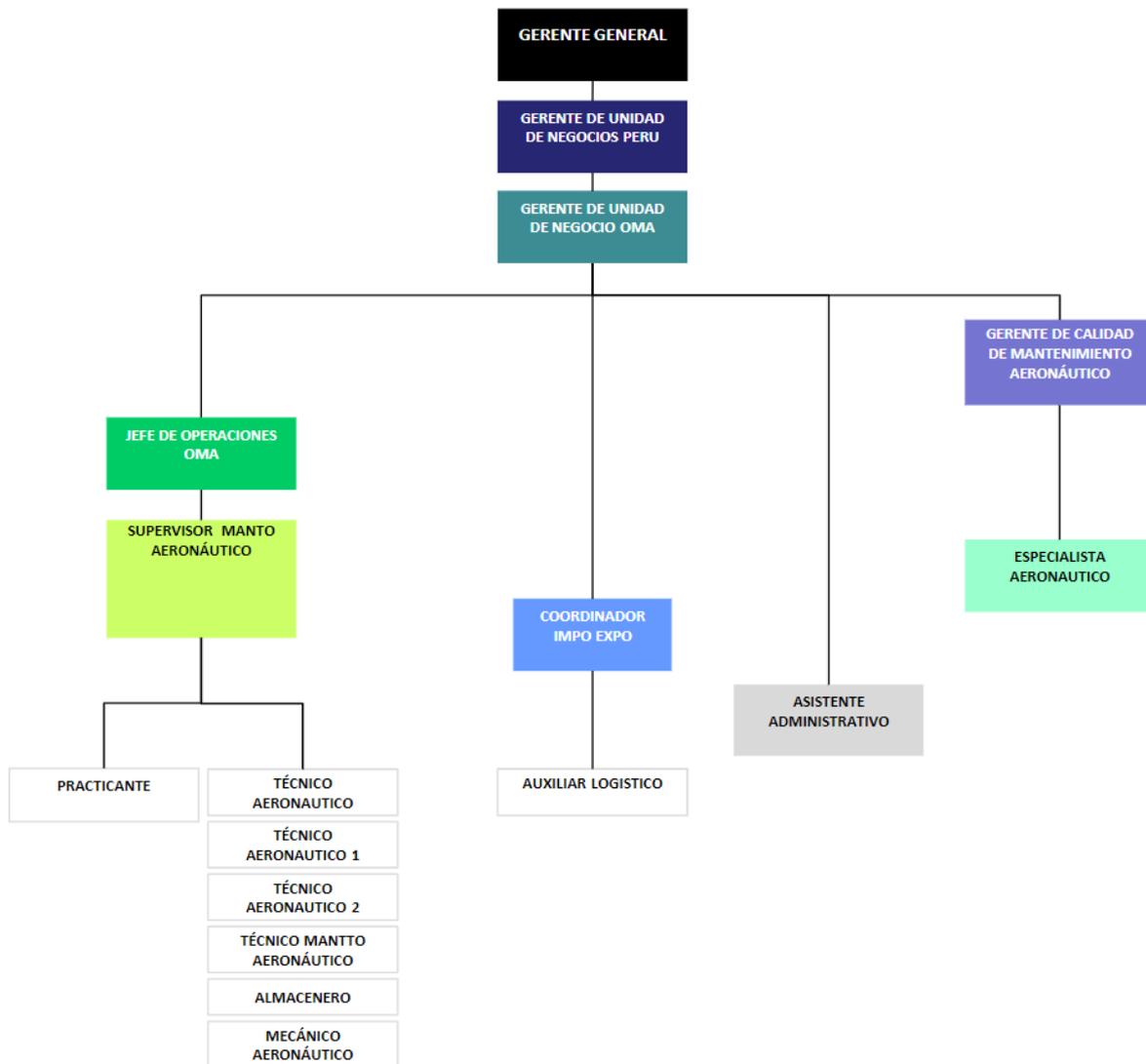
**Figura 8 Estructura ejecutiva**  
**Fuente: Empresa del Sector Aeroportuario**



**Figura 9 Equipo Auditoría Interna**  
**Fuente: Empresa del Sector Aeroportuario**



**Figura 10 Gerencia SIG**  
**Fuente: Empresa del Sector Aeroportuario**



**Figura 11 Gerencia de Mantenimiento Aeronáutico**  
**Fuente: Empresa del Sector Aeroportuario**

### 2.3. Referencias normativas:

La organización cuenta con estándares para garantizar una operación exitosa. Dentro de los pilares en los cuales se basa el sistema integrado de gestión, se cuenta con las siguientes normativas aplicada a su sector:

✓ ADUANA:

- D.L 1053: Ley General de Aduanas

Este Decreto Legislativo tiene por objeto regular la relación jurídica que se establece entre la Superintendencia Nacional de Administración Tributaria - SUNAT y las personas naturales y jurídicas que intervienen en el ingreso, permanencia, traslado y salida de las mercancías hacia y desde el territorio aduanero.

- D.S 010-2009-EF: Reglamento de la Ley General de Aduanas

Este Reglamento rige para todas las actividades aduaneras en el Perú y es aplicable a toda persona, mercancía y medio de transporte dentro del territorio aduanero.

- Ley N° 28008: Ley de delitos aduaneros  
Estipula todos los actos que son considerados como delitos aduaneros, especifica las infracciones vinculadas a dichos delitos.
- DS 031-2009-EF: tabla de sanciones de la ley general de ADUANAS Especifica las sanciones aplicables a las Infracciones previstas en la Ley General de Aduana
- Resolución de Superintendencia Nacional adjunta de Aduanas N°000332-2004-SUNAT-A: Procedimiento del control de mercancías peligrosas restringidas y prohibidas

✓ DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL

- Ley de aeronáutica civil (Ley 27261) y su reglamento (DS 050-2000): establece a la Autoridad Aeronáutica Civil Nacional, principios de circulación aérea, el ingreso, tránsito y salida de aeronaves del territorio peruano, infraestructura aeronáutica (aeródromos y aeropuertos), limitaciones de la propiedad privada aeronáutica, disposiciones de facilitación, disposiciones de aeronaves (nacionalidad, inscripción y matrícula), contrato de uso de aeronaves, lineamientos de aviación civil y aviación general, disposiciones de autorizaciones, derechos aerocomerciales, contratos de transporte aéreo, acuerdos de cooperación comercial, seguros, lineamientos de búsqueda, asistencia y salvamento, principios de investigación de accidentes de aviación e infracciones y sanciones.
- Ley de seguridad de la aviación civil (Ley 28404) y su reglamento (DS 0072006): esta norma legal define las responsabilidades específicas, en materia de seguridad, de cada ente involucrado en la aeronáutica civil y establece lineamientos sobre el transporte de mercancías peligrosas por vía aérea.
- Programa Nacional de Seguridad de la Aviación Civil (PNSAC) RM 6632015-MTC/01.02: este programa creado por la Ley 28404 establece responsabilidades con relación a todas las entidades públicas y privada que participan dentro de la industria aeronáutica en el Perú, con la finalidad de impedir que se cometan actos de interferencia ilícita en contra de la aviación.
- Programa de Seguridad Operacional del Estado Peruano (SSP): Es el conjunto integrado de reglamentación y actividades destinadas a mejorar la seguridad operacional. Comprende actividades específicas de seguridad operacional que debe realizar el Estado y reglamentos y directrices promulgados por el Estado para apoyar el cumplimiento de sus responsabilidades con respecto a la realización segura y eficiente de las actividades de aviación civil en el Estado. Se establece con el propósito de lograr un nivel aceptable de seguridad operacional (Acceptable Level of Safety – ALoS), por lo que corresponde a la

DGAC del Perú, como entidad competente dentro del Estado Peruano, liderar la estructuración e implantación de este sistema. El Programa tiene los siguientes componentes: Políticas y objetivos de seguridad operacional del Estado Peruano, Gestión de Riesgos de seguridad operacional por el Estado, Garantía de la seguridad operacional por el Estado y Promoción de la seguridad operacional por el Estado.

- RAP 109: esta norma aplica a los agentes acreditados autorizados por la DGAC con la finalidad de que implementen medidas de seguridad de la aviación y seguridad operacional como parte de la cadena de transporte aéreo de carga y correo.
- RAP 110: esta norma dispone los requerimientos aplicables al transporte de mercancías peligrosas efectuado en aeronaves peruanas y extranjeras, que operen en el espacio aéreo nacional, las mismas que rigen a todo explotador aéreo que opera bajo las Partes 121, 133 y 135, operador de aeródromo, agente acreditado, servicio especializado aeroportuario, fabricante de embalajes, así como a toda empresa o expedidor que intenta transportar mercancías peligrosas por vía aérea.
- RAP 111: dispone los requerimientos de seguridad para toda persona natural o jurídica que realice las funciones de un operador de servicios especializados aeroportuarios. Estos requerimientos abarcan servicios de atención, manejo o despacho de pasajeros, aeronaves, carga, correo, suministro de alimentos, bienes o combustible y demás facilidades requeridas en los aeropuertos por explotadores aéreos nacionales e internacionales que operen en el Perú.
- RAP 145: Esta norma dispone los requisitos para la emisión de aprobaciones a organizaciones de mantenimiento de aeronaves y componentes de aeronaves y establece las normas generales de operaciones para las Organizaciones de Mantenimiento Aprobadas (OMA) RAP 145. Cuando la aprobación es otorgada se aplica a toda la organización encabezada por un gerente responsable. Para la UN OMA aplicaban los requisitos de las autoridades aeronáuticas de aviación civil de los estados que emitieron un certificado de aprobación como OMA o su equivalente.

#### ✓ TRÁFICO ILÍCITO DE DROGAS

- Decreto Ley N° 22095: Ley de represión del tráfico ilícito de drogas
- Decreto Legislativo N° 122: Ley sobre tráfico ilícito de drogas
- Decreto Legislativo 824: Ley de lucha contra el narcotráfico
- Ley 27765: Ley penal contra el lavado de activos
- Ley 28355: Ley que modifica artículos de la Ley penal contra el lavado de activos
- DS 986: Ley que modifica la ley penal contra el lavado de activos
- Ley 28305: Ley de control de insumos químicos y productos fiscalizados y su reglamento DS 053-2005-PCM

- DS 021-98-ITINCI, DS 022-98-ITINCI: Normas sobre el insumo químico fiscalizado
  
- ✓ **MINISTERIO DE TRABAJO**  
Se detallará en la matriz de requisitos legales
  
- ✓ **BUENAS PRÁCTICAS DE ALMACENAMIENTO (BPA)**
  - Resolución ministerial R.M. N° 132-2015/MINSA: Manual de Buenas Prácticas de almacenamiento: Son un conjunto de normas que establecen requisitos y procedimientos operativos que deben cumplir los establecimientos para garantizar óptimas condiciones de almacenamiento para los productos farmacéuticos y dispositivos médicos.
  
- ✓ **SISTEMA ANTICORRUPCIÓN Y ANTISOBORNO**
  - Norma internacional ISO 37001:2016
  - NTP-ISO 37001:2017 Sistema de Gestión anti soborno
  - Ley 30424: Responsabilidad administrativa de las personas jurídica por el delito de cohecho coactivo transnacional
  - Decreto Ley 1352: Amplia la responsabilidad administrativa de las personas jurídicas
  - Ley N° 29660: Ley que establece medidas para sancionar la manipulación de precios en el mercado de valores
  - Hábeas Data Expediente N° 01805-2007-PHD/TC
  - Decreto Supremo N° 119 2012 PCM Aprueba Plan Nacional de Lucha contra la Corrupción 2012 2016
  - Ley N° 29976 - Ley que crea la Comisión de Alto Nivel Anticorrupción
  - DECRETO LEGISLATIVO N° 1327 - establece procedimientos y mecanismos para facilitar e incentivar las denuncias realizadas de buena fe de actos de corrupción y sancionar las denuncias realizadas de mala fe.
  - Convención Interamericana contra la corrupción
  - Convención de Naciones Unidas contra la corrupción
  - Plan andino de lucha contra la corrupción
  
- ✓ **SISTEMA DE CALIDAD, AMBIENTAL Y SEGURIDAD Y SALUD EN EL TRABAJO**
  - Norma Internacional ISO 9001:2015: Sistemas de Gestión de la Calidad - Requisitos.
  - Norma Internacional ISO 9000:2015: Sistemas de Gestión de la Calidad – Conceptos y Vocabulario
  - Norma Internacional ISO 14001:2015: Sistemas de Gestión Ambiental – Requisitos con orientación para su uso

- Norma Internacional ISO 14004:2015: Sistemas de Gestión Ambiental – Directrices Generales sobre Principios, Sistemas y Técnicas de apoyo.
  - Ley 28611: Ley General del ambiente
  - Ley 27314: Ley de Gestión Integral de Residuos sólidos
  - Norma Internacional ISO 45001:2018: Sistema de Gestión de Seguridad y Salud en el Trabajo.
  - MINTRA: Decreto Supremo N° 005-2012-TR
  - Reglamento de la Ley N° 29783, Ley de Seguridad y Salud en el Trabajo.
  - INDECI: Decreto Supremo N° 005-88-SGMD Reglamento de la Ley del Sistema Nacional de Defensa Civil, modificaciones y ampliaciones.
- ✓ SISTEMA DE SEGURIDAD OPERACIONAL
- Anexo 19 OACI: Sistemas de Gestión de la Seguridad Operacional.
  - Doc. OACI 9859: Manual de Gestión de la Seguridad Operacional.
  - DTE 001-2008: Requisitos para el Sistema de Gestión de la Seguridad Operacional.
  - RAP 145 NE Cap. C Sistema de Gestión de Seguridad Operacional, DGAC Perú.
  - CA.145-200-01: Implementación de la Fase 1 “Objetivos y Políticas de Seguridad Operacional” de un Sistema de Gestión de la Seguridad Operacional (SMS) en un Taller de mantenimiento Aeronáutico.
  - CA.145-200-02: Implementación de la Fase 2 “Gestión de Riesgos Reactivos de la Seguridad Operacional de las Organizaciones de Mantenimiento Aprobadas. (OMA).
  - CA. 121-110-04: Implementación de la Fase 3 “Gestión de Riesgos Proactivo/Predictivo de la Seguridad Operacional en un proveedor de Servicios Aeronáuticos.
  - C.A. 121-110-2015: Implantación de la Fase 4 “Implantación de la Garantía de la Seguridad Operacional” en un proveedor de servicios aeronáuticos.
  - ISAGO: IATA Safety Audit for Ground Operations. (Auditoria de Seguridad de Operaciones en Tierra de IATA.)
  - LAR 145 Capítulo C: Sistema de Gestión de Seguridad Operacional, SRVSOP.
  - DAN 154 Sistema de Gestión de Seguridad Operacional, DGAC Chile
  - RDAC 145 Cap. C, Sistema de Gestión de Seguridad Operacional
  - RAC 219, Normas Generales de Implantación del Sistema de Gestión de Seguridad Operacional, UAEAC Colombia
  - 14 CFR Sub Chapter A Part 5, FAA EE.UU.
- ✓ SISTEMA DE SEGURIDAD PARA LA CADENA DE SUMINISTRO
- Norma Internacional ISO 28000:2007: Sistema de Gestión de la Seguridad para la Cadena de Suministro.

- Norma Internacional ISO 28001:2007: Mejores prácticas para implementar evaluaciones y planes de seguridad.
  - Norma Internacional ISO 28003:2007: Requisitos para entidades de auditoría y certificación.
  - Norma Internacional ISO 28004:2006: Sistema de Gestión de la Seguridad para la Cadena de Suministro. Guías para la implementación de ISO 28000.
- ✓ **BASC:**
- BASC v.5-2017, Estándar 5.0.1 (Carga), Estándar 5.0.2 (Rampa).
- ✓ **NORMA DEL OPERADOR AEROPORTUARIO:**
- LAP, ADP, AAP, CORPAC: Normas establecidas por el operador aeroportuario, publicadas en sus manuales operativos.
- ✓ **NORMAS IATA:**
- GOSM: Ground Operation Standar Manual
  - IGOM
  - IRM
  - Manuales para operaciones específicas: DGR, PCR, LAR, ULDR, TCR, AHM, LBTR, ICHM, BRM
  - Entre otros aplicables
- ✓ **MANUALES DE OPERACIONES DEL CLIENTE**
- Se consideran todos los manuales operativos de las líneas aéreas con las que la organización mantiene relaciones contractuales.
- ✓ **REGULACIONES DE LA COMUNIDAD EUROPEA – RA3**
- Regulation (EU) No 2015/1998 (contained in Point 6.8 of the Annex thereto)
  - Commission Implementing Regulation (EU) No 2017/815

## ***2.4. Contexto de la organización***

### ***2.4.1. Comprensión de la organización y su contexto***

- Introducción – Presentación de la empresa: La organización es una empresa líder en el sector aerocomercial con más de 25 años de experiencia ofreciendo al mercado lo siguiente:
  - Servicio de Atención a la Aeronave en Rampa (Ground Handling),

- Servicio de Base especializado en Aviación Corporativa (Fixed Base Operator – FBO),
- Servicio de Manejo y Almacenaje de la carga nacional e internacional (Cargo Handling),
- Servicio de Agente de Asistencia en Tierra / Administración y Manejo de las Operaciones de carga (General Handling Agent – GHA),
- Servicio de Agente acreditado
- Servicio de Mantenimiento en línea y depósito de material de uso aeronáutico (DMA).
- Servicio de capacitación y entrenamiento especializado.

La organización cuenta con una red de servicios a escala nacional teniendo operaciones en 21 aeropuertos: Lima y 19 provincias más.

#### **2.4.2. Ubicación Geográfica**

La organización cuenta con oficinas administrativas e instalaciones en Lima (1 sede en el aeropuerto y 3 sedes de oficinas administrativas) y en distintas provincias del Perú (19 provincias con sedes dentro del aeropuerto)

Adicionalmente, se cuentan con sedes en la subsidiarias de México (3 instalaciones), Ecuador (7 instalaciones) y Colombia (20 instalaciones).

#### **2.4.3. Análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas)**

En el año 2015 se realizó el plan estratégico de la organización a través de talleres e interacción con las diversas áreas de la organización y el soporte de una consultoría especializada. Dicho planeamiento arrojó una serie de iniciativas, las mismas que se encuentran en desarrollo, asimismo durante el año 2016 se ha complementado con una evaluación de la organización con la finalidad de que acompañe al crecimiento de la misma.

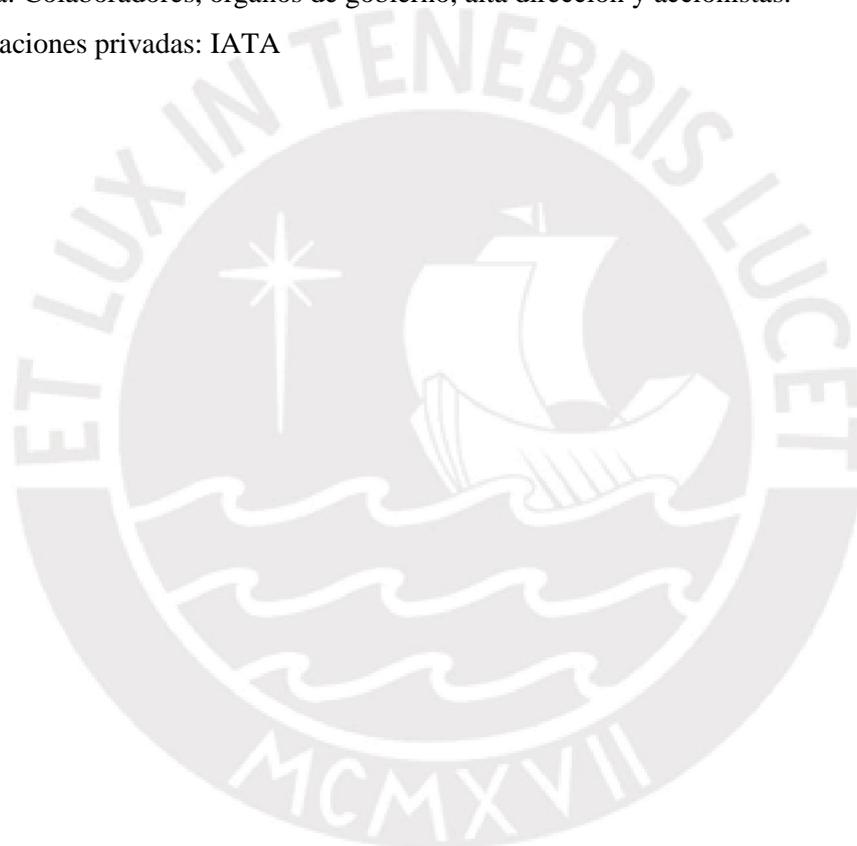
Para revisar el análisis del entorno, tanto externo como interno, se ha empleado la herramienta del FODA. Este es un análisis pertinente al propósito y dirección estratégica de la organización, de aquello que puede afectar la capacidad para lograr los resultados previstos en el Sistema Integrado de Gestión. Dentro de las principales fortalezas identificadas se encuentra el sólido know how y experiencia en el negocio, así como la relación cercana y de confianza con los clientes. Dentro de las principales debilidades se encuentra la falta de propuestas de valor para los diferentes segmentos de clientes. En el caso de las oportunidades, se encuentra la de tomar una posición regional y mejorar la imagen de la organización. Por último, como parte de las amenazas se encuentra el posible cambio de modelo de negocio ante el mercado disruptivo.

#### ***2.4.4. Análisis de requerimientos de las partes interesadas***

Como requisito del SGAS se identifican y grafican los flujos de los procesos para las operaciones de la organización las cuales servirán de base para la identificación de partes interesadas en el contexto interno y externo del SIG y la realización de la gestión de riesgos Anti-soborno de la organización.

Posterior a ello, se establecen las Partes Interesadas de la organización y sus requisitos de las mismas, quedando entre las principales partes interesadas externas, las siguientes instituciones:

- Autoridades: Congreso de la República, Ministerio de Salud, Ministerio de Transportes y Comunicaciones, DIGESA, Ministerio del Ambiente, Ministerio de Defensa, Ministerio de Economía y Finanzas, Ministerio de Energía y Minas, etc.
- Empresa: Colaboradores, órganos de gobierno, alta dirección y accionistas.
- Organizaciones privadas: IATA



### **3. ESQUEMA TEÓRICO METODOLÓGICO PARA IMPLEMENTAR LA GESTIÓN DE RIESGOS**

El siguiente esquema metodológico tendrá como base a las 2 normas explicadas en el Capítulo 1.5 “Normas Aplicadas a la Gestión del Riesgo: ISO 31000:2018 y COSO ERM 2017, ISO 31010:2019. En primer lugar, se comenzará el análisis con preguntas que busquen conocer y/o determinar la situación actual de una empresa en relación a su gestión de sus riesgos, de esta forma se logrará conocer su capacidad y madurez en relación al presente tema. Para la primera parte de la metodología a desarrollar, se plantea la elección de los principios considerados en la norma ISO 31000:2018, por lo que se desarrollarán preguntas que pretendan entender la brecha existente entre la situación actual y la deseada, cabe resaltar que la presente fase introductoria solo será aplicable para empresas en las cuales la gestión de riesgos ya se encuentre en marcha.

#### **3.1. Análisis para la implementación de los principios**

Como Paso 1, se realizarán preguntas generales establecidas en la Tabla 5, que deberán ser contestadas por el área actual administradora de riesgos, o en caso no se haya planteado previamente la necesidad de una, deberán ser contestadas por el gerente general:

**Tabla 5 Contexto general de la organización**

<b>Ítem</b>	<b>Preguntas</b>
1	¿Cómo define y opera, en la organización, el pensamiento basado en riesgo?
2	¿La organización cuenta con la solución de problemas y la toma de decisiones basadas en riesgo implementada en la compañía?
3	¿Qué valor o beneficio cree que se puede alcanzar o ya se ha alcanzado con el pensamiento basado en riesgo?
4	¿Planea la organización adoptar o implementar la gestión de riesgos?
5	¿Entiende la organización las principales diferencias entre ISO 31000 y COSO ERM?
6	¿Conoce la organización los requerimientos para armar, diseñar, implementar y asegurar la gestión de riesgos?
7	¿La organización se basará en COSO, ISO o en una combinación de ambos para la gestión de riesgos?
8	¿Cuál es la capacidad y madurez de la organización con respecto a riesgos?
9	¿Se tiene un análisis de brechas del estado actual con el deseado?
10	¿Tiene la organización una metodología para identificar diferentes tipos de incertidumbre?
11	¿El proceso de toma de decisiones evalúa entradas, procesos, y salidas deseadas?
12	¿Las decisiones tomadas son documentadas y validadas por expertos?

13	¿Cuál es el modelo de gobierno, riesgo y cumplimiento de la organización?
14	¿Cuál es el modelo de negocio?
15	¿A qué mercados obedece la organización?
16	¿Qué productos y/o servicios provee la organización?
17	¿Quiénes son los principales consumidores y cómo se clasifican?
18	¿Cómo define "valor" la organización?

Fuente: Hutchins (2018)

Como Paso 2, se deberá establecer y documentar la información del contexto interno y externo de la organización.

- ✓ Dentro del contexto externo se deberá incluir la siguiente información: requerimientos de stakeholders externos, clientes, y partes interesadas; preocupaciones históricas, geopolíticas, económicas y ambientales que puedan impactar a la organización; factores políticos, legales, financieros, económicos, competitivos, globales, etc.; geografía global, nacional y local; tendencias globales, históricas, culturales y sociales; valores, ética, gobierno y factores sociales internacionales y nacionales; estándares de riesgos y cumplimiento.
- ✓ Por otro lado, dentro del contexto interno de la organización, se deberá incluir lo siguiente: definir el gobierno, riesgo y cumplimiento de la organización; identificar stakeholders internos, clientes y partes interesadas; establecer estrategias de riesgos, requerimientos y planes para alcanzar los objetivos; definir los objetivos de la gestión del riesgo; desarrollar la política de riesgos, procedimientos, estándares, requerimientos y criterios; establecer la madurez organizacional con respecto a los riesgos.

Como Paso 3, se comenzará con las preguntas relacionadas a los principios establecidos por las normas, para este caso, similar al anterior, el cuestionario presentado en la Tabla 6, deberá ser aplicado al área gestora de los riesgos o al gerente de la organización:

- ✓ Se comienza con el primer principio: integración. Para este caso se opta por realizar preguntas específicas sobre la toma de decisiones y la solución de problemas basados en riesgos, también, se han considerado preguntas generales de la compañía y sobre los índices de medición usados en la actualidad.

**Tabla 6 Principio integrador**

Ítem	Preguntas
1	¿La organización tiene definidos los procesos de toma de decisiones y solución de problemas?
2	¿Las oportunidades y riesgos son evaluados usando un proceso consistente? ¿Cuál?
3	¿La organización cuenta con herramientas para la toma de decisiones y solución de problemas?

4	¿Se encuentra el riesgo incorporado en la toma de decisiones y solución de problemas de procesos, proyectos y servicios?
5	¿El apetito de riesgo y la tolerancia se encuentran claramente definidos?
6	¿Se considera el contexto de la organización en el diseño, implementación y aseguramiento de las decisiones críticas?
7	¿La junta directiva realiza seguimiento a la gestión de riesgos?
8	¿El reporte a la junta directiva incluye KPI's y KRI's?
9	¿Se encuentra la gestión de riesgos integrada al planeamiento estratégico?
10	¿Los procesos centrales han sido definidos y mapeados?
11	¿La gestión de riesgos es integral a los procesos centrales?

Fuente: Hutchins (2018)

- ✓ El segundo principio es: Gestión de riesgos estructura y exhaustiva, para el cual se verificará su cumplimiento mediante las preguntas establecidas en la Tabla 7.

**Tabla 7 Principio estructurado y exhaustivo**

Ítem	Preguntas
1	¿Serán las normas aplicadas sistemáticamente en todos los niveles de la organización?
2	¿Las tomas de decisiones son hechas en el tiempo adecuado?
3	¿Cuándo hay cambios en el sistema de gestión de riesgo, son estos aprobados por las partes interesadas?
4	¿El criterio de toma de decisiones ha sido definido en todos los niveles de la organización?
5	¿Son las decisiones estructuradas parte de un largo proceso de ciclo de decisión?
6	¿Se evalúa la efectividad de la toma de decisiones en relación a los riesgos?

Fuente: Hutchins (2018)

- ✓ El tercer principio es: Gestión de riesgos adaptada, para el cual se verificará su cumplimiento mediante las preguntas establecidas en la Tabla 8.

**Tabla 8 Principio de adaptabilidad**

Ítem	Preguntas
1	¿El contexto de la organización es entendido y definido?
2	¿La arquitectura y el diseño del marco de referencia se encuentran alineados con el contexto?
3	¿Los límites del marco de referencia de la gestión de riesgos se encuentran definidos?
4	¿Los elementos culturales y conductuales de la organización completamente definidos y entendidos?

Fuente: Hutchins (2018)

- ✓ El cuarto principio es: Gestión de riesgos inclusiva, para la cual se analizará su estado actual mediante las preguntas presentadas en la Tabla 9.

**Tabla 9 Principio de gestión de riesgos inclusiva**

Ítem	Preguntas
1	¿Las autoridades y responsabilidades se encuentran definidas en cada nivel de la organización?
2	¿Son los colaboradores entrenados en la gestión y control de riesgos en su área dónde son responsables?
3	¿Son los protocolos y procesos de la gestión del riesgo entendidos por todos los colaboradores?
4	¿Son los stakeholders, clientes y partes interesadas considerados en la toma de decisiones?

Fuente: Hutchins (2018)

- ✓ El quinto principio es: Gestión de riesgos dinámica, para cual se analizará el estado actual mediante las preguntas presentadas en la Tabla 10.

**Tabla 10 Principio de gestión de riesgos dinámica**

Ítem	Preguntas
1	¿El contexto interno y externo de la organización son constantemente monitoreados?
2	¿El proceso de gestión de riesgos es lo suficientemente adaptable a estos cambios?
3	¿Existen suficientes mecanismos de revisión que aseguren confiabilidad y correcta toma de decisiones, con relación al alcance de objetivos?
4	¿Los controles son evaluados en efectividad y eficiencia?
5	¿Los mecanismos son revisados y monitoreados para realizar seguimiento a los KPI's y KRI's?
6	¿Los controles son adecuados para lograr el cumplimiento de los objetivos según el apetito de riesgo de la organización?

Fuente: Hutchins (2018)

- ✓ El sexto principio a evaluar es contar con la mejor información disponible, para analizar la situación actual de una organización, se realizarán las preguntas establecidas en la Tabla 11.

**Tabla 11 Principio de Mejor información disponible**

Ítem	Preguntas
1	¿El proceso de toma de decisiones considera los tipos de información que deben ser reunidos?
2	¿Se identifica la mejor información disponible a ser aplicada en la gestión de riesgos? ¿Cómo?
3	¿Se evalúa la calidad, exactitud y confianza de la información?
4	¿Son los elementos de los contextos discutidos e identificados en la toma de decisiones?
5	¿Las suposiciones hechas en la toma de decisiones son validadas por expertos?
6	¿Son las decisiones revisadas periódicamente para asegurar su validez y actualización?

Fuente: Hutchins (2018)

- ✓ El séptimo principio son los factores humanos y culturales, los cuales serán analizados mediante las preguntas establecidas en la Tabla 12.

**Tabla 12 Principio: Factores humanos y culturales**

Ítem	Preguntas
1	¿Se ha desarrollado el caso de negocio y plan de implementación?
2	¿El patrocinador ejecutivo se encuentra directamente involucrado en la arquitectura, el diseño e implementación, y la garantía del plan de gestión de riesgos?
3	¿Son los indicadores apropiados para la organización?

Fuente: Greg Hutchins (2018)

- ✓ El último principio es el de mejora continua, para ello se analizará la situación actual de la organización mediante las preguntas establecidas en la Tabla 13.

**Tabla 13 Principio de mejora continua**

Ítem	Preguntas
1	¿Son los KPI's y KRI's mejorados continuamente?
2	¿Se tienen responsabilidades y autoridades específicas para la mejora continua?
3	¿Las compensaciones son relacionadas con los objetivos de la mejora continua?
4	¿Es la mejora continua una oportunidad en la gestión de riesgos?
5	¿Es la mejora continua monitoreada constantemente?

Fuente: Hutchins (2018)

Como Paso 4, se procederá con el cierre de brechas entre los hallazgos encontrados en el cuestionario anterior. Es importante recalcar, que la empresa deberá analizar el nivel de madurez de riesgo al que desea llegar, ya que según su planteamiento será necesario el cierre parcial o total de observaciones encontradas.

### ***3.2. Análisis para la Implementación del Marco de Referencia***

En el presente sub capítulo se describirá el liderazgo y compromiso de la organización, el diseño del marco de referencia, su implementación, evaluación y mejora.

#### ***3.2.1. Liderazgo y compromiso en la organización***

Posterior a ello, se comenzará con el análisis del marco de referencia actual en la organización. En primer lugar, se realizarán preguntas relacionadas al liderazgo y compromiso de la empresa con el marco de referencia, estas se encuentran planteadas en la Tabla 14.

**Tabla 14 Liderazgo y compromiso**

<b>Ítem</b>	<b>Preguntas</b>
1	¿Se encuentra el marco de referencia de la ISO 31000 o COSO adoptado y aceptado por la junta directiva y la alta gerencia?
2	¿La junta directiva provee vigilancia en la correcta implementación del sistema de gestión de riesgos?
3	¿Los objetivos estratégicos son incorporados en la gestión de riesgos?
4	¿Los KRI's y KPI's se encuentran alineados con los objetivos estratégicos?
5	¿Los KRI's de la organización son alcanzables?
6	¿Los indicadores son monitoreados y asegurados continuamente?
7	¿El sistema de gestión de riesgos contempla los principios mencionados en la sección anterior?
8	¿El sistema de gestión de riesgos es entendido por los colaboradores internos y las partes interesadas externas de la organización?

Fuente: Hutchins (2018)

En segundo lugar, la organización tendrá que plantear algunos elementos críticos para el diseño y elaboración del marco de referencia, estos se encuentran establecidos en la Tabla 15.

**Tabla 15 Elementos críticos del marco de referencia**

<b>Ítem</b>	<b>Elementos críticos para el diseño del marco de referencia</b>
1	Entender y definir el contexto organizacional.
2	Determinación del propósito y beneficio del marco de referencia.
3	Establecer el alcance del marco de referencia.
4	Establecer los objetivos el marco de referencia y sus requerimientos.
5	Asegurar que el marco de referencia sea flexible.
6	Armar el marco de referencia basado en el criterio del riesgo.
7	Diseño del marco de referencia usando las fases del ciclo de riesgos ya mencionada.
8	Asegurar que todos los elementos del proceso sean usados en el diseño y la implementación

Fuente: Greg Hutchins (2018)

En tercer lugar, se especificará la delegación correcta de responsabilidades y autoridades:

- ✓ Identificar los dueños de procesos.
- ✓ Asegurar que los dueños de riesgos sean responsables y cumplan con los requisitos de autoridad necesarios para manejarlos en su dominio.
- ✓ Identificar las partes interesadas que puedan impactar o ser impactadas por el marco de referencia, procesos, objetivos y requerimientos.
- ✓ Identificar los requerimientos, necesidades y objetivos de los stakeholders y partes interesadas en todos los niveles de la organización.

- ✓ Desarrollar KRI's y KPI's que se encuentren alineados con las estrategias organizacionales.
- ✓ Monitorear la varianza de los objetivos y asegurar que sean correctos y tratados según el apetito de riesgo de la organización.
- ✓ Asegurar que los KRI's y KPI's sean reportados periódicamente y si hay varianzas inaceptables, se deberá corregir la situación.

Asimismo, se deberá definir claramente los roles, responsabilidades de las partes interesadas. Según Hutchins (2018, pp. 124-126), se tienen los siguientes roles:

- ✓ Director Ejecutivo (CEO): Es responsable de la gestión de riesgos incluyendo las directivas para los controles de riesgos adicionales. Autoriza la política de gestión de riesgos y aprueba el apetito del mismo en la organización. Además, autoriza y posee el plan estratégico, políticas, y la estructura de control interno de la gestión de riesgos en la organización.
- ✓ Director de riesgos (CRO): Es el principal consejero del CEO, de los jefes de las unidades de negocio y de los jefes de funciones críticas en materias de riesgo. Este director es además responsable de la arquitectura, diseño, implementación y aseguramiento del programa de gestión de riesgos. El director junto con el comité de gestión de riesgos supervisa la identificación, evaluación, priorización, tratamiento, monitoreo, comunicación y aseguramiento de la empresa, proyectos y procesos, y los riesgos del servicio o producto.
- ✓ Dueños de riesgos: Unidades de negocio, funciones críticas y jefes planificadores de la organización sirven como propietarios finales del riesgo. Aunque puedan delegar dichas responsabilidades, la última responsabilidad recae en ellos. Estos participan activamente en los esfuerzos y desarrollo de controles de riesgo apropiados.
- ✓ Comité de riesgos: Este se encuentra compuesto por los jefes de las unidades de negocio, jefes de gestión de la cadena de suministro, ingeniería, finanzas, administración, TI y recursos humanos. El rol del comité es desarrollar e implementar los planes de riesgo, principios y procesos usados para priorizar riesgos en la organización. El comité también identifica. Asesora y trata los principales riesgos, además se asegura que la propuesta y valorización de los riesgos vaya acorde al apetito y nivel de gestión de los mismos.
- ✓ Equipo de gestión de riesgos de proyectos/procesos: Soporta al director de riesgos. Puede desarrollar y mantener las políticas, planes de riesgo, diseñar procesos controlados, desarrollar procedimientos y diseñar herramientas para proyectos y procesos críticos. También, podrán reunir data y desarrollar reportes de riesgo y asegurar que los controles son apropiados para la tolerancia de los mismos.

