UPN
UNIVERSIDAD PRIVADA DEL NORTE

FACULTAD DE NEGOCIOS

Carrera de Administración

"DISEÑO E IMPLEMENTACIÓN DE UNA MATRIZ DE RIESGOS GENERALES PARA UNA EMPRESA EMISORA DE DINERO ELECTRÓNICO"

Trabajo de suficiencia profesional para optar al título profesional de:

Licenciada en Administración

Autor:

Carmen Yare Boza Menacho

Asesor:

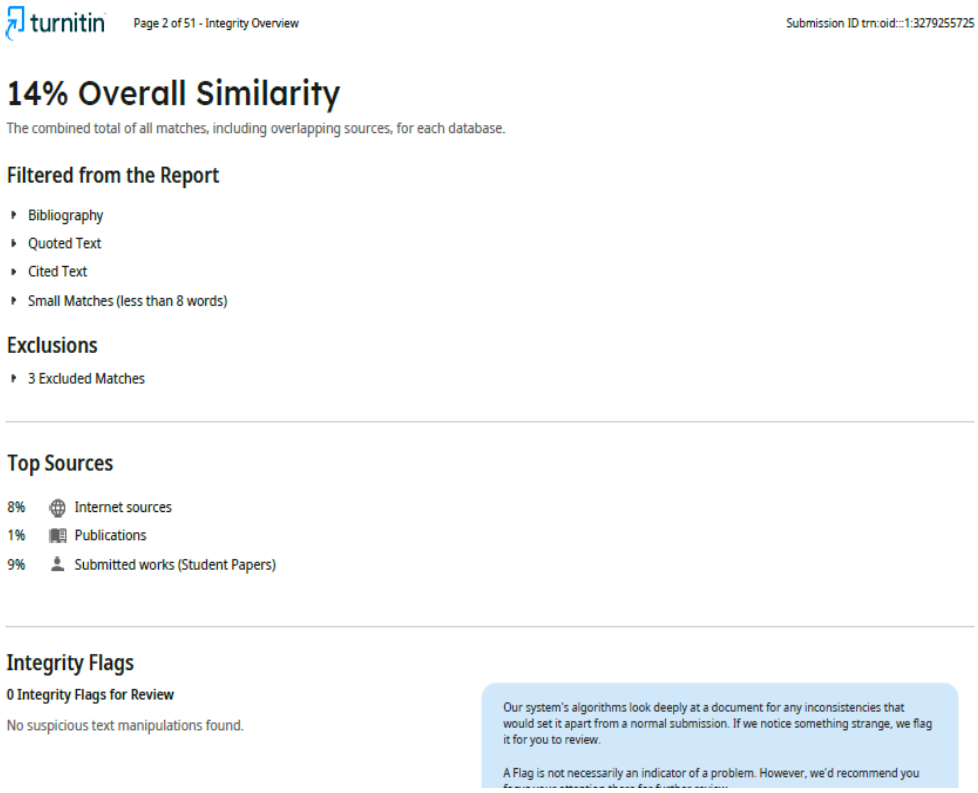
Dr. Mario Edison Ninaquispe Soto

https://orcid.org/0000-0002-6287-3291

Lima - **Perú**

2025

Informe de Similitud



turnitin Page 2 of 51 - Integrity Overview Submission ID trn:oid:::1:3279255725

14% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text
- Cited Text
- Small Matches (less than 8 words)

Exclusions

- 3 Excluded Matches

Top Sources

8% Internet sources
1% Publications
9% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you

DEDICATORIA

A mis padres Carmen y Héctor, por su amor incondicional, por cada sacrificio y por creer en mí incluso cuando yo dudaba. Este logro es también de ustedes, porque sin su apoyo constante no habría sido posible. A mi familia y a todas las personas que me acompañaron en este camino, gracias por su presencia, aliento y confianza.

Con profundo agradecimiento.

AGRADECIMIENTO

Expreso mi agradecimiento a Dios, por permitirme culminar esta etapa importante en mi vida profesional.

Agradezco de manera especial a mis padres y familia, por su apoyo incondicional, su comprensión y por ser parte fundamental en la consecución de este logro.

Extiendo mi reconocimiento a los docentes que, con su guía y conocimientos, aportaron significativamente a mi desarrollo académico y profesional.

Finalmente, a todas las personas e instituciones que me brindaron la oportunidad de crecer, aprender y seguir formándome como profesional.

Tabla de contenidos

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El presente tiene como objetivo expone el desarrollo e implementación de una matriz de riesgos corporativos en Tebca Perú, con el objetivo de fortalecer la gestión integral del riesgo a nivel organizacional. Esto nació a partir de una serie de incidentes no previstos, en donde se identificó la necesidad de contar con una herramienta que permita reconocer, evaluar y controlar riesgos transversales que afecten a la empresa, los cuales antes no eran gestionados de forma estructurada.

Para ello, se adoptó el modelo COSO ERM, aplicando una metodología que abarcó desde la identificación y clasificación de riesgos, hasta la evaluación de controles y diseño de planes de acción. Como resultado, se identificaron y evaluaron 20 riesgos clave, priorizando aquellos con alto nivel de exposición. Se analizaron los controles vigentes, identificando oportunidades de mejora y diseñando planes de acción específicos para mitigar los riesgos más críticos. Asimismo, se estableció un sistema de seguimiento continuo que promueve una gestión preventiva y dinámica del riesgo.

El informe evidencia que la implementación de la matriz no solo mejoró la identificación y control de riesgos, sino que también contribuyó a generar una cultura organizacional orientada a la prevención, la mejora continua y la toma de decisiones informada. Esta iniciativa representa un avance significativo en la capacidad de Tebca para enfrentar eventos adversos y garantizar su continuidad operativa en un entorno cambiante y exigente.

CAPÍTULO I. INTRODUCCIÓN

1.1. **Contextualización de problemática**

Todas las empresas, sin importar su tamaño o estructura, están expuestas a distintos riesgos que pueden afectar su sostenibilidad, competitividad, cumplimiento normativo y capacidad de adaptación frente a cualquier incertidumbre(Robles, Castañeda & Carrizo, 2019). Según Mejía Quijano (2004), una adecuada gestión de riesgos permite a las empresas evitar pérdidas económicas, proteger su reputación y garantizar su continuidad operativa.

Alcócer Barrientos (2019) recalca que una adecuada gestión del riesgo exige mejores procesos de control capaces de identificar deficiencias y mitiga oportunamente las consecuencias negativas. Para esto, el control interno debe plasmarse bajo una perspectiva de riesgo, logrando mejorar la objetividad en los procesos de auditoría, especialmente cuando no se dispone de normativas claramente establecidas.

En relación a lo anterior, Rodríguez López, Piñeiro Sánchez y Llano Monelos (2013) nos indican que las empresas deben contar con mecanismos que les permitan identificar la incertidumbre entro de sus procesos, evaluar los controles existentes y adoptar medidas que mantengan el riesgo dentro de niveles tolerables para la empresa.

La experiencia internacional muestra que países como México, Brasil y Argentina han adoptado modelos de gestión basados en buenas prácticas y tecnologías emergentes, con el objetivo de optimizar recursos, procesos y asegurar una gestión proactiva de riesgos (Mejía, Núñez, Villanueva & Jaraba, 2024).

En el ámbito público, Ortiz Mosquera (2021) sostiene que un modelo eficiente de gestión de riesgos contribuye significativamente a la toma de decisiones estratégicas y al cumplimiento de los objetivos institucionales.

En el caso peruano, Alexander (2018), vocero de SGS Academy, advierte que muchas empresas aún no están preparadas para enfrentar situaciones de riesgo o crisis. Señala que la mayoría no cuenta con planes adecuados de mitigación y que el proceso de implementación es lento y poco sistemático. Al respecto, Noblecilla Flores (2020) afirma que la implementación de un sistema de gestión de riesgos y continuidad del negocio permite comprender los procesos críticos y su impacto, mejorando así la resiliencia organizacional y el desempeño global.

