METODOLOGIA PARA LA ADMINISTRACION DE RIESGO OPERATIVO

Control e historial de modificaciones

Fecha	Versión	Descripción de la modificación
04/05/2023	1.0	Documento Original
16/02/2024	2.0	- Se actualiza formato control de documentación. - Se incluye cuadro para evidenciar la creación, revisión y aprobación de documentos.
15/08/2025	3.0	- Actualización sección Planes de acción. - Actualización de logo empresarial y encabezado.

Creado por:	Revisado por:	Aprobado por:
Firmado electrónicamente por: EDUARDO FRANCO VIVANCO GRANDA Validar únicamente con FirmaEC	Firmado electrónicamente por: ANA CRISTINA CEVALLOS MONTERO Validar únicamente con FirmaEC	Firmado electrónicamente por: ALFREDO PAUL NOBOA GARCIA Validar únicamente con FirmaEC
Eco. Eduardo Vivanco Administrador de Riesgos	Ing. Ana Cristina Cevallos Jefe de Gestión Calidad	Eco. Paúl Noboa Administrador

CONTENIDO

1. INTRODUCCIÓN 4
2. ALCANCE 4
3. OBJETIVOS 4
3.1 OBJETIVO GENERAL 4
3.2 OBJETIVOS ESPECÍFICOS 4
4. DEFINICIONES 5
5. METODOLOGÍA PARA IDENTIFICACIÓN, CUANTIFICACIÓN, MITIGACIÓN Y MONITOREO DEL RIESGO OPERACIONAL: MATRIZ DE RIESGOS 9
5.1 FASES DE LA GESTIÓN INTEGRAL DE RIESGOS 10
5.1.1 IDENTIFICACIÓN DE RIESGOS 11
5.1.2 ANÁLISIS DE LOS RIESGOS 15
5.1.3 VALORACIÓN DEL RIESGO 18
5.1.4 LÍMITES DE EXPOSICIÓN 18
5.1.5 FACTORES DE RIESGO OPERACIONAL 19
5.1.6 TIPOS DE EVENTOS DE RIESGO OPERATIVO 20
5.1.7 MAPA DE CALOR 24
5.1.8 ACCIONES DE VALORACIÓN DE RIESGO 25
5.1.9 TRATAMIENTO DEL RIESGO 26
5.1.10 EVALUACIÓN DE CONTROLES Y SU EFICACIA 28
5.1.11 MITIGACIÓN DEL RIESGO 39
5.1.13 PLANES DE ACCIÓN 41
5.1.14 SEGUIMIENTO Y REVISIÓN DEL RIESGO 42
5.2 REGISTRO E INFORME DEL RIESGO 44
7. VIGENCIA Y ACTUALIZACIÓN DE DOCUMENTACIÓN 44

1. INTRODUCCIÓN

Es necesario incrementar los esfuerzos en fortalecer el talento humano, procesos y tecnología, generando credibilidad y liderazgo; en el cual la gestión y administración de riesgo operativo juega un papel fundamental al momento de crear una ventaja competitiva frente a las demás instituciones; donde el propósito final es mantener la operatividad en el tiempo en base a los objetivos estratégicos planteados, minimizando las pérdidas económicas y maximizando las oportunidades de negocio.

Por tanto, se ha diseñado la presente metodología de matriz institucional de riesgo operativo para la identificación, medición, control y monitoreo de los riesgos a los que la Entidad se encuentra expuesto en el normal desarrollo de sus operaciones.

La Entidad debe ejecutar las etapas definidas para la administración integral del riesgo, que consisten en: identificar, medir, priorizar, controlar/mitigar, monitorear y comunicar sus exposiciones del Riesgo Operativo.

2. ALCANCE

El presente Manual Metodológico es de aplicación a nivel institucional y tiene alcance a todo el personal de ELTHON CEO.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Establecer la metodología a utilizar por parte del Administrador de Riesgos para la elaboración de la MATRIZ DE RIESGO INTEGRAL y MATRIZ DE RIESGO OPERATIVO.

3.2 OBJETIVOS ESPECÍFICOS

- Contar con metodologías actualizadas referentes a la Administración de Riesgo Operativo.
- Definir los criterios base, a partir de los cuales se elabora la matriz de riesgo institucional
- Identificar, clasificar, analizar, evaluar y monitorear los riesgos de pérdida asociados a los cuatro factores de riesgo operativo.