Otro punto a considerar previo al diseño del marco de referencia, tiene relación con el compromiso con la gestión de riesgos. Por ello, debemos asegurarnos que el marco de referencia y la gestión de

riesgos sean adoptados por la junta directiva. También, es necesario que se supervise directamente la implementación y el éxito del sistema. Por otro lado, con relación a los objetivos estratégicos de la organización, debemos asegurarnos que los objetivos se encuentren incorporados en la gestión, que se puedan medir mediante indicadores y que estos sean alcanzables. Teniendo todo ello, la organización debe asegurar que el sistema de gestión de riesgos sea entendido en la organización y por las partes interesadas.

### ***3.2.2. Diseño del marco de referencia***

Para el diseño del marco de referencia, se comenzará con el establecimiento de una política, según los lineamientos de la norma ISO 31000:2018. De esta forma se estarán identificando los riesgos globales de la organización. Esta política deberá encontrarse disponible para los empleados, contratistas y visitantes (Sidorenko, 2019 p. 62), y se presenta de esta forma un modelo de política propuesto por dicho autor.

Objetivo principal de la gestión de riesgos:

Reducción de los efectos negativos de la empresa.

Principios Principales de Gestión de Riesgos

1. El proceso de gestión de riesgos es una parte integral del sistema de gestión de la EMPRESA;
2. La gestión de riesgos es una función obligatoria para todos los empleados de la COMPAÑÍA; 3. El desarrollo de medidas de reducción de riesgos internos o externos debe ser documentado;
4. El propósito de la gestión de riesgos es identificar y prevenir posibles pérdidas y, en segundo lugar, minimizar las consecuencias de ese riesgo;
5. La gestión de riesgos en la empresa significa la aplicación de un enfoque unificado y estandarizado para la identificación, evaluación y gestión de riesgos.
6. Los administradores de todos los niveles son responsables de la identificación y evaluación oportuna de los riesgos, el desarrollo de las medidas de gestión de riesgos y la comunicación de estos riesgos.
7. El sistema de motivación de los empleados en la COMPAÑÍA tiene en cuenta la efectividad de la gestión de riesgos;
8. LA COMPAÑÍA se adhiere a un equilibrio razonable entre la gestión del riesgo y el monto potencial incurrido por la ocurrencia del riesgo. LA COMPAÑÍA no puede tomar ninguna medida adicional para reducir el riesgo si el nivel de riesgo está dentro de los límites del riesgo; 9. LA COMPAÑÍA asegura que el conocimiento de los riesgos, incluyendo el análisis de los riesgos;
10. La coordinación del sistema de gestión de riesgos de la empresa es realizado por el EMPLEADO;
11. La responsabilidad de la formulación, función y eficacia de la gestión de riesgos recae en el Director General de la EMPRESA

También, durante el diseño del marco de referencia se tiene que tomar en cuenta el planeamiento de los siguientes factores:

- ✓ Integración de la gestión de riesgos en los procesos organizacionales: Ya que todas las organizaciones solucionan problemas y toman decisiones, la gestión de riesgos necesita ser integrada en los planes, principios, procesos, procedimiento, etc. de la organización.
- ✓ Recursos para la gestión del riesgo: Las organizaciones necesitan adecuar sus recursos para diseñar, implementar, y monitorear la gestión del riesgo.
- ✓ Comunicaciones de riesgos: La normativa enfatiza tener procesos de comunicación para asegurar que la gestión de riesgos es adecuada, precisa y confiable. Para lo cual se deberá tomar en cuenta dos tipos de comunicaciones:
  - Comunicaciones internas y reporte: el propósito de las mismas es el de comunicar de forma adecuada y confiable información para asegurar el control de los riesgos según el apetito en la organización.
  - Comunicaciones externas y reporte: Dentro de ello, uno de los puntos importantes es el monitoreo continuo y medible de la satisfacción de las partes interesadas con la información presentada.

### ***3.2.3. Implementación del marco de referencia***

Para implementar el marco de referencia en la organización, se propone seguir la siguiente secuencia de acciones planteada por Hutchins (2018)

- ✓ Asegurar que la junta directiva y ejecutivos se encuentren comprometidos con la gestión de riesgos (solución de problemas, tomas de decisiones confiables y operaciones eficientes).
- ✓ Entender cómo manejar la incertidumbre para cumplir con los objetivos del negocio.
- ✓ Integrar el buen gobierno en la gestión de riesgos (estrategias, políticas y planes).
- ✓ Desarrollar una estrategia para implementar el marco de referencia en la organización.
- ✓ Implementar la gestión de riesgos en los procesos con beneficios reconocibles.
- ✓ Identificar y documentar los requisitos del riesgo con los jefes, clientes y partes interesadas.
- ✓ Asegurar que el RBPS y el RBDM sea alineado con las estrategias de la organización.
- ✓ Asegurar la capacitación de los sponsors claves, clientes y partes interesadas en la gestión de riesgos.
- ✓ Diseñar y adaptar el proceso de gestión de riesgos según el contexto organizacional, tamaño de la organización y requerimientos.
- ✓ Consultar siempre con partes interesadas, clientes y otros si el marco de referencia de la gestión de riesgos continúa cumpliendo sus requerimientos.

- ✓ Realizar un análisis de brechas para asegurar el entendimiento de los riesgos organizacionales y el desarrollo de un tratamiento adecuado de los mismos.
- ✓ Desarrollar el proceso de gestión de riesgos e implementar cambios para alinear las prácticas que no siguen el mismo.
- ✓ Integrar reportes operacionales de riesgos significativos en los reportes financieros.

Para las organizaciones grandes, es preferible un plan de implementación detallado que incluya hitos, entregables, recursos, ruta crítica y alcance. Otro punto importante, es que la implementación del marco de referencia siga un modelo de madurez de capacidad de riesgo (RCMM).

Si bien es cierto, la norma ISO no te da pasos específicos para la implementación de la gestión de riesgos, se puede considerar los siguientes puntos claves:

1. Identificar actividades específicas, hitos para implementar la ISO según el contexto de la organización.
2. Desarrollar una estructura de desglose de trabajo identificando secuencias de actividades para la implementación. También, las fechas de inicio y de fin, responsabilidades, y guías para la implementación.
3. Identificar las técnicas y las tareas a ser completadas por la organización.
4. Identificar autoridades, responsabilidades y para la implementación.
5. Desarrollar reportes y mecanismos para la resolución de conflictos.
6. Identificar riesgos en el plan y las opciones de solución para las mismas.

### 3.2.4. Evaluación del marco de referencia

Luego, se proseguirá estableciendo cómo se dará la evaluación del marco de referencia, la cual como se mencionó en la sección anterior, se tienen distintos conceptos los cuales serán presentados en la Figura 13.

Evaluación de gestión de riesgos			
Vigilancia: Consiste en la observación para asegurar que los sistemas, proyectos y procesos continuen con control y capaces de cumplir con los requerimientos objetivos.	Monitoreo: similar a vigilancia, los KPI's y KRI's son verificados para medir los objetivos en términos de costos, calidad, alcance y presupuesto.	Revisión: evaluación periódica de cambios en el ambiente, situación y contexto, de esta forma se pueden realizar acciones correctivas.	Auditoría: Comprende una evaluación de sistemas, políticas y procedimientos para determinar la satisfacción de estándares.

**Figura 12 Conceptos para la evaluación de gestión de riesgos**

Fuente: Greg Hutchins (2018)

A la junta directiva se deberá presentar reportes de cumplimiento de estándares, cumplimiento de estatutos puestos por el gobierno, que los controles se encuentren operando según lo requerido, que los objetivos de gestión y de negocio estén siendo alcanzados, que los riesgos residuales estén siendo identificados, etc.

### **3.2.5. Mejora del marco de referencia**

El marco de referencia de la organización debe ser adaptable y se debe poder mejorar continuamente, este debido al cambio del contexto o de las circunstancias. Para ello se deberá realizar una revisión periódica, también, debe ser evaluado cuando se presente algún iniciador tal como cambios en el ambiente competitivo, cambio en el modelo de negocio, requerimientos del cliente o cambio en el contexto, nuevos riesgos a nivel empresarial, descubrimiento de nuevos productos o servicios, o algún otro cambio sustancial en la organización.

## **3.3. Análisis para la implementación del proceso**

Se presentará, para cada uno de los componentes del proceso, sus objetivos, iniciadores, entradas, actividades y salidas.

### **3.3.1. Comunicación y Consulta**

- ✓ **Objetivos:** Mejorar el entendimiento de los riesgos, identificar stakeholders y clientes, identificar requerimientos, necesidades y expectativas de los stakeholders, identificar a los dueños del proceso y sus requerimientos, identificar a los dueños del tratamiento y control y sus requerimientos, consultar con los stakeholders, asegurar que el proceso de comunicación y consulta esté considerado en cada uno de los procesos de gestión de riesgos.
- ✓ **Iniciadores:** Revisión de riesgos programada, revisión periódica de los requerimientos de los stakeholders y clientes, revisión periódica o cambio en la estructura organizacional, misión o dirección en la gestión de riesgos, cambio en el modelo de gobierno, riesgo y conformidad, cambio en el modelo del negocio, en el core de la empresa, valor añadido diferenciador, posición competitiva, fusión, adquisición, etc. También, un evento disruptor, nuevos requerimientos de la junta directiva, cambio en requerimientos, leyes, regulaciones y gobierno, y ocurrencia o recurrencia de no cumplimiento con requerimientos.
- ✓ **Entradas:** Evaluación de riesgos en toda la cartera de la empresa o en niveles específicos de la misma (nivel empresa, procesos o proyectos o IT y nivel producción), cambios o mejoras en las normativas, procesos de gestión de riesgos, o necesidad de entrenamiento en riesgos, nueva lista de riesgos residuales, desarrollo de una lista de estrategias y planes para el tratamiento del riesgo, actualización de lista de dueños de proceso, stakeholders o clientes,

plan de gestión de riesgos, nuevas reglas y responsabilidades, nuevas capacidades, mapa de procesos de la empresa, actualización del registro de riesgos.

- ✓ Actividades: Se plantean las actividades y los entes responsables de cada una de ellas en la Tabla 16.

**Tabla 16 Actividades - Comunicación y consulta**

Actividades	Responsables
Desarrollo de un caso de negocio de riesgos	CRO
Desarrollo de un plan de proyecto para la implementación de riesgos	CRO
Identificación de stakeholders y clientes	Calidad
Compartir el caso de negocio de riesgo, plan de proyecto de riesgo, estructura de composición del trabajo de riesgo con los dueños de proceso, stakeholders, y clientes para comunicar el calendario de despliegue de riesgos, costos, recursos, alcance, calidad e hitos.	CRO
Evaluar la comunicación de stakeholders y necesidades de entrenamiento	Comité ERM
Determinar si las expectativas de stakeholders, clientes y partes interesadas han cambiado.	Calidad
Determinar la comunicación interna y externa con stakeholder y su necesidad de información.	Calidad
Determinar los recursos para cumplir con la estrategia y misión de los objetivos críticos	Comité de Gerencia
Mejora en las capacidades de gestión de riesgos de la organización.	Comité ERM
Monitorear las mejores prácticas de gestión de riesgos, publicaciones, benchmarks, conferencias, etc.	CRO y comité ERM
Consulta con profesionales de los riesgos dentro o fuera de la organización acerca de estrategias, planes y tácticas.	Equipos de evaluación de riesgos
Evaluación de la efectividad del marco de referencia, herramientas y técnicas.	Auditoría Interna y CRO
Recomendar a los dueños de proceso nuevas prácticas y procedimientos.	Comité ERM
Mejora en la madurez del riesgo y en la capacidad de requerimientos.	Equipo de proyectos y procesos
Resolver problemas relacionales al performance del proceso de gestión de riesgos	CRO y comité ERM
Ayudar en el desarrollo y entrenamiento de la gestión de riesgos	CRO y comité ERM
Realizar entrenamiento para los grupos de stakeholders	CRO y comité ERM
Desarrollo del marco de referencia y el proceso de documentación de gestión de riesgos.	CRO y comité ERM
Manejar el marco de referencia, proceso, desglose de recursos, y mantener el calendario de las actividades de gestión de riesgos.	Comité ERM
Incorporar cambios en los hitos de proyectos de riesgos.	CRO
Actualizar los planes y calendarios de gestión de riesgos a plazos definidos.	Comité ERM

- ✓ Salidas: Plan de comunicación de riesgos, consultas con dueños de procesos y stakeholders respecto al requerimiento de riesgos, cambios o mejoras en el marco de referencia, gestión de procesos, sistemas y planes de riesgos, análisis de requerimiento de los stakeholders y clientes, y entrenamiento culminado de stakeholders específicos.

### 3.3.2. *Establecimiento del contexto*

- ✓ Objetivos: Revisión de los objetivos estratégicos, planes de riesgo, contexto, objetivos de la gestión del riesgo y el criterio para determinar qué riesgos serán gestionados.
- ✓ Iniciadores: término del proceso de comunicación y consulta, cambio significativo en el contexto interno o externo, ocurrencia de un evento de alta consecuencia, revisión de los niveles de riesgo que puedan haber incrementado o disminuido, cambios crónicos, sistémicos, estructurales, materiales u otros cambios importantes que pueden afectar la organización, nuevos estatutos o eventos externos que cambien el perfil de riesgos de la organización, ocurrencia o recurrencia de eventos de riesgos mayores que cambien la probabilidad y consecuencia de los riesgos y generen que estos se encuentren fuera del apetito de riesgo o tolerancia establecida por la organización.
- ✓ Entradas: Visión, misión, metas estratégicas del negocio, cambios adicionales en el contexto, cambios en los criterios de riesgo o perfil, cambio en la política, cambio en el apetito, tolerancia, nuevos roles, responsabilidades y mapa de procesos en la organización. También, las políticas, procedimientos, instructivos existentes para la gestión del riesgo, nuevos KRI y/o KPI, nuevos alcances en las evaluaciones de riesgo, oportunidades de riesgo emergentes, cambios en los stakeholders, clientes y partes interesadas.
- ✓ Actividades: Se plantean las actividades y los entes responsables de cada una de ellas en la Tabla 17.

**Tabla 17 Actividades - establecimiento del contexto**

Evaluar el contexto interno y/o externo	Responsable
Revisión de la documentación existente, incluyendo la taxonomía del riesgo	CRO y comité ERM
Desarrollar un lenguaje y taxonomía común para los riesgos.	CRO y comité ERM
Determinar la capacidad y madurez del riesgo en la organización.	CRO y comité ERM
Evaluar las políticas y procedimientos para que estos reflejen la madurez y capacidad de la organización.	CEO y CRO
Determinar si los cambios en el ambiente externo e interno pueden resultar en riesgos adicionales.	CRO
Realizar un análisis para identificar los riesgos nuevos, la volatilidad, incertidumbre, complejidad y ambigüedad de la industria.	Comité ERM y equipo de proyectos y procesos
Discutir las amenazas nuevas o actuales y el impacto con los ejecutivos y dueños de proceso.	CRO y comité ERM
Evaluar cambios que puedan impactar en la compañía, incluyendo nuevas amenazas, tecnologías, peligros y cambios organizacionales.	CRO y comité ERM

Ajustar los criterios de evaluación de riesgos, políticas, y objetivos críticos.	CRO y comité ERM
Identificar eventos de riesgo que puedan impactar a la organización.	CRO, comité ERM y equipo de procesos y proyectos
Asegurar que las definiciones de riesgo y potenciales impactos sean reflejados correctamente en el apetito de riesgo y tolerancia de la organización.	CRO y comité ERM
Obtener guía sobre la efectividad de la gestión de riesgos por parte de stakeholders, clientes y partes interesadas.	CRO y comité ERM
Revisar y aprobar criterios de riesgo, políticas y asegurar que son apropiados para la organización.	CEO
Determinar cambios en el contexto interno y externo que pueda resultar en amenazas, peligros, tecnología, procesos, personal, cambio de leyes y regulaciones que puedan causar la reevaluación de los riesgos existentes.	CRO y comité ERM
Identificar nuevos riesgos	CRO, comité ERM y dueños de proceso
Asegurar que el comité de gestión de riesgos revise y apruebe el alcance de la evaluación de riesgos.	Calidad
Revisar los planes, políticas, procedimientos, organigrama y criterios de riesgos organizacionales.	CRO y comité ERM
Proveer comentarios y feedback en cambios de organigramas, KPIs y KRIs.	Calidad
Comunicar el desarrollo de los cambios y confirmar que las revisiones son aceptadas por los dueños de riesgos.	Equipo de proyectos y procesos
Determinar el alcance de la identificación del riesgo y evaluar actividades para la revisión anual y el registro.	CRO
Identificar actividades nuevas que requieran evaluación de riesgos.	CRO, comité ERM
Obtener entradas de los dueños de riesgo, stakeholders, y partes interesadas, definiendo el alcance de la evaluación de riesgos.	CRO, comité ERM
Determinar protocolos para la evaluación de riesgo de oportunidades.	CRO, comité ERM
Revisar el registro de competencias, exactitud y suposiciones.	CRO, comité ERM
Actualizar el registro de riesgos si es necesario. Así como también, planes, procesos y procedimientos.	CRO, comité ERM
Comunicar los cambios en los planes, proceso y procedimiento a las partes impactadas.	CRO, comité ERM

- ✓ Salidas: Nuevos KPIs y umbrales de tolerancia, actualizar la definición del contexto organizacional, actualizar el criterio de riesgo organizacional, actualizar la lista de dueños de riesgo y stakeholders, actualización del registro de riesgos de la organización, mapeo de actividades operacionales y procesos de riesgo, plan de riesgo, procesos y procedimientos actualizados.

### 3.3.3. Identificación de riesgos

- ✓ **Objetivos:** Desarrollar una lista de eventos de riesgo que puedan impactar potencialmente las metas estratégicas y los objetivos de la organización. También, seleccionar el método apropiado para la identificación de riesgos.
- ✓ **Iniciadores:** término del proceso de establecimiento del contexto, evaluación de riesgos debido a un cambio de perfil en los riesgos de la empresa, cambio en el apetito de riesgo, requerimiento de los dueños de proceso o stakeholders, falta de control de riesgos o efectividad de tratamiento.
- ✓ **Entradas:** Análisis del contexto actualizado, informes de auditoría previa y hallazgos negativos, cambios en los requerimientos de stakeholders, clientes o ingreso nuevo de los mismos. También, política, planes, etc. actualizados, declaración de apetito de riesgo actualizada, cambio en la tolerancia, nuevas reglas y responsabilidades o autoridades, escenario de análisis en el cual se identifica potenciales sucesos inesperados de gran magnitud u otras consecuencias de los eventos de riesgos. Otras entradas importantes serían, la re-determinación de escalas de probabilidad y consecuencia de herramientas y técnicas de evaluación de riesgos y nuevos procesos, proyectos o productos.
- ✓ **Actividades:** Se plantean las actividades y los entes responsables de cada una de ellas en la Tabla 18.

**Tabla 18 Actividades - Identificación de riesgos**

Actividades	Responsable
Identificar e investigar riesgos emergentes	CRO, comité ERM
Conducir un análisis de riesgos emergentes.	CRO, comité ERM
Identificar sucesos inesperados de gran magnitud.	CRO, comité ERM
Revisar riesgos mayores asociados a KPIs y KRIs existentes.	CRO, comité ERM
Identificar nuevas métricas de performance asociadas con el logro de objetivos críticos.	CRO, comité ERM
Identificar puntos de referencia en organizaciones para entender los puntos comunes y diferencias en los enfoques de riesgos.	CRO, comité ERM
Revisar el registro de riesgos para riesgos nuevos, modificados y/u obsoletos.	CRO, comité ERM
Revisar la taxonomía del riesgo para identificar riesgos críticos para un análisis.	CRO, comité ERM
Trabajar con los dueños de riesgo para apoyar la identificación de sus riesgos y los esfuerzos para la revisión de riesgos.	Comité ERM
Realizar talleres multifuncionales de RM y ERM para identificar aún más riesgos nuevos, cambios u obsoletos en términos de consecuencia y probabilidad.	CRO, comité ERM
Identificar factores de riesgo y consecuencias.	CRO, comité ERM, equipo de proyectos y procesos
Determinar una lista de riesgos preliminar basada en consecuencias y probabilidades.	CRO, comité ERM
Trabajar con patrocinadores ejecutivos en identificar dueños de riesgos para los nuevos riesgos.	CRO, comité ERM
Confirmar con los dueños de riesgo la existencia de nuevos riesgos, cambios o incrementos.	CRO, comité ERM, equipo de proyectos y procesos

Ayudar con la identificación para el personal que identifica y cuantifica los factores de riesgo y sus consecuencias. Si los riesgos son altos o tienden a serlo, elevarlos al registro empresarial.	Equipo de proyectos y procesos
Formar un panel de expertos para evaluar los nuevos factores de riesgos, consecuencias y probabilidades.	Equipo de evaluación de riesgos
Especificar objetivos estratégicos para posibles ajustes.	CRO
Comunicar nuevos KRIs o KPIs a los dueños de riesgo y stakeholders impactados.	CRO, comité ERM
Desarrollar nuevos negocios y objetivos incluyendo unidades de negocio y objetivos funcionales.	CRO, comité ERM
Desarrollar nuevos documentos de planes y procesos basados en cambios de contexto u objetivos.	CRO, comité ERM
Rexaminar y rehacer los objetivos empresariales, incluyendo los KRIs y KPIs	CRO, comité ERM
Asegurar que la tolerancia del riesgo sea expresada en términos de límites altos y bajos o umbrales de incumplimiento.	CRO, comité ERM
Actualizar la información en el registro de riesgos empresariales.	CRO, comité ERM
Verificar y validar los registros de riesgos empresariales, KRIs y KPIs, umbrales y objetivos.	CRO, comité ERM
Aceptar o dejar como obsoletos riesgos y documentar el motivo.	CRO, comité ERM

- ✓ Salidas: Nuevos KPIs y KRIs con umbrales de tolerancia, objetivos de riesgo y de negocio actualizados, dueños de riesgo actualizados, registro de riesgos empresariales actualizado.

### 3.3.4. Análisis de riesgos

- ✓ Objetivos: Identificar la probabilidad y consecuencia de riesgos usando métodos cualitativos/cuantitativos o una combinación de ambos. También, seleccionar el método de análisis adecuado.
- ✓ Iniciadores: Término del proceso de identificación de riesgos, ocurrencia o recurrencia de un riesgo, una varianza en la evaluación de riesgos entre diferentes stakeholders, conclusiones diferentes de probabilidad y consecuencia de un riesgo, diferente interpretación de la efectividad de un control, contexto cambiante que pueda impactar la evaluación de un riesgo o un cambio en el cronograma de análisis de riesgos.
- ✓ Entradas: Análisis cuantitativo o determinístico, habilidades de evaluación cualitativa, reportes de contexto interno y externo, clientes o stakeholders, registros nuevos o actualizados de riesgo, fuentes de información externas e internas.
- ✓ Actividades: Se plantean las actividades y los entes responsables de cada una de ellas en la Tabla 19.

**Tabla 19 Actividades - análisis de riesgos**

Actividades	Responsables
Facilitar la evaluación de riesgos cualitativa o cuantitativa.	CRO, comité ERM
Asignar clasificaciones a los riesgos.	CRO, comité ERM y

	equipo de proyectos y procesos
Determinar causas y correlaciones entre riesgos.	Equipo de evaluación de riesgos
Determinar personal calificado para estimar probabilidad y consecuencia	CRO, comité ERM
Solicitar apoyo a los dueños de riesgo para realizar el análisis de los mismos.	CRO
Determinar la información apropiada y la relación entre informes.	CRO, comité ERM
Agregar y priorizar riesgos 1. Empresariales, 2. Proyectos y procesos, 3. Producción/Transacción	CRO, comité ERM
Asignar calificaciones de consecuencia y probabilidades a cada riesgo y registrarlo.	CRO, comité ERM, equipo de proyectos y procesos
Evaluar riesgos que cuenten con una alta consecuencia o alta prioridad.	CRO, comité ERM
Priorizar riesgos para un análisis crítico adicional	CRO, comité ERM
Acumular el riesgo desde el nivel transaccional / de producto hasta el nivel empresarial para fines de visualización	CRO, comité ERM
Analizar riesgos basados en evaluaciones cualitativas, tales como consecuencias de calor y escalas de probabilidad.	CRO, comité ERM
Desarrollo de árboles de eventos y otros tipos de evaluación de riesgos.	CRO, comité ERM
Asegurar que los stakeholders y clientes estén familiarizados con la evaluación de riesgos y la herramienta de análisis.	CRO, comité ERM
Solicitar input a los stakeholders acerca de selecciones para herramientas de evaluación de riesgos.	CRO, comité ERM
Reunir a expertos en riesgos para analizar los riesgos en cascada, interdependientes, dependientes y otros	CRO, comité ERM
Identificar posibles materiales, cascada, espacios en blanco, dependencia, interdependencia, crónicos, sistémicos y otros tipos de riesgo.	CRO, comité ERM, equipo de evaluación de riesgos
Desarrollar cadenas de eventos casuales o de correlación que podrían generar un impacto o generar riesgos adicionales.	CRO, comité ERM
Reconocer eventos de riesgo que pueden conducir a factores de riesgo secundarios o en cascada que finalmente conducen a eventos de riesgo.	CRO, comité ERM
Identificar cadenas de impactos de riesgo y sus consecuencias resultantes de una ocurrencia de riesgo que puede vincularse a impactos secundarios.	CRO, comité ERM
Facilitar entrenamiento y desarrollo de riesgos.	CRO, comité ERM
Proveer entrenamiento en cómo desarrollar un registro de riesgos.	CRO, comité ERM
Alertar a los dueños de riesgo en prevenir problemas de riesgo potenciales.	Comité ERM, equipo de proyectos y procesos
Apoyar a los dueños de riesgos en identificar KRIs y KPIs.	Comité ERM, equipo de proyectos y procesos
Cuantificar riesgos seleccionados.	CRO, comité ERM, equipo de evaluación de riesgos
Estimar la frecuencia de riesgo dl evento basado en cambios o en factores de riesgo.	CRO, comité ERM, equipo de evaluación de riesgos

Determinar la probabilidad de que los factores secundarios de riesgo se conviertan en primarios.	CRO, comité ERM, equipo de evaluación de riesgos
Determinar si los factores de riesgo de tercer nivel necesitan ser analizados.	CRO, comité ERM, equipo de evaluación de riesgos
Desarrollar un portafolio de riesgos empresariales basado en medidas de riesgo calculadas.	CRO, comité ERM, equipo de evaluación de riesgos
Comunicar el nivel de los riesgos empresariales.	CRO, comité ERM
Monetizar los riesgos en términos de valor de riesgo, porcentaje de presupuesto en riesgo o de forma similar.	CRO, comité ERM, equipo de evaluación de riesgos

- ✓ Salidas: medidas a nivel empresarial que resultan en un riesgo de cartera, análisis de árbol de eventos, análisis de riesgo secundario y terciario, nuevos KPIs y KRIs, relaciones causales y correlación identificada entre riesgos, análisis cuantitativo y cualitativo adicional según lo requerido, mapas de riesgo y registros actualizados.

### 3.3.5. Evaluación de riesgos

- ✓ Objetivos: Desarrollar una lista priorizada de riesgos en los tres niveles de la empresa, evaluar los riesgos para la aceptación de los mismos y evaluar los riesgos para posibles tratamientos.
- ✓ Iniciadores: Término del proceso de análisis de riesgo, cambio en el contexto, cambio en los criterios de riesgo, cambio en el ambiente de control, nuevos KPIs, KRIs u objetivos, revisión de eventos emergentes o nuevos riesgos.
- ✓ Entradas: Revisión del análisis del tratamiento de riesgo pasado, revisión de la efectividad de los controles actuales, resultados de análisis de riesgo efectuados, cálculos de riesgos para los riesgos empresariales, KRIs, KPIs, análisis cualitativo y cualitativo, el apetito de riesgo y los umbrales de tolerancia, input de clientes y stakeholders, mapas de riesgo y registro de riesgos.
- ✓ Actividades: Se plantean las actividades y los entes responsables de cada una de ellas en la Tabla 20.

**Tabla 20 Actividades - evaluación de riesgos**

Actividades	Responsables
Comparar niveles de riesgo y criterios.	CRO, comité ERM, equipo de evaluación de riesgos
Comparar los niveles de riesgos calculados con el apetito de riesgo y los umbrales de tolerancia.	CRO, comité ERM, equipo de evaluación de riesgos
Proveer de input en la priorización de riesgos.	CRO, comité ERM, equipo de evaluación de riesgos
Revisar los impactos de riesgos, misión, objetivos críticos, tolerancia de riesgo y el criterio para los umbrales.	CRO, comité ERM, equipo de evaluación de riesgos
Revisar los rankings de riesgos.	CRO, comité ERM, equipo de evaluación de riesgos
Priorizar riesgos en función al apetito de riesgo calculado y los niveles de	CRO, comité ERM, equipo

tolerancia del riesgo.	de evaluación de riesgos
Revisar la evaluación cualitativa de riesgos.	CRO, comité ERM, equipo de evaluación de riesgos
Revisar técnicas cuantitativas de evaluación de riesgos, incluyendo árboles de riesgos y correlación de los mismos.	CRO, comité ERM, equipo de evaluación de riesgos
Revisar riesgos sistémicos, crónicos, materiales, de dependencia e interdependencia	CRO, comité ERM, equipo de evaluación de riesgos
Priorizar tratamientos de riesgo.	CRO, comité ERM, equipo de evaluación de riesgos
Revisar riesgos casuales y de correlación entre eventos, amenazas, riesgos, Etc.	CRO, comité ERM, equipo de evaluación de riesgos
Desarrollar un ranking de riesgos críticos a ser tratados.	CRO, comité ERM, equipo de evaluación de riesgos
Proveer un enfoque preliminar para el tratamiento de riesgos.	CRO, comité ERM, equipo de evaluación de riesgos
Presentar riesgos al comité de riesgos y a los dueños de procesos.	CRO, comité ERM, equipo de evaluación de riesgos
Actualizar riesgos y el ranking en el registro.	CRO, comité ERM, equipo de evaluación de riesgos
Revisar y obtener la aprobación de la priorización de riesgos por parte del director de riesgos y la gerencia ejecutiva.	CRO, comité ERM, equipo de evaluación de riesgos
Revisar y desarrollar una lista final de riesgos a ser considerados para el tratamiento.	CRO, comité ERM, equipo de evaluación de riesgos
Guiar a los comités de riesgo y a los dueños de proceso en controles adicionales para los riesgos.	CRO, comité ERM, equipo de evaluación de riesgos

- ✓ Salidas: Lista priorizada de riesgos que requieren tratamiento, aporte de los stakeholder para los nuevos riesgos, riesgos y su registro actualizados.

### **3.3.6. Tratamiento del riesgo**

- ✓ Objetivos: Determinar la estructura apropiada de controles internos según el contexto y objetivos, determinar las opciones apropiadas para el tratamiento de riesgos, optimizar los recursos de la organización, manejar un portafolio basado en el umbral de apetito de riesgos.
- ✓ Iniciadores: Término de la etapa de evaluación de riesgos. Cambios en el profile de riesgos, evaluación anual o según sea requerida, falta de estabilidad en los controles, capacidad o mejoras, evento de cisne negro, riesgos significativos, crónicos, sistémicos o materiales.
- ✓ Entradas: Identificar leyes y regulaciones relevantes al impacto de riesgos, revisar las estrategias y tácticas de tratamiento de riesgos pasada y actual, evaluar el plan de continuidad y de gestión de crisis, evaluar plan de entrenamiento y comunicación previa, priorizar riesgos altos que requieren tratamiento, conducir un análisis de stakeholders y clientes.
- ✓ Actividades: Se plantean las actividades y los entes responsables de cada una de ellas en la Tabla 21.

**Tabla 21 Actividades - tratamiento del riesgo**

Actividades	Responsables
Revisar KPIs, KRIs y objetivos para su idoneidad.	CRO, comité ERM
Diseñar y verificar el entorno general de control interno.	CRO, comité ERM
Desarrollar la estrategia para el tratamiento de riesgo, planes y tácticas de ejecución.	CRO, comité ERM
Desarrollar un plan detallado de proyecto con hitos para tratamiento y control.	CRO, comité ERM
Identificar opciones para el tratamiento de riesgos.	CRO, comité ERM
Desarrollar un plan de tratamiento de riesgos.	CRO, comité ERM
Desarrollar un plan detallado de proyecto con estructura de desglose de trabajo identificando actividades incluyendo las opciones de tratamiento,	CRO, comité ERM
Recursos, hitos, cronograma, presupuesto, revisión y estatus.	
Asegurar presupuesto para el plan de tratamiento de los riesgos.	CRO, comité ERM
Trabajar con dueños de riesgos con respecto a la implementación del tratamiento de riesgos y el reporte de progreso de stakeholders críticos.	CRO, comité ERM
Monitorear la implementación del plan de tratamiento de riesgos.	CRO, comité ERM
Actualizar la información con respecto a factores de riesgo y consecuencias de los mismos, incluyendo frecuencias anuales, probabilidades, consecuencia y estrategias para tratamientos existentes y controles en el registro de riesgos.	CRO, comité ERM
Monitorear el estatus del plan de tratamiento de riesgos contra los hitos.	CRO, comité ERM
Alertar a los dueños de riesgos y stakeholders si las fechas límites no serán cumplidas.	CRO, comité ERM
Determinar e implementar qué hitos de acciones correctivas no han sido cumplidos.	CRO, comité ERM
Reasignar el trabajo para el tratamiento de riesgos si es necesario.	CRO, comité ERM
Identificar recursos adicionales que apoyen con el tratamiento de riesgos y su control.	CRO, comité ERM
Comunicar con las personas apropiadas para el reasignamiento de tareas.	CRO, comité ERM
Realizar seguimiento a los plazos de tratamiento de riesgo perdidos.	CRO, comité ERM
Tomar acciones correctivas para resolver problemas, quitar barreras de tratamiento y plazos perdidos.	CRO, comité ERM
Desarrollar expectativas realistas para asegurar que los plazos son cumplidos y los niveles de riesgo residual serán alcanzados.	CRO, comité ERM
Revisar opciones de control.	CRO, comité ERM
Evaluar el tratamiento general y la efectividad de los controles.	CRO, comité ERM
Revisar las estrategias de tratamiento de riesgos existentes y controles.	CRO, comité ERM
Identificar factores de riesgo que puedan ser mitigados, eliminados, reducidos ya sea la probabilidad y/o consecuencia de los mismos.	CRO, comité ERM
Identificar las consecuencias que puedan ser aceptadas o evitadas	CRO, comité ERM
Revisar los puntos de referencia para los riesgos enumerados en la lista priorizada de riesgos que requieren tratamiento.	CRO, comité ERM
Evaluar el tratamiento de los riesgos y las opciones para el control.	CRO, comité ERM
Revisar los planes de seguros, analizar los límites y su efectividad	CRO, comité ERM
Identificar los proyectos que puedan impactar la probabilidad y consecuencia de los riesgos.	CRO, comité ERM
Revisar la efectividad de los controles de riesgo de los proyectos y IT.	CRO, comité ERM
Revisar el tratamiento de riesgos en los procesos, servicios, medio ambiente, seguridad informática, cadena de suministro, etc. y la efectividad de los controles de riesgos.	CRO, comité ERM
Documentar factores de riesgo y posibles tratamientos adicionales para los riesgos de TI, proyectos y procesos.	CRO, comité ERM

Coordinar las opciones de tratamiento de riesgos con el equipo de gestión y el CRO.	CRO, comité ERM
Proveer a los dueños de riesgo con información acerca de opciones de tratamiento existentes.	CRO, comité ERM
Determinar el costo de implementar las opciones de tratamiento de riesgos identificadas.	CRO, comité ERM
Evaluar cuantitativamente y cualitativamente las consecuencias que podría desarrollarse en la reducción o eliminación de los riesgos para cada opción planteada.	CRO, comité ERM
Apoyar el equipo de gestión en la identificación del costo efectivo de las opciones de tratamiento.	CRO, comité ERM
Trabajar en conjunto con el equipo de proyectos y programas para optimizar esfuerzos y eliminar duplicación.	CRO, comité ERM
Comparar el riesgo residual contra el apetito de riesgo o la tolerancia.	CRO, comité ERM
Determinar la combinación de tratamiento de costo más efectivo que reduzca el riesgo bajo el apetito de la organización.	CRO, comité ERM
Revisar que las opciones de tratamiento cumplan con las leyes, regulaciones y estatus establecido por la organización.	CRO, comité ERM
Determinar el nivel apropiado y el tipo de tratamiento de riesgo, que pueda incluir evitar el riesgo, aceptarlo, reducirlo o transferirlo.	CRO, comité ERM
Revisar las opciones de tratamiento de riesgo con los dueños de proceso y stakeholders.	CRO, comité ERM
Discutir y preparar los planes para estas opciones con los dueños de proceso.	CRO, comité ERM
Realizar un análisis de costo beneficio a las opciones de tratamiento de riesgos.	CRO, comité ERM
Proveer comentarios y feedback al equipo de gestión y CRO en la efectividad de los controles y tratamiento. Asimismo, en la eficiencia y economía.	CRO, comité ERM
Obtener la aprobación de las opciones de tratamientos de riesgos.	CRO, comité ERM
Determinar el plan para la implementación del tratamiento de riesgo, incluyendo a las personas autorizadas y responsables de la implementación del mismo.	CRO, comité ERM
Calcular el riesgo residual final y compararlo con el apetito de riesgo y los niveles de tolerancia, para de esta forma determinar si necesita algún tratamiento adicional.	CRO, comité ERM
Determinar si es que hubo reducciones en la probabilidad o consecuencia de un riesgo.	CRO, comité ERM
Comparar los beneficios y costos luego del tratamiento contra los beneficios actuales.	CRO, comité ERM

- ✓ Salidas: Alcance, cronograma, costo y actualización de la calidad de los proyectos para los riesgos, actualización del registro de riesgo con la calificación de los riesgos residuales, evaluación del control interno, actualización de las estrategias, tácticas y planes para los tratamientos, análisis de costo beneficio de los tratamientos, lista de riesgos residuales, revisión y aceptación de riesgos residuales.