1.2 **Descripción de la empresa**

Servitebca Perú, conocida comercialmente como Tebca Perú, es una empresa fintech autorizada por la Superintendencia de Banca, Seguros y AFP (SBS) para operar como emisora de dinero electrónico. Fue fundada el 15 de octubre de 2008 y está ubicada en Av. Circunvalación del Club Golf los Incas, Lima - Santiago de Surco (Superintendencia de Banca, Seguros y AFP, s.f.).

Tebca Perú forma parte del grupo regional, el cual tiene presencia en Venezuela, Panamá y Ecuador, lo cual respalda su experiencia en el rubro tecnológico. En Perú esta especializa en el desarrollo e implementación de soluciones digitales para facilitar y optimizar la gestión de pagos, tanto para personas como para empresas, haciendo uso de tecnologías que impulsan la eficiencia operativa (Tebca, s.f.).

1.2.2 **Misión**

"Facilitar los pagos y hacer que las empresas y personas tengan una mejor gestión financiera y ordenen su economía" (MiPlata, s.f., párr. 1).

1.2.3 Visión

"Ser reconocidos como la empresa líder en la administración y gestión de programas prepago en el Perú" (MiPlata, s.f., párr. 1).

1.2.4 Productos

Tebca ofrece soluciones de pago orientados a facilitar pagos corporativos, organizados en cuatro verticales:

- Alimentación: Tarjetas prepago utilizadas como beneficio alimentario para colaboradores.
- Viáticos: Herramientas para gestionar los gastos de viaje de personal.
- Fondos fijos: Administración de pequeñas cajas para gastos operativos.
- Gasolina: Control y optimización del consumo de combustible corporativo.

Además, Tebca cuenta con una plataforma digital que permite la consulta de saldos, historial de movimientos y bloqueo/desbloqueo de tarjetas, promoviendo la autonomía del usuario y reduciendo la carga operativa de las empresas. (Tebca, s.f.).

12.3.5 Organigrama

La estructura organizacional de Tebca se encuentra liderada por la Gerencia

General, quien tiene a su cargo la gerencia comercial, Operaciones y Tecnología, Riesgos y cumplimiento y Administración y finanzas.

Estas gerencias desarrollan funciones específicas

- Gerencia Comercial: En cargada de elaborar estrategias de ventas, posicionamiento, fidelización y crecimiento de portafolio de clientes. Esta gerencia promueve el ingreso de nuevos clientes.
- Gerencia de Riesgos y Cumplimiento: Vela por la mitigación de riesgos operacionales y supervisa el cumplimiento normativo establecido por la SBS y otros entes reguladores,
- Gerencia de Operaciones y Tecnología: Encargada de garantizar la eficiencia operativa y la continuidad de los servicios digitales.
- Gerencia de Recursos Humanos: Encargado de los procesos de atracción, desarrollo, evaluación y retención del talento humano. Promueve la cultura organizacional, lidera los programas de bienestar, capacitación y desempeño, y asegura el cumplimiento de la normativa laboral.
- Gerencia Legal: Encargado de supervisar el cumplimiento normativo y representa a la empresa ante entidades regulatorias, administrativas o judiciales cuando corresponde.

Este flujograma (Figura 1) permite visualizar la jerarquía y distribución de responsabilidades dentro de Tebca. Asimismo, se incluye en el Anexo 1 el flujograma general, donde se detalla de manera completa la estructura organizacional de la empresa, incluyendo las áreas operativas y de soporte.

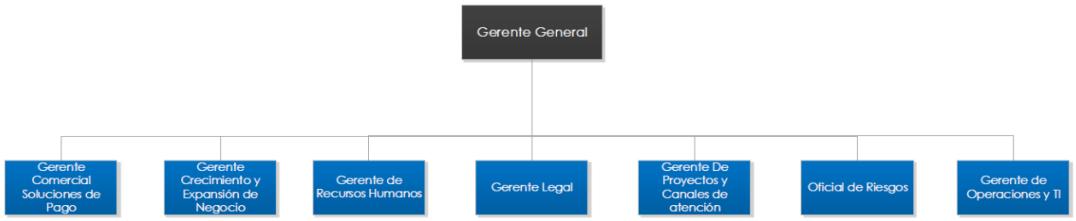


Ilustración 1 Organigrama de Tebca

Nota. Gráfico tomado de un documento interno de Tebca (2025). No publicado.

1.3 Problemática detectada en la empresa

Desde fines de 2023, Tebca ha experimentado una creciente recurrencia de incidencias que afectan los procesos de atención y respuesta al usuario. Esta situación ha incrementado el riesgo de pérdidas económicas y de daño reputacional frente a los clientes. El análisis reveló que la totalidad de los incidentes correspondía a riesgos no identificados previamente, los cuales no contaban con monitoreo ni control activo.

Hasta ese momento, Tebca solo gestionaba riesgos operativos asociados a procesos específicos. No existía un mapeo de riesgos transversales o corporativos que, al no estar asociados a un proceso puntual, habían quedado fuera del radar, a pesar de su potencial impacto significativo.

Frente a esta situación, se propuso diseñar e implementar una Matriz de Riesgos Corporativos, cuyo propósito es identificar, monitorear y controlar los riesgos que afectan transversalmente a la organización, facilitando una toma de decisiones informada y oportuna.

CAPÍTULO II. MARCO TEÓRICO

Riesgo

El riesgo puede definirse como la posibilidad de que ocurra un evento que afecte negativamente el logro de los objetivos de una organización, ya sea en sus procesos, personas o sistemas, generando potenciales pérdidas (Estupiñán, 2006). Cassidy et al. (2001, como se citó en Gutiérrez & Sánchez-Ortiz, 2018) amplían esta noción al describir el riesgo como cualquier amenaza que compromete la capacidad de una organización para alcanzar sus metas estratégicas. Estos autores identifican cinco categorías principales de riesgo:

Riesgo estratégico: Relacionado con la afectación de la misión, visión y objetivos organizacionales. Este riesgo puede surgir por amenazas externas o internas que alteren la dirección estratégica de la empresa (Mejía, 2013, como se citó en Mejía Quijano & Villanueva Herrera, 2014).

Riesgo financiero: Deriva de la incertidumbre en el rendimiento económico debido a factores como la inestabilidad de los mercados o cambios en el entorno económico (Mascareñas, 2008, como se citó en Riesgo financiero en las empresas de Medellín, 2015).

Riesgo operativo: Surge de fallas en los procesos internos, sistemas tecnológicos o errores humanos, que pueden generar pérdidas para la organización (Becerra, Guzmán & Trujillo, 2006).

Riesgo de cumplimiento: Está relacionado con la posibilidad de

incumplimiento de normas legales, reglamentos internos o compromisos voluntarios asumidos por la organización (International Organization for Standardization, 2021, como se citó en Plasencia Soler et al., 2023).

Riesgo reputacional: Se refiere a los daños que puede sufrir la imagen de la empresa, lo cual puede repercutir en su valor de mercado, ingresos y confianza de los stakeholders (Rodríguez López, Piñeiro Sánchez & de Llano Monelos, 2013).

2.2 Herramientas para medición del riesgo

2.2.1 Matriz de riesgo

La matriz de riesgos es una herramienta clave para la gestión del riesgo, ya que permite organizar los eventos potenciales, priorizar aquellos con mayor impacto y planificar respuestas eficaces (Schaeffer García, 2008). Esta herramienta facilita la identificación de procesos críticos, el nivel de riesgo asociado a cada actividad, y funciona como mecanismo de control y gestión (Elizarzaburu, Barriga, Burneo & Noriega, 2019).

No obstante, su implementación exige un conocimiento profundo del negocio y del marco legal vigente, tanto por parte del gobierno corporativo como del personal involucrado (Albanese, 2012).