### **3.3.7. Monitoreo y revisión**

- ✓ Objetivos: Monitorear el progreso de las estrategias de gestión de riesgo, mejorar la gestión de riesgos en la organización y la capacidad de tratamiento, mejorar el performance del

programa y actividades de la gestión de riesgos, monitorear las mejoras en los KPI y KRI, evaluar las estrategias y tácticas de gestión de riesgos, anticipar eventos de riesgos antes que estos ocurran.

- ✓ **Iniciadores:** Cambios en el gobierno de riesgo y los niveles de aseguramiento, cambios materiales en los perfiles de riesgos estratégicos, operacionales y financieros, cambios significativos en riesgos de procesos, proyectos y TI, ocurrencia o recurrencia de eventos críticos de riesgo o desencadenantes de nuevos riesgos, cronogramas predeterminados para la evaluación o tratamiento de riesgos, o requisitos de los informes de riesgo.
- ✓ **Entradas:** KPI's, KRI's, umbrales de apetito de riesgo y de tolerancia, estrategias, tácticas y planes para el tratamiento de riesgos, nivel de aseguramiento de riesgo, análisis costo-beneficio de gestión de riesgos y estrategias de tratamiento, nuevas reglas, política actualizada, umbrales de riesgo nuevos, nuevas responsabilidades, nuevos proveedores, nueva lista de gestión de riesgos, registro actualizado de riesgos con controles adicionales y con riesgos residuales calificados.
- ✓ **Actividades:** Se plantean las actividades y los entes responsables de cada una de ellas en la Tabla 22.

**Tabla 22 Actividades - monitoreo y revisión**

Actividades	Responsables
Determinar el aseguramiento de riesgos para la organización.	CRO, comité ERM
Evaluar el ambiente interno de control.	CRO, comité ERM
Desarrollar planes de monitoreo de riesgos para cada KPI y KRI.	CRO, comité ERM
Desarrollar planes de monitoreo de tratamiento y control para riesgos críticos.	CRO, comité ERM
Identificar al personal responsable de monitorear y revisar los KPI's, KRI's, aseguramiento del riesgo y tratamiento del riesgo.	CRO, comité ERM
Identificar al personal independiente responsable de monitorear, reportar los umbrales de riesgos, cambios en el contexto, aseguramiento del riesgo, frecuencia de monitoreo, etc.	CRO, comité ERM
Revisar los umbrales de límites en los KPI's y KRI's	CRO, comité ERM
Diseñar el monitoreo de riesgos y la notificación de desviaciones, variaciones, infracciones y otros eventos importantes a las partes interesadas, clientes y partes interesadas.	CRO, comité ERM
Identificar problemas de riesgo recurrentes y soluciones basadas en responsabilidad, rango de control, delegación de autoridades y responsabilidades de monitoreo.	CRO, comité ERM
Desarrollar ejemplos de dashboards de monitoreo y reportes a stakeholders, clientes, y partes interesadas específicas.	CRO, comité ERM
Controlar el aumento de KPI's y KRI's y responder a los cambios y riesgos.	CRO, comité ERM
Asegurar que los umbrales de riesgo sean realistas o si necesitan ser modificados.	CRO, comité ERM
Revisar tendencias o cambios en los umbrales de riesgo.	CRO, comité ERM
Recomendar tratamiento si los eventos de riesgo o incumplimiento puedan ocurrir.	CRO, comité ERM
Comunicar incumplimientos, tendencias o requerimientos inusuales que requieran acciones correctivas.	CRO, comité ERM
Comunicar tratamiento para cambios en los perfiles de riesgo, contextos,	CRO, comité ERM

apetito de riesgo, tolerancia, consecuencia y probabilidad.	
Monitorear si los riesgos pueden desencadenar en cascada, espacios en blanco, dependencia o interdependencia.	CRO, comité ERM
Apoyar a los dueños de riesgos a identificar los umbrales de KPI's y KRI's.	CRO, comité ERM
Grabar y analizar los eventos de riesgo, falta de cumplimiento de objetivos, casi fallas, amenazas, peligros, y sorpresas.	CRO, comité ERM
Proveer una descripción del evento o riesgo e identificar a la persona responsable de su seguimiento, análisis e identificación del síntoma, causa raíz, acción correctiva, controles y tratamiento.	CRO, comité ERM
Recomendar una evaluación de riesgos nueva o más amplia.	CRO, comité ERM
Documentar y analizar los eventos de riesgo.	CRO, comité ERM
Determinar acciones correctivas a ser tomadas.	CRO, comité ERM
Revisar los eventos de riesgo, amenazas, peligros para acciones correctivas eficaces y eficientes.	CRO, comité ERM
Revisar acciones correctivas y proveer el input y la guía necesaria.	CRO, comité ERM
Elevar a los dueños de riesgo para tratamiento adicionales en el caso de los riesgos crónicos, sistémicos o materiales.	CRO, comité ERM
Preparar diariamente, semanalmente, mensualmente, cuatrimestralmente y anualmente reportes de riesgo.	CRO, comité ERM
Preparar reportes basados en eventos de riesgo inesperados y peligros.	CRO, comité ERM
Notar si los cambios impactarán a stakeholders, clientes y partes interesadas.	CRO, comité ERM
Revisar y reforzar las acciones correctivas a través de toda la organización y todas las funciones.	CRO, comité ERM

- ✓ Salidas: Análisis de la efectividad, eficacia y economía del programa, análisis de estrategias de tratamiento, tácticas y efectividad del plan, análisis, documentación y escalamiento de los riesgos mayores cuando corresponda. También, se tendrán cambios en el proceso de gestión de riesgo, identificación de mejoras en el monitoreo y revisión, también en la comunicación y entrenamiento. Comunicación de los cambios mayores en el contexto, los stakeholders estarán informados de los cambios de objetivos estratégicos y perfiles de riesgo, desviaciones en los KRI y eventos de riesgos, resultados del KPI para el alcance de objetivos e informes de riesgo programados o especiales.

### **3.3.8. Grabación e informes**

- ✓ Objetivos: informe sobre el control y efectividad del tratamiento de riesgos, comunicar información para RBPS y RBDM, informar sobre los resultados del proceso de gestión de riesgos, informar a los interesados sobre el proceso de gestión de riesgos específicos y los requisitos del marco de referencia.
- ✓ Iniciadores: término del proceso de tratamiento de riesgos, o del proceso de comunicación y consulta o del proceso de monitoreo y revisión. También, requerimientos de nuevos stakeholders y la falta de control en la estabilidad, capacidad o mejora.
- ✓ Entradas: Identificación de nuevos requerimientos de stakeholders, revisión de las diferentes necesidades de informes de las partes interesadas específicas, revisión de los registros de acciones correctivas y/o acciones preventivas, revisión del registro de riesgos.

- ✓ Actividades: Se plantean las actividades y los entes responsables de cada una de ellas en la Tabla 23.

**Tabla 23 Actividades - Grabación e informes**

Actividades	Responsables
Revisar los resultados críticos para informar a los niveles de la empresa.	CRO, comité ERM
Registrar los resultados de las actividades críticas incluyendo el alcance de los objetivos.	CRO, comité ERM
Informar los resultados de RBPS y RBDM.	CRO, comité ERM
Desarrollar nuevos métodos de registro para los stakeholders y partes interesadas nuevas.	CRO, comité ERM
Revisar e informar sobre KPI's, KRI's y objetivos.	CRO, comité ERM
Revisar el costo, la frecuencia y la puntualidad de la presentación de informes a interesados específicos.	CRO, comité ERM
Revisar la idoneidad de los métodos de reporte	CRO, comité ERM
Determinar nuevos métodos de reporte.	CRO, comité ERM
Compartir información sobre las mejoras en la gestión de riesgos.	CRO, comité ERM
Informar a la junta de directores el logro de objetivos y riesgos claves.	CRO, comité ERM
Determinar los requisitos reglamentarios y de cumplimiento para informar datos.	CRO, comité ERM
Enviar reportes reglamentarios y de cumplimiento a tiempo.	CRO, comité ERM
Apoyar a la gerencia ejecutiva en los informes	CRO, comité ERM
Revisar una posible cascada, interdependencia, dependencia, y material de riesgo.	CRO, comité ERM
Revisar el costo / beneficio de la extensión y el tipo de informe	CRO, comité ERM
Determinar si se requiere de alguna garantía especial para informar.	CRO, comité ERM
Revisar que los reportes sean adecuados basándose en los objetivos organizacionales, solución de problemas y toma de decisiones.	CRO, comité ERM

- ✓ Salidas: Reportes para la junta directiva, reportes a los stakeholders legales y de cumplimiento, reporte del logro de objetivos, reporte de cisnes negros y reporte de costo beneficio.

### **3.4. Aplicación de las actividades pendientes**

Posterior al análisis realizado en el sistema de la organización, se procederá a ponderar las actividades pendientes para seleccionar las prioridades en base al impacto que estas generan en la organización. El análisis del impacto a generar, será evaluado de forma cualitativa considerando factores escogidos en base a la experiencia de los dueños de proceso y del personal especializado en gestión de riesgos.

## **4. ANÁLISIS DE BRECHAS DE LA ORGANIZACIÓN CONTRA LA NORMATIVA**

En el presente capítulo, se realizará el análisis de brechas entre la organización y la ISO 31000:2018, para ello se procederá a analizar cada punto presentado en el capítulo tres.

### **4.1. Análisis para la implementación de los principios**

Como Paso 1, el área administradora de riesgos contesta las preguntas generales establecidas en la Tabla 24:

**Tabla 24 Contexto general de la organización**

<b>Ítem</b>	<b>Preguntas</b>	<b>Respuestas</b>
1	¿Cómo define y opera, en la organización, el pensamiento basado en riesgo?	Ante la implementación de un nuevo proceso o un nuevo lineamiento se realiza una Gestión del Cambio analizando los riesgos de mayor impacto.
2	¿La organización cuenta con la solución de problemas y la toma de decisiones basadas en riesgo implementada en la compañía?	Sí, cuando se realiza alguna observación o no conformidad, se analizan los riesgos de los mismos.
3	¿Qué valor o beneficio cree que se puede alcanzar o ya se ha alcanzado con el pensamiento basado en riesgo?	Tomar decisiones con una base clara de los riesgos que acarrearán las mismas.
4	¿Planea la organización adoptar o implementar la gestión de riesgos?	Ya se cuenta con una gestión de riesgos actual; sin embargo, se plantea la mejora continua.
5	¿Entiende la organización las principales diferencias entre ISO 31000 y COSO ERM?	Sí, en el presente caso se ha optado por el marco metodológico de la ISO 31000.
6	¿Conoce la organización los requerimientos para armar, diseñar, implementar y asegurar la gestión de riesgos?	Sí lo conoce.
7	¿La organización se basará en COSO, ISO o en una combinación de ambos para la gestión de riesgos?	Se basará en la ISO 31000, por ser un marco muy reconocido a nivel mundial.
8	¿Cuál es la capacidad y madurez de la organización con respecto a riesgos?	Actualmente, la madurez es media.
9	¿Se tiene un análisis de brechas del estado actual con el deseado?	No se cuenta.

10	¿Tiene la organización una metodología para identificar diferentes tipos de incertidumbre?	Sí, realiza un análisis de riesgos por proceso, de forma que se identifican los riesgos asociados a los mismos.
11	¿El proceso de toma de decisiones evalúa entradas, procesos, y salidas deseadas?	Sí, la Gestión del Cambio incluye las entradas, nuevos/cambios en procesos y el objetivo/salidas del proceso.
12	¿Las decisiones tomadas son documentadas y validadas por expertos?	Sí, las decisiones se analizan entre las partes interesadas internas de la organización. Cuando incluye decisiones que impliquen mayor monto presupuestal, se revisa con la gerencia general.
13	¿Cuál es el modelo de gobierno, riesgo y cumplimiento de la organización?	EL modelo tiene un enfoque estratégico, basado en la colaboración de stakeholders internos y externos.
14	¿Cuál es el modelo de negocio?	Servicios.
15	¿A qué mercados obedece la organización?	Los mercados se encuentran mencionados en el capítulo 2.1.2 Concepción de cliente y de producto o servicio.
16	¿Qué productos y/o servicios provee la organización?	Los productos y servicios se encuentran mencionados en el capítulo 2.1.2 Concepción de cliente y de producto o servicio.
17	¿Quiénes son los principales consumidores y cómo se clasifican?	Los clientes y consumidores se encuentran mencionados en el capítulo 2.1.2 Concepción de cliente y de producto o servicio.
18	¿Cómo define "valor" la organización?	El valor en la organización está definido por la calidad de los servicios brindados a los clientes.

Como Paso 2, se relaciona al contexto de la organización, el mismo que se encuentra detallado en el Capítulo 2.4.1. Comprensión de la organización y su contexto.

Como Paso 3, se procede a analizar la relación de la organización con los principios planteados en la normativa. En la Tabla 25, se procederá a analizar el principio integrador:

**Tabla 25 Principio integrador**

Ítem	Preguntas	Respuestas
1	¿La organización tiene definidos los procesos de toma de decisiones y solución de	Sí, se plantea un análisis de 5 por qué's llegando a la causa raíz y actualizando la

	problemas?	matriz de riesgos.
2	¿Las oportunidades y riesgos son evaluados usando un proceso consistente? ¿Cuál?	Sí, actualmente el proceso consiste en una revisión anual de las oportunidades y riesgos. Adicionalmente, cuando algún riesgo se materializa, se revisa la evaluación del mismo.
3	¿La organización cuenta con herramientas para la toma de decisiones y solución de problemas?	Se cuenta con un formato en Excel para el análisis de los cambios realizados (Gestión de Cambios)
4	¿Se encuentra el riesgo incorporado en la toma de decisiones y solución de problemas de procesos, proyectos y servicios?	Sí se encuentra incorporado.
5	¿El apetito de riesgo y la tolerancia se encuentran claramente definidos?	Se encuentra definida la tolerancia; sin embargo, el apetito de riesgo no se encuentra claramente definido.
6	¿Se considera el contexto de la organización en el diseño, implementación y aseguramiento de las decisiones críticas?	Sí, siempre se evalúa los nuevos proceso o unidades de negocio a implementar en base al contexto y los riesgos que acarrea.
7	¿La junta directiva realiza seguimiento a la gestión de riesgos?	Sí; sin embargo, la frecuencia es anual, se realiza en el comité de Riesgos.
8	¿El reporte a la junta directiva incluye KPI's y KRI's?	Actualmente, se cuenta con KPI's básicos. Los riesgos críticos no cuentan con indicadores específicos.
9	¿Se encuentra la gestión de riesgos integrada al planeamiento estratégico?	Sí, como parte del planeamiento estratégico se cuenta con el modelo de negocio, las principales partes interesadas y sus riesgos.
10	¿Los procesos centrales han sido definidos y mapeados?	Sí, se cuenta con los procedimientos específicos para cada proceso, los mismos que están integrados en el mapa de procesos presentado en las Figuras 4,5 y 6.
11	¿La gestión de riesgos es integral a los procesos centrales?	Sí, se realiza una evaluación de riesgos por procesos.

En la Tabla 26, se procede a analizar el Principio estructura y exhaustivo.

**Tabla 26 Principio estructurado y exhaustivo**

Ítem	Preguntas	Respuestas
------	-----------	------------

1	¿Serán las normas aplicadas sistemáticamente en todos los niveles de la organización?	Sí, la Gestión de Riesgos aplica tanto para los procesos de Alta Dirección y operativos.
2	¿Las tomas de decisiones son hechas en el tiempo adecuado?	Sí se toman en el momento indicado; sin embargo, por la proximidad de las necesidades de implementación, no se siguen los pasos adecuados.
3	¿Cuándo hay cambios en el sistema de gestión de riesgo, son estos aprobados por las partes interesadas?	Sí, son revisados y aprobados por las partes internas interesadas. Sin embargo, las partes externas no están involucradas.
4	¿El criterio de toma de decisiones ha sido definido en todos los niveles de la organización?	Sí, la toma de decisiones se evalúa tanto en la parte gerencial como con las partes interesadas involucradas.
5	¿Son las decisiones estructuradas parte de un largo proceso de ciclo de decisión?	Sí, las decisiones siguen un proceso de Gestión del Cambio, según lo sugerido por la ISO 9001:2015.
6	¿Se evalúa la efectividad de la toma de decisiones en relación a los riesgos?	Se evalúan los riesgos en base a los nuevos controles implementados en los procesos.

En la Tabla 27, se procede a analizar el Principio de adaptabilidad.

**Tabla 27 Principio de adaptabilidad**

Ítem	Preguntas	Respuestas
1	¿El contexto de la organización es entendido y definido?	Sí, el contexto se encuentra definido en el Capítulo 2.4 “Contexto de la Organización”
2	¿La arquitectura y el diseño del marco de referencia se encuentran alineados con el contexto?	Sí.
3	¿Los límites del marco de referencia de la gestión de riesgos se encuentran definidos?	Sí, el marco de referencia es aplicable a toda la organización.
4	¿Los elementos culturales y conductuales de la organización completamente definidos y entendidos?	Sí.

En la Tabla 28, se procede a analizar el Principio de Gestión de Riesgos inclusiva.

**Tabla 28 Principio de Gestión de Riesgos Inclusiva**

Ítem	Preguntas	Respuestas
1	¿Las autoridades y responsabilidades se	Sí, las autoridades se encuentran definidas por

	encuentran definidas en cada nivel de la organización?	cada puesto de la organización. Asimismo, cada puesto de trabajo cuenta con su perfil incluido.
2	¿Son los colaboradores entrenados en la gestión y control de riesgos en su área dónde son responsables?	Los colaboradores conocer los riesgos asociados a su puesto de trabajo. En el caso de los colaboradores operativos, cuentan con capacitaciones sobre los mismos. Sin embargo, los colaboradores administrativos, los aprenden en su inducción.
3	¿Son los protocolos y procesos de la gestión del riesgo entendidos por todos los colaboradores?	Los protocolos y procesos son entendidos por los colaboradores de alta gerencia y los colaboradores administrativos que tienen injerencia con los mismos.
4	¿Son los stakeholders, clientes y partes interesadas considerados en la toma de decisiones?	Sí, se revisa con las partes interesadas la factibilidad y riesgos asociados. Asimismo, se analiza con los clientes los procedimientos establecidos.

En la Tabla 29, se procede a analizar en Principio de Gestión de Riesgos dinámico.

**Tabla 29 Principio de Gestión de Riesgos Dinámica**

Ítem	Preguntas	Respuestas
1	¿El contexto interno y externo de la organización son constantemente monitoreados?	Son revisados cada dos años con una consultora. Adicionalmente, cuando ocurren cambios críticos, se analiza el contexto con las partes interesadas.
2	¿El proceso de gestión de riesgos es lo suficientemente adaptable a estos cambios?	El proceso de Gestión de Riesgos está basado en la mejora continua, por lo cual sí es adaptable a los cambios.
3	¿Existen suficientes mecanismos de revisión que aseguren confiabilidad y correcta toma de decisiones, con relación al alcance de objetivos?	Mediante la Gestión del Cambio, se evalúan los nuevos procesos, posterior a la implementación de los mismos. Se evalúan los riesgos residuales.
4	¿Los controles son evaluados en efectividad y eficiencia?	Sí, se realiza la evaluación de riesgos de cada riesgo residual, tomando en consideración la implementación de los controles.
5	¿Los mecanismos son revisados y	Únicamente se manejan indicadores de los

	monitoreados para realizar seguimiento a los KPI's y KRI's?	riesgos de mayor relevancia e impacto para la organización.
6	¿Los controles son adecuados para lograr el cumplimiento de los objetivos según el apetito de riesgo de la organización?	Existen algunos riesgos críticos en la organización; sin embargo, la mayor parte de los mismos se encuentran controlados.

En la Tabla 30, se procede a analizar el Principio de Mejor Información Disponible.

**Tabla 30 Principio de Mejor Información Disponible**

Ítem	Preguntas	Respuestas
1	¿El proceso de toma de decisiones considera los tipos de información que deben ser reunidos?	Sí, considera la información del proceso, el objetivo, los precedentes, los riesgos asociados y las partes involucradas.
2	¿Se identifica la mejor información disponible a ser aplicada en la gestión de riesgos? ¿Cómo?	Sí se identifica. Se toma información de fuentes confiables, especialmente de las autoridades aeronáuticas y de transporte en el Perú.
3	¿Se evalúa la calidad, exactitud y confianza de la información?	Sí se evalúa.
4	¿Son los elementos de los contextos discutidos e identificados en la toma de decisiones?	Sí son discutidos.
5	¿Las suposiciones hechas en la toma de decisiones son validadas por expertos?	Sí, la toma de decisiones es en base al expertise de las partes interesadas.
6	¿Son las decisiones revisadas periódicamente para asegurar su validez y actualización?	Sí, son revisadas en los comités de Gerencia, evaluándose cualquier desviación.

En la Tabla 31, se analizará el Principio Factores Humanos y Culturales:

**Tabla 31 Principio Factores Humanos y Culturales**

Ítem	Preguntas	Respuestas
1	¿Se ha desarrollado el caso de negocio y plan de implementación?	Sí.
2	¿El gerente ejecutivo se encuentra directamente involucrado en la arquitectura, el diseño e implementación, y la garantía del plan de gestión de riesgos?	Sí, se encuentra involucrado el Gerente General y el Gerente Corporativo. Ellos fomentan el análisis basado en riesgo y revisan los riesgos de mayor importancia para la compañía.
3	¿Son los indicadores apropiados para la	Los indicadores actuales son apropiados; sin

organización?	embargo, se recomienda implementar indicadores adicionales.
---------------	---

En la Tabla 32, se analizará el Principio de Mejora Continua.

**Tabla 32 Principio de Mejora Continua**

Ítem	Preguntas	Respuestas
1	¿Son los KPI's y KRI's mejorados continuamente?	La revisión de los indicadores se realiza de forma anual. Asimismo, trimestralmente se monitorean los mismos en busca de desviaciones.
2	¿Se tienen responsabilidades y autoridades específicas para la mejora continua?	Sí, se cuenta con un área específica de mejora continua, para ello se cuenta con una planificación anual, que puede ser mejorada ante necesidades específicas.
3	¿Las compensaciones son relacionadas con los objetivos de la mejora continua?	Sí, los bonos de productividad se encuentran basados en el cumplimiento de objetivos.
4	¿Es la mejora continua una oportunidad en la gestión de riesgos?	Sí, permite que la organización cuente con los riesgos actualizados.
5	¿Es la mejora continua monitoreada constantemente?	Sí, en las reuniones mensuales del comité de Gerencia.

#### **4.2. Análisis para la implementación del marco de referencia**

Como siguiente paso, se procederá a analizar el marco de referencia actual de la organización, en contraste con el marco de referencia de la ISO 31000.

##### **4.2.1. Liderazgo y compromiso**

**Tabla 33 Liderazgo y compromiso de la organización**

Ítem	Preguntas	Respuesta
1	¿Se encuentra el marco de referencia de la ISO 31000 o COSO adoptado y aceptado por la junta directiva y la alta gerencia?	El procedimiento de gestión de riesgos solo se encuentra aprobado por el área de Sistemas Integrados de Gestión.
2	¿La junta directiva provee vigilancia en la correcta implementación del sistema de gestión de riesgos?	Actualmente, la junta directiva revisa anualmente los riesgos de mayor relevancia y enfoca parte del presupuesto en la mitigación de los mismos.

3	¿Los objetivos estratégicos son incorporados en la gestión de riesgos?	Sí, en la identificación de riesgos se analiza el objetivo estratégico impactado.
4	¿Los KRI's y KPI's se encuentran alineados con los objetivos estratégicos?	Actualmente, se cuenta con KPI's en las distintas unidades de negocio; sin embargo, solo se cuenta con KRI's para el sistema de gestión de SST.
5	¿Los KRI's de la organización son alcanzables?	Sí, se encuentran controlados de acuerdo al apetito de la organización.
6	¿Los indicadores son monitoreados y asegurados continuamente?	Los KRI y algunos indicadores son revisados mensualmente en los distintos comités. Asimismo, los indicadores de los riesgos relevantes son revisados una vez al año en el comité de riesgos.
7	¿El sistema de gestión de riesgos contempla los principios mencionados en la normativa?	En su mayor parte; sin embargo, falta reforzar la cultura en los colaboradores operativos de la organización.
8	¿El sistema de gestión de riesgos es entendido por los colaboradores internos y las partes interesadas externas de la organización?	Es entendido por los dueños de proceso, y en menor medida por la parte operativa de la organización.

#### **4.2.2. Diseño del marco de referencia**

La organización no cuenta con una política de gestión de riesgos, por lo cual se recomienda la elaboración de la misma y esta deberá encontrarse disponible para los empleados, contratistas y visitantes. Por otro lado, la organización, sí cuenta con los procesos integrados, lo que deberá mejorar es la designación de recursos para la gestión y la comunicación interna y externa de cómo se están gestionando algunos de los riesgos de la organización.

#### **4.2.3. Implementación del marco de referencia**

- ✓ La organización cuenta con un buen gobierno, dicho estatuto se encuentra sustentado en la validación recibida por la organización como Empresa Socialmente Responsable, en la cual muchos de sus requerimientos se encuentran basados en el buen gobierno corporativo.
- ✓ Se cuenta con los requerimientos de los stakeholders de la organización en el Manual de Sistemas Integrados de Gestión.

- ✓ Queda pendiente la integración de los reportes operacionales de riesgo significativos a los reportes financieros de la organización.

#### ***4.2.4. Evaluación del marco de referencia***

- ✓ Actualmente, la organización cuenta con un área de Auditoría Interna, la cual realiza auditorías basadas en riesgo a todos los procesos de la organización. Asimismo, a lo largo del año se reciben auditorías externas por parte de clientes, la autoridad y empresas certificadoras.
- ✓ El equipos de vigilancia, monitoreo y revisión para los distintos procesos de la organización está contemplado por el área de Sistema Integrado de Gestión y por Auditoría Interna.

#### ***4.2.5. Mejora del marco de referencia***

- ✓ La revisión periódica de nuestro sistema de gestión de riesgos se encuentra establecida a un plazo de un año por parte del área de Sistemas Integrados de Gestión y los dueños de procesos.
- ✓ Cuando se presentan cambios en el ambiente competitivo de la compañía, el modelo de negocio, requerimientos de los clientes o un cambio en el contexto interno o externo, se realiza una Gestión del Cambio, incluyendo los riesgos relevantes del mismo.

### ***4.3. Análisis para la implementación del proceso***

A continuación, se procederá con el análisis de brechas del proceso de Gestión de Riesgos actual y el sugerido por la ISO 31000.

#### ***4.3.1. Liderazgo y compromiso de la organización***

Se inicia objetivo del marco de referencia, el cual es establecer una metodología que permita gestionar el riesgo a nivel organizacional, bajo el enfoque de la ISO 31000, definiendo la metodología de “Probabilidad por consecuencia”.

Se realiza el análisis del contexto, para iniciar la gestión del riesgo, ello permitirá captar los objetivos de la organización, el entorno en el que se persiguen estos objetivos, las partes interesadas y los criterios del riesgo. Todos estos elementos nos ayudarán a revelar y evaluar la naturaleza y complejidad de los riesgos. La metodología y criticidad descrita en el marco de referencia (procedimiento) puede ser aplicada a cualquier tipo de riesgo, cualquiera que sea su naturaleza, ya sea positivo o negativo. Se pretende que dicho procedimiento se utilice para armonizar la gestión del riesgo existente y las normas o compromisos futuros que adapta la compañía. El presente procedimiento tiene un alcance a todos los procesos de la organización en las distintas sedes que se decida gestionar los mismos.

### 4.3.2. Comunicación y consulta

En la Tabla 34, se puede apreciar el análisis de brechas en la Comunicación y Consulta deseada con la actual, obteniéndose un cumplimiento bueno de 83%.

**Tabla 34 Análisis de brechas - comunicación y consulta**

Actividades	Situación Real	Valor	Implementación
Desarrollo de un caso de negocio de riesgos	No se cuenta con un análisis de costo – beneficio.	0	No se llevará a cabo ya que requiere una madurez de riesgo mayor a la actual.
Desarrollo de un plan de proyecto para la implementación de riesgos	No se cuenta con un plan para la implementación del mismo.	0	No se llevará a cabo ya que requiere una madurez de riesgo mayor a la actual.
Identificación de stakeholders, clientes y partes interesadas	Sí se encuentran identificados en el manual de sistema integrado de gestión.	2	Ya se encuentra implementado.
Compartir el caso de negocio de riesgo, plan de proyecto de riesgo, estructura de composición del trabajo de riesgo con los dueños de proceso, stakeholders, clientes y partes interesadas para comunicar el calendario de despliegue de riesgos, costos, recursos, alcance, calidad e hitos.	No se cuenta con el caso de negocio.	0	No se llevará a cabo ya que requiere una madurez de riesgo mayor a la actual.
Evaluar la comunicación de stakeholders y necesidades de entrenamiento	La comunicación con los stakeholders internos es óptima ya que los mismos conocen sus riesgos y cómo mitigarlos. La comunicación con stakeholders externos es óptima, y son informados ante nuevos procesos.	2	Ya se encuentra implementado.
Determinar si las expectativas de stakeholders, clientes y partes interesadas han cambiado.	Ante el cambio de las expectativas se realizar una Gestión del Cambio.	2	Ya se encuentra implementado.
Determinar la comunicación interna y externa con stakeholder y su necesidad de información.	Sí se encuentra determinado. Asimismo, se conocen los canales de comunicación.	2	Ya se encuentra implementado.
Determinar los recursos para cumplir con la estrategia y misión de los objetivos críticos	Los recursos son determinados por cada área responsable de sus procesos, ello en búsqueda del cumplimiento de los objetivos organizacionales.	2	Ya se encuentra implementado.
Mejora en las capacidades de gestión de riesgos de la organización.	La organización provee cursos internos a los colaboradores para la concientización de sus riesgos, con frecuencia anual.	2	Ya se encuentra implementado.

Monitorear las mejores prácticas de gestión de riesgos, publicaciones, benchmarks, conferencias, etc.	El área de Sistemas Integrados de Gestión es la encargada de monitorear las mejores prácticas.	2	Ya se encuentra implementado.
Consulta con profesionales de los riesgos dentro o fuera de la organización acerca de estrategias, planes y tácticas.	Existe la guía por parte de los integrantes del área de sistemas integrados de gestión.	2	Ya se encuentra implementado.
Evaluación de la efectividad del marco de referencia, herramientas y técnicas.	Se evalúa la efectividad únicamente de la gestión de riesgos importantes y críticos para la organización.	1	Se plantea contar con una mayor cantidad de indicadores para la Gestión de Riesgos.
Recomendar a los dueños de proceso nuevas prácticas y procedimientos.	Se realiza dichas recomendaciones; sin embargo, y se documenta según lo indicado en el procedimiento de gestión del cambio.	2	Ya se encuentra implementado.
Mejora en la madurez del riesgo y en la capacidad de requerimientos.	Sí, la Gestión del Riesgo está en búsqueda de la mejora continua.	2	Ya se encuentra implementado.
Resolver problemas relacionales al performance del proceso de gestión de riesgos	En caso de encontrarse desviaciones en los indicadores, se analizan y resuelven los problemas.	2	Ya se encuentra implementado.
Ayudar en el desarrollo y entrenamiento de la gestión de riesgos	Se realizan capacitaciones anuales al personal, en el cual se explican los riesgos a los cuales están expuestos.	2	Ya se encuentra implementado.
Realizar entrenamiento para los grupos de stakeholders	Se realizan capacitaciones anuales al personal, en el cual se explican los riesgos a los cuales están expuestos.	2	Ya se encuentra implementado.
Desarrollo del marco de referencia y el proceso de documentación de gestión de riesgos.	Se cuenta con un marco de referencia y con un registro de riesgos por proceso.	2	Ya se encuentra implementado.
Manejar el marco de referencia, proceso, desglose de recursos, y mantener el calendario de las actividades de gestión de riesgos.	Se cuenta con un cronograma anual de auditorías y en caso se presente un proyecto de Gestión de Riesgos, se maneja un Gantt.	2	Ya se encuentra implementado.
Incorporar cambios en los hitos de proyectos de riesgos.	Para los riesgos de proyectos un grupo especializado evalúa el cumplimiento.	2	Ya se encuentra implementado.
Actualizar los planes y calendarios de gestión de riesgos a plazos definidos.	Para los riesgos de proyectos un grupo especializado evalúa el cumplimiento.	2	Ya se encuentra implementado.

#### 4.3.3. Establecimiento del Contexto

En la Tabla 35, se puede apreciar el análisis de brechas en el Establecimiento de Contexto deseado con el actual, obteniéndose un cumplimiento óptimo del 96%.

**Tabla 35 Análisis de brechas - establecimiento del contexto**

Actividades	Situación Real	Valor	Implementación
Evaluar el contexto interno y/o externo	Se evalúa el contexto interno y externo.	2	Ya se encuentra implementado.
Revisión de la documentación existente, incluyendo la taxonomía del riesgo	Se revisa anualmente por el área de Sistema Integrados de Gestión y los dueños de proceso.	2	Ya se encuentra implementado.
Desarrollar un lenguaje y taxonomía común para los riesgos.	Se cuenta con un lenguaje y estructura definida para su gestión.	2	Ya se encuentra implementado.
Determinar la capacidad y madurez del riesgo en la organización.	La capacidad y madurez de encuentra en un 40%.	2	Ya se encuentra implementado.
Evaluar las políticas y procedimientos para que estos reflejen la madurez y capacidad de la organización.	La evaluación del procedimiento es anual; sin embargo, no se cuenta con una política.	1	Se implementará una política de gestión de riesgos.
Determinar si los cambios en el ambiente externo e interno pueden resultar en riesgos adicionales.	Al cambio de contexto, se realiza una nueva hoja de ruta para la organización.	2	Ya se encuentra implementado.
Realizar un análisis para identificar los riesgos nuevos, la volatilidad, incertidumbre, complejidad y ambigüedad de la industria.	Se realiza una revisión mensual identificando riesgos nuevos.	2	Ya se encuentra implementado.
Discutir las amenazas nuevas o actuales y el impacto con los ejecutivos y dueños de proceso.	Se realiza y se encuentra documentado en el procedimiento de gestión de cambios.	2	Ya se encuentra implementado.
Evaluar cambios que puedan impactar en la compañía, incluyendo nuevas amenazas, tecnologías, peligros y cambios organizacionales.	Se realiza y se encuentra documentado en el procedimiento de gestión de cambios.	2	Ya se encuentra implementado.
Ajustar los criterios de evaluación de riesgos, políticas, y objetivos críticos.	No se cuenta con una política. Los objetivos son ajustados ante cambios en entorno.	1	Se implementará una política de gestión de riesgos.
Identificar eventos de riesgo que puedan impactar a la organización.	Se identifican estos eventos en las matrices.	2	Ya se encuentra implementado.
Asegurar que las definiciones de riesgo y potenciales impactos sean reflejados correctamente en el apetito de riesgo y tolerancia de la organización.	La organización tiene parametrado el apetito de riesgo y la tolerancia para los mismos.	2	Ya se encuentra implementado.
Obtener guía sobre la efectividad de la gestión de riesgos por parte de stakeholders, clientes y partes interesadas.	Se obtiene un análisis de efectividad mediante el input de reportes por parte de ellos.	2	Ya se encuentra implementado.
Revisar y aprobar criterios de riesgo, políticas y asegurar que son apropiados para la organización.	Se aprueban anualmente en el Comité de Riesgos.	2	Ya se encuentra implementado.