2.2.2 Mapa de riesgos

El mapa de riesgos es una representación visual que busca identificar y analizar los procesos expuestos a riesgos, cuantificando la probabilidad de

ocurrencia y el daño potencial (Rodríguez López, Piñeiro Sánchez & de Llano Monelos, 2013). Esta herramienta ofrece una visión integral de las amenazas, favoreciendo la toma de decisiones estratégicas.

Entre los principales beneficios del mapa de riesgos se destacan:

- Brinda una visión global de los riesgos identificados.
- Facilita la gestión y priorización de recursos.
- Contribuye al control de mando y al monitoreo continuo.
- Permite alinear los planes de tratamiento de riesgos con los objetivos organizacionales (Celada López, Quintero Castaño & Ríos Sanabria, 2016).

2.3 **Metodologías de gestión de riesgos**

COSO ERM

El marco COSO ERM (Enterprise Risk Management) proporciona un enfoque estructurado para la identificación, evaluación, respuesta y monitoreo del riesgo, alineado con los objetivos estratégicos de la organización. Este modelo facilita:

- La alineación del riesgo con la estrategia organizacional.
- La integración entre riesgo, rendimiento y crecimiento.
- La mejora de las decisiones y respuestas frente al riesgo.
- La minimización de sorpresas operativas.
- La racionalización del uso de recursos (Sánchez Sánchez, 2015).

Estupiñán (2006) describe los cinco componentes esenciales del modelo COSO ERM:

- Ambiente de control
- Evaluación de riesgos
- Actividades de control
- Información y comunicación
- Monitoreo

Este enfoque permite fortalecer el control interno y fomentar una cultura de gestión de riesgos sólida y transversal.

2.4 Evaluación del riesgo

La evaluación de riesgos es un proceso continuo que permite a la organización comprender cómo los eventos podrían afectar sus objetivos. Este análisis considera tanto el riesgo inherente (riesgo sin controles) como el riesgo residual (riesgo posterior a la aplicación de controles) (Pasos Chávez, 2018).

2.4.1 **Probabilidad**

La probabilidad se refiere a la frecuencia estimada de ocurrencia de un riesgo, tomando en cuenta datos históricos y el juicio de expertos. Su evaluación considera qué tan probable es que el evento se materialice en ausencia de controles (Rodríguez López et al., 2013).

2.4.2 **Actividades del control**

Las actividades de control son mecanismos diseñados para prevenir, detectar o corregir los riesgos. Estas pueden clasificarse en:

- Controles preventivos
- Controles detectivos
- Controles correctivos
- Controles manuales o tecnológicos
- Controles administrativos (Celada López et al., 2016)

Estas actividades deben formar parte integral de los procesos operativos y ser monitoreadas de forma continua para garantizar su eficacia.

2.5 Limitaciones en la elaboración del proyecto

Durante el desarrollo del presente proyecto se identificaron las siguientes limitaciones:

- El plazo disponible para la elaboración e implementación de la matriz fue reducido debido a la urgencia del requerimiento.
- La disponibilidad de tiempo de los gerentes fue limitada para coordinar reuniones y validaciones.
- Se detectó un nivel de conocimiento limitado en temas de riesgo por parte de algunas gerencias, lo que requirió acciones adicionales de capacitación y acompañamiento.

CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA

3.1. Ingreso a la empresa

Mi incorporación a Tebca Perú se dio en junio de 2024, luego de un primer contacto a través de la red profesional LinkedIn, donde la Gerencia de Riesgos me informó sobre la disponibilidad de una posición vacante. Fui contratada bajo la modalidad de contrato a plazo indeterminado para asumir el cargo de Analista de Riesgo Operacional y Continuidad del Negocio, posición que desempeño actualmente.

Dentro de este rol, tengo a mi cargo funciones fundamentales como la priorización de procesos críticos, la identificación y evaluación de riesgos mediante la estimación de su impacto y probabilidad, así como la elaboración e implementación de planes de acción correctivos y preventivos. Además, lidero la definición y monitoreo de los Indicadores Clave de Riesgo (KRI), asegurando su seguimiento periódico.

En cuanto a la gestión de proveedores críticos, participo en sus evaluaciones periódicas y en la identificación de riesgos asociados. En el marco de la Continuidad del Negocio, me encargo de la actualización de planes de contingencia, ejecución de pruebas de escritorio y simulacros, además de brindar capacitaciones a los colaboradores en temas relacionados con continuidad operativa y gestión de riesgos.

3.2 Elaboración del proyecto

El proyecto desarrollado tuvo como objetivo principal diseñar y estructurar una Matriz Integral de Riesgos a nivel corporativo, con el propósito de identificar, clasificar y evaluar los riesgos que afectan transversalmente a la organización. Esta herramienta permite conocer el nivel real de exposición al riesgo y facilita la toma de decisiones estratégicas orientadas a la prevención y a la continuidad operativa del negocio.

El desarrollo del proyecto se estructuró en siete etapas, organizadas de manera secuencial, en colaboración con las distintas gerencias de la empresa:

ETAPAS DE MATRIZ DE RIESGOS

Etapa	Desarrollo
01. Planificación y Preparación	• Selección de metodología a trabajar • Diseño de formatos y herramientas para levantamiento de riesgos
02. Identificación de Riesgos	• Realizar talleres y entrevistas con las gerencias para identificar eventos que puedan afectar el logro de los objetivos. • Clasificar los riesgos en categorías como estratégicos, operativos, financieros, de cumplimiento, tecnológicos, reputacionales, entre otros.
03. Evaluación de Riesgos	• Analizar la probabilidad y el impacto de cada riesgo identificado. • Utilizar una matriz de riesgos (por ejemplo, 5x5) para determinar el nivel de riesgo inherente. • Considerar múltiples dimensiones de impacto, como financiero y reputacional.
04. Evaluación de Controles Existentes	• Identificar los controles actuales que mitigan cada riesgo. • Evaluar la efectividad de estos controles para determinar el riesgo residual.
05. Desarrollo de Planes de Acción	• Para los riesgos con niveles residuales inaceptables, desarrollar planes de acción específicos. • Asignar responsables y establecer plazos para la implementación de las acciones correctivas..
06. Monitoreo y Revisión	• Programar revisiones periódicas de la matriz de riesgos y de la efectividad de los controles implementados.

Ilustración 2 Ejecución del Proyecto

Fuente: Elaboración Propia

Se detalla los puntos realizados por cada etapa

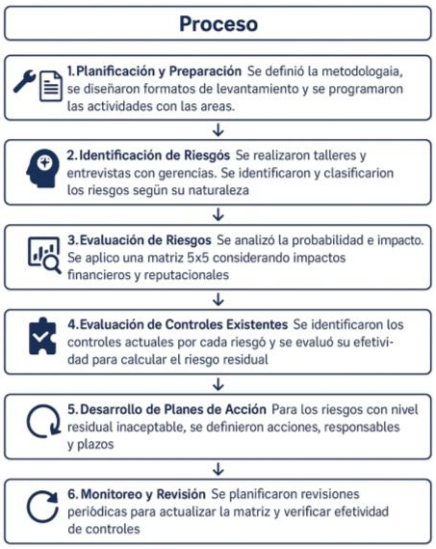


Ilustración 3 Desarrollo de etapas

Fuente: Elaboración Propia

Etapa 1: Planificación y Preparación

En esta etapa se conformó el equipo de trabajo que apoyaría en la identificación de riesgos, integrando representantes de las distintas gerencias. Asimismo, se definió la metodología a utilizar, para lo cual se sostuvieron reuniones virtuales mediante Microsoft Teams con la Gerencia de Riesgos y Cumplimiento. En estas sesiones se evaluaron diversas metodologías y se seleccionó el enfoque COSO ERM, por su alineación con los objetivos estratégicos de la organización y su estructura clara para la identificación y evaluación de riesgos.

Como parte del proceso, se elaboró una presentación en PowerPoint para Gerencia General, en la que se explicaron las escalas de probabilidad e impacto, y se propuso el uso de una matriz estructurada. Posteriormente, se diseñó una plantilla en Excel como formato base para el levantamiento de información por parte de las áreas.

Tras la validación y retroalimentación de la alta dirección, se realizaron los ajustes

requeridos y se aprobó la versión final de la matriz, habilitándola para su uso en las siguientes etapas.

Etapa 2: Identificación del riesgo

Se convocó a las principales gerencias de Tebca (Legal, Riesgos y Cumplimiento, Operaciones, Proyectos, Producto y Comercial) para participar en el proceso de identificación de riesgos. En una primera reunión virtual, se brindó una **capacitación introductoria** sobre conceptos clave de gestión de riesgos, tales como: definición de riesgo, tipos de causas, niveles de impacto, controles existentes y proceso de levantamiento.

Cada gerencia recibió un paquete de trabajo que incluía:

- Matriz de riesgos en blanco.
- Instrucciones detalladas para el llenado.
- Preguntas orientadoras para facilitar un análisis reflexivo.

Posteriormente, se agendaron reuniones individuales con cada gerencia para **acompañar la revisión y validación de los riesgos identificados**, retroalimentando sobre su clasificación y detalle

Etapa 3: Evaluación de Riesgos

Con los riesgos ya identificados, se realizó una reunión presencial que incluyó a Gerencia General y las demás gerencias participantes. En esta sesión se aplicó una matriz de 5x5, considerando dos dimensiones de impacto (financiero y reputacional) y una escala de probabilidad.

Este proceso permitió establecer el nivel de riesgo inherente de cada evento, priorizando aquellos que requerían atención inmediata.

Etapa 4:Evaluación de controles existentes

Se realizaron reuniones presenciales para identificar los controles actualmente aplicados a cada riesgo. Se analizó su cobertura, frecuencia y documentación, con el fin de determinar su grado de efectividad.

Esta evaluación permitió calcular el nivel de riesgo residual, es decir, el riesgo que persiste luego de aplicar los controles. El análisis ayudó a distinguir entre riesgos con medidas de mitigación suficientes y aquellos que necesitaban ser reforzados.

Etapa 5: Desarrollo de planes de acción

Se elaboraron planes de acción específicos para los riesgos con nivel residual alto o con controles insuficientes. Cada plan se estructuró respondiendo a las preguntas clave: ¿quién? ¿cuándo? ¿cómo? ¿dónde?, incluyendo responsables, cronograma y actividades concretas de mejora.

La validación de estos planes se realizó en conjunto con las áreas responsables, alineándolos con los recursos y capacidades de cada unidad.

Etapa 6: Monitoreo y revisión

Se estableció un cronograma de revisión semestral de la matriz de riesgos, con el objetivo de mantener su vigencia ante posibles cambios en el entorno, procesos o estructura organizacional.

Asimismo, se definió una frecuencia mensual de seguimiento de planes de acción, y se dispuso la actualización sistemática de la información en el sistema de gestión de riesgos, incluyendo evidencias de avance y cumplimiento.

CAPÍTULO IV. RESULTADOS

Etapa 1: Planificación y preparación: Se seleccionó como metodología el marco COSO ERM, priorizando un análisis de los objetivos.

En esta etapa se desarrollaron las herramientas de trabajo para el levantamiento de los riesgos. A continuación, se detallan cuales fueron:

Plantilla de levantamiento de riesgos: Se diseño la estructura de la matriz de riesgos en donde cada gerencia levantaría la información, considerando el nombre del riesgo, tipo de evento causas, controles, entre otros. En la Figura 4 se presenta una parte representativa de la matriz. La versión completa puede consultarse en el Anexo 2.

LEVANTAMIENTO DE RIESGOS

Tipo de Riesgo	Riesgo identificado	Causa	Factor de Riesgo	Probabilidad	Comentarios probabilidad	Impacto Financiero	Impacto Reputacional	Comentarios Impacto	Impacto Ge

Ilustración 4 Vista parcial de la matriz de levantamiento de riesgos

Fuente: Elaboración propia. Matriz modificada a partir del autor Ayol (s.f.).

En relación con las escalas de medición de la probabilidad de ocurrencia y el impacto se estructuraron en una escala de muy bajo a muy alto. A continuación, se muestra los niveles para la probabilidad

Tabla 1 Niveles de medición de la probabilidad

Periodicidad	Descripción
Muy baja	El riesgo podría presentarse una vez cada 10 años.
Baja	El riesgo podría presentarse una vez cada 5 años.
Medio	El riesgo podría presentarse una vez cada 12 meses
Alto	El riesgo podría presentarse una vez cada 6 meses.
Muy alta	El riesgo podría presentarse una vez por mes o más

Elaboración: Adaptación de la matriz Del autor Brayan Ayol

Para medición del impacto se consideraron dos dimensiones: financiera y reputacional cada uno con sus respectivos niveles, presentados en la tabla 2 y 3 respectivamente

Tabla 2 Niveles de medición de impacto financiero

Periodicidad	Descripción
Muy baja	Pérdida de hasta S/ 5,635
Baja	Pérdida entre De S/ 5,636 a S/ 23,407
Medio	Pérdida entre De S/ 5,636 a S/ 23,407
Alto	Pérdida entre De S/ 5,636 a S/ 23,407
Muy alta	Pérdida superior a S/ 86,694

Elaboración: Propia

Fuente: ingresos de Tebca 2024

Tabla 3 Niveles de medición de impacto reputacional

Periodicidad	Descripción
Muy baja	Uno a dos reclamos de clientes
Baja	Uno a dos reclamos de clientes
Medio	Reclamos repetitivos informando disconformidad
Alto	Pérdida de 2 o más clientes
Muy alta	Pérdida de más de 4 clientes relevantes

Elaboración: Propia

Fuente: Adaptación de la matriz Del autor Brayan Ayol

Con relación a la Matriz de calor, se estructuró una matriz 5x5 que cruza los niveles de probabilidad e impacto para determinar el nivel de riesgo inherente. Esta herramienta se utilizó para clasificar los riesgos en las etapas siguientes.

Matriz de Calor de Riesgos

PROBAILIDAD	IMPACTO				
	Muy Baja	Baja	Media	Alta	Muy Alta
Muy Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
Bajo	Bajo	Bajo	Moderado	Moderado	Moderado
Medio	Bajo	Moderado	Moderado	Alto	Alto
Alto	Bajo	Moderado	Alto	Crítico	Crítico
Muy Alto	Bajo	Moderado	Alto	Crítico	Crítico

Ilustración 5 Mapa de calor

Fuente: Elaboración Propia

Esta fue una etapa clave porque permitió alinear desde el inicio el proyecto con los objetivos de la empresa. La validación de la Gerencia General dio legitimidad al

trabajo y facilitó el compromiso de las demás gerencias.

Etapa 2: Identificación de riesgos:

Como resultado del proceso de identificación, se obtuvieron 30 riesgos, identificados en las reuniones con las gerencias responsables. Posteriormente estos riesgos se evaluaron con todas las gerencias en conjunto en donde se consideraron quedarse con un total de 20 riesgos, los cuales representan principalmente los riesgos que afectan el cumplimiento de los objetivos estratégicos de Tebca

Los riesgos identificados se separaron por tipo de riesgo, tales como: tecnológicos, operativos, legales, reputacionales y de cumplimiento. Esta clasificación permitió tener una visión transversal de los principales factores de exposición de Tebca

Además, se documentaron las causas asociadas a cada riesgo, agrupadas de manera ordenada según los factores internos o externos que podrían originarlos, lo que facilitará su posterior análisis y un adecuado tratamiento.