Determinar cambios en el contexto interno y externo que pueda resultar en amenazas, peligros, tecnología, procesos, personal, cambio de leyes y regulaciones que puedan causar la reevaluación de los riesgos existentes.	Se analiza el contexto interno y externo cada dos años.	2	Ya se encuentra implementado.
Identificar nuevos riesgos	Se identifican nuevos riesgos con una Gestión del Cambio.	2	Ya se encuentra implementado.
Asegurar que el comité de gestión de riesgos revise y apruebe el alcance de la evaluación de riesgos.	Se realiza el Comité de Riesgos de forma anual.	2	Ya se encuentra implementado.
Revisar los planes, políticas, procedimientos, organigrama y criterios de riesgos organizacionales.	Se realizan revisiones ante cambios en los distintos procesos, o ante cambios organizacionales.	2	Ya se encuentra implementado.
Proveer comentarios y feedback en cambios de organigramas, KPIs y KRIs.	Se analizan los KRI's y KPI's en los comités de alta gerencia.	2	Ya se encuentra implementado.
Comunicar el desarrollo de los cambios y confirmar que las revisiones son aceptadas por los dueños de riesgos.	Los cambios en el Procedimiento de Gestión de Riesgos son comunicados por correos internos.	2	Ya se encuentra implementado.
Determinar el alcance de la identificación del riesgo y evaluar actividades para la revisión anual y el registro.	Se contempla la revisión anual en la cual se registra una nueva versión de la matriz.	2	Ya se encuentra implementado.
Identificar actividades nuevas que requieran evaluación de riesgos.	Los dueños de proceso comunican las nuevas actividades que se presentan en las operaciones.	2	Ya se encuentra implementado.
Obtener entradas de los dueños de riesgo, stakeholders, y partes interesadas, definiendo el alcance de la evaluación de riesgos.	Se obtiene un análisis de efectividad mediante el input de reportes por parte de ellos.	2	Ya se encuentra implementado.
Determinar protocolos para la evaluación de riesgo de oportunidades.	Se cuenta con las definiciones para las oportunidades a identificar.	2	Ya se encuentra implementado.
Revisar el registro de competencias de los gestores de riesgo.	Se cuenta con un perfil de puesto para los altos mandos.	2	Ya se encuentra implementado.
Actualizar el registro de riesgos si es necesario. Así como también, planes, procesos y procedimientos.	Se actualizan los registros de riesgo y procedimiento a solicitud y evaluación.	2	Ya se encuentra implementado.
Comunicar los cambios en los planes, proceso y procedimiento a las partes impactadas.	Sí son comunicados en correos internos.	2	Ya se encuentra implementado.

#### **4.3.4. Identificación de riesgos**

En la Tabla 36, se puede apreciar el análisis de brechas en el proceso de identificación de riesgos entre la situación deseada contra la actual, obteniéndose un cumplimiento óptimo de 94%.

**Tabla 36 Análisis de brechas - identificación de riesgos**

Actividades	Situación Real	Valor	Implementación
Identificar e investigar riesgos emergentes	Se identifican nuevos riesgos con una frecuencia anual.	2	Ya se encuentra implementado.
Conducir un análisis de riesgos emergentes.	Se analizan los riesgos nuevos identificados con los dueños de proceso.	2	Ya se encuentra implementado.
Identificar sucesos inesperados de gran magnitud.	Se identifican sucesos inesperados tales como desastres, los cuales se encuentran contemplados en el plan de continuidad.	2	Ya se encuentra implementado.
Revisar riesgos mayores asociados a KPIs y KRIs existentes.	Se analizan los KRI's y KPI's en los comités de alta gerencia.	2	Ya se encuentra implementado.
Identificar nuevas métricas de performance asociadas con el logro de objetivos críticos.	Se analizan los KRI's y KPI's en los comités de alta gerencia.	2	Ya se encuentra implementado.
Identificar puntos de referencia en organizaciones para entender los puntos comunes y diferencias en los enfoques de riesgos.	Alta gerencia identifica en sus comités los puntos comunes y diferencias en el enfoque de riesgos.	2	Ya se encuentra implementado.
Revisar el registro de riesgos para riesgos nuevos, modificados y/u obsoletos.	Se realiza dicha revisión anualmente.	2	Ya se encuentra implementado.
Revisar la taxonomía del riesgo para identificar riesgos críticos para un análisis.	Sí se realiza una verificación especial de los riesgos marcados como críticos.	2	Ya se encuentra implementado.
Trabajar con los dueños de riesgo para apoyar la identificación de sus riesgos y los esfuerzos para la revisión de riesgos.	Sí se trabaja con los dueños de proceso anualmente y cada vez que ocurre un accidente.	2	Ya se encuentra implementado.
Realizar talleres multifuncionales de RM y ERM para identificar aún más riesgos nuevos, cambios u obsoletos en términos de consecuencia y probabilidad.	Dichos talleres o reuniones son realizadas ante un cambio en el contexto o nuevos procedimientos.	2	Ya se encuentra implementado.
Identificar factores de riesgo y consecuencias.	Se identifican los factores de riesgo.	2	Ya se encuentra implementado.
Determinar una lista de riesgos preliminar basada en consecuencias y probabilidades.	Se cuenta con las matrices de riesgo para la representación de los mismos.	2	Ya se encuentra implementado.
Trabajar con patrocinadores ejecutivos en identificar dueños de riesgos para los nuevos riesgos.	Se trabaja junto con los gerentes de las distintas áreas.	2	Ya se encuentra implementado.
Confirmar con los dueños de riesgo la existencia de nuevos riesgos, cambios o incrementos.	Se realizan las reuniones en las cuales los dueños de proceso indican la existencia de alguno de dichos cambios.	2	Ya se encuentra implementado.
Ayudar con la identificación para el personal que identifica y cuantifica los factores de riesgo y sus consecuencias. Si los riesgos son altos o tienden a serlo, elevarlos al	Los riesgos altos son elevados al comité de gerencia mensual; sin embargo, no son registrados.	1	Implementación de un registro de riesgos.

registro empresarial.			
Formar un panel de expertos para evaluar los nuevos factores de riesgos, consecuencias y probabilidades.	Se reúne anualmente el área de SIG con los dueños de proceso, también cuando se presenta un suceso que afecte el análisis.	2	Ya se encuentra implementado.
Especificar objetivos estratégicos para posibles ajustes.	Se tienen mapeados los objetivos estratégicos de la organización.	2	Ya se encuentra implementado.
Comunicar nuevos KRIs o KPIs a los dueños de riesgo y stakeholders impactados.	Se comunican los KRI's y KPI's a la primera línea de gerencia.	2	Ya se encuentra implementado.
Desarrollar nuevos negocios y objetivos incluyendo unidades de negocio y objetivos funcionales.	Se analizan los objetivos cada dos años en conjunto con una empresa consultora.	2	Ya se encuentra implementado.
Desarrollar nuevos documentos de planes y procesos basados en cambios de contexto u objetivos.	Se actualizan los riesgos cuando se presentan nuevos objetivos estratégicos en la organización.	2	Ya se encuentra implementado.
Rexaminar y rehacer los objetivos empresariales, incluyendo los KRIs y KPIs	Se analizan los KRI's y KPI's y el impacto en los objetivos cada dos años.	2	Ya se encuentra implementado.
Asegurar que la tolerancia del riesgo sea expresada en términos de límites altos y bajos o umbrales de incumplimiento.	La tolerancia al riesgo y los límites se encuentran definidos en el marco de referencia.	2	Ya se encuentra implementado.
Actualizar la información en el registro de riesgos empresariales.	No se cuenta con un registro de riesgos empresariales.	0	Implementación de un registro de riesgos por sistema afectado.
Verificar y validar los registros de riesgos empresariales, KRIs y KPIs, umbrales y objetivos.	Se realiza dicha verificación y validación con una frecuencia anual.	2	Ya se encuentra implementado.
Aceptar o dejar como obsoleto riesgos y documentar el motivo.	Se evidencia dicho ítem en las matrices de gestión de riesgos.	2	Ya se encuentra implementado.

#### 4.3.5. Análisis de riesgo

En la Tabla 37, se puede apreciar el análisis de brechas en el proceso de análisis de riesgos entre la situación deseada contra la actual, obteniéndose un cumplimiento regular de 55%.

**Tabla 37 Análisis de brechas - análisis de riesgos**

Actividades	Situación Real	Valor	Implementación
Facilitar la evaluación de riesgos cualitativa o cuantitativa.	Se facilita la evaluación de riesgos cualitativa.	1	Se evaluarán la implementación de un software que permita la evaluación de riesgos cuantitativa.
Asignar clasificaciones a los riesgos.	Se clasifican los riesgos por el sistema al cual impactan.	2	Ya se encuentra implementado.
Determinar causas y correlaciones entre riesgos.	Se determinan los peligros y las consecuencias de los riesgos.	2	Ya se encuentra implementado.

Determinar personal calificado para estimar probabilidad y consecuencia	Se cuenta con personal calificado (SIG y dueños de proceso)	2	Ya se encuentra implementado.
Solicitar apoyo a los dueños de riesgo para realizar el análisis de los mismos.	El análisis se realiza en conjunto con los dueños de riesgo.	2	Ya se encuentra implementado.
Determinar la información apropiada y la relación entre informes.	Solo se toma en cuenta el expertis de los dueños de proceso, mas no la data de auditoría y/o reportes.	1	Se implementará un software de evaluación que considere los reportes y auditorías.
Agregar y priorizar riesgos 1. Empresariales, 2. Proyectos y procesos, 3. Producción / Transacción	Se prioriza y analiza según el orden indicado.	2	Ya se encuentra implementado.
Asignar calificaciones de consecuencia y probabilidades a cada riesgo y registrarlos.	Se realiza dicha asignación y se registra en la matriz de riesgos.	2	Ya se encuentra implementado.
Evaluar riesgos que cuenten con una alta consecuencia o alta prioridad.	Los riesgos que se encuentran fuera de los límites permitidos son evaluados nuevamente.	2	Ya se encuentra implementado.
Priorizar riesgos para un análisis crítico adicional	Se priorizan los riesgos que se encuentran fuera del umbral	2	Ya se encuentra implementado.
Acumular el riesgo desde el nivel transaccional / de producto hasta el nivel empresarial para fines de visualización	No se presentan gráficos ni estadísticas para la visualización solicitada.	0	Se implementará un software para el apoyo en la gestión del riesgo.
Analizar riesgos basados en evaluaciones cualitativas, tales como mapas de calor y escalas de probabilidad.	No se cuenta con mapas de calor en la organización.	0	Se implementará un software para el apoyo en la gestión del riesgo.
Desarrollo de árboles de eventos y otros tipos de evaluación de riesgos.	No se cuenta con una metodología específica.	0	Se implementará un software para el apoyo en la gestión del riesgo.
Asegurar que los stakeholders y clientes estén familiarizados con la evaluación de riesgos y la herramienta de análisis.	Los stakeholders conocen el uso de la Matriz de Riesgos y la Gestión del Cambio.	2	Ya se encuentra implementado.
Solicitar input a los stakeholders acerca de selecciones para herramientas de evaluación de riesgos.	No se solicita dicho input a los stakeholders.	0	No se llevará a cabo ya que requiere una madurez de riesgo mayor a la actual.
Reunir a expertos en riesgos para analizar los riesgos en cascada, interdependientes, dependientes y otros.	No se cuenta con una clasificación de riesgos en cascada o interdependientes.	0	No se llevará a cabo ya que requiere una madurez de riesgo mayor a la actual.
Identificar posibles materiales, cascada, espacios en blanco, dependencia, interdependencia, crónicos, sistémicos y otros tipos de riesgo.	No se cuenta con una clasificación de riesgos en cascada o interdependientes.	0	No se llevará a cabo ya que requiere una madurez de riesgo mayor a la actual.
Desarrollar cadenas de eventos casuales o de correlación que	No se cuenta con una clasificación de riesgos en	0	No se llevará a cabo ya que requiere una

podrían generar un impacto o generar riesgos adicionales.	cascada o interdependientes.		madurez de riesgo mayor a la actual.
Reconocer eventos de riesgo que pueden conducir a factores de riesgo secundarios o en cascada que finalmente conducen a eventos de riesgo.	No se cuenta con una clasificación de riesgos en cascada o interdependientes.	0	No se llevará a cabo ya que requiere una madurez de riesgo mayor a la actual.
Identificar cadenas de impactos de riesgo y sus consecuencias resultantes de una ocurrencia de riesgo que puede vincularse a impactos secundarios.	No se cuenta con una clasificación de riesgos en cascada o interdependientes.	0	No se llevará a cabo ya que requiere una madurez de riesgo mayor a la actual.
Facilitar entrenamiento y desarrollo de riesgos.	Se cuenta con un presupuesto para la Gestión de Riesgos anual, en el se incluyen capacitaciones para los expertos.	2	Ya se encuentra implementado.
Proveer entrenamiento en cómo desarrollar un registro de riesgos.	Se cuenta con especialistas en Gestión de Riesgos.	2	Ya se encuentra implementado.
Alertar a los dueños de riesgo en prevenir problemas de riesgo potenciales.	Se alerta a los dueños de riesgo cuando estos se salen de los umbrales permitidos.	2	Ya se encuentra implementado.
Apoyar a los dueños de riesgos en identificar KRIs y KPIs.	El comité de gerencia y el área de SIG apoya en la identificación de indicadores.	2	Ya se encuentra implementado.
Cuantificar riesgos seleccionados.	El análisis de riesgo se realiza de forma cualitativa.	0	Se implementará un software para el apoyo en la gestión del riesgo.
Estimar la frecuencia de riesgo del evento basado en cambios o en factores de riesgo.	Se estima la probabilidad de forma cualitativa.	1	Se implementará un software para el apoyo en la gestión del riesgo.
Determinar la probabilidad de que los factores secundarios de riesgo se conviertan en primarios.	No se determina dicha probabilidad.	0	No se llevará a cabo ya que requiere una madurez de riesgo mayor a la actual.
Determinar si los factores de riesgo de tercer nivel necesitan ser analizados.	Los riesgos de menor impacto no son analizados ya que son aceptables para la compañía.	2	Ya se encuentra implementado.
Desarrollar un portafolio de riesgos empresariales basado en medidas de riesgo calculadas.	Se cuentan con las matrices de riesgos empresariales.	2	Ya se encuentra implementado.
Comunicar el nivel de los riesgos empresariales.	Se comunican anualmente en el directorio.	2	Ya se encuentra implementado.
Monetizar los riesgos en términos de valor de riesgo, porcentaje de presupuesto en riesgo o de forma similar.	No se monetizan los riesgos.	0	Se implementará un software para el apoyo en la gestión del riesgo.

#### 4.3.6. Evaluación de riesgos

En la Tabla 38, se puede apreciar el análisis de brechas en el proceso de evaluación de riesgos entre la situación deseada contra la actual, obteniéndose un cumplimiento bueno de 83%.

**Tabla 38 Análisis de brechas - Evaluación de riesgos**

Actividades	Situación Real	Valor	Implementación
Comparar niveles de riesgo y criterios.	Se comparan los niveles de riesgo con los máximos permitidos.	2	Ya se encuentra implementado.
Comparar los niveles de riesgos calculados con el apetito de riesgo y los umbrales de tolerancia.	Se comparan los niveles de riesgo con los máximos permitidos.	2	Ya se encuentra implementado.
Proveer de input en la priorización de riesgos.	Se priorizan los riesgos por su nivel obtenido.	2	Ya se encuentra implementado.
Revisar los impactos de riesgos, misión, objetivos críticos, tolerancia de riesgo y el criterio para los umbrales.	Se analizan las consecuencias, el sistema impactado, FODA y objetivo estratégico.	2	Ya se encuentra implementado.
Revisar los rankings de riesgos.	Se revisan los rankings.	2	Ya se encuentra implementado.
Priorizar riesgos en función al apetito de riesgo calculado y los niveles de tolerancia del riesgo.	Se priorizan los riesgos con un nivel más alto.	2	Ya se encuentra implementado.
Revisar la evaluación cualitativa de riesgos.	Se revisa la evaluación con los dueños de proceso para la implementación de controles	2	Ya se encuentra implementado.
Revisar técnicas cuantitativas de evaluación de riesgos, incluyendo árboles de riesgos y correlación de los mismos.	No se revisan las técnicas cuantitativas de Gestión de Riesgos.	0	Se implementará un software para el apoyo en la gestión del riesgo.
Revisar riesgos sistémicos, crónicos, materiales, de dependencia e interdependencia	No se cuenta con dicha clasificación de riesgos.	0	No se llevará a cabo ya que requiere una madurez de riesgo mayor a la actual.
Priorizar tratamientos de riesgo.	Se priorizan los tratamientos de los riesgos críticos.	2	Ya se encuentra implementado.
Revisar riesgos casuales y de correlación entre eventos, amenazas, riesgos, Etc.	No se clasifican los riesgos teniendo en cuenta dichas características.	0	No se llevará a cabo ya que requiere una madurez de riesgo mayor a la actual.
Desarrollar un ranking de riesgos críticos a ser tratados.	Se cuenta con un ranking de acuerdo al resultado de probabilidad x consecuencia	2	Ya se encuentra implementado.
Proveer un enfoque preliminar para el tratamiento de riesgos.	Se plantean las medidas en los controles para el tratamiento de riesgos residuales.	2	Ya se encuentra implementado.
Presentar riesgos al comité de riesgos y a los dueños de procesos.	Son presentados al comité de forma anual. Los dueños de proceso conocen sus riesgos.	2	Ya se encuentra implementado.
Actualizar riesgos y el ranking en el registro.	Se actualizan los riesgos una vez al año o en caso se cree un nuevo proceso u ocurra un evento.	2	Ya se encuentra implementado.

Revisar y obtener la aprobación de la priorización de riesgos por parte del director de riesgos y la gerencia ejecutiva.	Se revisan los riesgos de forma anual, clasificando los riesgos importantes y críticos.	2	Ya se encuentra implementado.
Revisar y desarrollar una lista final de riesgos a ser considerados para el tratamiento.	Se cuenta con dichos controles por proceso.	2	Ya se encuentra implementado.
Guiar a los comités de riesgo y a los dueños de proceso en controles adicionales para los riesgos.	El área de SIG apoyará en los controles para los riesgos.	2	Ya se encuentra implementado.

#### 4.3.7. Tratamiento del riesgo

En la Tabla 39, se puede apreciar el análisis de brechas en el proceso de tratamiento de riesgos entre la situación deseada contra la actual, obteniéndose un cumplimiento óptimo de 90%.

**Tabla 39 Análisis de brechas - tratamiento del riesgo**

Actividades	Situación Real	Valor	Implementación
Revisar KPIs, KRIs y objetivos para su idoneidad.	Se revisan los indicadores en el comité de gerencia de la organización.	2	Ya se encuentra implementado.
Diseñar y verificar el entorno general de control interno.	Se verifican los controles internos para cada riesgo.	2	Ya se encuentra implementado.
Desarrollar la estrategia para el tratamiento de riesgo, planes y tácticas de ejecución.	Se desarrollan dichos ítems y son colocados en las matrices de gestión de riesgos.	2	Ya se encuentra implementado.
Desarrollar un plan detallado de proyecto con hitos para tratamiento y control.	Solo se desarrolla un plan detallado para los proyectos complejos que incluyen un presupuesto considerable.	2	Ya se encuentra implementado.
Identificar opciones para el tratamiento de riesgos.	Se identifican las opciones con el personal especializado y los dueños de proceso.	2	Ya se encuentra implementado.
Desarrollar un plan de tratamiento de riesgos.	Se desarrollan los controles para los riesgos.	2	Ya se encuentra implementado.
Desarrollar un plan detallado de proyecto con estructura de desglose de trabajo identificando actividades incluyendo las opciones de tratamiento,	Solo se desarrolla un plan detallado para los proyectos complejos que incluyen un presupuesto considerable.	2	Ya se encuentra implementado.
Recursos, hitos, cronograma, presupuesto, revisión y estatus.	Solo se desarrolla un plan detallado para los proyectos complejos que incluyen un presupuesto considerable.	2	Ya se encuentra implementado.
Asegurar presupuesto para el plan de tratamiento de los riesgos.	Se incluye en el presupuesto los ítems a desarrollar.	2	Ya se encuentra implementado.
Trabajar con dueños de riesgos con respecto a la implementación del tratamiento de riesgos y el reporte de progreso de stakeholders críticos.	Los dueños de proceso son los responsables de la implementación, el área SIG realiza el seguimiento.	2	Ya se encuentra implementado.

Monitorear la implementación del plan de tratamiento de riesgos.	El área SIG realiza el monitoreo de dichos tratamientos.	2	Ya se encuentra implementado.
Actualizar la información con respecto a factores de riesgo y consecuencias de los mismos, incluyendo frecuencias anuales, probabilidades, consecuencia y estrategias para tratamientos existentes y controles en el registro de riesgos.	Se actualiza la matriz de gestión de riesgos según se van implementando los controles.	2	Ya se encuentra implementado.
Monitorear el estatus del plan de tratamiento de riesgos contra los hitos.	El área SIG realiza el monitoreo de dichos tratamientos.	2	Ya se encuentra implementado.
Alertar a los dueños de riesgos y stakeholders si las fechas límites no serán cumplidas.	El área SIG realiza el monitoreo de dichos tratamientos.	2	Ya se encuentra implementado.
Determinar e implementar qué hitos de acciones correctivas no han sido cumplidos.	El área SIG realiza el monitoreo de dichos tratamientos.	2	Ya se encuentra implementado.
Reasignar el trabajo para el tratamiento de riesgos si es necesario.	La reasignación del tratamiento de riesgos se realiza de forma interna en el área.	1	Se implementará un software para un mejor seguimiento.
Identificar recursos adicionales que apoyen con el tratamiento de riesgos y su control.	Cuando son proyectos de gran magnitud se involucra a personal de áreas de soporte.	2	Ya se encuentra implementado.
Comunicar con las personas apropiadas para el reasignamiento de tareas.	No se encuentra definido el canal ni el medio para realizar dicho reasignamiento.	0	Se implementará un software para un mejor seguimiento.
Tomar acciones correctivas para resolver problemas, quitar barreras de tratamiento y plazos perdidos.	Se reportan las complicaciones en los monitoreos realizados y se toman acciones correctivas.	2	Ya se encuentra implementado.
Desarrollar expectativas realistas para asegurar que los plazos son cumplidos y los niveles de riesgo residual serán alcanzados.	Se asignan fechas posibles para la implementación de controles propuestos.	2	Ya se encuentra implementado.
Revisar opciones de control.	Se revisan las opciones de control entre el área SIG y los dueños de proceso.	2	Ya se encuentra implementado.
Evaluar el tratamiento general y la efectividad de los controles.	Se evalúa la efectividad de los controles en las revisiones anuales.	2	Ya se encuentra implementado.
Revisar las estrategias de tratamiento de riesgos existentes y controles.	Se cuentan con estrategias definidas.	2	Ya se encuentra implementado.
Identificar factores de riesgo que puedan ser mitigados, eliminados, reducidos ya sea la probabilidad y/o consecuencia de los mismos.	Se identifican los tipos de control para cada riesgo identificado.	2	Ya se encuentra implementado.
Identificar las consecuencias que puedan ser aceptadas o evitadas	Se evalúan y establecen controles para las mismas.	2	Ya se encuentra implementado.
Revisar los puntos de referencia para los riesgos enumerados en la lista priorizada de riesgos que	Se revisan los tratamientos de los riesgos residuales.	2	Ya se encuentra implementado.

requieren tratamiento.			
Evaluar el tratamiento de los riesgos y las opciones para el control.	Se evalúan los riesgos después de implementar los controles de cada uno de ellos.	2	Ya se encuentra implementado.
Revisar los planes de seguros, analizar los límites y su efectividad	Se revisan los planes de seguros de forma anual, obteniendo la siniestralidad de los mismos.	2	Ya se encuentra implementado.
Identificar los proyectos que puedan impactar la probabilidad y consecuencia de los riesgos.	Se identifican los riesgos en los proyectos de la organización.	2	Ya se encuentra implementada.
Revisar la efectividad de los controles de riesgo de los proyectos y IT.	El director del proyecto y su equipo revisan la efectividad de los controles propuestos.	2	Ya se encuentra implementada.
Revisar el tratamiento de riesgos en los procesos, servicios, medio ambiente, seguridad informática, cadena de suministro, etc. y la efectividad de los controles de riesgos.	Se revisan los tratamientos de forma anual y cada vez que exista un evento disruptor relacionado a ello.	2	Ya se encuentra implementada.
Documentar factores de riesgo y posibles tratamientos adicionales para los riesgos de TI, proyectos y procesos.	Se documentan los factores descritos en las matrices de riesgo.	2	Ya se encuentra implementada.
Coordinar las opciones de tratamiento de riesgos con el equipo de gestión y el CRO.	Se coordinan los tratamientos con el área de SIG; sin embargo, no con el CRO.	1	Incluir al CRO en la coordinación de opciones de tratamiento de riesgos.
Proveer a los dueños de riesgo con información acerca de opciones de tratamiento existentes.	Se analizan las opciones de tratamiento junto con los dueños de riesgo.	2	Ya se encuentra implementada.
Determinar el costo de implementar las opciones de tratamiento de riesgos identificadas.	Se analiza el costo de los controles que ocupan un costo considerable para la gerencia.	2	Ya se encuentra implementada.
Evaluar cuantitativamente y cualitativamente las consecuencias que podría desarrollarse en la reducción o eliminación de los riesgos para cada opción planteada.	Se analiza solo de forma cualitativa las consecuencias.	1	Se implementará un software de Gestión de Riesgos para evaluar las consecuencias.
Apoyar el equipo de gestión en la identificación del costo efectivo de las opciones de tratamiento.	No se evalúa el costo de cada tratamiento, solo de los costos mayores.	1	Se implementará un software de Gestión de Riesgos para cuantificar las consecuencias.
Trabajar en conjunto con el equipo de proyectos y programas para optimizar esfuerzos y eliminar duplicación.	El área de sistemas integrados de gestión trabaja de forma conjunta con los dueños de proceso.	2	Ya se encuentra implementada.
Comparar el riesgo residual contra el apetito de riesgo o la tolerancia.	Se compara el riesgo residual, con la tolerancia establecida por la organización.	2	Ya se encuentra implementada.
Determinar la combinación de tratamiento de costo más efectivo que reduzca el riesgo bajo el apetito de la organización.	La mayoría de tratamientos no se encuentran monetizados.	2	Se monetizará los costos de los tratamientos.

Revisar que las opciones de tratamiento cumplan con las leyes, regulaciones y estatus establecido por la organización.	Se cuenta con la identificación de requerimientos por parte de leyes, regulaciones y normativas.	2	Ya se encuentra implementada.
Determinar el nivel apropiado y el tipo de tratamiento de riesgo, que pueda incluir evitar el riesgo, aceptarlo, reducirlo o transferirlo.	Se identifica el tratamiento a utilizar para cada riesgo.	2	Ya se encuentra implementada.
Revisar las opciones de tratamiento de riesgo con los dueños de proceso y stakeholders.	Se revisan las opciones en los comités con los dueños de proceso y los stakeholders.	2	Ya se encuentra implementada.
Discutir y preparar los planes para estas opciones con los dueños de proceso.	Se discuten los controles entre el área de SIG y los dueños de proceso.	2	Ya se encuentra implementada.
Realizar un análisis de costo beneficio a las opciones de tratamiento de riesgos.	No se realiza el análisis de costo – beneficio.	0	Se implementará un software para el apoyo en dicha tarea.
Proveer comentarios y feedback al equipo de gestión y CRO en la efectividad de los controles y tratamiento. Asimismo, en la eficiencia y economía.	Se realiza dicho feedback anualmente en las revisiones con los dueños de proceso.	2	Ya se encuentra implementada.
Obtener la aprobación de las opciones de tratamientos de riesgos.	Se obtiene la aprobación de la gerencia general en los tratamientos de riesgos más complejos.	2	Ya se encuentra implementada.
Determinar el plan para la implementación del tratamiento de riesgo, incluyendo a las personas autorizadas y responsables de la implementación del mismo.	Se implementan las acciones de mitigación.	2	Ya se encuentra implementada.
Calcular el riesgo residual final y compararlo con el apetito de riesgo y los niveles de tolerancia, para de esta forma determinar si necesita algún tratamiento adicional.	Se calcula el riesgo residual final y se compara con la tolerancia establecida por la compañía.	2	Ya se encuentra implementada.
Determinar si es que hubo reducciones en la probabilidad o consecuencia de un riesgo.	En las evaluaciones anuales, se revisa las reducciones en probabilidad o consecuencia.	2	Ya se encuentra implementada.
Comparar los beneficios y costos luego del tratamiento contra los beneficios actuales.	No se realiza un análisis de costo beneficio después de los tratamientos.	0	No se implementará en esta oportunidad debido al nivel de madurez del riesgo.

#### 4.3.8. Monitoreo y Revisión

En la Tabla 40, se puede apreciar el análisis de brechas en el proceso de monitoreo y revisión de riesgos entre la situación deseada contra la actual, obteniéndose un cumplimiento óptimo de 98%.

**Tabla 40 Análisis de brechas - Monitoreo y revisión**

Actividades	Situación Real	Valor	Implementación
-------------	----------------	-------	----------------

Determinar el aseguramiento de riesgos para la organización.	Se realiza el monitoreo de la evaluación de los riesgos.	2	Ya se encuentra implementada.
Evaluar el ambiente interno de control.	Se evalúa el ambiente de control con los dueños de procesos.	2	Ya se encuentra implementada.
Desarrollar planes de monitoreo de riesgos para cada KPI y KRI.	Se desarrollan controles para los indicadores principales.	2	Ya se encuentra implementada.
Desarrollar planes de monitoreo de tratamiento y control para riesgos críticos.	Se cuenta con un monitoreo; sin embargo, el mismo es manual.	1	Se implementará un software para apoyo en la gestión de dicha tarea.
Identificar al personal responsable de monitoreos y revisar los KPI's, KRI's, aseguramiento del riesgo y tratamiento del riesgo.	Se cuentan con los responsables de cada riesgos definido, de igual forma se realiza el seguimiento a su gestión.	2	Ya se encuentra implementada.
Identificar al personal independiente responsable de monitorear, reportar los umbrales de riesgos, cambios en el contexto, aseguramiento del riesgo, frecuencia de monitoreo, etc.	Se cuenta con el apoyo de una consultora tercera para ítems nombrados.	2	Ya se encuentra implementada.
Revisar los umbrales de límites en los KPI's y KRI's	Se revisan los indicadores mensualmente en el comité de gerencia de la organización.	2	Ya se encuentra implementada.
Diseñar el monitoreo de riesgos y la notificación de desviaciones, variaciones, infracciones y otros eventos importantes a las partes interesadas, clientes y partes interesadas.	Se comunican las desviaciones en los riesgos en los comités internos como en los comités con stakeholders.	2	Ya se encuentra implementada.
Identificar problemas de riesgo recurrentes y soluciones basadas en responsabilidad, rango de control, delegación de autoridades y responsabilidades de monitoreo.	Se identifican los riesgos recurrentes en los distintos procesos y se plantean controles estandarizados para los mismos.	2	Ya se encuentra implementada.
Desarrollar ejemplos de dashboards de monitoreo y reportes a stakeholders, clientes, y partes interesadas específicas.	Se cuenta con dashboards y estadísticas de indicadores presentados a stakeholders y partes interesadas.	2	Ya se encuentra implementada.
Controlar el aumento de KPI's y KRI's y responda a los cambios y riesgos.	Se controlan los indicadores y en base a ello, se implementan controles.	2	Ya se encuentra implementada.
Asegurar que los umbrales de riesgo sean realistas o si necesitan ser modificados.	Se revisan anualmente los umbrales de riesgo de la organización,	2	Ya se encuentra implementada.
Revisar tendencias o cambios en los umbrales de riesgo.	Se revisan los cambios de umbrales de riesgo en el sector de forma anual.	2	Ya se encuentra implementada.
Recomendar tratamiento si los eventos de riesgo o incumplimiento puedan ocurrir.	El área de apoyo SIG recomienda tratamientos para los riesgos a los dueños de proceso.	2	Ya se encuentra implementada.
Comunicar incumplimientos, tendencias o requerimientos	Cuando existan incumplimiento o requerimientos inusuales se	2	Ya se encuentra implementada.

inusuales que requieran acciones correctivas.	solicitan acciones correctivas.		
Comunicar tratamiento para cambios en los perfiles de riesgo, contextos, apetito de riesgo, tolerancia, consecuencia y probabilidad.	Cuando ocurre un cambio en alguno de dichos puntos, es comunicado a las partes interesadas mediante reuniones.	2	Ya se encuentra implementada.
Monitorear si los riesgos pueden desencadenar en cascada, espacios en blanco, dependencia o interdependencia.	No se monitorean los riesgos en cascada, dependencia ni interdependencias.	2	Ya se encuentra implementada.
Apoyar a los dueños de riesgos a identificar los umbrales de KPI's y KRI's.	Se encuentran identificados los umbrales de indicadores.	2	Ya se encuentra implementada.
Grabar y analizar los eventos de riesgo, falta de cumplimiento de objetivos, casi fallas, amenazas, peligros, y sorpresas.	Se registran dichos cambios en las matrices de gestión de riesgos.	2	Ya se encuentra implementada.
Proveer una descripción del evento o riesgo e identificar a la persona responsable de su seguimiento, análisis e identificación del síntoma, causa raíz, acción correctiva, controles y tratamiento.	Se analiza todos los ítems descritos y se registran en las matrices de riesgo.	2	Ya se encuentra implementada.
Documentar y analizar los eventos de riesgo.	Se registran en la matriz de riesgos.	2	Ya se encuentra implementada.
Determinar acciones correctivas a ser tomadas.	Se registran en la matriz de riesgos.	2	Ya se encuentra implementada.
Revisar los eventos de riesgo, amenazas, peligros para acciones correctivas eficaces y eficientes.	Se registran en la matriz de riesgos.	2	Ya se encuentra implementada.
Revisar acciones correctivas y proveer el input y la guía necesaria.	Se revisan las acciones correctivas entre los dueños de procesos y el área SIG.	2	Ya se encuentra implementada.
Elevar a los dueños de riesgo para tratamiento adicionales en el caso de los riesgos crónicos, sistémicos o materiales.	Se elevan los tratamientos cuando el nivel del riesgo asociado es crítico o importante.	2	Ya se encuentra implementada.
Preparar diariamente, semanalmente, mensualmente, cuatrimestralmente y anualmente reportes de riesgo.	Se reportan los riesgos de forma mensual y a la vez de forma anual.	2	Ya se encuentra implementada.
Preparar reportes basados en eventos de riesgo inesperados y peligros.	Cuando hay un riesgo o peligro inesperado estos son reportados en los comités correspondientes.	2	Ya se encuentra implementada.
Notar si los cambios impactarán a stakeholders, clientes y partes interesadas.	Se realiza la Gestión del Cambio, evaluando los riesgos y su impacto en las partes interesadas.	2	Ya se encuentra implementada.
Revisar y reforzar las acciones correctivas a través de toda la organización y todas las funciones.	La analista de aseguramiento de l calidad revisa y refuerza las acciones correctivas planteadas.	2	Ya se encuentra implementada.

### 4.3.9. Grabación e informes

En la Tabla 41, se puede apreciar el análisis de brechas en el proceso de grabación e informes de riesgos entre la situación deseada contra la actual, obteniéndose un cumplimiento bueno de 84%.