Tabla 4 Riesgos identificados

N°	Tipo de Riesgo	Riesgo identificado	Causa	Factor de Riesgo
01	Tecnológico	Riesgo de ciberataque masivo	Falta de medidas de ciberseguridad y monitoreo continuo	Tecnológico
02	Tecnológico	Fuga de información sensible de clientes	Accesos mal gestionados y ausencia de cifrado en la base de datos	Tecnológico
03	Tecnológico	Caída prolongada de la plataforma de transacciones	Falla en infraestructura, ausencia de contingencia o respaldo	Tecnológico
04	Fraude Interno	Riesgo de fraude interno	Falta de controles internos y revisión de transacciones	Recurso Humano

05	Cumplimiento	Incumplimiento de requerimientos de la SBS	Falta de monitoreo regulatorio o errores en reportes	Procesos
06	Legal	Uso de la plataforma para lavado de activos	Deficiencias en el sistema de prevención de LA/FT	Procesos
07	Financiero	Fallas en la conciliación contable o de fondos	Errores en conciliación diaria y falta de automatización	Procesos
08	Proveedores	Dependencia de un solo proveedor tecnológico crítico	Proveedor único sin contrato de respaldo o evaluación periódica	Proveedores
09	Financiero	Errores en el registro contable de operaciones	Errores manuales y falta de doble verificación contable	Procesos
10	Seguridad de la información	Acceso inadecuado de terceros a sistemas internos	Terceros con permisos amplios o sin restricciones de acceso	Tecnológico
11	Legal	Falla en la validación de identidad de usuarios	Validación ineficaz de documentos o falta de autenticación biométrica	Procesos
12	Tecnológico	Desactualización del software Core	Parcheo postergado y falta de polí-tica de actualización	Tecnológico
13	Operativo	Errores en la emisión de reportes internos	Errores de digitación y falta de revisión de informes	Procesos
14	Operativo	Retrasos en la atención de requerimientos del usuario interno	Procesos lentos en áreas de soporte por falta de indicadores	Procesos
15	Operativo	Demora en el procesamiento de operaciones no críticas	Automatización limitada o cuellos de botella operativos	Procesos
16	Cultura organizacional	Baja participación de Áreas en talleres de concientización	Desinterés o falta de cultura de riesgo en algunos equipos	Recurso Humano
17	Reputacional	Incidentes menores en comunicaciones masivas a clientes	Errores en bases de datos de marketing o validación	Procesos
18	Organizacional	Rotación de personal sin transferencia de conocimiento	Salidas no planificadas y ausencia de manuales operativos	Recurso Humano
19	Legal	Errores en plantillas	Falta de revisión legal de	Procesos

		de contratos o formularios no vigentes	formatos antes de su difusión	
20	Organizacional	Incumplimiento de cronogramas en proyectos internos	Baja capacidad de seguimiento en áreas de soporte de proyectos	Procesos

Fuente: elaboración propia

Se evidencia que la mayoría de los riesgos son de tipo tecnológico, lo cual nos alerta indica que Tebca está altamente expuesta a riesgos relacionados con tecnología, como ciberataques, fallos en sistemas o pérdida de datos, también se observa que muchas causas de los riesgos tienen relación con procesos internos o falta de controles, lo que muestra la necesidad de fortalecer la documentación y estandarización de procedimientos.

Etapa 3: Evaluación de Riesgos

En esta etapa se evaluaron los 20 riesgos identificados, considerando el impacto y la probabilidad, obteniendo como resultado 6 riesgos Altos (30%), 6 como Moderados (30%) y 8 como Bajos (40%).

Los riesgos altos fueron aquellos que, además de tener un impacto fuerte, también tienen alta probabilidad de ocurrir. como:Ciberataque, fraude interno, fuga de información, caída de plataformas, incumplimiento normativo, lavado de activos

Esto nos muestra que la probabilidad es un factor clave para que los principales riesgos sean altos.

El detalle completo de la evaluación se presenta en el Anexo 3 – Matriz de riesgos evaluados.

Etapa 4:Evaluación de controles existentes

En esta etapa se identificaron los controles actualmente aplicados para mitigar cada uno de los riesgos evaluados. Luego, se analizó su efectividad considerando aspectos como su nivel de aplicación, frecuencia y cobertura en los procesos, con el fin de determinar el riesgo residual de cada evento, es decir, el nivel de exposición que aún persiste una vez implementados los controles. Esto permitió distinguir entre aquellos riesgos que ya cuentan con medidas de mitigación suficientes y aquellos que requieren reforzar o diseñar nuevos controles.

Los principales hallazgos fueron:

- 15 riesgos cuentan con controles ya implementados, sea de forma total o parcial.
- 5 riesgos no tienen controles identificados o los existentes no son adecuados.
- 10 controles fueron considerados efectivos o con un nivel de efectividad aceptable.
- 5 controles se calificaron como débiles o poco eficaces.
- En 5 riesgos, al no contar con controles vigentes, el riesgo residual permanece igual al riesgo inherente.

Esta evaluación permitió establecer prioridades claras para el tratamiento de riesgos, enfocando los esfuerzos en aquellos que requieren intervención urgente. La siguiente tabla resume los resultados obtenidos:

Tabla 5

Tabla 5 Controles existentes

N°	Riesgo identificado	Cuenta con control	Nivel de efectividad del control	Nivel de riesgo residual
01	Riesgo de ciberataque masivo	SÍ	Moderado	Alto
02	Fuga de información sensible de clientes	SÍ	Débil	Alto
03	Caída prolongada de la plataforma de transacciones	SÍ	Moderado	Alto
04	Riesgo de fraude interno	SÍ	Débil	Alto
05	Incumplimiento de requerimientos de la SBS	SÍ	Moderado	Medio
06	Uso de la plataforma para lavado de activos	SÍ	Débil	Alto
07	Fallas en la conciliación contable o de fondos	SÍ	Moderado	Medio
08	Dependencia de un solo proveedor tecnológico crítico	NO	-	Alto
09	Errores en el registro contable de operaciones	SÍ	Moderado	Bajo
10	Acceso inadecuado de terceros a sistemas internos	SÍ	Moderado	Bajo
11	Falla en la validación de identidad de usuarios	SÍ	Débil	Medio
12	Desactualización del software Core	NO	-	Medio
13	Errores en la emisión de reportes internos	SÍ	Efectivo	Bajo
14	Retrasos en la atención de requerimientos del usuario interno	NO	-	Bajo
15	Demora en el procesamiento de operaciones no críticas	SI	Efectivo	Bajo
16	Baja participación de Áreas en talleres de concientización	NO	-	Bajo
17	Incidentes menores en comunicaciones masivas a clientes	SI	Efectivo	Bajo
18	Rotación de personal sin transferencia de conocimiento	NO	-	Bajo
19	Errores en plantillas de contratos o formularios no vigentes	SI	Moderado	Bajo
20	Incumplimiento de cronogramas en proyectos internos	SI	Moderado	Bajo

Fuente: Elaboración propia

Se obtuvo como resultado la efectividad de los controles, lo que no nos asegura que un riesgo no se materialice. Algunos controles estaban implementados, sim embargo, no aseguraba un correcto seguimiento. Asimismo, se evidencian riesgos sin controles, especialmente en temas como proveedores críticos, rotación de personal sin transferencia de conocimiento o validación de identidad. Esto resalta la necesidad de mejorar el diseño y documentación de controles internos.

Etapa 5 : Desarrollo de planes de acción

Durante esta etapa se priorizaron los riesgos con niveles residuales altos, así como aquellos con controles débiles o inexistentes. Los planes de acción definidos incluyen actividades concretas, responsables asignados y plazos establecidos para su implementación y seguimiento.

Los principales resultados de esta etapa fueron:

- Se diseñaron planes de acción para 7 riesgos con nivel de riesgo residual alto.
- Se asignaron responsables específicos para cada plan, incluyendo a las áreas dueñas del proceso y de soporte.
- Se establecieron plazos de implementación de corto y mediano plazo (entre 30 y 90 días).
- En 2 casos se recomendó el diseño de nuevos controles, y en otros 5 se planteó el reforzamiento o mejora de los controles ya existentes.