**Tabla 41 Análisis de brechas - Grabación e informes**

Actividades	Situación Real	Valor	Implementación
Revisar los resultados críticos para informar a los niveles de la empresa.	Se informan los riesgos con un nivel inaceptable.	2	Ya se encuentra implementada.
Registrar los resultados de las actividades críticas incluyendo el alcance de los objetivos.	Se registran los resultados de dichas actividades.	2	Ya se encuentra implementada.
Informar los resultados de RBPS y RBDM.	Se informan los resultados de los monitoreos y auditorías realizadas.	2	Ya se encuentra implementada.
Métodos de registro para los stakeholders y partes interesadas nuevas.	No se cuenta con métodos de registro de riesgos.	0	Se contará con un registro de riesgos que podrá ser presentado a las partes interesadas.
Revisar e informar sobre KPI's, KRI's y objetivos.	Se revisan e informan dichos indicadores en los comités de alta gerencia.	2	Ya se encuentra implementada.
Revisar el costo, la frecuencia y la puntualidad de la presentación de informes a interesados específicos.	Los interesados específicos que revisan dichos informes es el área SIG.	2	Ya se encuentra implementada.
Revisar la idoneidad de los métodos de reporte	Se necesita llevar un registro automatizado de reportes.	1	Se implementará un software para el apoyo en dicha tarea.
Determinar nuevos métodos de reporte.	Se determinan nuevos métodos de acuerdo a requerimientos.	2	Ya se encuentra implementada.
Compartir información sobre las mejoras en la gestión de riesgos.	Se comparten las mejoras con los dueños de proceso.	2	Ya se encuentra implementada.
Informar a la junta de directores el logro de objetivos y riesgos claves.	Se informan dichos puntos en los comités semanales de gerencia.	2	Ya se encuentra implementada.
Determinar los requisitos reglamentarios y de cumplimiento para informar datos.	Se cuentan con los requisitos en una matriz.	2	Ya se encuentra implementada.
Enviar reportes reglamentarios y de cumplimiento a tiempo.	Se envían dichos reportes.	2	Ya se encuentra implementada.
Apoyar a la gerencia ejecutiva en los informes	En los comités de riesgos se analiza en conjunto con el área ejecutiva los riesgos de mayor impacto.	2	Ya se encuentra implementada.
Revisar una posible cascada, interdependencia, dependencia, y material de riesgo.	No se revisa dicha interdependencia.	0	Debido a la madurez del riesgo, aún no será implementada.
Revisar el costo / beneficio de la extensión y el tipo de informe	Se evalúan los costos de impacto de los riesgos críticos e importantes en el comité anual de Gestión de Riesgos.	2	Ya se encuentra implementada.

Determinar si se requiere de alguna garantía especial para informar.	No aplica.	.	.
Revisar que los reportes sean adecuados basándose en los objetivos organizacionales, solución de problemas y toma de decisiones.	Los reportes son adecuados.	2	Ya se encuentra implementada.

#### ***4.4. Aplicación de las actividades pendientes***

En el presente capítulo se desarrollarán los puntos pendientes establecidos en el análisis de brechas del capítulo anterior. Uno de los factores importantes a considerar es que solo se desarrollarán aquellos que se encuentran alineados a la madurez de la gestión de riesgos de la organización, por ello, se presentan los puntos a implementar:

- Política de gestión de riesgos: esta política deberá incluir los esfuerzos de la Junta Directiva por apoyar la Gestión de Riesgos en la organización, incluir el cumplimiento de los principios propuestos por la normativa, esta deberá ser publicada en todos los ambientes de la organización.
- Matriz de comunicación: se desarrollará la matriz de comunicación con los distintos entes involucrados en la gestión de riesgos de la organización.
- Portafolio de Riesgos: Se establecerá los riesgos por Sistema de Gestión al cual afectan.
- Software para el proceso de gestión de riesgos: Se presentará una comparación de 3 software para la gestión de riesgos, estos deberán incluir la comparación de riesgos mediante mapas de calor

##### ***4.4.1. Política de gestión de riesgos***

A continuación, se establecerá la política de gestión de riesgos de la organización, esta deberá ser revisada y aprobada por el gerente general. Posterior a ello, será publicada en diversos espacios en las instalaciones y difundida al personal de la organización:

## **POLÍTICA DE GESTIÓN DE RIESGOS**

Objetivo principal de la gestión de riesgos:

Reducción de los efectos negativos ante la materialización de riesgos en la empresa.

Principios principales de Gestión de Riesgos

1. El proceso de gestión de riesgos es una parte integral del sistema de gestión de la EMPRESA;
2. La gestión de riesgos es una función obligatoria para todos los empleados de la COMPAÑÍA;
3. El desarrollo de medidas de reducción de riesgos internos o externos debe ser documentado;
4. El propósito de la gestión de riesgos es identificar y prevenir posibles pérdidas y, en segundo lugar, minimizar las consecuencias de ese riesgo;
5. La gestión de riesgos en la empresa significa la aplicación de un enfoque unificado y estandarizado para la identificación, evaluación y gestión de riesgos.
6. Los administradores de todos los niveles son responsables de la identificación y evaluación oportuna de los riesgos, el desarrollo de las medidas de gestión de riesgos y la comunicación de los mismos.
7. El sistema de motivación de los empleados en la COMPAÑÍA tiene en cuenta la efectividad de la gestión de riesgos;
8. LA COMPAÑÍA se adhiere a un equilibrio razonable entre la gestión del riesgo y el monto potencial incurrido por la ocurrencia del riesgo. LA COMPAÑÍA no puede tomar ninguna medida adicional para reducir el riesgo si el nivel de riesgo está dentro de los límites del riesgo;
9. LA COMPAÑÍA asegura el conocimiento de los riesgos a los colaboradores, incluyendo el análisis de los mismos;
10. La coordinación del sistema de gestión de riesgos de la empresa es realizado por el EMPLEADO;
11. La responsabilidad de la formulación, función y eficacia de la gestión de riesgos recae en el Director General de la EMPRESA.

---

Gerente general de la compañía

#### 4.4.2. Registro de riesgos – Portafolio

Como parte del cumplimiento de la metodología, se establece un portafolio de riesgos para cada una de las normativas que puedan ser afectadas (Calidad, Seguridad, Medio Ambiente, Antisoborno, SMS, entre otras).

**Tabla 42 Registro de Peligros y Riesgos de SST**

Listas de Peligros y Riesgos					
CO D	TIPO	PELIGROS	RIESGOS		CONSECUENCIA
			Seguridad	Salud	
L1	LOCATIVO	Deficiencias en el suelo (huecos, rajaduras y desniveles en el piso)	Caídas al mismo nivel, golpes, tropezones, detención de equipos en su operación		Lesiones en diferentes partes del cuerpo, daño de equipos e infraestructura.
L2	LOCATIVO	Objetos en el suelo (cajas vacías, Bolsas, cajas llenas, papeles, objetos)	Caídas al mismo nivel, golpes, tropezones, resbalones		Lesiones en diferentes partes del cuerpo.
L3	LOCATIVO	Líquidos en el suelo	Caídas al mismo nivel, golpes, tropezones, resbalones.		Lesiones en diferentes partes del cuerpo.
L4	LOCATIVO	Superficies en mal estado u obstruidos	Caídas al mismo nivel, golpes, tropezones, resbalones, cortes, detención del apilador		Lesiones en diferentes partes del cuerpo, daño de equipos e infraestructura.
L5	LOCATIVO	Malos apoyos de anaqueles, estructuras deformadas	Caídas al mismo nivel, golpes, cortes, heridas.	Infección por herida	Lesiones en diferentes partes del cuerpo, daño de equipos e infraestructura.
L6	LOCATIVO	Falta de Orden y Limpieza	Aplastamiento, golpes, caídas a nivel		Lesiones en diferentes partes del cuerpo.
L7	LOCATIVO	Objetos encima o suspendido en o por equipos, muebles o infraestructura	Caída de objetos		Lesiones en diferentes partes del cuerpo.
L8	LOCATIVO	Manipulación de Objetos encima de equipos o infraestructura	Caída de Objetos de altura		Lesiones en diferentes partes del cuerpo.

L9	LOCATIVO	Transporte inadecuado de carga y ULD	Caída de Objetos, atrapamiento, aplastamiento, arrastre		Lesiones en diferentes partes del cuerpo.
L10	LOCATIVO	Superficies resbaladizas	Caída a nivel		Lesiones en diferentes partes del cuerpo.
L11	LOCATIVO	Fuga de Humo	Contaminación por humo, asfixia	Asfixia por inhalación	Daño al sistema respiratorio
L12	LOCATIVO	Carga en altura, o almacenados en pasadizos en segundo piso y en las escaleras	Caída de Objetos de altura		Lesiones en diferentes partes del cuerpo, incapacidad permanente, Muerte
L13	LOCATIVO	Condición Subestándar (Estructuras de concreto en mal estado)	Desprendimiento, caída de la infraestructura		Lesiones a distintas partes del cuerpo/muerte
L14	LOCATIVO	Condición Subestándar (Infraestructura en mal estado)	Desprendimiento, caída de la infraestructura		Lesiones a distintas partes del cuerpo/muerte
L15	LOCATIVO	Espacio reducido de trabajo	Atrapamiento, caída a nivel o desnivel		Lesiones a distintas partes del cuerpo
M1	MECÁNICO	Objetos, estante no asegurado	Caída de objetos		Lesiones a distintas partes del cuerpo
M2	MECÁNICO	Condición Subestándar (Luminarias mal fijadas o fijadas de manera deficiente, sin protección)	Caída de objetos	Potencial TEC (traumatismo encéfalo craneano)	Lesiones a distintas partes del cuerpo
M3	MECÁNICO	Herramientas, equipos y/o partes no aseguradas	Desprendimiento, caída de objetos, atrapamiento, raspones.		Lesiones a distintas partes del cuerpo
M4	MECÁNICO	Material punzo cortante	Cortes	Infección por herida	Heridas, deterioro de la salud
M5	MECÁNICO	Equipos (de transmisión) o partes de movimiento	Atrapamiento, atropello, arrastre		Lesiones a distintas partes del cuerpo/muerte
M6	MECÁNICO	Potencial desprendimiento o de techos	Caída de objetos	Potencial TEC (traumatismo encéfalo craneano)	Lesiones a distintas partes del cuerpo/muerte

M7	MECÁNICO	Condición Subestándar (Vehículos/ Equipos en mal estado)	Atrapamiento, atropello, arrastre		Lesiones a distintas partes del cuerpo.
M8	MECÁNICO	Vehículos en movimiento (maquinaria liviana, pesada, grúa, etc.).	Atrapamiento, atropello, arrastre		Lesiones a distintas partes del cuerpo/muerte
M9	MECÁNICO	Exposición a vehículos en movimiento	Atrapamiento, atropello, arrastre		Lesiones a distintas partes del cuerpo/muerte
M10	MECÁNICO	Uso de escalera	Caída a desnivel		Lesiones a distintas partes del cuerpo.
M11	MECÁNICO	Trabajo en altura	Caída a desnivel		Lesiones a distintas partes del cuerpo/muerte
M12	MECÁNICO	Turbina de aeronave en rotación	Succión / expulsión por turbina		Lesiones a distintas partes del cuerpo/muerte
M13	MECÁNICO	Uso de herramientas	Corte, atrapamiento, golpe		Lesiones a distintas partes del cuerpo
M14	MECÁNICO	Traslado de cargas	Corte, atrapamiento, golpe		Lesiones a distintas partes del cuerpo
M15	MECÁNICO	Trabajos en profundidad	Caída a desnivel		Lesiones a distintas partes del cuerpo/muerte
M16	MECÁNICO	Compresores	Explosión o implosión		Lesiones a distintas partes del cuerpo/muerte
M17	MECÁNICO	Partículas en proyección	Exposición a partículas en proyección		Lesiones a distintas partes del cuerpo
Q1	QUIMICOS	Sustancias irritantes o alergizantes	Contaminación corporal	Contaminación corporal	Alergias, quemaduras
Q2	QUIMICOS	Sustancias asfixiantes	Inhalación	Inhalación	Asfixia por inhalación
Q3	QUIMICOS	Sustancias tóxicas	Intoxicación	Intoxicación	Deterioro de la salud, muerte

Q4	QUIMICOS	Manipulación y almacenamiento de materiales peligrosos	Atrapamiento, golpes	Contaminación corporal	Lesiones a distintas partes del cuerpo/deterioro de la salud/ muerte.
EL 1	ELÉCTRICO	Baja Tensión (cables expuestos y cableado sin cierre y mal diseñado, Caja ciega en deteriorada)	Descarga eléctrica		Quemadura I grado, Shock Eléctrico,
EL 2	ELÉCTRICO	Baja Tensión (cableado expuesto en zona de tránsito y/o en lugar de reposo de pies/piernas)	Descarga eléctrica		Quemadura I grado, Shock Eléctrico,
EL 3	ELÉCTRICO	Sistema contra incendios inhabilitado	Incendio		Quemaduras
EL 4	ELÉCTRICO	Contacto con energía eléctrica directa/ indirecta	Descarga eléctrica		Quemaduras, shock Eléctrico
EL 5	ELÉCTRICO	Equipo energizado sin protección o aislamiento	Descarga eléctrica		Quemaduras, shock Eléctrico
EL 6	ELÉCTRICO	Manipulación de equipos energizados (computadora, impresora, otros)	Descarga eléctrica		Quemadura I grado, Shock Eléctrico,
FQ 1	FISICO QUIMICO	Sustancias inflamables.	Explosión, Incendio		Quemadura, lesiones a distintas partes del cuerpo
FQ 2	FISICO QUIMICO	Acumulación de material combustible	Incendio		Quemadura, lesiones a distintas partes del cuerpo
FQ 3	FISICO QUIMICO	Manipulación y trasvase de productos inflamables	Explosión, incendio.	Ingesta o inhalación	Intoxicación, asfixia, alergias, problemas dermatológicos.
FQ 4	FISICO QUIMICO	Focos de ignición	Explosión, incendio	Ingesta o inhalación	Intoxicación, asfixia, alergias, problemas dermatológicos.

F1	FISICOS	Fuentes Radioactivas Niveles superiores a límites permitidos		Exposición prolongada o breve	Lesión o Enfermedad por metabolismo de células malignas
F2	FISICOS	Radiación UV		Exposición Prolongada	Lesión o Enfermedad a la vista, piel
F3	FISICOS	Radiación IR		Exposición Prolongada	Lesión o Enfermedad a la vista, piel
F4	FISICOS	PVD (monitores)		Exposición Prolongada	Lesión o Enfermedad a la vista
F5	FISICOS	Sensación de confort: ILUMINACIÓN inadecuada (excesiva)		Deslumbramiento	Lesión o Enfermedad a la vista
F6	FISICOS	Sensación de confort: ILUMINACIÓN inadecuada (deficiente)		Fatiga o sobre esfuerzo visual	Lesión o Enfermedad a la vista
F7	FISICOS	Sensación de confort: Calor (ventilación inadecuada déficit de viento)		Exposición a fuente de calor	Estrés térmico por calor
F8	FISICOS	Sensación de confort: Frío (ventilación excesiva de viento)		Exposición a fuente de frío	Estrés térmico por frío
F9	FISICOS	Exposición al sol		Exposición Prolongada	Lesión a la piel, irritación, alergias, quemaduras, potencial desarrollo de cáncer a la piel
F10	FISICOS	Condición Subestándar (Pisos contaminados con aceite o grasa)	Caida a nivel, golpes, cortes.	Alergias, problemas dermatológicos	Lesión a distintas partes del cuerpo, deterioro de la salud
F11	FISICOS	Material inflamable (papeles, cajas, útiles de escritorio y otros)	Incendio		Quemaduras

F12	FISICOS	Ruido o emisión de ruidos		Exposición a ruido	Lesión auditiva/enfermedad ocupacional: Hipoacusia laboral
F13	FISICOS	Emisión de rayos luminosos por soldadura		Exposición a rayos luminosos por soldadura	Lesión a los ojos: irritación, infecciones, pérdida de capacidad visual
F14	FISICOS	Espacio confinado		Exposición a gases o falta de oxígeno, atrapamiento	Asfixia/sofocación/desmayos /muerte
F15	FISICOS	Vibraciones	Lesiones a distintas partes del cuerpo/enfermedad ocupacional	Devaluación ergonómica.	Lesiones irreversibles a extremidades, columna y sistema nervioso.
F16	FISICOS	Fluidos a presión	Liberación de fluido a presión		Lesiones a distintas partes del cuerpo
F17	FISICOS	Radiación no ionizante		Exposición prolongada	Afecciones a la salud
F18	FISICOS	Superficies calientes		Exposición prolongada o breve	Dermatitis, quemaduras
F19	FISICOS	Humedad	Caída a nivel, golpes, cortes.	Exposición excesiva	Lesiones a distintas partes del cuerpo, afectaciones al sistema respiratorio.
F20	FISICOS	Ventilación deficiente		Sofocación	Afectaciones respiratorias, enfermedades
F21	FISICOS	Ventilación excesiva		Exposición a fuente de frío	Afectaciones respiratorias, enfermedades
B1	BIOLOGICOS	Vegetales exógenos		Contaminación corporal	Intoxicación, enfermedades, infecciones, malestares
B2	BIOLOGICOS	Agentes patógenos en aire, suelo o agua.		Exposición a patógenos en el entorno de trabajo	Intoxicación, enfermedades, infecciones,
B3	BIOLOGICOS	Presencia de vectores, artrópodos, parásitos		Exposición a vectores en el entorno de trabajo	Intoxicación, enfermedades, infecciones,
B4	BIOLOGICOS	Presencia de animales agresores	Agresión física	Exposición a enfermedades	Intoxicación, enfermedades, infecciones, malestares. Lesión a distintas partes del cuerpo
B5	BIOLOGICOS	Virus		Exposición a virus	Afecciones a la salud

B6	BIOLOGICOS	Hongos		Exposición a hongos	Lesiones a la piel, afecciones a la salud.
B7	BIOLOGICOS	Residuos médicos		Contaminación corporal	Afecciones a la salud
B8	BIOLOGICOS	Mordedura/Picadura de insectos		Exposición a enfermedades	Lesiones a la piel, afecciones a la salud.
B9	BIOLOGICOS	Bacterias, gérmenes		Exposición a bacterias, gérmenes	Afecciones a la salud
B10	BIOLOGICOS	Mordedura de animales (perros, murciélagos)		Exposición a enfermedades	Afecciones a la salud
B11	BIOLOGICOS	Manipulación de residuos sólidos	Cortes diversos	Contaminación corporal	Infecciones, Lesiones a la piel, afecciones a la salud. Lesión a distintas partes del cuerpo
B12	BIOLOGICOS	Manipulación de residuos fecales		Contaminación corporal	Alergias, afecciones a la salud
B13	BIOLOGICOS	Exposición a personas enfermas o restos humanos		Contaminación corporal	Afecciones a la salud
B14	BIOLOGICOS	Manejo / exposición a fluidos corporales (sangre, saliva, etc.)		Contaminación corporal	Infecciones, afecciones a la salud
E1	ERGONOMICO	Mobiliario No Ergonómico (inadecuado para el puesto de trabajo)	Lesiones a distintas partes del cuerpo	Disergonomico	Enfermedad ocupacional: (ergonómica). Lumbalgias, escoliosis.
E2	ERGONOMICO	Inadecuada altura de Pantalla de monitor (muy baja)		Disergonomico	Enfermedad ocupacional: Devaluación ergonómica. Lumbalgias, escoliosis, problemas / dolores en articulaciones / dolores de cabeza, tendinitis
E3	ERGONOMICO	Inadecuada altura de Pantalla de monitor (muy alta)		Disergonomico	Enfermedad ocupacional: Devaluación ergonómica. Lumbalgias, escoliosis, problemas / dolores en articulaciones / dolores de cabeza, tendinitis

E4	ERGONOMICO	Exceso de iluminación desde detrás de pantalla de monitor (ubicación inadecuada: v-m-p)		Disergonomico	Deslumbramiento – Lesión o Enfermedad por Exposición Prolongada
E5	ERGONOMICO	Reflejo por iluminación en pantalla de monitor (ubicación inadecuada: p-m-v)		Disergonomico	Fatiga o sobre esfuerzo visual. Lesión o Enfermedad por Exposición Prolongada a la vista
E6	ERGONOMICO	Silla inadecuada para la actividad / no ergonómica / en mal estado		Disergonomico	Enfermedad ocupacional por exposición prolongada: Devaluación ergonómica. Lumbalgias, escoliosis, problemas / dolores en articulaciones. Dolor en las cervicales, lumbagos o problemas de disco
E7	ERGONOMICO	Disconfort por Silla semiergonómica – No regula altura de apoyo a brazos –apoyo cómodo del codo, en una caída relajada de ambos brazos a los lados del cuerpo.		Disergonomico	Fatiga o sobre esfuerzo por postura incómoda. Lesiones a muñecas, mala circulación (adormecimiento de dedos, manos, brazos), tendinitis, contracturas, dolor en las cervicales
E8	ERGONOMICO	Disconfort por Silla semiergonómica – No se regula distancia entre cojín, respaldar, largo de muslo.		Disergonomico	Presión sobre los vasos sanguíneos de los muslos, entumecimiento de las piernas, las venas varicosas.
E9	ERGONOMICO	Disconfort por uso de Silla – ALTURA mínima – persona requiere apoyo para pies		Disergonomico	Presión sobre los vasos sanguíneos de los muslos, entumecimiento de las piernas, las venas varicosas.

E9	ERGONOMICO	Disconfort por uso de Silla muy pequeña para persona alta / no se puede regular altura		Disergonómico	Presión sobre los vasos sanguíneos de los muslos, entumecimiento de las piernas, las venas varicosas.
E10	ERGONOMICO	Silla no adecuada para el trabajo (respaldar grande sin apoyo a zona lumbar)		Disergonómico	Enfermedad ocupacional por exposición prolongada: Devaluación ergonómica Lumbalgias, escoliosis, problemas / dolores en articulaciones. Dolor en las cervicales, lumbagos o problemas de disco
E11	ERGONOMICO	Inadecuado uso de silla ergonómica o semi-ergonómica		Disergonómico	Enfermedad ocupacional por exposición prolongada: Devaluación ergonómica. Lumbalgias, escoliosis, problemas / dolores en articulaciones. Presión sobre los vasos sanguíneos de los muslos, entumecimiento de las piernas, las venas varicosas.
E13	ERGONOMICO	Esfuerzos por empujar o tirar de objetos	Lesiones a distintas partes del cuerpo	Disergonómico	Enfermedad ocupacional por exposición prolongada: Devaluación ergonómica. Lumbalgias, escoliosis, problemas / dolores en articulaciones
E14	ERGONOMICO	Esfuerzos por el uso de herramientas		Disergonómico	Enfermedad ocupacional: Devaluación ergonómica. Lumbalgias, escoliosis, problemas / dolores en articulaciones
E15	ERGONOMICO	Esfuerzos por manipulación de cargas		Disergonómico	Enfermedad ocupacional: Devaluación ergonómica. Lumbalgias, escoliosis, problemas / dolores en articulaciones
E16	ERGONOMICO	Movimientos repetitivos		Disergonómico	Enfermedad ocupacional por exposición prolongada: Devaluación ergonómica. Lumbalgias, escoliosis, problemas / dolores en articulaciones
E17	ERGONOMICO	Movimientos bruscos		Disergonómico	Enfermedad ocupacional por exposición prolongada: Devaluación ergonómica. Lumbalgias, escoliosis, problemas / dolores en articulaciones

E18	ERGONOMICO	Posturas Inadecuadas		Disergonómico	Síndrome del túnel carpiano
E19	ERGONOMICO	Uso de mouse, teclado y computadora		Disergonómico	Enfermedad ocupacional por exposición prolongada: Devaluación ergonómica. Lumbalgias, escoliosis, problemas / dolores a tendones
PS1	PSICOSOCIAL	Personal agresivo	Agresión física/verbal	Estrés laboral, síndrome de burnout	Trastornos físicos, psíquicos, conductual
PS2	PSICOSOCIAL	Acoso (mobbing)		Estrés laboral.	Trastornos físicos, psíquicos, conductual, renuncia del trabajador
PS3	PSICOSOCIAL	Contenido de la tarea (monotonía, repetitividad, insatisfacción)		Estrés laboral, síndrome de burnout	Trastornos físicos, psíquicos, conductual
PS4	PSICOSOCIAL	Relaciones humanas (Deficiencia en la jerarquía, función, participación)		Estrés laboral, fatiga, cansancio, peleas	Trastornos físicos, psíquicos, conductual
PS5	PSICOSOCIAL	Organización del tiempo de trabajo (Deficiencia en el ritmo, pausas, turnos y/o recarga de trabajo)		Estrés laboral, fatiga, somnolencia	Trastornos físicos, psíquicos, conductual
PS6	PSICOSOCIAL	Gestión del personal (falta de liderazgo y/o motivación)		Estrés laboral, fatiga, cansancio, peleas	Trastornos físicos, psíquicos, conductual, renuncia del trabajador
PS7	PSICOSOCIAL	Carga mental		Estrés laboral, fatiga, cansancio	Trastornos físicos, psíquicos, conductual
PS8	PSICOSOCIAL	Insatisfacción laboral		Estrés laboral, fatiga, cansancio	Trastornos físicos, psíquicos, conductual, renuncia del trabajador
PS9	PSICOSOCIAL	Inestabilidad laboral		Estrés laboral, síndrome de burnout	Trastornos físicos, psíquicos, conductual
PS10	PSICOSOCIAL	Comunicación deficiente y falta de desarrollo profesional		Estrés laboral, síndrome de burnout	Trastornos físicos, psíquicos, conductual, renuncia del trabajador

FN 1	FENÓMENOS NATURALES/ CONDICIONES CLIMÁTICAS – GEOGRÁFICAS	Inundaciones	Exposición a desastre natural		Lesiones a distintas partes del cuerpo / muerte
FN 2	FENÓMENOS NATURALES/ CONDICIONES CLIMÁTICAS – GEOGRÁFICAS	Terremotos / Tsunami	Exposición a desastre natural		Lesiones a distintas partes del cuerpo / muerte
FN 3	FENÓMENOS NATURALES/ CONDICIONES CLIMÁTICAS – GEOGRÁFICAS	Huaycos, derrumbes	Exposición a desastre natural		Lesiones a distintas partes del cuerpo / muerte
FN 4	FENÓMENOS NATURALES/ CONDICIONES CLIMÁTICAS – GEOGRÁFICAS	Lluvia		Exposición a fenómeno natural	Afecciones a la salud
FN 5	FENÓMENOS NATURALES/ CONDICIONES CLIMÁTICAS – GEOGRÁFICAS	Neblina		Exposición a fenómeno natural	Afecciones a la salud

**Tabla 43 Lista de Peligros y Riesgos Ambientales**

Aspectos Ambientales	Código	Impacto Ambiental
<b>Residuos peligrosos</b> (baterías, pilas, líquidos inflamables, explosivos, carburantes, desperdicio de los EPP, efluentes, entre otros)	AA-01	Generar gran volumen de residuos peligrosos (baterías, pilas, líquidos inflamables, explosivos, carburantes, desperdicio de los EPP, efluentes, entre otros)
		Contaminación del suelo y aguas subterráneas debido a los residuos peligrosos (baterías, pilas, líquidos inflamables, explosivos, carburantes, desperdicio de los EPP, efluentes, entre otros) encontrados
<b>Residuos no peligrosos</b> (papeles, madera, vidrio, plástico, tetrapak)	AA-02	Generar gran volumen de residuos no peligrosos (papeles, madera, vidrio, plástico, tetrapak)
<b>Residuos orgánicos</b> (restos de alimentos)	AA-03	Generación de gran volumen de residuos orgánicos (restos de alimentos)
<b>Ruido</b> (equipos motorizados/aeronaves de clientes/equipos de terceros)	AA-04	Generación de ruido ambiental debido a los motores/APU de las aeronaves de nuestros clientes
		Generación de ruido ambiental debido a nuestros equipos motorizados
<b>Emisión de gases contaminantes</b> (equipos motorizados/aeronaves/equipos de terceros)	AA-05	Emisión de gases de nuestros equipos motorizados
		Emisión de gases de aeronaves/equipos de terceros
<b>Uso de recursos naturales</b> (combustibles, madera, agua, consumo de energía, entre otros)	AA-06	Reducción gradual recursos naturales no renovables (energía eléctrica)
		Reducción gradual recursos naturales no renovables (agua)
		Reducción gradual recursos naturales no renovables (petróleo)
<b>Ondas electromagnéticas</b>	AA-07	Generación de ondas electromagnéticas debido al uso de dispositivos móviles
<b>Emisión de rayos X</b>	AA-08	Generación de rayos x, debido al uso de máquinas
<b>Líquidos contaminantes</b> (hidrocarburos, refrigerante, entre otros)	AA-09	Derrame de líquidos peligrosos (combustible, aceite, etc.)
		Derrame de mercancías peligrosas (DGR)

**4.4.3. Softwares para la evaluación de riesgos**

A continuación, se procederá a evaluar herramientas que apoyen en la Gestión de Riesgos dentro de la organización. Se evaluaron 3 softwares, esto debido a que los presentes cumplen con las especificaciones planteadas en el análisis de brechas realizado.

a) Peat's Enterprise risk management & risk registers

Software desarrollado por el doctor Jhonathan Mun, el cual cuenta con las siguientes características:

- ✓ En la Figura 14, se muestra la configuración global de las categorías de indicadores de riesgo (1-5 o 1-10) con codificación de color personalizable de KRI (indicadores clave de riesgo) a través de una matriz de riesgos.
- ✓ División de riesgos. Creación de múltiples divisiones dentro de la empresa, de modo que la empresa puede administrar múltiples perfiles de riesgo para cada división.
- ✓ En la Figura 15, se muestra la taxonomía de riesgo (G.O.P.A.D.). Creación y asignación de G.O.P.A.D. categorías (geográfico, operaciones, productos, actividad o proceso y departamento) de modo que los encargados pueden deslizar y cortar el perfil de riesgo de la empresa desde múltiples puntos de vista, seleccione y cree consultas de G.O.P.A.D. para analizar, etc.
- ✓ En la Figura 17, se muestra la creación de categorías de riesgo personalizadas o utilización de biblioteca de categorías de riesgo predefinidas.
- ✓ Creación de usuarios a cargo de ciertos riesgos, completa con información del contacto (dueños de riesgo).
- ✓ Mapeo de riesgos. Creación y vinculación de categorías de riesgo a una o más G.O.P.A.D. y en una o más divisiones. Esto le permite al encargado la capacidad de ver cómo un cierto riesgo permea a través de la organización y cómo el elemento de riesgo específico puede tocar múltiples departamentos, divisiones, procesos, etc.
- ✓ Creación de múltiples registros de riesgo donde cada registro de riesgo tiene múltiples elementos de riesgo que consisten en causas de riesgo, consecuencias de riesgo, Respuesta a la mitigación de riesgos, Asignaciones de gestores de riesgos, Categoría de riesgo, Estado de riesgo, probabilidad, impacto, indicadores clave de riesgo (KRI), fechas de riesgo (creación, Edición y fechas de vencimiento), Total \$ Niveles de riesgo, Residual \$ Niveles de riesgo, Mitigación Costo, y así sucesivamente.
- ✓ Creación de las siguientes vistas personalizadas del Panel de riesgos completo con informes, cuadrículas de datos, gráficos y visuales, donde los analistas pueden seleccionar de un G.O.P.A.D. específico, División, Categoría de riesgo o Fechas de riesgo: Elementos de riesgo (visualización de KRI y gráficos de Pareto), Mapas de riesgo (mapas de calor de riesgo de recuentos de KRI), Grupos de riesgo (acumulación de riesgo por G.O.P.A.D.), Exposición al riesgo (diales de riesgo y paneles de la categoría seleccionada versus la totalidad Empresa),

Taxonomía de riesgo (vista de arriba hacia abajo para profundizar y ver la estructura de la corporación y sus asociaciones de riesgo, frente a una visión ascendente de cómo un riesgo específico impregna en toda la corporación), Inventario de riesgos (ejecución de consultas SQL para obtener los perfiles de riesgo personalizados y el riesgo informes por división, G.O.P.A.D., categoría de riesgo, fechas de riesgo, etc.), probabilidad de riesgo (calculando PDF y CDF de la probabilidad de un evento de riesgo discreto montos de riesgo continuo o continuo basados en la experiencia histórica)

- ✓ Creación de proyectos de compromiso de riesgo múltiple donde cada uno de las siguientes subsecciones tiene múltiples elementos de riesgo: Riesgos previos al compromiso, riesgos de compromiso, lecciones aprendidas (post-compromiso)
- ✓ Creación personalizada de sus propios diagramas de riesgo con ready-made plantillas en Bowtie Hazard Diagrams, Cause and Effect Ishikawa Fishbone, diagramas detallados, diagramas de influencia, mapas mentales y nodo.
- ✓ Los usuarios pueden crear múltiples diagramas de riesgo personalizados con esta herramienta.
- ✓ Controles de riesgo. Determine si un evento de riesgo específico está bajo control o fuera de control.
- ✓ Pronósticos de riesgo. Utilizando datos de riesgo históricos, los analistas ahora pueden aplicar predicciones modelado para pronosticar futuros estados de riesgo, así como el seguimiento de riesgos, series temporales
- ✓ Previsiones de riesgo, PDF / CDF Probabilidad de ocurrencia, Instantáneas por período y a través del tiempo
- ✓ Mitigación de riesgos. Determinar si una estrategia o técnica específica de mitigación de riesgos es adecuada, desde el punto estadístico. Recopile datos de antes y después de un riesgo. Se implementa la estrategia de mitigación y se determina si existe una estadística diferencia significativa entre los dos.
- ✓ Sensibilidad al riesgo. El análisis de tornados ayuda a identificar los factores críticos de éxito o qué elemento de riesgo es el que más contribuye al perfil de riesgo final de la empresa (o segmento de riesgo) al perturbar estáticamente cada uno de los elementos de riesgo niveles de riesgo financiero
- ✓ Escenarios de riesgo. El análisis de escenarios ayuda a crear múltiples escenarios de riesgo de sus cantidades de riesgo actuales o totales de elementos de riesgo individuales para determinar el impacto en el perfil de riesgo corporativo y crear mapas de calor de escenarios.
- ✓ Simulación de riesgos. supuestos de simulación. Ejecute simulaciones de riesgo de Monte Carlo en sus elementos de riesgo miles a cientos de miles de veces para generar distribuciones probabilísticas y perfiles de riesgo cuantitativos. Resultados de la simulación. Los resultados de la simulación de riesgo de Monte Carlo corren de miles a cientos de miles de veces se presentan como distribuciones de probabilidad y estadísticas momentos, percentiles e

intervalos de confianza. Superposición de resultados. Superponga múltiples perfiles de riesgo uno al lado del otro para determinar sus respectivos Impactos y efectos de incertidumbre en el perfil de riesgo corporativo

- ✓ Análisis de alternativas. Compare los resultados simulados de varios perfiles de riesgo.
- ✓ Sensibilidad dinámica. Identificar la contribución a la varianza y la incertidumbre de cada riesgo. elemento a la corporación, división o G.O.P.A.D. total, así como clasificar e identificar los factores críticos de éxito o qué elemento de riesgo contribuye más al riesgo final perfil cuando se simula en un entorno dinámico.
- ✓ Informes de riesgos. Generación automática de informes y extracción a capacidades de Excel, así como gráficos de Pareto, inventario de riesgos, perfiles de riesgo por división y G.O.P.A.D.