A continuación, se detallan los riesgos que dieron lugar a planes de acción:

Tabla 6 Planes de acción

N°	Riesgo identificado	Nivel de riesgo residual	Plan de acción
01	Riesgo de ciberataque masivo	Alto	Fortalecimiento de ciberseguridad y monitoreo
02	Fuga de información sensible de clientes	Alto	Implementación de cifrado y revisión de accesos
03	Caída prolongada de la plataforma de transacciones	Alto	Activación de plan de contingencia y backups
04	Riesgo de fraude interno	Alto	Reforzamiento de revisión y segregación de funciones
06	Uso de la plataforma para lavado de activos	Alto	Mejora del sistema de prevención de LA/FT
08	Dependencia de un solo proveedor tecnológico crítico	Alto	Evaluación de proveedor alterno y contrato respaldo
11	Falla en la validación de identidad de usuarios	Medio	Mejora en el proceso de autenticación

Fuente: Elaboración propia

Se obtuvieron mayor visualización de cuáles son los riesgos que representaban un alto peligro para la operación y reputación de Tebca, y se plantearon soluciones específicas según el nivel del riesgo, lo cual refuerza una cultura proactiva en la gestión de riesgos, donde no basta con identificar, sino que hay que actuar.

Etapa 6: Monitoreo y revisión

Como parte final del proceso de gestión de riesgos, se estableció la programación de actividades de seguimiento continuo para asegurar que tanto los controles implementados como los planes de acción definidos mantengan su efectividad en el tiempo.

Se acordó lo siguiente:

- Realizar revisiones periódicas de la matriz de riesgos cada 6 meses, o antes si

se presentan cambios importantes en procesos, tecnología, productos o estructura organizacional.

- Evaluar la efectividad de los controles existentes como parte de las auditorías internas y en coordinación con los líderes de procesos.
- Realizar un seguimiento mensual de los planes de acción vigentes hasta su cierre, verificando avances, cumplimiento de plazos y resultados obtenidos.
- Actualizar el estatus de los riesgos y controles en el sistema de gestión de riesgos, dejando evidencia de cada revisión.

La gestión de riesgos no es estática. Este resultado muestra que Tebca está promoviendo un enfoque preventivo y dinámico, donde los riesgos se revisan con frecuencia y los planes no quedan olvidados. Esto también permitirá reaccionar ante nuevos riesgos o cambios en el entorno. Además, involucrar a los líderes de proceso en las auditorías ayudará a fortalecer la cultura organizacional de control y mejora continua.

Cambios observados a partir de la implementación de la matriz

Con la implementación de la matriz de riesgos marcó un cambio importante en como Tebca gestiona sus riesgos. Antes, estaba más enfocado a los riesgos operativos. Muchos eventos se gestionaban de manera reactiva, sin priorización, sin responsables definidos y sin una evaluación real de los controles.

A partir de esto, se amplió el enfoque, incorporando riesgos tecnológicos, legales, reputacionales y organizacionales. La participación de todas las gerencias fue clave en la identificación y análisis, lo que permitió tener una visión más completa de los riesgos que enfrentamos.

Uno de los cambios más visibles fue en la gestión de riesgos tecnológicos. Antes, los incidentes como caídas de plataforma o accesos indebidos eran frecuentes, pero poco documentados y con un tratamiento más informal. Hoy, estos riesgos han sido priorizados, se han mejorado los controles, y como resultado, se ha logrado reducir tanto la frecuencia como las pérdidas asociadas a este tipo de incidentes, las cuales pasaron de S/.85000 a S/30000 en lo que va del año.

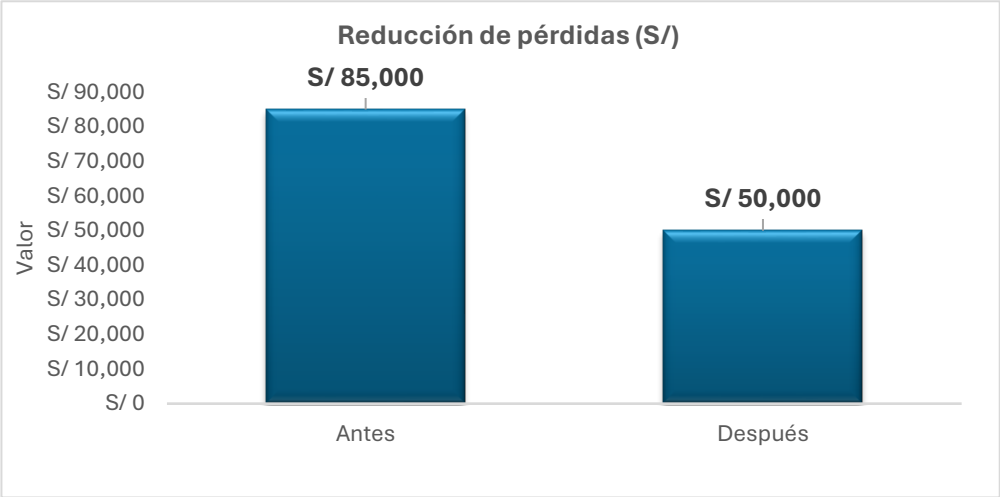


Figura 6: Reducción de pérdidas
Fuente: Elaboración Propia

También se definieron planes de acción para los riesgos más críticos y se estableció un seguimiento constante, lo que permite asegurar que el trabajo no se quede en el diagnóstico, sino que se traduzca en mejoras concretas. En resumen, se pasó de una gestión reactiva y parcial a un enfoque más ordenado, preventivo y compartido entre todas las áreas.

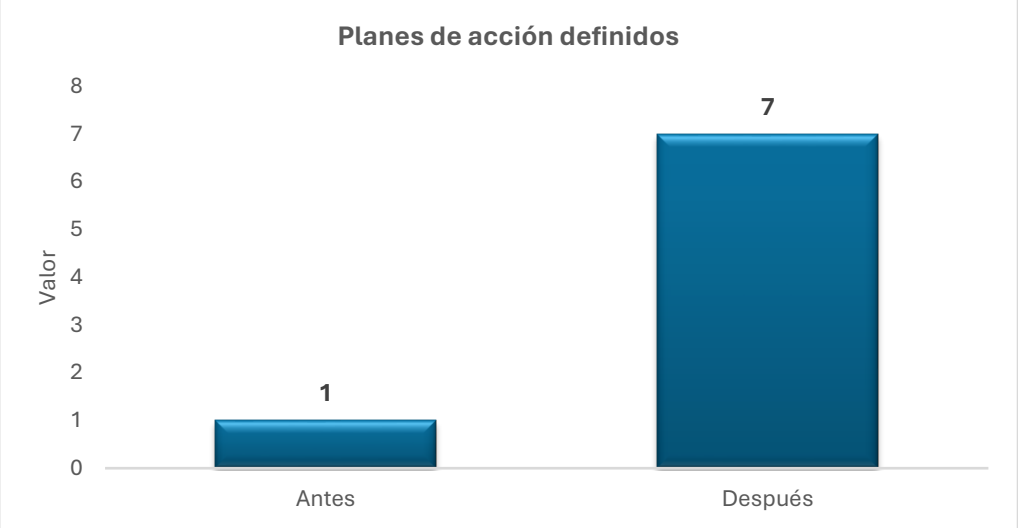


Figura 7: Planes de acción definidos
Fuente: Elaboración Propia

Como se puede visualizar, el total de número de riesgos gestionados pasó de 5 a 20 incrementando en un 300%, los controles efectivos se incrementaron de 3 a 10, siendo un aumento del 233% , y los planes de acción aumentaron de 1 a 7, teniendo un crecimiento de 600%.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- La implementación del modelo COSO ERM permitió estructurar el proceso de gestión de riesgos de forma ordenada y estratégica. Esto coincide con lo planteado por Sánchez Sánchez (2015), quien sostiene que este marco facilita la priorización y el control efectivo de los riesgos al alinearlos con los objetivos organizacionales.

- Durante el proceso se evidenció que la mayoría de los riesgos identificados en Tebca tienen origen tecnológico, lo que refleja una alta exposición en esta área. Esto es coherente con lo señalado por Alexander (2018), quien advertía que muchas empresas en Perú no están preparadas para enfrentar amenazas tecnológicas, como ciberataques o fallas en plataformas.

- También se identificó que, aunque algunos riesgos ya contaban con controles establecidos, muchos de ellos eran débiles, no estaban documentados o no se aplicaban con regularidad. Esto limitó su capacidad para reducir el riesgo residual. Esta observación se relaciona con lo propuesto por Alcócer Barrientos (2019), quien afirma que los controles deben ser oportunos y eficaces para que la gestión de riesgos sea efectiva.
- Finalmente, la elaboración de la matriz permitió identificar riesgos

corporativos que no estaban contemplados en los registros operativos. Esto permitió ampliar la visión hacia una gestión de riesgos más transversal, tal como lo sugieren Robles, Castañeda y Carrizo (2019), quienes enfatizan la necesidad de contemplar todos los niveles y áreas de la organización en la gestión de riesgos.

Recomendaciones

- Fortalecer la ciberseguridad. Dada la alta concentración de riesgos tecnológicos, es prioritario implementar mejores controles como autenticación multifactor, cifrado de información y monitoreo de accesos. Esto ayudará a reducir el riesgo residual de eventos críticos como ciberataques o fuga de datos.
- Capacitar constantemente a las áreas. Es necesario desarrollar sesiones periódicas de formación en gestión de riesgos, con un enfoque práctico, para que todas las gerencias comprendan su rol y mejoren la identificación y tratamiento de riesgos.
- Revisar y documentar los controles existentes. Se sugiere establecer una rutina semestral para revisar la efectividad de los controles actuales, asegurando que estén documentados, actualizados y alineados a los procesos reales.
- Incluir a proveedores y productos nuevos en el análisis de riesgos. Ampliar el enfoque de evaluación a terceros críticos y servicios nuevos permitirá anticipar vulnerabilidades externas y tomar decisiones más informadas desde el inicio de una contratación.

- Implementar KRI e informes estratégicos. Utilizar indicadores clave de riesgo ayudará a dar seguimiento medible a los riesgos más importantes. Además, el seguimiento mensual de estos.

REFERENCIAS

Albanese, D. E. (2012). Análisis y evaluación de riesgos: Aplicación de una matriz de riesgo en el marco de un plan de prevención contra el lavado de activos. BASE – Revista de Administração e Contabilidade da Unisinos, 9(3). https://repositoriodigital.uns.edu.ar/bitstream/handle/123456789/4099/Análisis%20y%20Evaluación%20de%20riesgos.pdf

Alcócer Barrientos, C. (2019). Control interno y gestión de los riesgos corporativos en los gobiernos locales de la Región Junín [Tesis de maestría, Universidad Nacional del Centro del Perú]. https://repositorio.uncp.edu.pe/bitstream/handle/20.500.12894/5914/T010_19930920_M.pdf

Becerra, G., Guzmán, A., & Trujillo, M. A. (2006). La importancia de la administración del riesgo operativo en las entidades crediticias. Universidad & Empresa, 5(10), 271–290. https://www.redalyc.org/pdf/1872/187217412012.pdf

Boronat Ombuena, G. J., Leotescu, R. M., Jiménez, S., & Pérez, C. (2019). Gestión financiera. Técnica Contable y Financiera, (15). https://gb-consultores.es/wp-content/uploads/dlm_uploads/2019/03/Artículo-Gestion-Mapa-de-Riesgos-TCF-Enero-2019.pdf

Catagua Briones, M. L., Pinargote Macías, M. F., & Mendoza Vinces, M. E. (2023). Control interno y modelo COSO en la gestión administrativa y financiera empresarial. Podium, (44), 151–166. https://revistas.uap.edu.pe/ojs/index.php/CYD/article/view/2665/2653

Celada López, E., Quintero Castaño, G., & Ríos Sanabria, T. (2016). Gobierno, riesgo y cumplimiento básicos para PYMES [Tesis de maestría, Universidad EAFIT]. https://repository.eafit.edu.co/server/api/core/bitstreams/29d776ff-14aa-40db-9b68-0a043726f7a2/content

Gutiérrez, Y. E., & Sánchez-Ortiz, A. (2018). Diseño de un modelo de gestión de riesgos basado en ISO 31000:2012 para los procesos de docencia de pregrado en una universidad chilena. Formación Universitaria, 11(4), 65–76. https://www.scielo.cl/scielo.php?pid=S071850062018000400015&script=sci_arttext

Lavielle Fuchslocher, V. (2016). Desarrollo de gestión de riesgos en contratos de construcción, bajo el estándar ISO 31000, orientado hacia la calidad y la sustentabilidad [Tesis de ingeniería, Universidad de Chile]. https://repositorio.uchile.cl/handle/2250/141778

Lizarzaburu, E. R., Barriga, G., Burneo, K., & Noriega, E. (2019). Gestión integral de riesgos y antisoborno: Un enfoque operacional desde la perspectiva ISO 31000 e ISO 37001. Revista Universidad y Empresa, 21(36), 1–20. http://www.scielo.org.co/scielo.php?pid=S0124-

46392019000100079&script=sci_arttext

Lizarzaburu, E. R., Barriga Ampuero, G., Noriega, L., López, L., & Mejía, P. Y. (2017). Gestión de riesgos empresariales: Marco de revisión ISO 31000. Revista Espacios, 38(59), 8. https://repositorio.esan.edu.pe/handle/20.500.12640/2056

Mejía, R. C., Núñez, M. A., Villanueva, E., & Jaraba, I. (2020). Administración de riesgos: Un enfoque empresarial (2ª ed. revisada y ampliada). Universidad EAFIT. https://books.google.es/books?id=oYsqEQAAQBAJ

Mejía Quijano, R. C. (2004). La administración de riesgos empresariales. ADMINISTER – Revista de la Facultad de Administración, (76). https://publicaciones.eafit.edu.co/index.php/administer/article/view/679/605

Mejía Quijano, R. C., & Villanueva Herrera, E. H. (2014). Metodología para monitorear riesgos estratégicos. Revista de Investigaciones – Universidad del Quindío, (127). https://ojs.uniquindio.edu.co/ojs/index.php/riuq/article/view/138/135

MiPlata. (s.f.). Nosotros. https://miplata.com.pe/nosotros/

MiPlata. (s.f.). Nuestra misión y visión. https://www.miplata.com.pe

Noblecilla Flores, D. L. (2020). Relación entre la gestión de riesgos empresarial y el desempeño organizacional en las grandes empresas de los sectores alimentos y bebidas en Perú 2019 [Tesis de licenciatura, Universidad San Ignacio de Loyola]. https://repositorio.usil.edu.pe/handle/20.500.14005/10713

Pasos Chávez, K. (2018). ¿Qué es la gestión integral de riesgos? Nexia Nicaragua. https://www.hmendozaya.com/Boletines/15-%20Gestión%20Integral%20de%20Riesgos.pdf

Plasencia Soler, J. A., Bajo Sanjuán, A., Marrero Delgado, F., & Nicado García, M. (2023). La gestión de riesgos de cumplimiento con enfoque en valores organizacionales: Aplicación en un caso de estudio en Cuba. Visión de Futuro, 27(2). https://www.scielo.org.ar/scielo.php?pid=S1668-87082023000200001&script=sci_arttext

Rodríguez López, M., Piñeiro Sánchez, C., & de Llano Monelos, P. (2013). Mapa de riesgos: Identificación y gestión de riesgos. Atlantic Review of Economics, (2). Colegio de Economistas de A Coruña. https://ruc.udc.es/dspace/bitstream/handle/2183/41590/Lopez_Rodriguez_Manuel_2013_Mapa%20de%20Riesgos.pdf

Sánchez Sánchez, L. R. (2015). COSO ERM y la gestión de riesgos. Qwipukamayoc: Revista de la Facultad de Ciencias Contables, 23(44), 43–50. https://d1wqtxts1xzle7.cloudfront.net/74741021/COSO_ERM_y_la_gestion_de_riesgos-libre.pdf