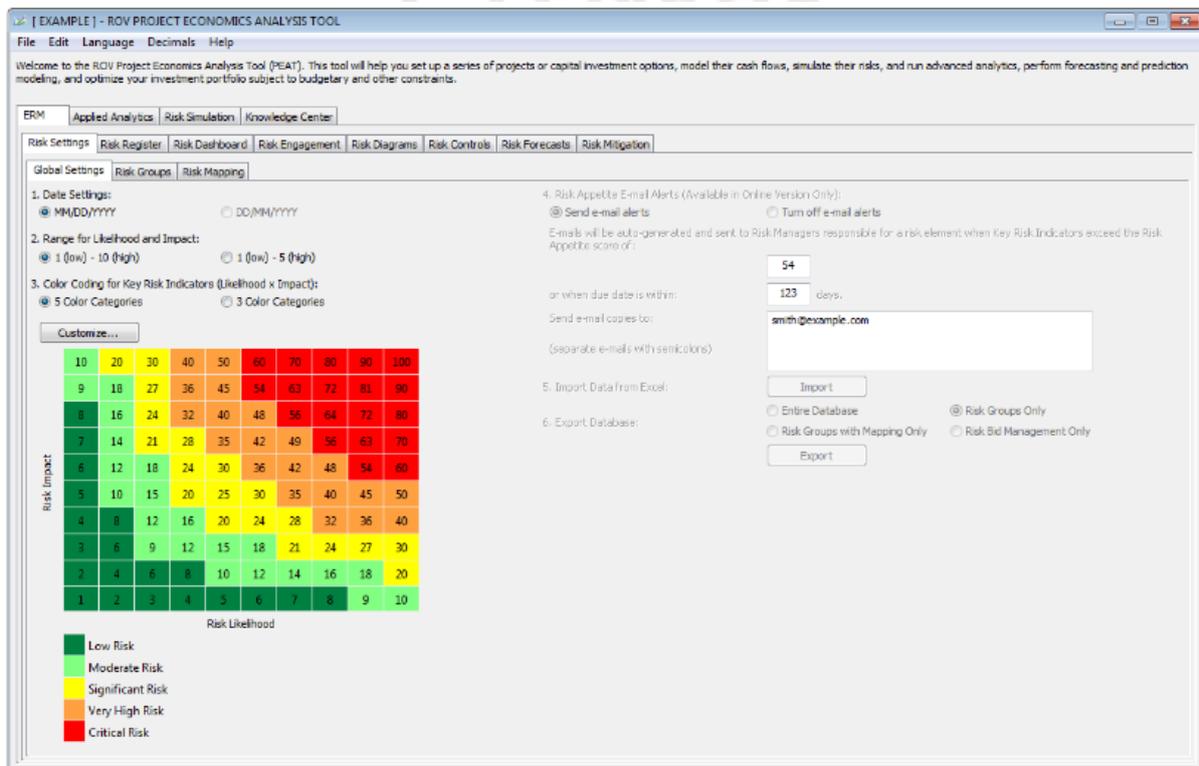


Figura 13 KRI de riesgo: Configuración global de categorías de riesgo

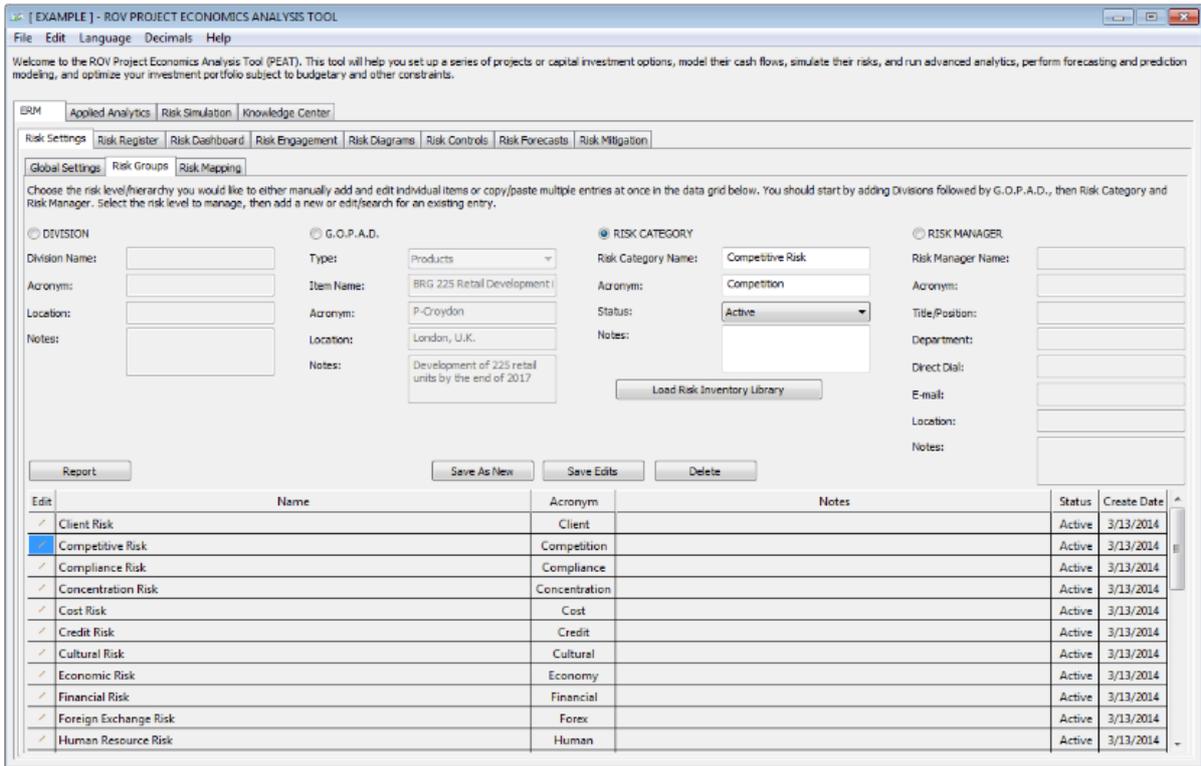


Figura 14 Divisiones de riesgo, riesgo G.O.P.A.D., categorías de riesgo y gestores de riesgo

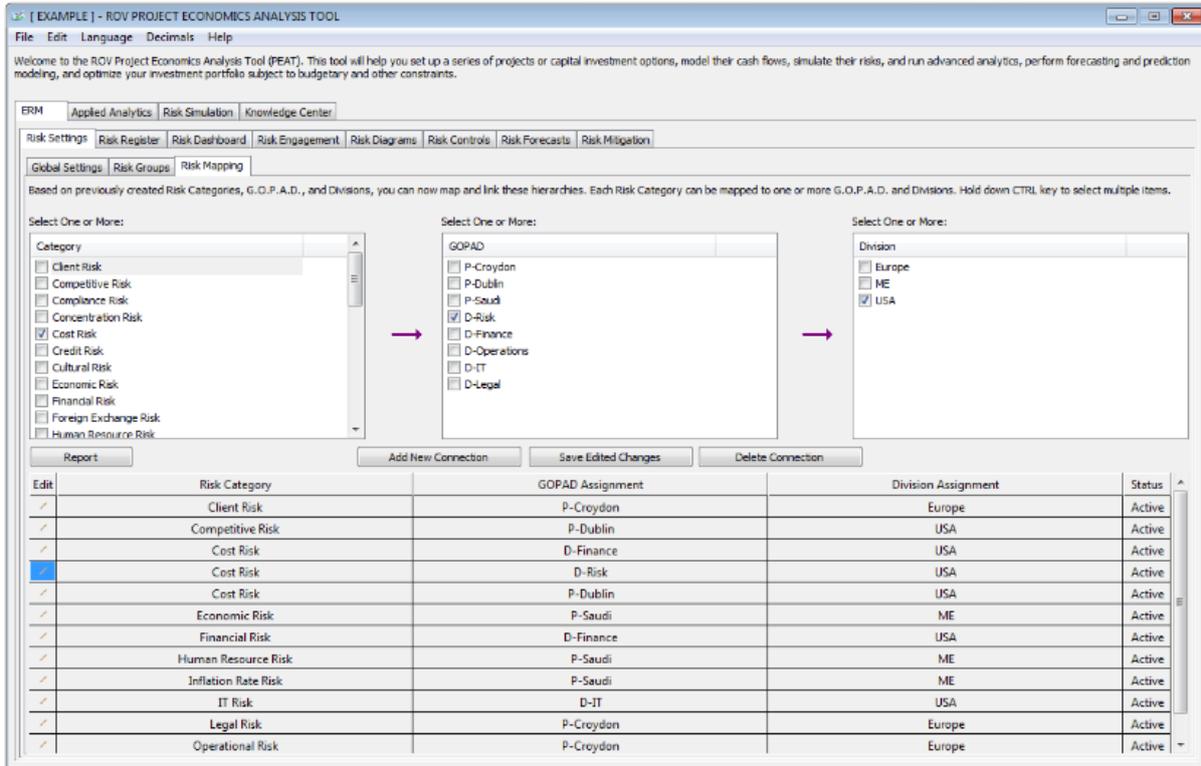


Figura 15 Mapeo de riesgos: Creación y vinculación de categorías de riesgos a una o más G.O.P.A.D. y a una o más divisiones

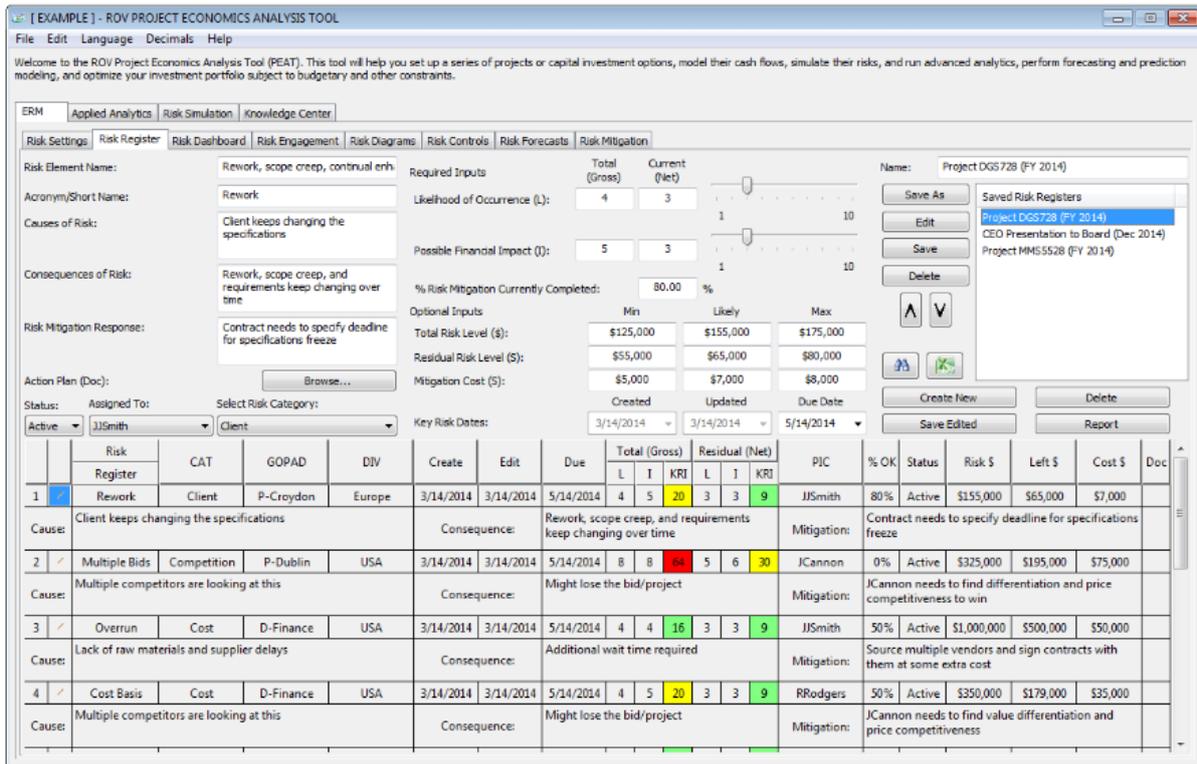


Figura 16 Creación de múltiples registros de riesgo

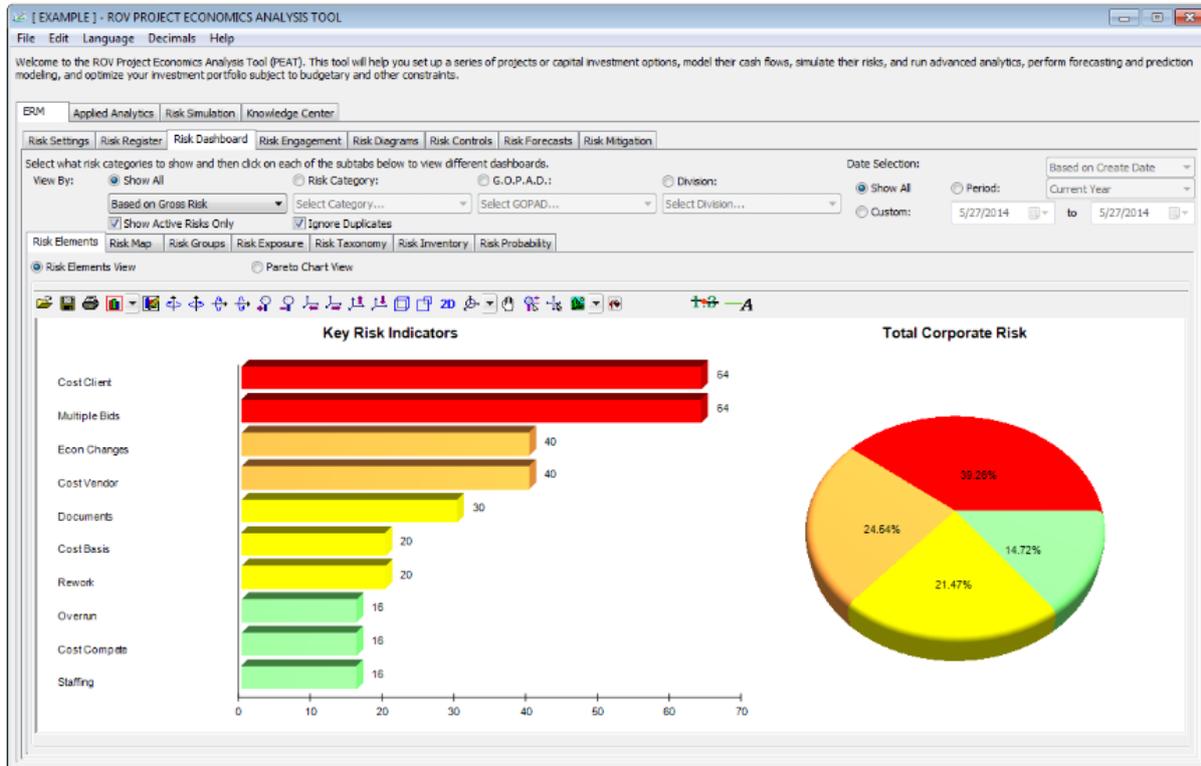


Figura 17 Paneles de riesgo: elementos de riesgo (visualización de KRI's y gráficos de Pareto)



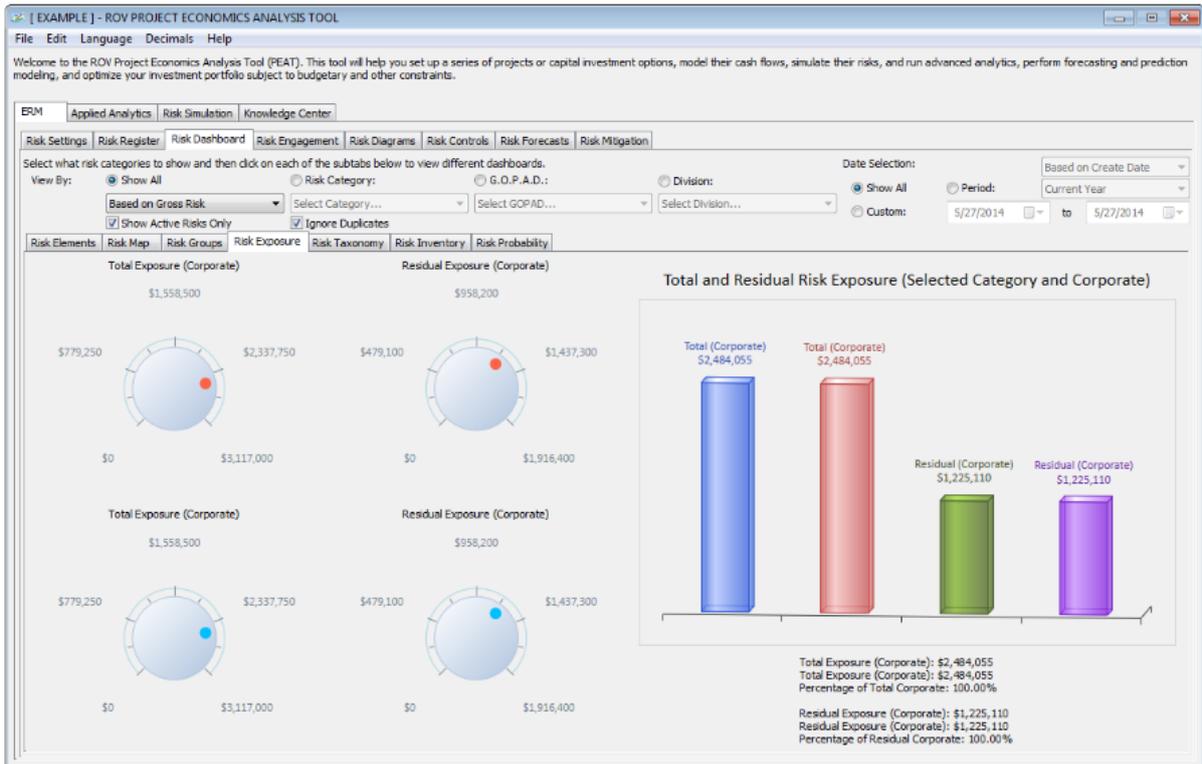


Figura 20 Panel de riesgos: exposición al riesgo (categoría seleccionada versus la empresa)

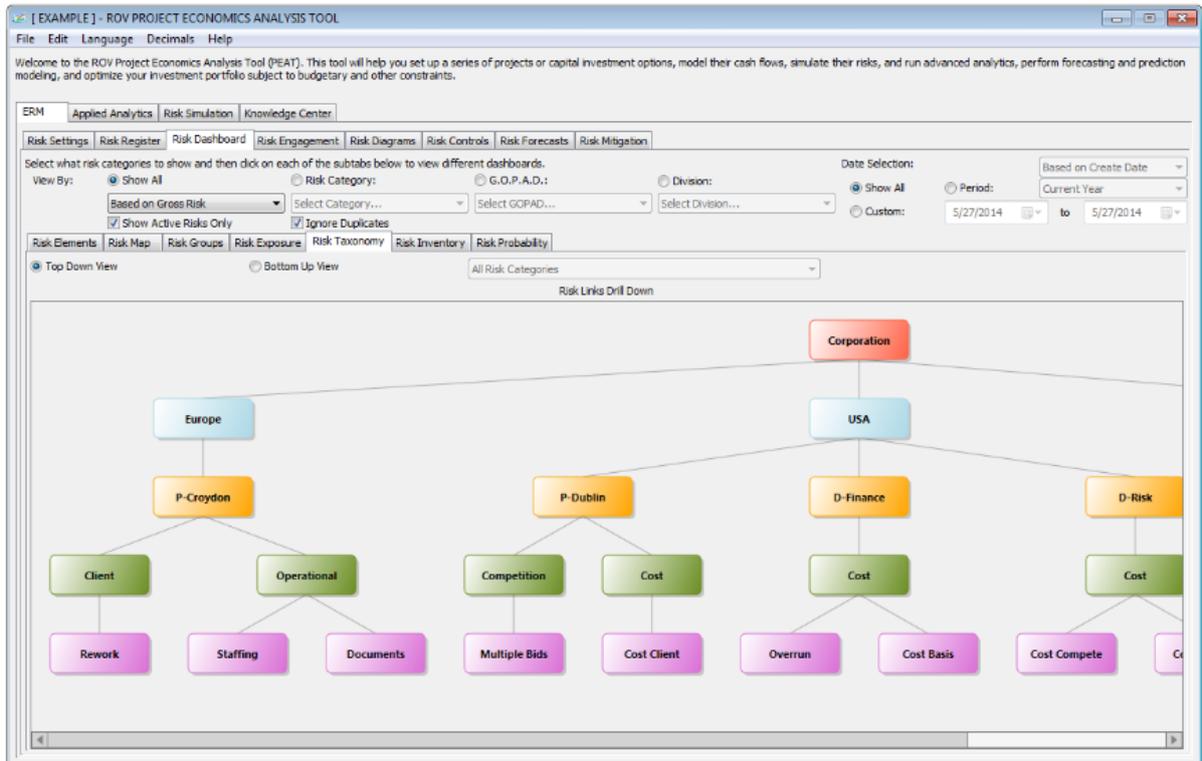


Figura 21 Dashboard - Taxonomía del riesgo

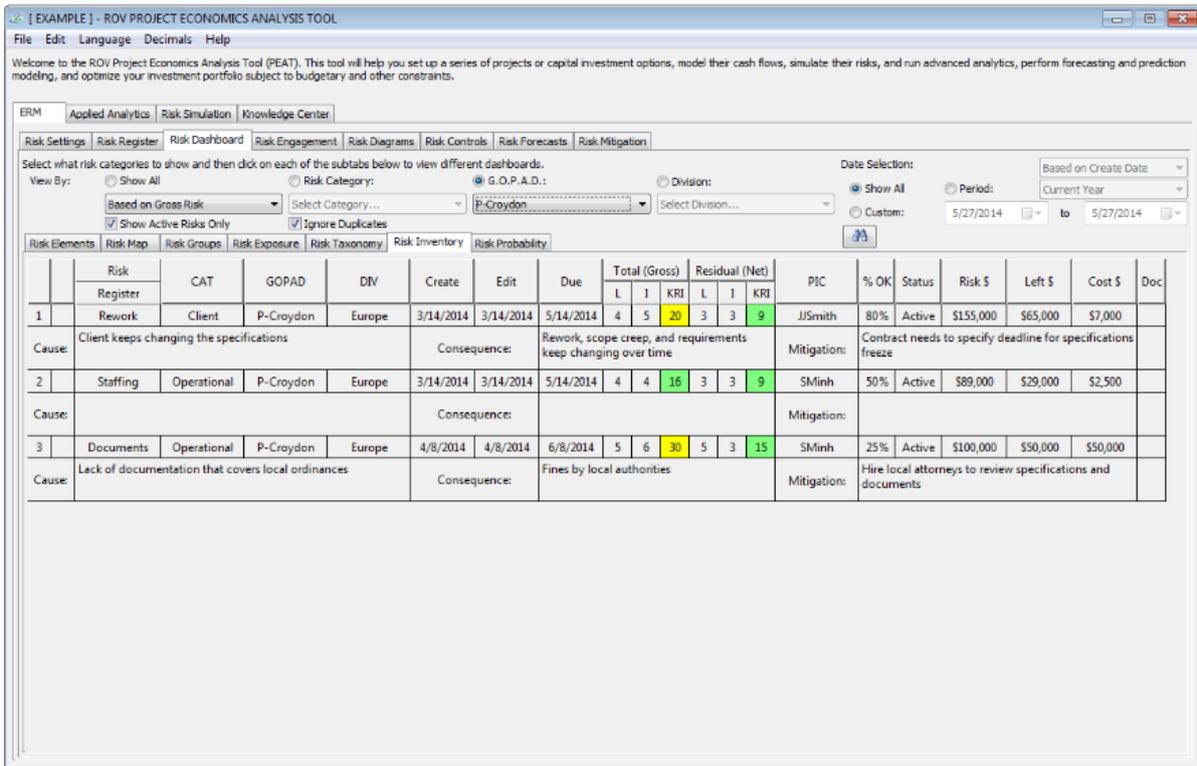


Figura 22 Panel de riesgo - inventario (SQL Queries)

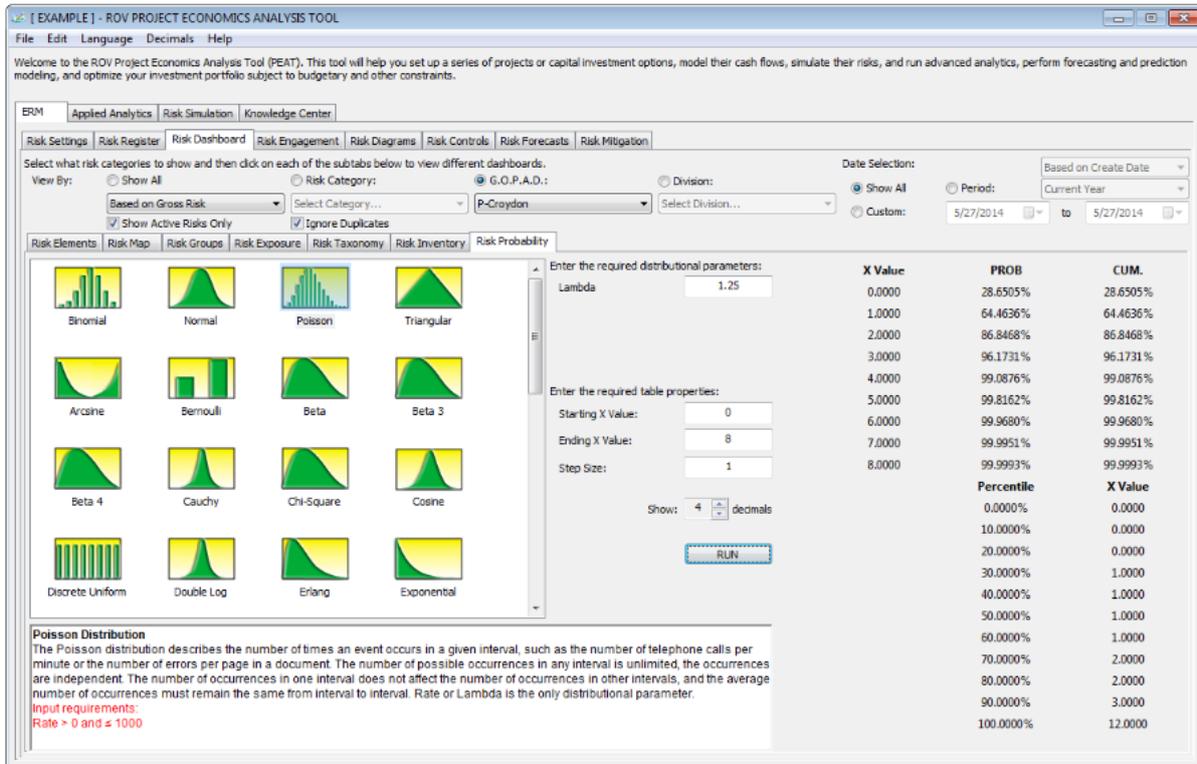


Figura 23 Panel de riesgos - probabilidad

[ EXAMPLE ] - ROV PROJECT ECONOMICS ANALYSIS TOOL

Welcome to the ROV Project Economics Analysis Tool (PEAT). This tool will help you set up a series of projects or capital investment options, model their cash flows, simulate their risks, and run advanced analytics, perform forecasting and prediction modeling, and optimize your investment portfolio subject to budgetary and other constraints.

ERM | Applied Analytics | Risk Simulation | Knowledge Center

Risk Settings | Risk Register | Risk Dashboard | Risk Engagement | Risk Diagrams | Risk Controls | Risk Forecasts | Risk Mitigation

Pre-Engagement or Pre-Bid | Engagement or Bid Assessment | Lessons Learned

Project Name: Project Saturn: Residential Housing Develop | Name: Project Synecor 2015 | Save As | Engagement

Project ID #: RH-563162 | Notes: Development of 1000 residential units in the outskirts of Crydon, London, anticipated bid | Save | John Smith

Updated: 3/11/2014 | Report | Show: 30 rows | Risk Library | Edit | Project Synecor 2015

Custom Categories | Copy | Delete

ITEM	CATEGORIES	EXPLANATIONS & DETAILS	DATA SOURCE	RISK CRITERIA			NOTES
				Low Risk	Significant Risk	Critical Risk	
Client Profile	Experience dealing with client (integrity, ontime payment, frequent	We have dealt with the client before in the past and they are very picky on technical details and keep changing	Past Experience		Manageable risk if our contracts are air tight on scope creeps		
Partnerships	Potential partners and subcontractors available to reduce project risk	We can mitigate any technical risks with our pool of partners		We have a pool of existing partners			
Project Profile	Insufficient information on bid order, RFP has limited details, future	RFP has some technical issues missing such as who will implement the architectural changes to plots C-DE	RFP		We can state this in the contract that client's responsibility		
Competitors	Key competitors for the project	HHSC and RMBH are two main competitors in the bid that we foresee	Competitive Database	We can significantly outprice them			
Financial Profitability	Potential for financial losses if resource, cost, and schedule risks are not	Lowered pricing will cause profits to shrink and if overrun happens, we may make losses on early phases	Pricing Model		Pricing is a significant risk		
Internal Capabilities	Potential lack of expertise and experience in executing and						
Contractual Obligations	Potential complex contract negotiations and loopholes						
Cost Risk	Potential for cost and budget overruns from human resources and raw						

Figura 24 Riesgos previos al compromiso

[ EXAMPLE ] - ROV PROJECT ECONOMICS ANALYSIS TOOL

Welcome to the ROV Project Economics Analysis Tool (PEAT). This tool will help you set up a series of projects or capital investment options, model their cash flows, simulate their risks, and run advanced analytics, perform forecasting and prediction modeling, and optimize your investment portfolio subject to budgetary and other constraints.

ERM | Applied Analytics | Risk Simulation | Knowledge Center

Risk Settings | Risk Register | Risk Dashboard | Risk Engagement | Risk Diagrams | Risk Controls | Risk Forecasts | Risk Mitigation

Pre-Engagement or Pre-Bid | Engagement or Bid Assessment | Lessons Learned

Project Name: Project Mars: Residential Housing Develop | Name: Jaddyn Turner | Save As | Engagement

Project ID #: RH-613356 | Notes: Development of 2500 residential units in the outskirts of Leicester, London, completion was | Save | Jaddyn Turner

Updated: 3/11/2014 | Report | Show: 20 rows | Risk Library | Edit | Corporate Project 163

Custom Categories | Copy | Delete

ITEM	RISK ISSUES, EVENTS, CONCERNS	POTENTIAL IMPACT DETAILS	RELEVANT?	RISK CRITERIA			PROPOSED ACTIONS
				L	I	KRI	
Business Develop...	Increase of strong competitors in the area	Aggressive pricing impacts and lowering our opportunity for a viable financial strategy	YES	3	5	15	
Technical Work	Insufficient technical knowledge	Need to hire three additional technical draftsmen to determine the final specifications (RFP items XI-XIV)	YES	3	2	6	

Figura 25 Compromiso de riesgo

[ EXAMPLE ] - ROV PROJECT ECONOMICS ANALYSIS TOOL

File Edit Language Decimals Help

Welcome to the ROV Project Economics Analysis Tool (PEAT). This tool will help you set up a series of projects or capital investment options, model their cash flows, simulate their risks, and run advanced analytics, perform forecasting and prediction modeling, and optimize your investment portfolio subject to budgetary and other constraints.

ERM Applied Analytics Risk Simulation Knowledge Center

Risk Settings Risk Register Risk Dashboard Risk Engagement Risk Diagrams Risk Controls Risk Forecasts Risk Mitigation

Pre-Engagement or Pre-Bid Engagement or Bid Assessment Lessons Learned

Project Name: Project Mars: Residential Housing Developme Name: Jaddyn Turner Save As Engagement  
 Project ID #: RH-613396 Notes: Development of 2500 residential units in the Save Jaddyn Turner  
 Updated: 3/11/2014 Edit  
 Custom Categories Copy Report Show: 20 rows Delete

ITEM	CATEGORIES	ISSUES (WHAT)	CAUSE (WHY)	IMPACT (CONSEQUENCES)	ACTIONS TAKEN & RECOMMENDATIONS	IMPACT AREAS	NOTES
Project Management	Technical staff required	Need project managers who are more technical or have a technical	Schedule overruns was in part due to bad project management	Cost and budget overruns causing losses	Hire and train better PMs	Operations and PM	
Cost Analysis	Cost analysts required	Cost calculations are high level estimates and were highly inaccurate	Cost overruns was in part due to bad forecasting of costs	Cost and budget overruns causing losses	Risk Simulation with Monte Carlo cost risk models are required	PM and Cost Anlysis	
Schedule Modeling	Senior management oversight	Schedule on bid was too optimistic	Schedule overruns was in part due to bad project management	Cost and budget overruns causing losses		PM and Cost Anlysis	
Schedule Modeling	Technical training required	Schedule calculations are high level estimates and were highly inaccurate	Schedule delays were in part due to bad forecasting of time to	Cost and budget overruns causing losses	Risk Simulation with Monte Carlo schedule risk models are required	PM and Cost Anlysis	