Schaeffer García, R. A. (2008). Evaluación del riesgo empresarial a través de matrices de riesgos en una entidad prestadora de servicios de consultoría administrativa y financiera [Tesis de licenciatura, Universidad de San Carlos de Guatemala]. https://d1wqtxts1xzle7.cloudfront.net/36326255/MATRICES_RIESGO-libre.pdf

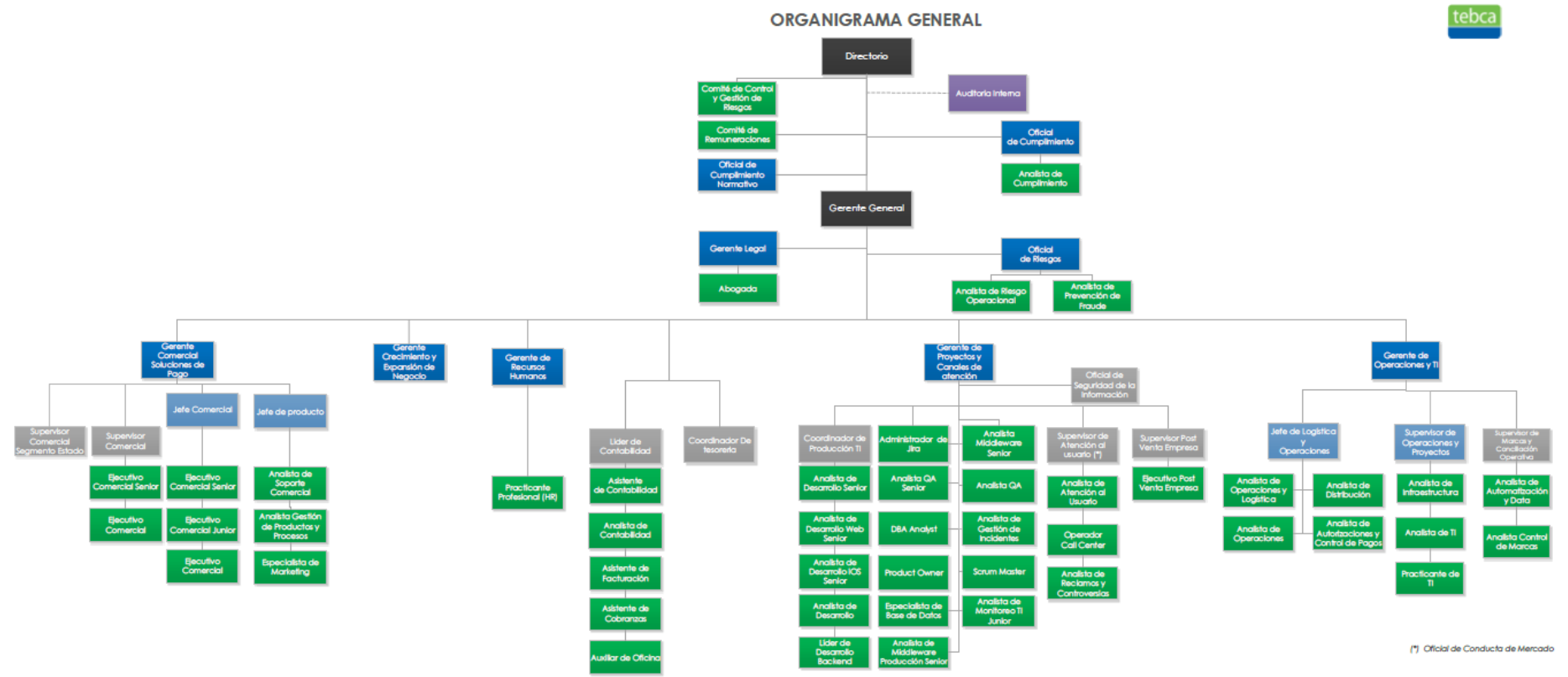
Superintendencia de Banca, Seguros y AFP. (s.f.). Empresas emisoras de dinero electrónico autorizadas. https://www.sbs.gob.pe

Superintendencia de Banca, Seguros y AFP. (s.f.). Registro de Empresas Emisoras de Dinero Electrónico. https://www.sbs.gob.pe

Tebca. (s.f.). Soluciones digitales para el control de pagos corporativos. https://www.tebca.com.pe

ANEXOS

Anexo 1 - Flujograma general Tebca



ANEXO 2 - VISTA GENERA L DE LA MATRIZ DE LEVANTAMIENTO DE RIESGOS

Tipo de Riesgo	Riesgo identificado	Causa	Factor de Riesgo	Probabilidad	Comentarios probabilidad	Impacto Financiero	Impacto Reputacional	Comentarios Impacto	Impacto General

Nivel de Riesgo Inherente	Controles existentes	Efectividad del Control	Probabilidad.	Impacto	Nivel Riesgo Residual	Planes de acción	Responsable	F. de implementación

ANEXO 3 – MATRIZ DE RIESGOS EVALUADOS

N°	Tipo de Riesgo	Riesgo identificado	Causa	Factor de Riesgo	Impacto	Probabilidad	Nivel de riesgo
01	Tecnológico	Riesgo de ciberataque masivo	Falta de medidas de ciberseguridad y monitoreo continuo	Tecnológico	5	5	25
02	Tecnológico	Fuga de información sensible de clientes	Accesos mal gestionados y ausencia de cifrado en la base de datos	Tecnológico	5	4	20
03	Tecnológico	Caída prolongada de la plataforma de transacciones	Falla en infraestructura, ausencia de contingencia o respaldo	Tecnológico	5	4	20
04	Fraude Interno	Riesgo de fraude interno	Falta de controles internos y revisión de transacciones	Recurso Humano	5	5	25
05	Cumplimiento	Incumplimiento de requerimientos de la SBS	Falta de monitoreo regulatorio o errores en reportes	Procesos	5	4	20
06	Legal	Uso de la plataforma para lavado de activos	Deficiencias en el sistema de prevención de LA/FT	Procesos	5	5	25
07	Financiero	Fallas en la conciliación contable o de fondos	Errores en conciliación diaria y falta de automatización	Procesos	4	3	12
08	Proveedores	Dependencia de un solo proveedor tecnológico crítico	Proveedor único sin contrato de respaldo o evaluación periódica	Proveedores	4	4	16
09	Financiero	Errores en el registro contable de operaciones	Errores manuales y falta de doble verificación contable	Procesos	3	3	9
10	Seguridad de la información	Acceso inadecuado de terceros a sistemas internos	Terceros con permisos amplios o sin restricciones de acceso	Tecnológico	3	3	9
11	Legal	Falla en la validación de identidad de usuarios	Validación ineficaz de documentos o falta de autenticación biométrica	Procesos	3	3	9
12	Tecnológico	Desactualización del software Core	Parcheo postergado y falta de polí-tica de actualización	Tecnológico	3	3	9
13	Operativo	Errores en la emisión de reportes internos	Errores de digitación y falta de revisión de informes	Procesos	2	2	4

14	Operativo	Retrasos en la atención de requerimientos del usuario interno	Procesos lentos en áreas de soporte por falta de indicadores	Procesos	2	2	4
15	Operativo	Demora en el procesamiento de operaciones no críticas	Automatización limitada o cuellos de botella operativos	Procesos	2	2	4
16	Cultura organizacional	Baja participación de Áreas en talleres de concientización	Desinterés o falta de cultura de riesgo en algunos equipos	Recurso Humano	2	2	4
17	Reputacional	Incidentes menores en comunicaciones masivas a clientes	Errores en bases de datos de marketing o validación	Procesos	2	2	4
18	Organizacional	Rotación de personal sin transferencia de conocimiento	Salidas no planificadas y ausencia de manuales operativos	Recurso Humano	2	1	2
19	Legal	Errores en plantillas de contratos o formularios no vigentes	Falta de revisión legal de formatos antes de su difusión	Procesos	2	2	4
20	Organizacional	Incumplimiento de cronogramas en proyectos internos	Baja capacidad de seguimiento en áreas de soporte de proyectos	Procesos	2	2	4