Figura 26 Compromiso de riesgo - lecciones aprendidas

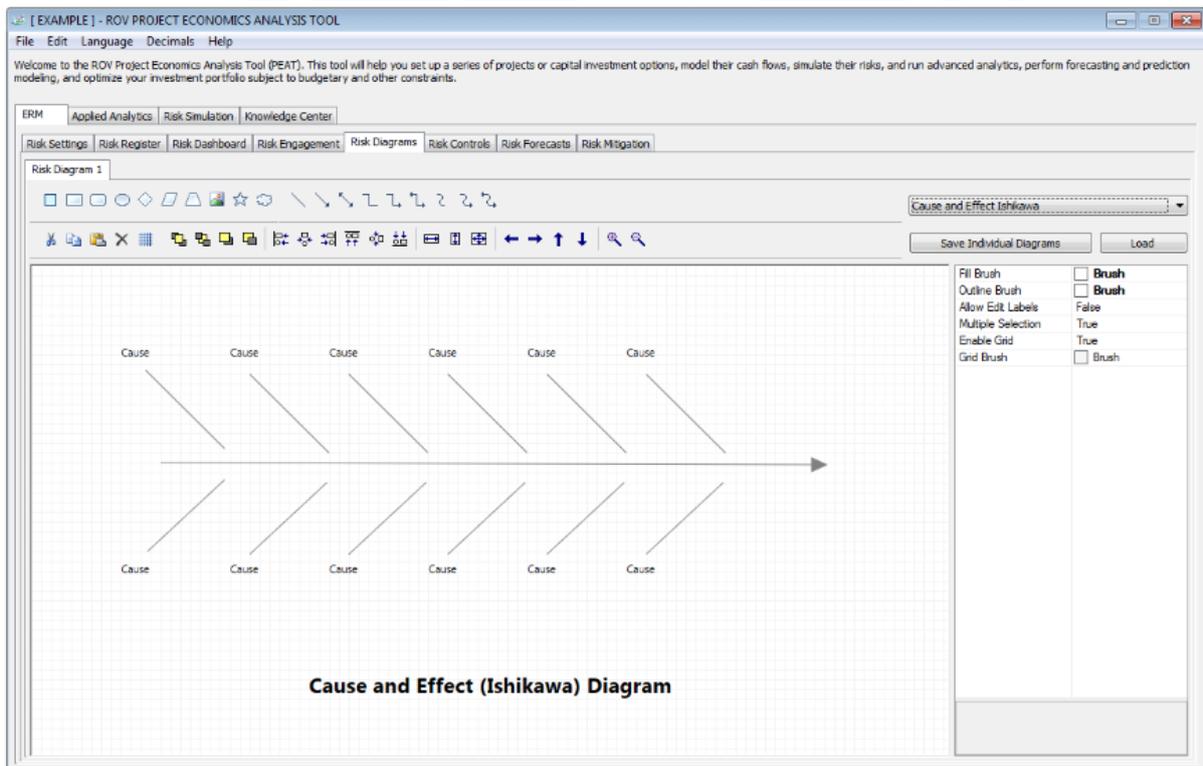


Figura 27 Diagramas de riesgo - espina de pescado

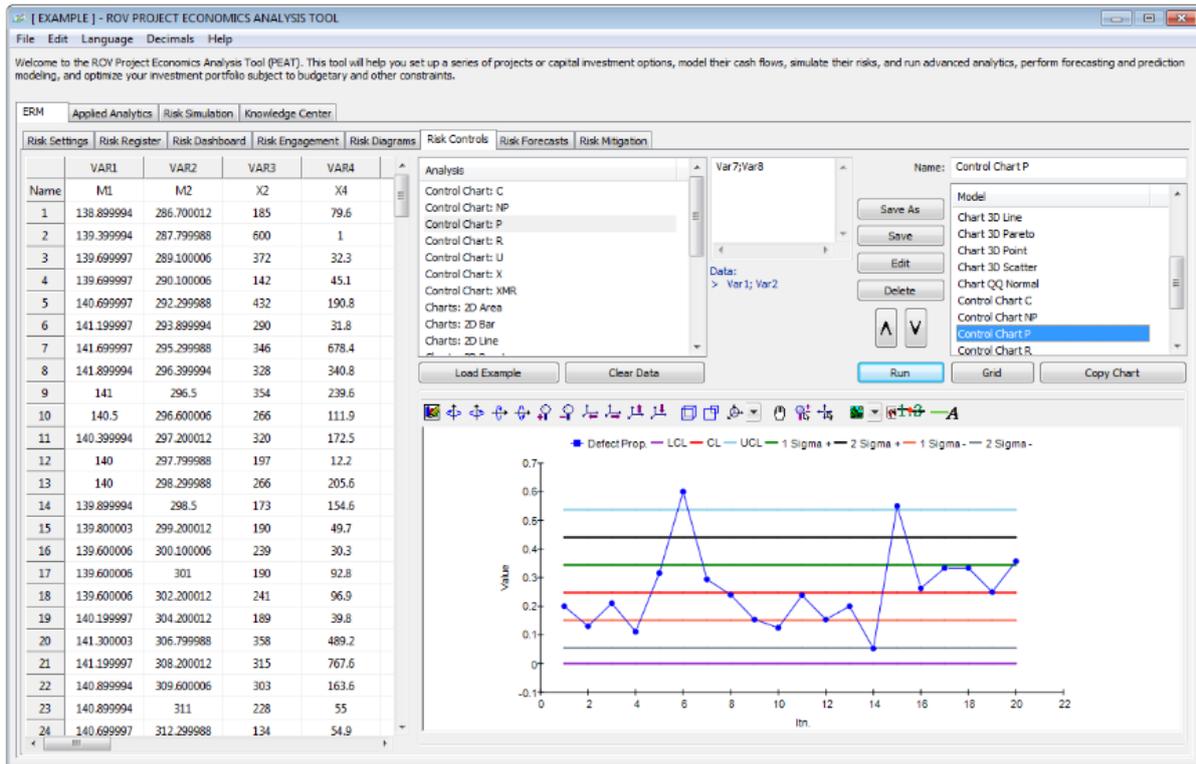


Figura 28 Control de riesgos

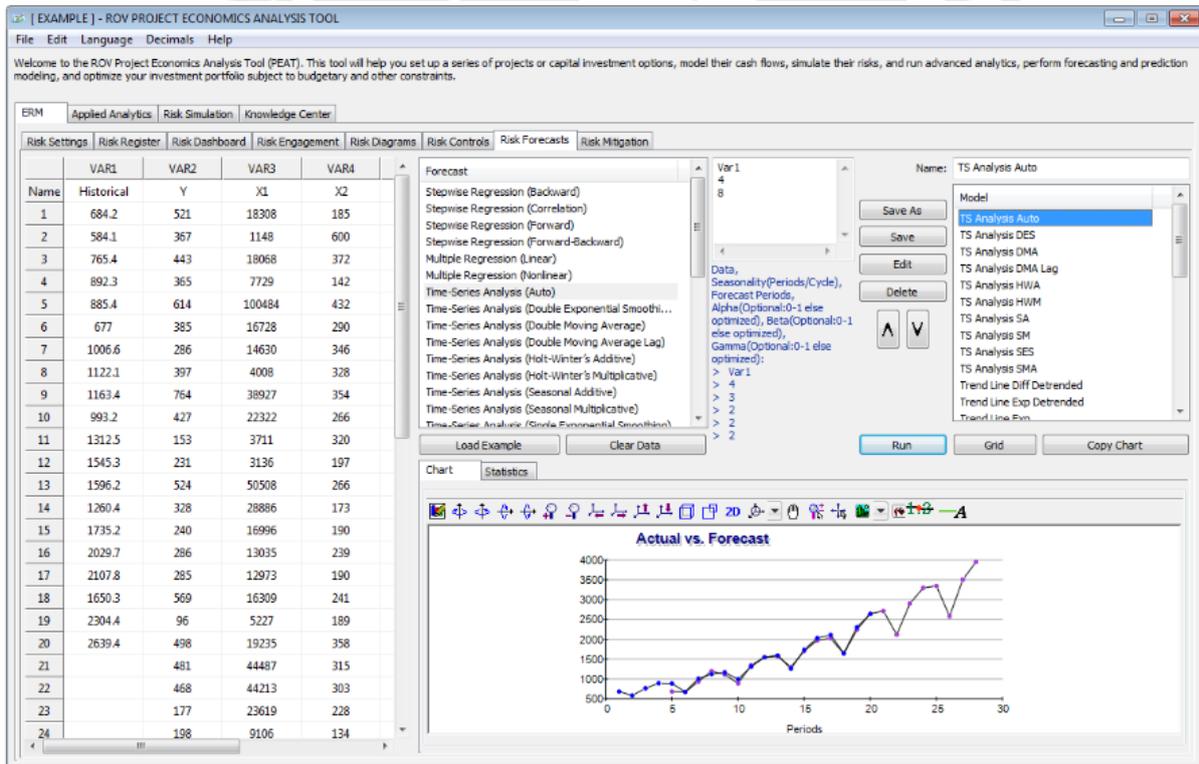


Figura 29 Pronósticos de riesgos

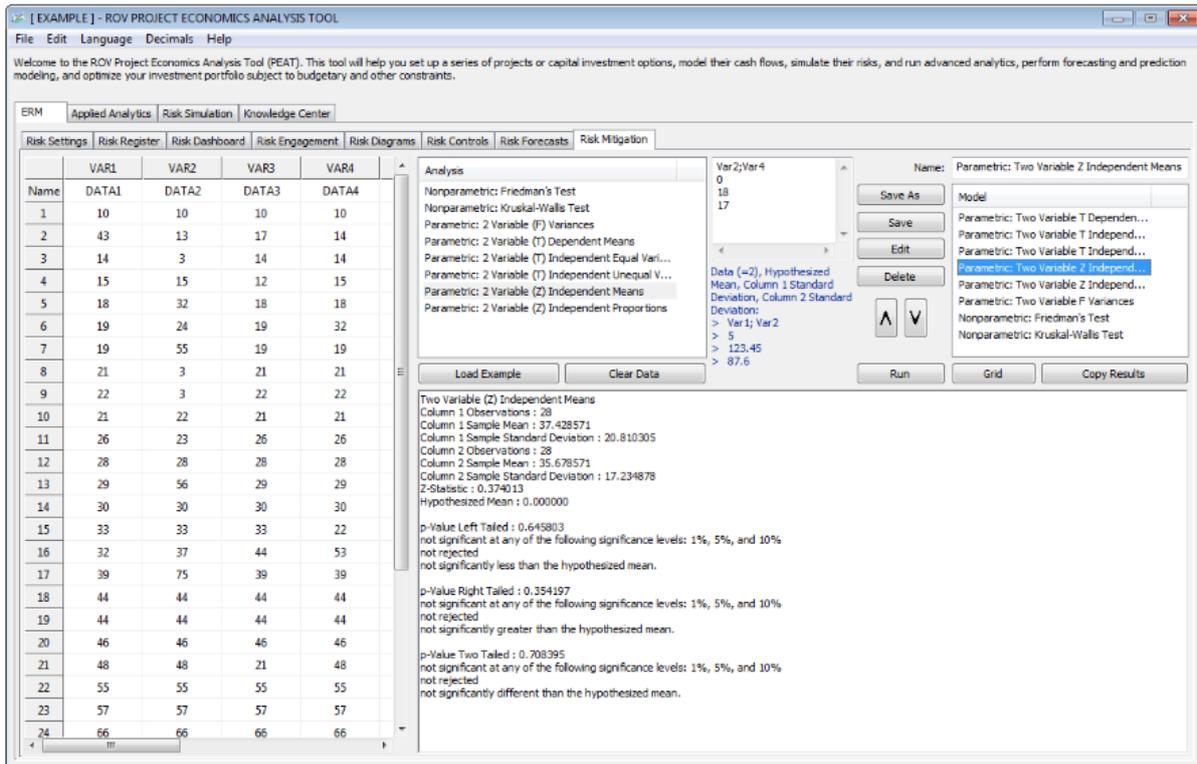


Figura 30 Mitigación de riesgos

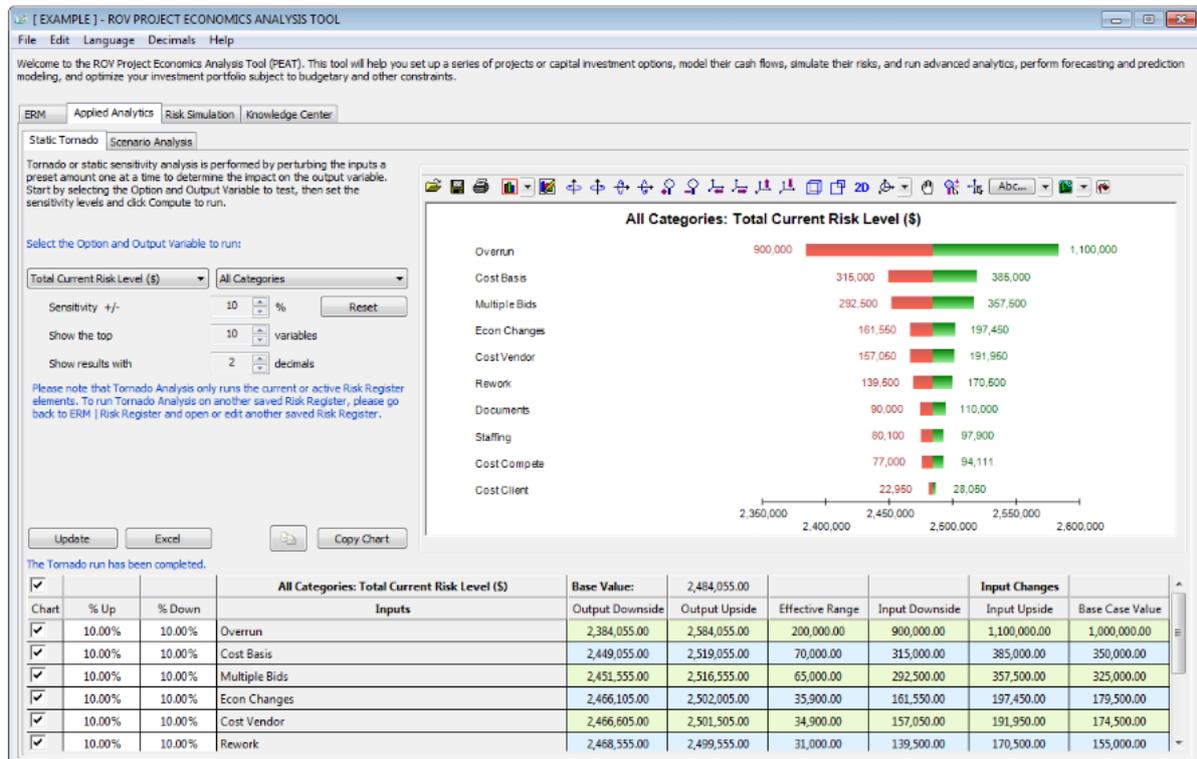


Figura 31 Sensibilidad de riesgo - análisis tornado

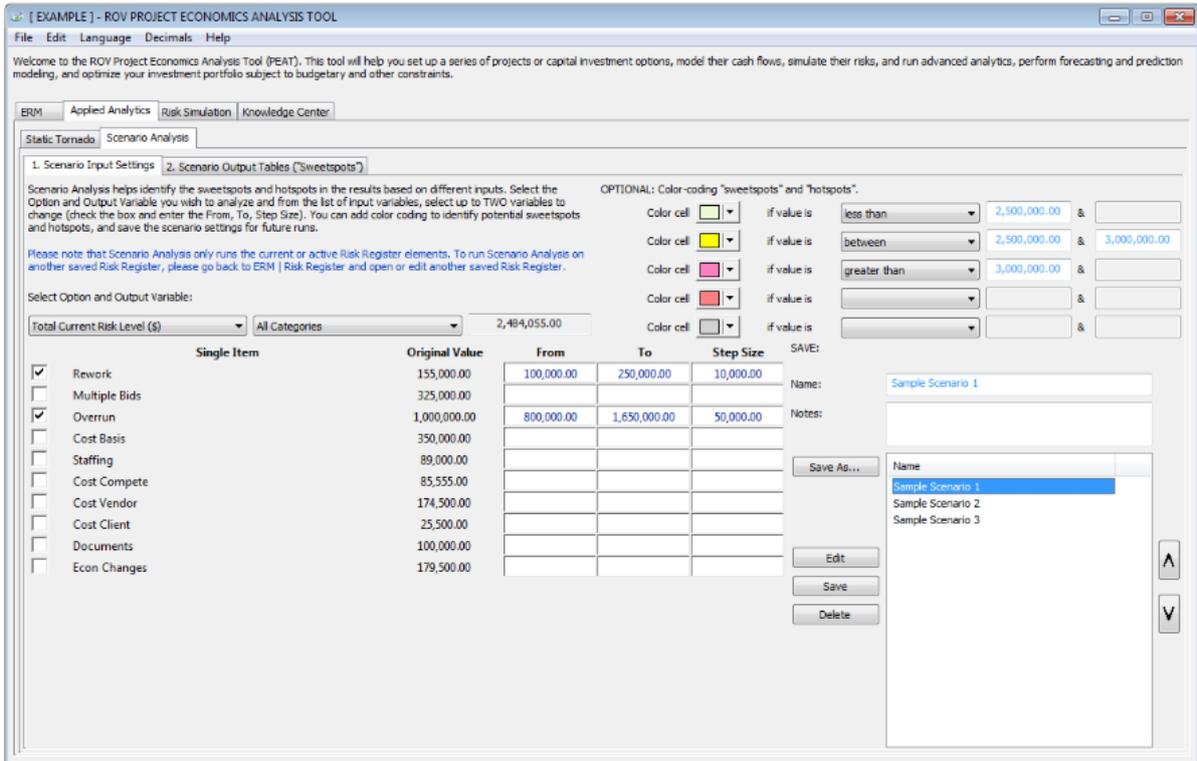


Figura 32 Escenarios de riesgo - análisis de escenarios múltiples

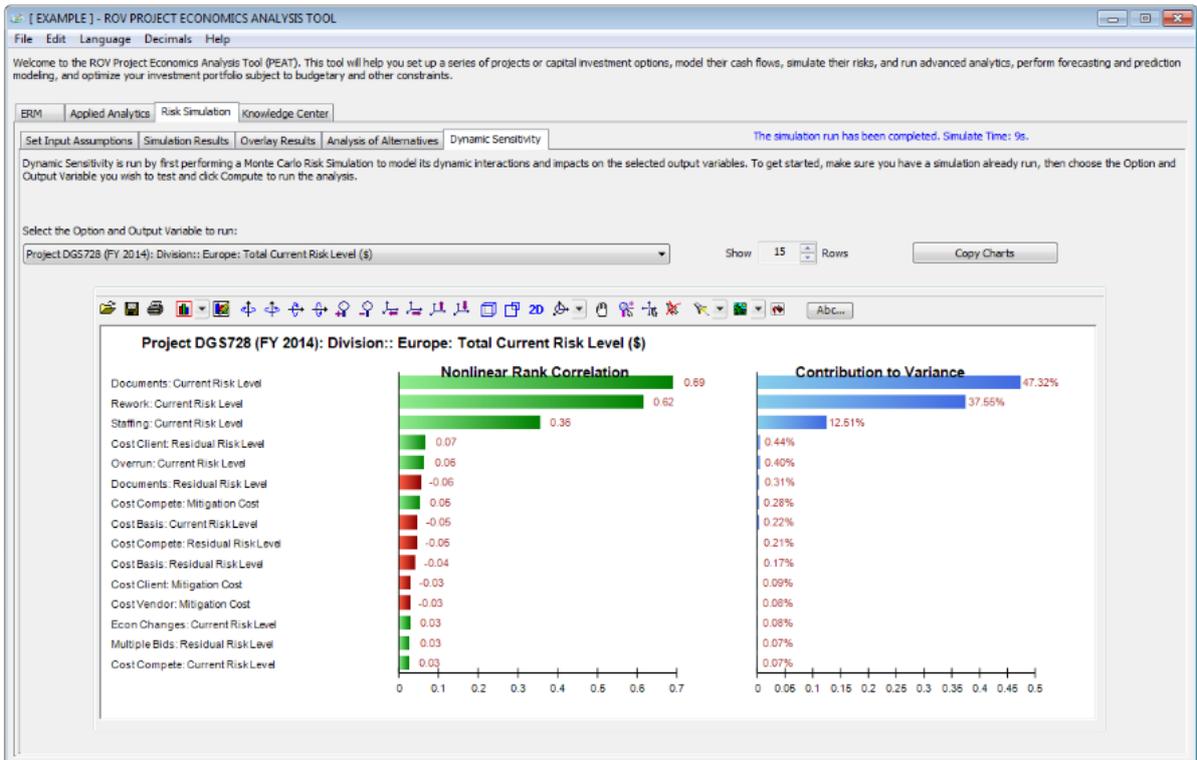


Figura 33 Simulación de riesgos - sensibilidad dinámica

b) ISOTools – Módulo de gestión de riesgos

Se evaluó también el software proporcionado por la empresa ISOTools. Este es un módulo de gestión de riesgos que también permite la gestión de riesgos por procesos, explicada de forma matricial. Dentro de la evaluación, es importante mencionar, que la empresa trabaja con distintos módulos de ISOTools, tales como gestor documental, no conformidades y calibraciones. Por lo tanto, se consideran las siguientes características:

- ✓ Procesos de la matriz de riesgo linkeados por el mapa de procesos del módulo de gestor documental. Ello permite una rápida visualización de sus riesgos asociados.
- ✓ Configuración global de las categorías de indicadores de riesgo (1-5) con codificación de color personalizable de KRI (indicadores clave de riesgo) a través de una matriz de riesgos.
- ✓ Cuenta con una base de datos editable, en las cuales se realiza el registro de fuentes de riesgo, riesgo, y posibles consecuencias.
- ✓ Permite separar las matrices de riesgo por la normativa afectada, estas normativas son editables. Como ejemplo, se indica calidad, seguridad, medio ambiente y seguridad de la información.
- ✓ Se pueden exportar las matrices a Excel o PDF.
- ✓ No se pueden aplicar filtros fácilmente en las matrices, lo cual dificulta su visualización cuando se requiere puntos específicos.
- ✓ Se puede visualizar un mapa de calor de los distintos riesgos; sin embargo, no se puede realizar un comparativo de las variaciones año a año.
- ✓ Se puede visualizar un mapa de burbujas, en el cual sí se puede realizar comparaciones de valoraciones de los riesgos año a año.

The screenshot shows the ISOTools interface for 'Gestión de Riesgos'. The main content is a table titled 'Riesgo Bruto' for the 'Evaluación 2017'. The table has 8 columns: Número, Unidad de Ne..., Proceso, Riesgo, Probabilidad, Severidad, Resultado, and Condición. The 'Condición' column is color-coded: green for 1, red for 9, and yellow for 3 and 6.

Número	Unidad de Ne ...	Proceso	Riesgo	Probabilidad	Severidad	Resultado	Condición
1	Línea de procesado de activos	Seguridad, Salud y Ambiental	Vertido al lecho rocoso	Baja	Baja	1	1
2	Línea de seguros	Ventas	Riesgo de fuga de comediales	Alta	Alta	9	9
3		Seguridad, Salud y Ambiental	Riesgo de desgaste de maquinaria	Alta	Alta	9	9
4	Línea de carga y descarga	Ventas	Riesgo de fuga de comediales	Alta	Baja	3	3
5			Vertido al lecho rocoso	Media	Alta	6	6

**Figura 34 Ejemplo de Matriz de Riesgos**

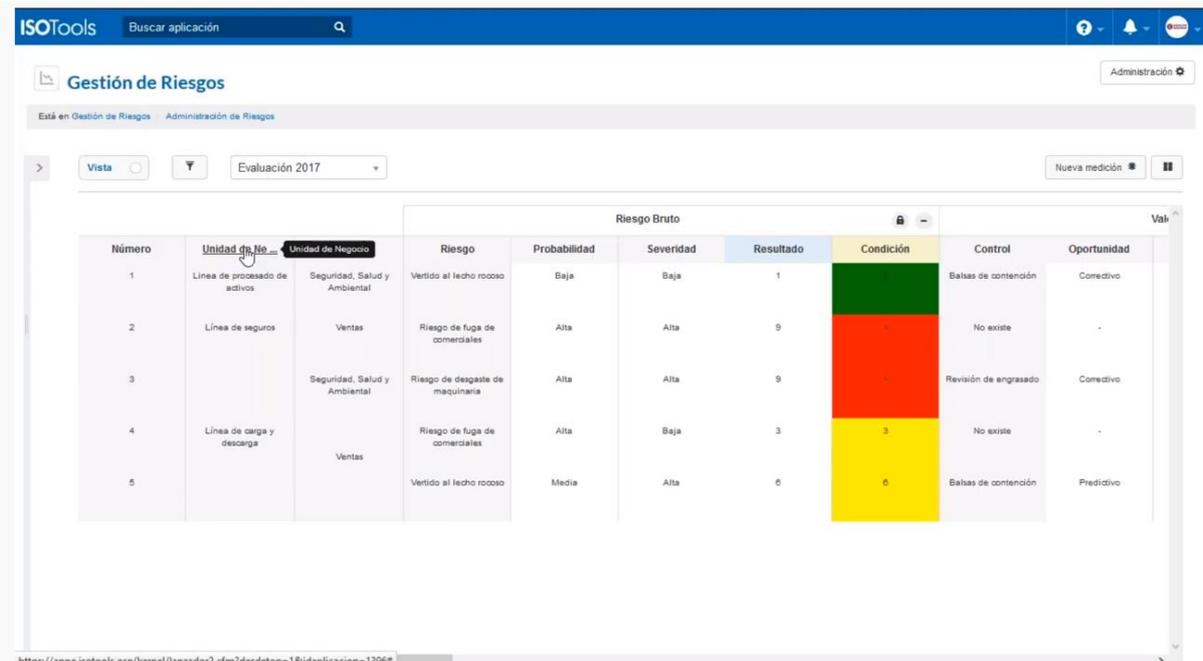


Figura 35 Filtros por encabezados

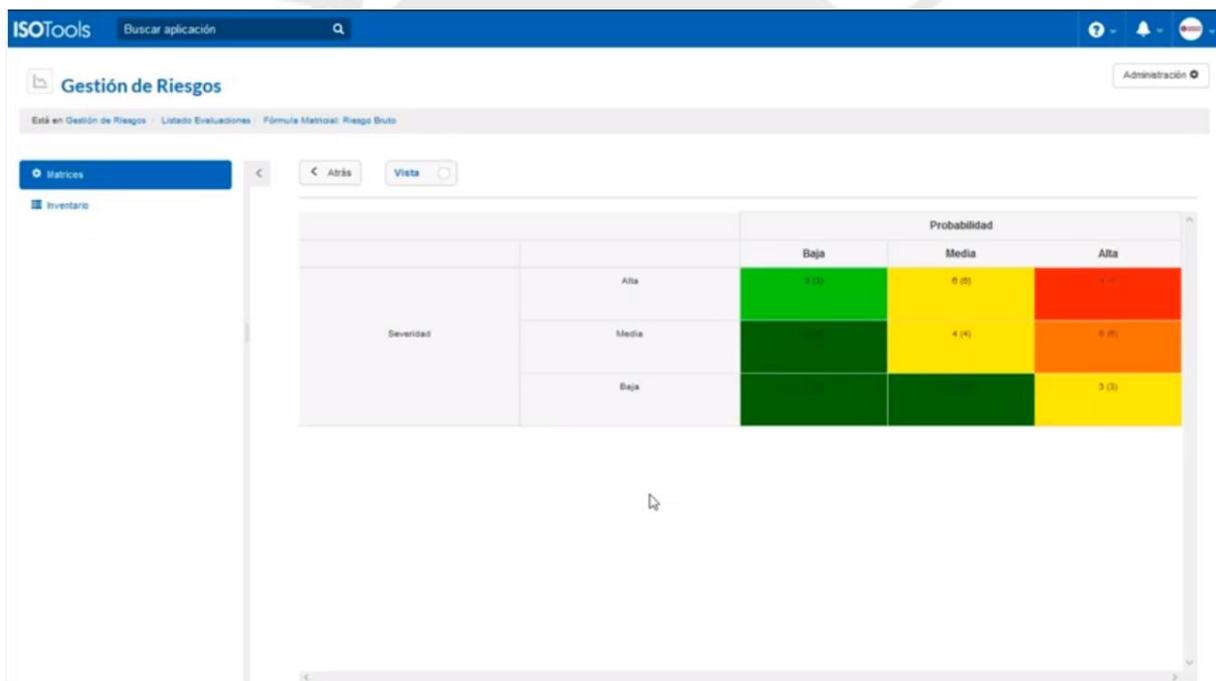


Figura 36 Segmentación por nivel de riesgo

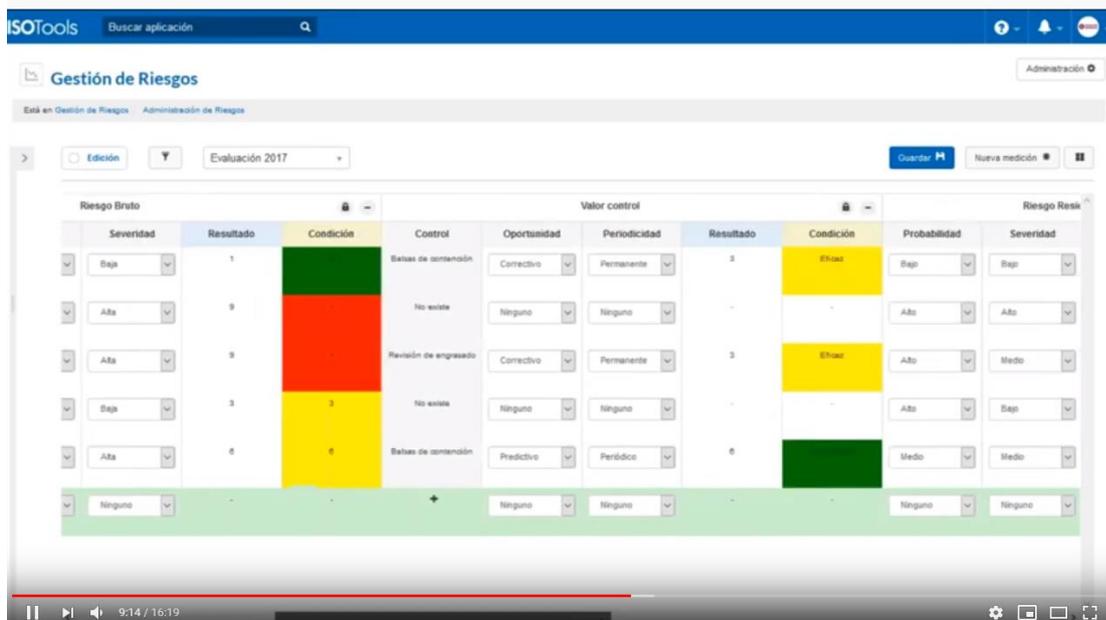


Figura 37 Evaluación de Riesgos Residuales

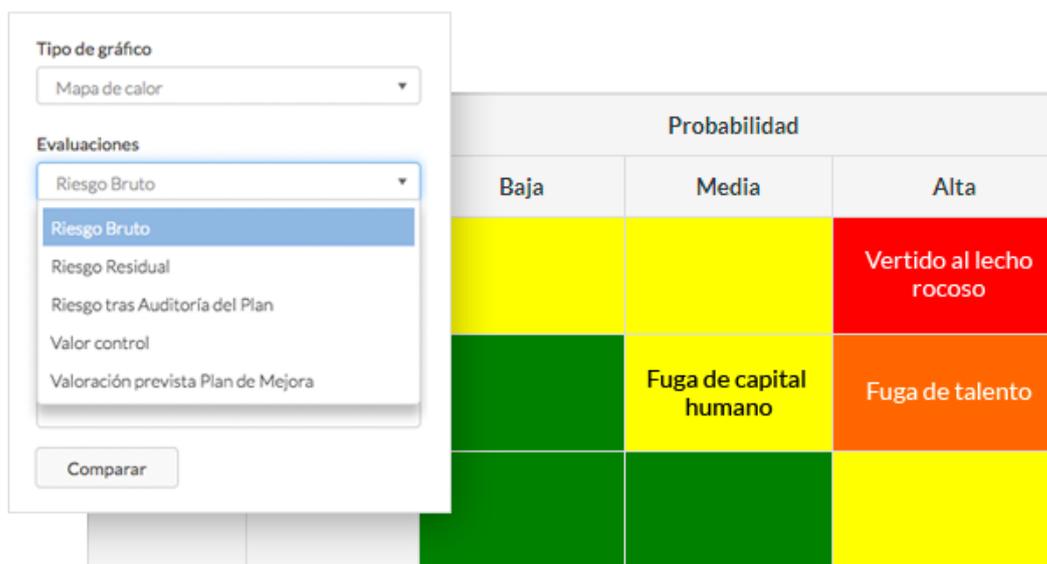


Figura 38 Ejemplo de mapa de calor

c) Matriz de Riesgos usando Macros VBA Excel

Por otro lado, se propone el continuar con una herramienta tal como un Excel con macros para la identificación, análisis, evaluación y tratamiento de los riesgos. El objetivo será registrar, identificar y calificar los riesgos de cada Unidad de Negocio (UN) de la empresa mediante una metodología corporativa. El alcance del mismo es el siguiente: El alcance del documento está definido en la identificación de los riesgos dentro de los siguientes dimensiones: Social, Reputacional, Ambiental y de Negocio de la compañía. Una vez identificados y calificados, se relevan cuáles son las

medidas/acciones que están siendo llevadas a cabo para la mitigación de su Nivel de Exposición, dando lugar al Riesgo Residual. En la Tabla 40, se muestra el proceso a seguir en el Excel:

**Tabla 44 Proceso a seguir en el Excel**

<p>- El archivo cuenta con 2 "solapas" o "hojas" para ser completadas</p> <p>1. <i>Registrar Riesgos</i>: <b>debe</b> ser completada en el transcurso del Taller de Identificación y Evaluación de Riesgos Ambientales y Sociales No Técnicos.</p> <p>2. <i>Registrar Tratamientos</i>: <b>puede</b> ser completada en el transcurso del Taller de Identificación y Evaluación de Riesgos, o en una instancia posterior, dependiendo del tiempo disponible. <b>Debe</b> ser completado para generar el <b>Plan de Gestión de Riesgos</b>.</p>
<p>- En la solapa "<i>Registrar Riesgos</i>", se registran los riesgos identificados (durante talleres o reuniones de trabajo interdisciplinario) y se los clasifica según su "Probabilidad de Ocurrencia" y su "Impacto". Registrar uno por fila.</p>
<p>- En la solapa "<i>Registrar Tratamientos</i>", se registran las acciones actuales de tratamiento, afectando ya sea la <b>Probabilidad de Ocurrencia</b> o el <b>Impacto asociado</b>, a los riesgos registrados en la solapa anterior.</p>
<p>- Puede existir más de una acción de tratamiento actual por riesgo.</p>
<p>- Las celdas que se encuentran con color Gris (claro u oscuro) <b>no deben ser completadas</b> por el usuario ya que las mismas se calcularán automáticamente.</p>
<p>- Los criterios de "Probabilidad de Ocurrencia", "Impacto", "Nivel de Exposición" o "Mapa de Riesgos"; "Tratamientos"; "Categorías" y "UN" puede ser cambiados realizando los mismos únicamente en los ANEXOS.</p>

En la Figura 40, se muestra la identificación de los riesgos usada para este ejemplo, posterior a ello, en la Figura 41, se muestran los tratamientos y su efecto mitigador de los mismos. Un punto importante a resaltar, es que en dicha matriz se asocian los conceptos al dinero, es decir nos apoyamos con la monetización de riesgos. En la figura 42, se muestra el mapa de calor, el cual es una herramienta muy importante para la ubicación de los riesgos según el nivel de los mismos. Además, nos permite compararlos con los resultados obtenidos en años anteriores. La Figura 43, representa un registro de riesgos de una compañía, a su vez separa los mismos según al ente afectado, tales como personas, organización, negocio, etc. Asimismo, en la Tabla 41, se muestra los rangos de probabilidades escogidos en el presente análisis, el mismo que varía desde una probabilidad remota hasta una probabilidad muy alta. A raíz de ello, en la Figura 45, se plantea la matriz usada para categorizar los riesgos y los umbrales y tolerancia permitidas por la organización. Por último, en la Figura 46, se presenta una calificación de eficiencia para todos los controles planteados para los riesgos.

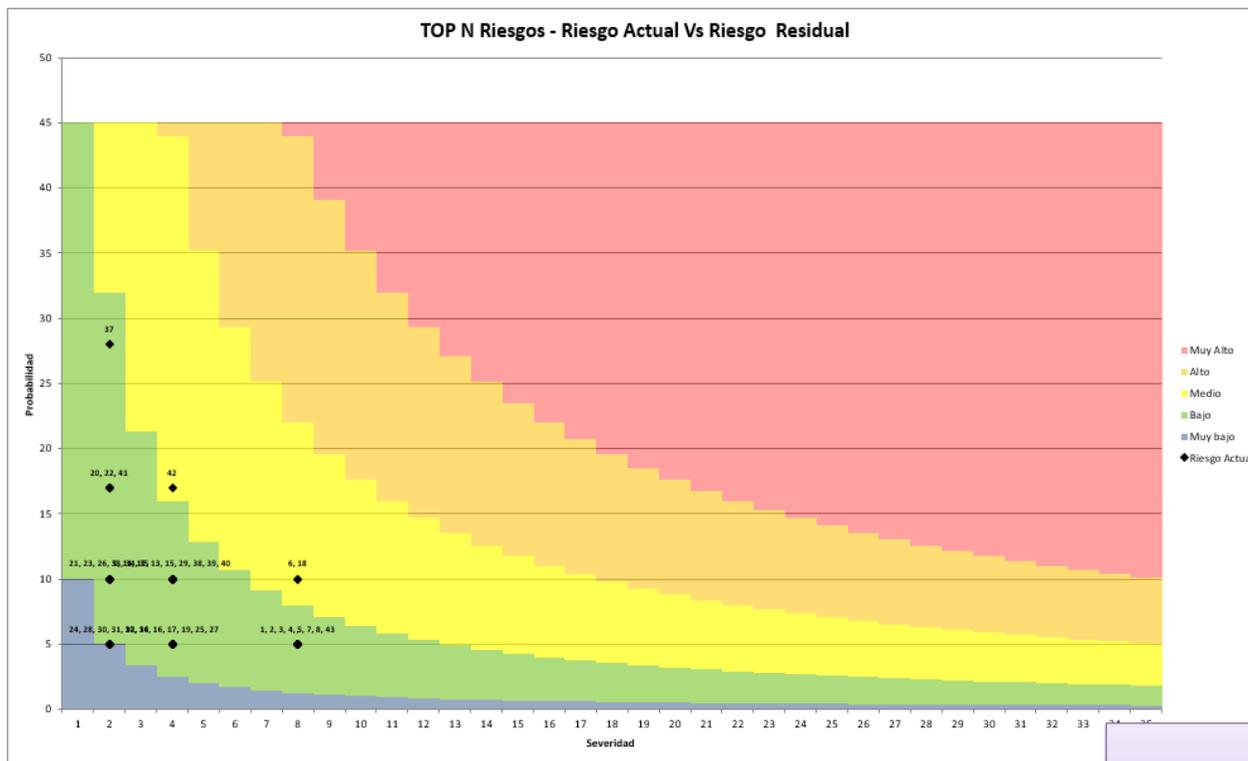




TOP N riesgos

Filtrar sin considerar los ceros "0"

ID Riesgo	Riesgo Act	Riesgo Res	Probabilidad	Impacto	Prob R	Imp R	Manej
1	40	5	5	8	1.8	2.8	0.13
2	40	5	5	8	1.8	2.8	0.13
3	40	5	5	8	1.8	2.8	0.13
4	40	10	5	8	2.5	4	0.25
5	40	10	5	8	2.5	4	0.25
6	80	10	10	8	3.54	2.83	0.125
7	40	5	5	8	1.77	2.83	0.125
8	40	5	5	8	1.77	2.83	0.125
9	40	5	10	4	3.54	1.41	0.125
10	20	2.5	5	4	1.77	1.41	0.125
11	40	5	10	4	3.54	1.41	0.125
12	40	5	10	4	3.54	1.41	0.125
13	40	5	10	4	3.54	1.41	0.125
14	20	2.5	5	4	1.77	1.41	0.125
15	40	5	10	4	3.54	1.41	0.125
16	20	2.5	5	4	1.77	1.41	0.125
17	20	2.5	5	4	1.77	1.41	0.125
18	80	20	10	8	5	4	0.25
19	20	2.5	5	4	1.77	1.41	0.125
20	34	8.5	17	2	8.5	1	0.25
21	20	2.5	10	2	3.54	0.71	0.125
22	34	4.25	17	2	6.01	0.71	0.125
23	20	2.5	10	2	3.54	0.71	0.125
24	10	1.25	5	2	1.77	0.71	0.125
25	20	5	5	4	2.5	2	0.25
26	20	2.5	10	2	3.54	0.71	0.125
27	20	2.5	5	4	1.77	1.41	0.125
28	10	1.25	5	2	1.77	0.71	0.125
29	40	10	10	4	5	2	0.25
30	10	1.25	5	2	1.77	0.71	0.125
31	10	1.25	5	2	1.77	0.71	0.125
32	10	1.25	5	2	1.77	0.71	0.125
33	20	2.5	10	2	3.54	0.71	0.125
34	20	5	10	2	5	1	0.25
35	20	2.5	10	2	3.54	0.71	0.125
36	10	1.25	5	2	1.77	0.71	0.125
37	56	7	28	2	9.9	0.71	0.125
38	40	5	10	4	3.54	1.41	0.125
39	40	10	10	4	5	2	0.25
40	40	5	10	4	3.54	1.41	0.125
41	34	4.25	17	2	6.01	0.71	0.125
42	68	8.5	17	4	6.01	1.41	0.125



Actualizar:  
1) Seleccionar gráfico  
2) Ctrl + Shift + "I"

Figura 41 Mapa de calor de los riesgos TOP identificados

Impacto	Negocio						Peso (Matriz)	Ambiental	Peso (Matriz)	Personas					Reputacional	Peso (Matriz)	
	Proyectos				Operación					Personal PP+Cont	Peso (Matriz)	Terceros	Peso (Matriz)	Social			Peso (Matriz)
	OPEX	CAPEX	Producción / Ingresos	Plazos	Afectación de Activos PD+B+O+E (MMUSD)	Continuidad del Negocio											
<b>Muy bajo 1</b>	Desvío menor al 3%	Desvío menor al 3%	Desvío menor al 1%	Desvío menor al 5%	PPC < 0,1 Otras UN < 0,01	Hasta 1 día de producción	2	Impacto ambiental no significativo.	2	Sobreeposición de una persona sin afecciones a la salud. Caso con lesiones no registrable (Primer Auxilio).	2	Probable exposición de un tercero	2	Afectación limitada y no permanente de un bien material o inmaterial de un único tercero y su núcleo familiar directo	2	Se trata de situaciones con bajo o nulo efecto mediático	2
<b>Bajo 2</b>	Desvío mayor al 3%	Desvío mayor al 3%	Desvío mayor al 1%	Desvío mayor al 5%	PPC < 1 Otras UN < 0,1	1 a 3 días	4	Daño ambiental restringido dentro de los límites de la instalación.	4	Una persona con afección reversible, o sobre exposición de varias personas sin afecciones a la salud. Caso con lesión registrable pero sin pérdida de tiempo (Trabajo Restringido y Tratamiento Médico).	4	Sobreeposición de un tercero sin afecciones a la salud	4	Afectación limitada y no permanente de un bien material o inmaterial de un grupo reducido de terceros y sus núcleos familiares directos	4	Si son acontecimientos de corta duración y rápida solución. Tienen un mínimo impacto en la imagen de la Compañía. Su alcance por lo general es de baja repercusión en medios locales y provinciales	4
<b>Medio 3</b>	Desvío mayor al 10%	Desvío mayor al 10%	Desvío mayor al 2%	Desvío mayor al 15%	PPC < 50 Otras UN < 5	3 días a 1 semana	8	Daño ambiental que alcanza áreas externas a la instalación afectando ecosistemas comunes.	8	Una persona con afecciones irreversibles, o varias con afecciones a la salud reversibles. Caso con lesión registrable con pérdida de tiempo.	8	Un tercero con afección reversible, o sobre exposición de varios sin afecciones a la salud. Lesión no permanente a un tercero	8	Afectación limitada y permanente de un bien material o inmaterial de un grupo reducido de terceros y sus núcleos familiares directos	8	Hay repercusiones en los medios principalmente locales y provinciales e intervención de autoridades gubernamentales competentes. Altas probabilidades de escalar el tema en medios audiovisuales a nivel nacional. Su efecto se ramifica rápidamente a través de redes digitales	8
<b>Alto 4</b>	Desvío mayor al 25%	Desvío mayor al 25%	Desvío mayor al 4%	Desvío mayor al 25%	PPC < 500 Otras UN < 50	1 semana a 1 mes	16	Daño ambiental que alcanza áreas externas a la instalación afectando ecosistemas comunes que albergan especies raras o amenazadas o afectando ecosistemas raros y/o amenazados.	16	Varias personas con afecciones a la salud irreversibles. Una fatalidad.	16	Un tercero con afecciones irreversibles, o varios con afecciones a la salud reversibles. Lesión permanente a un tercero	16	Afectación extendida y permanente de un bien material o inmaterial de un grupo reducido de terceros y sus núcleos familiares directos	16	La reputación e imagen de la Compañía toma relevancia pública en distintos canales y medios de comunicación. Intervienen autoridades gubernamentales a nivel nacional y el impacto se ramifica a otros públicos de interés. Dependiendo su alcance, magnitud y tiempo de duración puede tener efectos regionales/Internac.	16

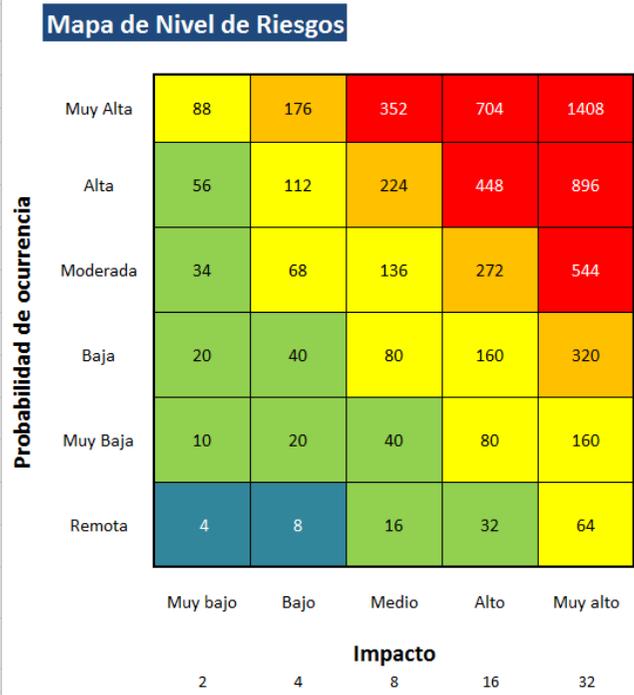
Figura 42 Descripción del impacto en los riesgos

**Tabla 45 Rango de probabilidades planteado**

Rango de Probabilidad	Proyectos	Para operaciones	Peso (Matriz)
<b>Remota A</b>	Evento físicamente posible pero del que no se tienen referencias o solo ocurrido excepcionalmente.	< 1 E-5	<b>2</b>
<b>Muy Baja B</b>	Suceso que ha ocurrido en la industria.	1 E-5 - 1 E-4	<b>5</b>
<b>Baja C</b>	Suceso no esperado durante la vida útil.	1 E-4 - 1 E-3	<b>10</b>
<b>Moderada D</b>	Suceso que puede ocurrir una vez durante la vida útil	1 E-3 - 1 E-2	<b>17</b>
<b>Alta E</b>	Suceso que se espera que ocurra una o más veces durante la vida útil.	1 E-2 - 1 E-1	<b>28</b>
<b>Muy Alta F</b>	Suceso que se espera que ocurra varias veces en la vida útil	> 1 E-1	<b>44</b>

	Riesgo Intolerable - Inaceptable	Los escenarios en la zona de Riesgo Intolerable (Zona Roja) deberán someterse a las acciones inmediatas para reducción de riesgo, debido a que la combinación de Frecuencia y Severidad asociadas lo ubican en una posición que requiere su tratamiento inmediato Para continuar las Operaciones / Oportunidad / Proyecto, las medidas de control adicionales deberán ser implementadas previamente.
	Riesgo Tolerable ALARP	Los escenarios ubicados en la zona de riesgo Tolerable (zona amarilla) requieren medidas adicionales de control y una adecuada gestión. En líneas generales, en activos existentes, es probable que los escenarios analizados se ubiquen mayoritariamente en la zona de riesgo Tolerable debiendo gestionarse los más críticos haciendo un uso estratégico de los recursos. Las medidas de reducción de riesgos son siempre deseables, pero no se puede implementar si su costo es desproporcionado en relación con el beneficio obtenido (ALARP: Acrónimo de "As Low As Reasonably Practicable". Identifica "la zona" donde el nivel de riesgo es Tolerable si se implementan las medidas de control adecuadas considerando la proporcionalidad entre inversión y la reducción de riesgo obtenida, refiriéndose a esto el término "tan bajo como sea razonablemente implementable")
	Riesgo Aceptable	Nivel de Riesgo Aceptable (zona verde) por debajo del cual no se requieren medidas adicionales de control debido a que la combinación de Frecuencia y Severidad asociadas no representan una amenaza significativa para la operación. La adopción de las buenas prácticas de la industria es suficiente. En las fases de diseño, se deberá velar por lograr niveles de riesgo Aceptable implementando las medidas correspondientes desde el origen de la instalación

**Figura 43 Niveles de riesgo planteados**



Nivel de Exposición	
Muy Alto $\geq$	352
Alto $\geq$	176
Medio $\geq$	64
Bajo $\geq$	10
Muy Bajo $<$	10

Para cambiar el peso de los Criterios, hacerlo desde aquí

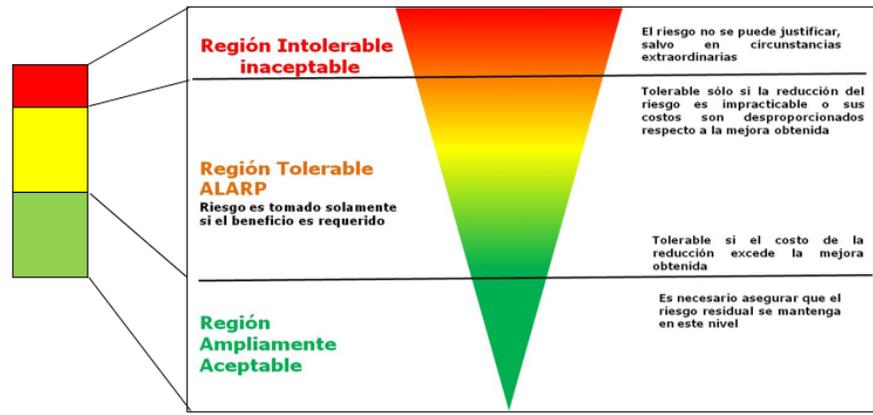


Figura 2 Marco para la Tolerabilidad del Riesgo (By Steve Lewis)

Figura 44 Mapa de nivel de riesgos planteado

Calificación del Tratamiento	Descripción	Efectividad s/ probabilidad	Efectividad s/ impacto
No efectivo / Inexistente	Los controles o acciones de tratamiento no son adecuados y no funcionan	1	1
Medianamente Efectivo	Los controles y/o acciones de tratamiento son adecuados y funcionan, pero tienen debilidades importantes	0.75	0.5
Efectivo	Los controles y/o acciones de tratamiento son adecuados y funcionan, pero cuentan con algunas debilidades	0.5	0.25
Altamente Efectivo	Los controles y/o acciones de tratamiento funcionan adecuadamente	0.25	0.125

**Figura 45 Calificación del tratamiento del riesgo**

Por último, se realizará el análisis de costos entre las tres alternativas para ello se evalúan las alternativas según la ponderación brindada a las características de la tabla inferior:

**Tabla 46 Ponderación de alternativas de software**

Ítem	Valoración	Alternativa 1	Alternativa 2	Alternativa 3
Costo de la alternativa	15	3	5	10
Métodos comparativos entre los riesgos	15	8	5	5
Facilidad para emitir reportes a gerencia.	10	8	5	5
Capacidad de gestionar indicadores.	10	8	6	5
Capacidad de registro de reportes y hallazgos de auditoría.	20	8	4	7
Capacidad de obtener un análisis cuantitativo de riesgos.	20	8	5	6
Registro o control de cambios	10	8	6	4
Puntaje obtenido		725	500	625

Como se puede observar, se escoge la alternativa número 1, de acuerdo a las ponderaciones brindadas según las prioridades de la organización. De este modo, se puede concluir que el software a utilizar será el de Peat's Enterprise Risk Management.



## 5. ANÁLISIS COSTO – BENEFICIO

A continuación, se presentará el ahorro con la implementación de los puntos mencionados en sub capítulo 4.4. “Aplicación de las actividades pendientes”. Para ello, se procederá a analizar el aumento de las primas en los seguros contratados por la organización para transferir sus riesgos. Para ello, se presentará en primer lugar los seguros con los que se cuenta:

Tipo de seguro	Vigencia del servicio	Importe asegurado	Prima Neta
<p>Todo Riesgo – Incluye los riesgos operativos a presentarse durante la ejecución de las funciones en la organización.</p>	<p>Vigencia 01/11/16 al 01/05/18</p> <hr/> <p>Vigencia anterior 01/05/18 al 01/05/19</p> <hr/> <p>Vigencia actual 01/05/19 Al 01/05/20</p>	<p><u>DECLARACIÓN ANTERIOR</u> <u>Del 01/11/16 al 01/05/18:</u> &gt; Edificaciones - USD 9,365,404 &gt; Maquinaria fija y móvil - USD 28,546,992 &gt; Lucro cesante - USD 74,119,224</p> <hr/> <p><u>DECLARACIÓN ANTERIOR</u> <u>Del 01/05/18 al 01/05/19:</u> &gt; Edificaciones - USD 9,147,232.13 &gt; Maquinaria fija y móvil – USD 36,510,939.35 &gt; Lucro cesante - USD 80,892,022.00</p> <hr/> <p><u>DECLARACIÓN ACTUAL</u> <u>DEL 01/05/19 al 01/05/20:</u> &gt; Edificaciones - USD 8,884,225.51 &gt; Maquinaria fija y móvil – USD 38,542,786.10 &gt; Lucro cesante - USD 88,922,100</p>	<p><u>Vigencia actual</u> Prima neta actual = USD 225,633.42</p>
<p>Responsabilidad Civil General</p>	<p>Vigencia anterior 01/11/16 al 01/05/18</p> <hr/> <p>Vigencia anterior 01/05/18 al 01/05/19</p> <hr/> <p>Vigencia actual 01/05/19 Al 01/05/20</p>	<p><u>DECLARACIÓN ANTERIOR</u> <u>Del 01/11/16 al 01/05/18:</u> <u>Cobertura básica / suma asegurada</u> &gt; Responsabilidad Civil Extracontractual - USD 7,500,000 &gt; Responsabilidad Civil Patronal – USD 2,500,000 &gt; Responsabilidad Civil Contractual – USD 2,500,000 &gt; Responsabilidad Civil de Productos – USD 200,000 &gt; Responsabilidad Civil de Almaceneros – USD 250,000 y LAV USD 1,000,000 &gt; Responsabilidad Civil Trabajos Terminados – USD 1,000,000 &gt; Gastos Penales – USD 10,000 &gt; Gastos Admitidos – USD 5,000 por evento y USD 20,000 en LAV</p> <p><u>DECLARACIÓN ANTERIOR</u> <u>Del 01/15/18 al 01/05/19:</u> Mismos términos y condiciones</p>	<p><u>Vigencia actual</u> Prima neta actual = USD 15,767.31</p>

		<p align="center"><u>DECLARACIÓN ACTUAL</u> Del 01/15/19 al 01/05/20: Mismos términos y condiciones</p>	
3D – cubre los actos de deshonestidad de los colaboradores	<p align="center">Vigencia anterior 01/11/16 al 01/05/18</p> <hr/> <p align="center">Vigencia anterior 01/05/18 al 01/05/19</p> <hr/> <p align="center">Vigencia actual 01/05/19 Al 01/05/20</p>	<p align="center"><u>DECLARACIÓN ANTERIOR</u> Del 01/11/16 al 01/05/18: &gt; CONVENIO I – USD 500,000 &gt; CONVENIO II – USD 35,000 &gt; CONVENIO III – USD 25,000 &gt; CONVENIO IV – USD 250,000 &gt; CONVENIO V – USD 250,000 &gt; CONVENIO VI – USD 500,000</p> <p align="center"><u>DECLARACIÓN ANTERIOR</u> Del 01/05/18 al 01/05/19: Mismos condiciones</p> <p align="center"><u>DECLARACIÓN ACTUAL</u> Del 01/15/19 al 01/05/20: Mismos términos y condiciones</p>	<p align="center"><u>Vigencia actual</u> Prima MÍMINA neta actual = USD 6,586.34</p>
Vehículos – ante el daño de las unidades utilizadas en las operaciones.	<p align="center">Vigencia anterior Del 01/11/16 al 01/05/18</p> <hr/> <p align="center">Vigencia anterior Del 01/05/18 al 01/05/19</p> <hr/> <p align="center">Vigencia actual 01/05/19 Al 01/05/20</p>	<p align="center"><u>DECLARACIÓN ANTERIOR</u> Del 01/11/16 al 01/05/18: &gt; RC TERCEROS USD 250,000 &gt; RC GLOBAL USD 500,000 &gt; ACCIDENTES OCUPANTES (MUERTE) USD 40,000 &gt; ACCIDENTES OCUPANTES (INVALIDEZ) USD 40,000 &gt; ACCIDENTES OCUPANTES (GASTOS DE CURACION) USD 8,000 &gt; ACCIDENTES OCUPANTES (GASTOS DE SEPELIO) USD 4,000 &gt; ACCESORIOS MUSICALES USD 2,000 &gt; RIESGOS POLITICOS – HASTA EL VALOR CONVENIO EN DOLARES &gt; GASTOS DE BUSQUEDA Y/O RECUPERACION USD 30,000 &gt; RIESGOS DE LA NATURALEZA USD HASTA EL VALOR CONVENIDO &gt; AUSENCIA DE CONTROL USD HASTA EL VALOR COVENIDO &gt; R.C. POR AUSENCIA DE CONTROL USD HASTA EL VALOR CONVENIDO</p> <p align="center"><u>DECLARACIÓN ANTERIOR</u> Del 01/05/18 al 01/05/19: Mismos términos y condiciones</p> <p align="center"><u>DECLARACIÓN ACTUAL</u> Del 01/15/19 al 01/05/20: Mismas términos y condiciones</p>	<p align="center"><u>Vigencia actual</u> Prima neta actual = USD 12,327.49</p>

<p>Transporte (STP) – Seguro para el transporte de carga</p>	<p><u>Vigencia anterior</u> Del 13/02/17 al 13/08/18</p> <p><u>Vigencia actual</u> Del 12/09/18 al 12/03/20</p>	<p><u>DECLARACIÓN ANTERIOR</u> <u>Del 13/02/17 al 13/08/18:</u> &gt; MERCADERIA USD 170,000,000 &gt; ORO USD 500,000 &gt; TERREMOTO USD 170,000,000</p> <p><u>DECLARACIÓN ACTUAL</u> <u>Del 12/03/18 al 12/03/20:</u> &gt; MERCADERIA USD 104,000,000 &gt; ORO USD 500,000 &gt; TERREMOTO USD 104,000,000</p>	<p><u>Vigencia actual</u> Prima neta actual = USD 520,142.06</p>
<p>Directores (D&amp;O) – ofrece a los directores la seguridad que necesitan para desempeñar sus funciones.</p>	<p><u>Vigencia anterior</u> Del 01/11/16 al 01/05/18</p> <p><u>Vigencia anterior</u> Del 01/05/18 al 01/05/19</p> <p>EN PRORROGA hasta el 30/07/19</p>	<p><u>DECLARACIÓN ANTERIOR</u> <u>Del 01/11/16 al 01/05/18:</u> &gt; SUMA ASEGURADA USD 5,000,000</p> <p><u>DECLARACIÓN ANTERIOR</u> <u>Del 01/05/18 al 01/05/19:</u> Mismos términos y condiciones</p> <p><u>DECLARACIÓN ACTUAL</u> Mismos términos y condiciones</p>	<p>En proceso de negociación</p>
<p>Responsabilidad Civil Aeroportuaria</p>	<p><u>Vigencia anterior</u> Del 30/04/16 al 30/10/17</p> <p><u>Vigencia anterior</u> Del 30/10/17 al 30/04/19</p> <p><u>Vigencia actual</u> Del 30/04/19 al 30/04/20</p>	<p><u>DECLARACIÓN ANTERIOR</u> <u>Del 30/04/16 al 30/10/17:</u> &gt; SUMA ASEGURADA USD 50,000,000</p> <p><u>DECLARACIÓN ANTERIOR</u> <u>Del 30/10/17 al 30/04/19:</u> Mismos términos y condiciones</p> <p><u>DECLARACIÓN ACTUAL</u> <u>Del 30/04/19 al 30/04/20:</u> Mismos términos y condiciones</p>	<p><u>Vigencia actual</u> Prima neta actual = USD 256,084.82</p>
<p>Seguro Complementario de Trabajo de Riesgo</p>	<p><u>Vigencia anterior</u> Del 01/06/18 al 01/06/19</p> <p><u>Vigencia actual</u> 01/06/19 al 01/06/20</p>	<p><u>DECLARACIÓN ANTERIOR:</u> <u>Del 01/06/18 al 01/06/19:</u> &gt; COBERTURA ILIMITADA</p> <p><u>DECLARACIÓN ACTUAL:</u> <u>Del 01/06/18 al 01/06/19:</u> &gt; COBERTURA ILIMITADA Variación de tasas</p>	<p><u>Vigencia anterior</u> Tasa de Salud = 0.44% Tasa de Pensión = 0.15%</p> <p><u>Vigencia actual</u> Tasa de Salud = 0.42% Tasa de Pensión = 0.14%</p>

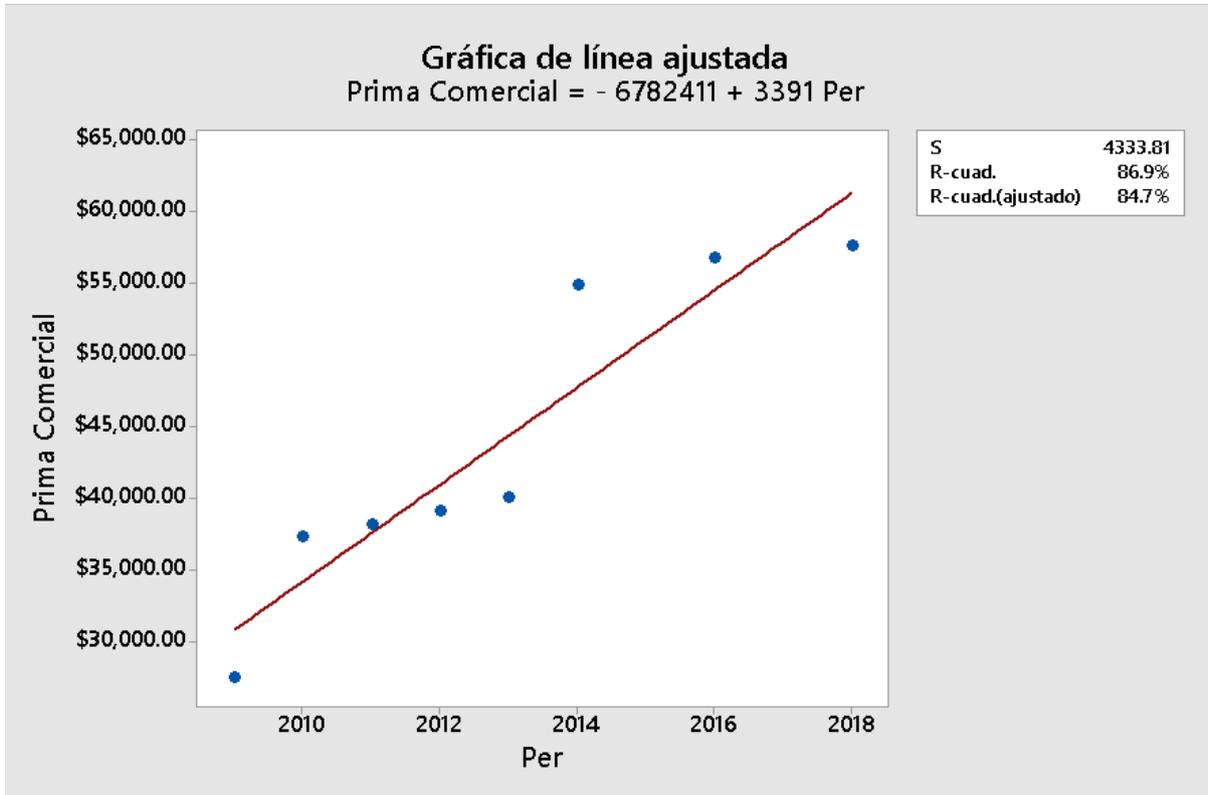
EPS – Seguro de Salud privado	<u>Vigencia anterior</u> Del 01/06/18 al 01/06/19 <hr/> <u>Vigencia actual</u> 01/06/19 al 01/06/20	<u>DECLARACIÓN ANTERIOR</u> Del 01/06/18 al 01/06/19: > COBERTURA ILIMITADA Cobertura oncológica - Reaseguro  <u>DECLARACIÓN ACTUAL</u> Del 01/06/19 al 01/06/20: > COBERTURA ILIMITADA Cobertura oncológica – Plan AMC de Rímac	Según tabla de costos por plan de afiliación y composición familiar
Accidentes contra terceros	<u>Vigencia anterior</u> Del 18/03/18 al 18/03/19 <hr/> <u>Vigencia actual</u> 18/03/19 al 18/03/20	<u>DECLARACIÓN ANTERIOR</u> Del 18/03/18 al 18/03/19: > MUERTE ACCIDENTAL - USD 50,000 > INVALIDEZ PERMANENTE - USD 50,000 > GASTOS DE CURACION - USD 5,000 > GASTOS DE SEPELIO - USD 3,000  <u>DECLARACIÓN ANTERIOR</u> Del 18/03/19 al 18/03/20: Mismos términos y condiciones	<u>Vigencia actual</u> Prima neta actual = USD 1,853.99
FOLA – Seguro para practicantes.	<u>Vigencia actual</u> Del 01/06/18 al 01/06/19 <hr/> <u>Vigencia actual</u> 01/06/19 al 01/06/20	<u>DECLARACIÓN ANTERIOR</u> Del 01/06/18 al 01/06/19: > BENEFICIO MÁXIMO ANUAL POR ENFERMEDAD - S/. 17,500.00 > BENEFICIO MÁXIMO POR ASEGURADO PARA ACCIDENTES - S/. 37,500.00  <u>DECLARACIÓN ACTUAL</u> Del 01/06/19 al 01/06/20: Mismas condiciones	-

El valor de las primas se ha incrementado constantemente, ello debido al bajo nivel de madurez de riesgos con el cual se contaba. Para la investigación, se decidió analizar uno de los seguros contratados por la organización y analizar las variaciones del mismo. Cabe resaltar que dichas variaciones son similares para todos los seguros, exceptuando el seguro FOLA. A continuación, en la Tabla 47, se presentará la prima neta, prima comercial, prima bruta y la variación porcentual de la prima comercial del seguro de responsabilidad civil de la organización y en la Figura 47, se observa su línea ajustada con un  $R^2$  cercano al 87%,

**Tabla 47 Variación porcentual del seguro de Responsabilidad Civil**

Periodo	Prima Neta	Derecho Emisión	Prima Comercial	IGV	Prima Bruta	Prima Mensual	Variación porcentual
2012-2013	\$26,730.00	\$801.90	\$27,531.90	\$5,231.06	\$32,762.96	\$2,196.99	
2013-2014	\$36,271.00	\$1,088.13	\$37,359.13	\$7,098.23	\$44,457.36	\$2,981.18	36%

2014-2015	\$37,061.19	\$1,111.84	\$38,173.03	\$7,252.87	\$45,425.90	\$2,032.61	2%
2015-2016	\$38,000.99	\$1,140.03	\$39,141.02	\$7,436.79	\$46,577.81	\$4,367.93	3%
2016-2017	\$38,877.31	\$1,166.32	\$40,043.63	\$7,608.29	\$47,651.92	\$2,136.12	2%
2017-2018	\$53,310.42	\$1,599.31	\$54,909.73	\$10,432.85	\$65,342.58	\$2,913.14	37%
2018-2019	\$55,157.53	\$1,654.73	\$56,812.26	\$10,794.33	\$67,606.58	\$3,030.63	3%
2019-2020	\$56,000.60	\$1,680.02	\$57,680.62	\$10,959.32	\$68,639.94	\$4,602.79	2%



**Figura 46 Gráfica de línea ajustada**

Asimismo, se muestra la Tabla 47, en la cual se muestra el porcentaje de siniestralidad para cada uno de los años evaluados, como se observa la ocurrencia de siniestros comenzó desde el año 2014, ello debido al constante aumento de actividad en la organización y a una falta de mejoría en el nivel de madurez de la gestión de riesgos de la organización.

**Tabla 48 Porcentaje de siniestralidad por año**

Periodo	Gasto	Siniestros	% Siniestralidad
2012	\$21,969.86		0%
2013	\$27,932.22		0%
2014	\$33,876.99		0%
2015	\$24,391.28		0%
2016	\$40,738.54		0%
2017	\$27,865.20	\$10,000	39%
2018	\$29,518.50	\$47,000	159%
2019	\$35,192.64	\$780,883	2219%

2020	\$36,367.60	\$0	0%
2021	\$48,944.85	\$34,834	114%

Por otro lado, al implementarse dichas actividades pendientes especificadas en el capítulo 4.4. Aplicación de las actividades pendientes, se realizó un comité en la organización para poder determinar en conjunto la reducción final de la probabilidad y consecuencia de los riesgos en la organización. En este comité asistieron dueños de proceso, áreas de soporte y los expertos tales como el área de sistema integrado de gestión y auditoría interna. Después de un extenso debate, llegaron a la conclusión que los eventos generadores de riesgo, disminuirían en un 15%, por ello en la Tabla 49, se muestra la proyección de costos de Prima Neta para el año 2021 para la cual solo se considera el 85% de la Prima Neta Actual.

**Tabla 49 Proyección de Costos de Prima Neta**

Tipo de seguro	Prima Neta	Proyección año 2020
Todo Riesgo	<u>Vigencia actual</u> Prima neta actual = USD 225,633.42	<u>USD 191,788.41</u>
Responsabilidad Civil General	<u>Vigencia actual</u> Prima neta actual = USD 15,767.31	<u>USD 13,402.21</u>
3D	<u>Vigencia actual</u> Prima MÍMINA neta actual = USD 6,586.34	<u>USD 5,598.39</u>
Vehículos	<u>Vigencia actual</u> Prima neta actual = USD 12,327.49	<u>USD 10,478.37</u>
Transporte (STP)	<u>Vigencia actual</u> Prima neta actual = USD 520,142.06	<u>USD 442,120.75</u>
Directores (D&O)	En proceso de negociación	-
Responsabilidad Civil Aeroportuaria	<u>Vigencia actual</u> Prima neta actual = USD 256,084.82	<u>USD 217,672.10</u>
Seguro Complementario de Trabajo de Riesgo	<u>Vigencia actual</u> Tasa de Salud = 0.42% Tasa de Pensión = 0.14%	-
EPS	Según tabla de costos por plan de afiliación y composición familiar	-

Accidentes contra terceros	<u>Vigencia actual</u> Prima neta actual = USD 1,853.99	<u>USD 1,575.8915</u>
FOLA	-	-
Ahorro Total		<u>USD 155,759.31 = S/.</u> <u>528,024.08</u>

Según ello, se procede a calcular los costos para evaluar la factibilidad de implementación de los cambios en la organización. La Tabla 50, muestra los costos de forma detallada.

**Tabla 50 Costos totales por implementación**

Ítem	Cantidad	Costo	Total
Política de Gestión de Riesgos			
H-H	5	S/. 21.88	S/. 109.38
Impresión en material Celtex A3	100	S/. 23.00	S/. 2,300.00
Portafolio de riesgos			
H-H	60	S/. 21.88	S/. 1,312.50
Software para la evaluación de riesgos			
Compra de licencias de software	10	S/. 5,000.00	S/. 50,000.00
H-H desarrollo	120	S/. 21.88	S/. 2,625.00
H-H Capacitación	40	S/. 21.88	S/. 875.00
H-H Recolección de data	120	S/. 21.88	S/. 2,625.00
<b>Costos totales por implementación</b>			<b>S/. 59,846.88</b>

Como resultado del primer año, se cuenta con un ahorro de S/. 468,177.20.

## **6. CONCLUSIONES Y RECOMENDACIONES**

### **6.1 Conclusiones**

Se tienen las siguientes conclusiones para la organización del sector aeroportuario:

- ✓ Definir e implementar el sistema de gestión de riesgos en una empresa logística del sector aéreo, generará un ahorro de S/. 468,177.20, el cual deberá ser presentado a la alta gerencia para la ejecución de los elementos propuestos.
- ✓ Se implementará la política de gestión de riesgos, la cual nos apoyará en asegurar el apoyo de la gerencia en nuestra gestión, así como también, nos apoyará en establecer lineamientos generales para la gestión de riesgos de la organización.
- ✓ Se contará con un registro de riesgos por sistema afectado, esto nos servirá para poder estandarizar controles básicos en riesgos repetitivos de la organización.
- ✓ Se implementará un software de gestión de riesgos, que a pesar de ser el más costoso, apoyará de forma efectiva en el análisis de riesgo cuantitativo y su seguimiento y medición de los mismos.

### **6.2 Recomendaciones**

Se tienen las siguientes recomendaciones para la organización del sector aeroportuario:

- ✓ Se recomienda realizar un análisis de la madurez de la gestión de riesgos de la organización de forma anual, ello permitirá que se sigan implementando medidas conforme a las normativas seleccionadas.
- ✓ Se recomienda la mejora en la comunicación con los clientes, stakeholders y partes interesadas, de esta forma se afianzarán las relaciones y la confianza de los mismos hacia la compañía.
- ✓ Se recomienda el uso de los indicadores de riesgos claves para la sectorización de procesos en las auditorías realizadas por el área interna, ello permitirá estar mejor preparados ante una auditoría externa.

## 7. BIBLIOGRAFIA

AVALOS, Carlos

2012 ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE RIESGO OPERACIONAL PARA ENTIDADES FINANCIERAS - SIRO. Tesis de Magister en Informática con mención en ingeniería del software, Lima: Pontificia Universidad Católica del Perú.

BRAVO, Oscar y SANCHEZ, Marleni

2012 Gestión Integral de Riesgos. Colombia: pp. 17-49  
<https://b-ok.cc/book/2693612/bd00a9>

DE SENA, Alicia

2018 “A more effective audit after COSO ERM 2017 or after ISO 31000:2009?” Europa: pp. 11-12.

DICKINSON, G.

2001 Enterprise Risk Management: Its Origins and Conceptual Foundation. The Geneva Papers on Risk and Insurance. Issues and Practice, 360-366.

DVORSKI, Ivana

2018 “Enterprise Risk Management: a literature survey”. Veintiseisava conferencia científica internacional de economía y desarrollo social. Croacia.

FARROMEQUE, Rafael

2015 CAF, Banco de Desarrollo de América Latina Análisis de Inversiones Aeroportuarios y Portuarias p.19-21. <https://scioteca.caf.com/handle/123456789/1160?show=full>

FOX, Carol

2018 “Understanding the New ISO and COSO Updates” Forefronte pp. 4-7.

GONZALES, Ada

2016 Gestión del riesgo empresarial en la atención del cliente: Caso de la empresa de transportes Mi Chaperito, 2016. Tesis de licenciatura en Gestión, Lima: Pontificia Universidad Católica del Perú.

INTERNATIONAL ORGANIZATION FOR STANDARIZATION (ISO)

2012 ISO 31010:2012 Técnicas de apreciación del riesgo. Lima: Pontificia Universidad Católica de Perú, Sistema de Bibliotecas.

INTERNATIONAL ORGANIZATION FOR STANDARIZATION (ISO)

2018 ISO 31000:2018 Gestión de Riesgos. Lima: Pontificia Universidad Católica de Perú, Sistema de Bibliotecas.

MEHMET

2011 Comparación entre ISO 31000 y COSO ERM Turquía: pp.12.

MOELLER, Robert

2011 COSO Enterprise Risk Management – Establishing effective GOVERNANCE Risk, and Compliance processes Nueva Jersey: 32-45

MOTET, Gilles

2017 “Uncertainty: New Perspectives, Questions and Proposals”. The Illusion of Risk Control What Does it Take to Live With Uncertainty? Toulouse: pp. 2-4.

<http://www.springer.com/series/15119>

MUN, Johnathan

2015 Modelación de Riesgos – Aplicación de la Simulación de Monte Carlo, Análisis de Opciones Reales, Pronóstico Estocástico, Optimización de Portafolio, Análisis de Datos, Inteligencia de Negocios, y Modelación de Decisiones. California: pp. 39-40.

OLIVEIRA, Killbert

2018 “Critical success factors associated with the implementation of Enterprise risk managente”.  
<http://www.tandonline.com/loi/rjrr20>

OSORIO, Juan

2017 “El proceso de gestión de riesgos como componente empresarial”. Boletín de estudios económicos. Madrid.

PAAPE, SPEKLE (2012, p.2),

PFOHL, H., GALLUS, P., y THOMAS, D.

2011 Interpretive structural modeling of supply chain risks. International Journal of Physical Distribution & Logistics Management, 41(9), 839–859

SALMÓN, Juan

2017 LAP – Lima Airport Partners. Informe Integrado de Sostenibilidad 2017

[https://www.lima-](https://www.lima-airport.com/esp/Documents/Informe_de_Sostenibilidad_y_Memoria_2017.pdf)

[airport.com/esp/Documents/Informe de Sostenibilidad y Memoria 2017.pdf](https://www.lima-airport.com/esp/Documents/Informe_de_Sostenibilidad_y_Memoria_2017.pdf)

SIDORENKO, Alex & DEMIDENKO, Elena

2017 Free risk management book: Guide to Effective Risk Management 3.0.

[https://www.researchgate.net/publication/323254437\\_FREE\\_RISK\\_MANAGEMENT\\_BOOK\\_GUIDE\\_TO\\_EFFECTIVE\\_RISK\\_MANAGEMENT\\_30](https://www.researchgate.net/publication/323254437_FREE_RISK_MANAGEMENT_BOOK_GUIDE_TO_EFFECTIVE_RISK_MANAGEMENT_30)

TRANCHARD, Sandrine

2018 The New ISO 31000 Keeps risk management simple  
Feature article Risk Management: pp. 180-182.