4. DEFINICIONES

- Actividad: Es el conjunto de tareas que ejecutan las entidades controladas.
- Administración de la continuidad del negocio: Es un proceso permanente que garantiza la continuidad de las operaciones de las entidades controladas, a través del mantenimiento efectivo de un sistema de gestión de continuidad del negocio.
- Administración de la información: Es el proceso mediante el cual se captura, procesa, almacena y transmite información, independientemente del medio que se utilice; ya sea impreso, escrito, almacenado electrónicamente, transmitido por correo o por medios electrónicos o presentado en imágenes.
- Alfanumérico: Es el conjunto de caracteres conformado por letras y números.
- Aplicación informática: Se refiere a los procedimientos programados a través de alguna herramienta tecnológica, que permiten la administración de la información y la oportuna toma de decisiones.
- Banca electrónica: Son los servicios suministrados por las entidades controladas a los clientes y/o usuarios, a través de protocolos de internet, indistintamente del dispositivo tecnológico del cual se acceda.
- Banca móvil: Son los servicios suministrados por las entidades controladas a los clientes y/o usuarios, a través de aplicaciones propias de los dispositivos móviles mediante los protocolos de estos equipos.
- Cajeros automáticos (ATM): Son máquinas conectadas informáticamente a una entidad controlada que permite efectuar al cliente ciertas transacciones.
- Canales electrónicos Se refiere a todas las vías o formas a través de las cuales los clientes y/o usuarios pueden efectuar transacciones con las entidades controladas, mediante el uso de elementos o dispositivos electrónicos o tecnológicos, utilizando o no tarjetas. Principalmente, son canales electrónicos: los cajeros automáticos (ATM), dispositivos de puntos de venta (POS y PIN Pad), sistemas de audio respuesta (IVR), banca electrónica, banca móvil, u otros mecanismos electrónicos similares.
- Centro de procesamiento de datos: Es la infraestructura que permite alojar los recursos relacionados con la tecnología que admite el procesamiento, almacenamiento y transmisión de la información.
- Ciberseguridad: Conjunto de medidas de protección de la infraestructura tecnológica y de la información, a través del tratamiento de las amenazas que ponen en riesgo la información procesada por los diferentes componentes tecnológicos interconectados.
- Cifrar: Es el proceso mediante el cual la información o archivos son alterados en forma lógica, con el objetivo de evitar que alguien no autorizado pueda interpretarlos al verlos o copiarlos, por lo que se utiliza una clave en el origen y en el destino.
- Computación en la nube: Es la provisión de servicios informáticos accesibles a través de la internet, estos pueden ser de infraestructura, plataforma y/o software.

- Confiabilidad: Es el atributo de que la información es la apropiada para la administración de la entidad, la ejecución de transacciones y el cumplimiento de sus obligaciones.
- Confidencialidad: Es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.
- Corresponsales no bancarios (CNB): Son canales mediante los cuales las entidades de los sectores financieros público y privado, bajo su entera responsabilidad, pueden prestar sus servicios a través de terceros que estén conectados a la entidad financiera mediante sistemas de transmisión de datos, previamente autorizados por el organismo de control, identificados y que cumplan con todas las condiciones de control interno, seguridades físicas y de tecnología de información, entre otras.
- Cumplimiento: Se refiere a la observancia y aplicación de las leyes, reglamentos y demás normativa, así como los acuerdos contractuales en los procesos, actividades y operaciones a los que las entidades están sujetas.
- Datos: Es cualquier forma de registro sea este electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido.
- Datos personales: Datos que identifican o hacen identificable a una persona natural, directa o indirectamente.
- Disponibilidad: Es el atributo de que los usuarios autorizados tienen acceso a la información cada vez que lo requieran a través de los medios que satisfagan sus necesidades.
- Elasticidad en la nube: Es la capacidad que se tiene en la nube para adaptarse a las demandas variables de infraestructura y los recursos que se dispone según las necesidades de la entidad.
- Estándar TIA-942: Guía que proporciona una serie de recomendaciones y directrices para la instalación de las infraestructuras de centros de procesamiento de datos en los aspectos de: telecomunicaciones, arquitectura, sistema eléctrico y sistema mecánico.
- Evento de riesgo operativo: Es el hecho que deriva en pérdidas para las entidades controladas, originado por fallas o insuficiencias en los factores de riesgo operativo.
- Factores de riesgo operativo: Son las fuentes generadoras de riesgos operativos tales como: personas, procesos, tecnología de la información y eventos externos
- Indicadores Claves de Riesgo: Es una métrica para determinar qué tan posible es que la probabilidad de un evento, combinada con sus consecuencias, supere el apetito de riesgo operativo, cuantifican el perfil de riesgo operativo de la entidad; y, ayudan a tomar acciones oportunas y corregir las desviaciones de metas, antes de que sucedan.
- Impacto: Es la afectación financiera que podría tener la entidad, en el caso de que ocurra un evento de riesgo.
- Información: Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios, toma de decisiones, ejecución de una transacción o entrega de un servicio.

- Incidente de tecnología de la información: Es el evento asociado a posibles fallas en la tecnología de la información, fallas en los controles, o situaciones con probabilidad de comprometer las operaciones del negocio.
- Incidente de seguridad de la información: Es el evento asociado a posibles fallas en la seguridad de la información, o una situación con probabilidad de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- Información crítica: Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones.
- Insumo: Es el conjunto de materiales, datos o información que sirven como entrada a un proceso.
- Integridad: Es el atributo de mantener la totalidad y exactitud de la información y de los métodos de procesamiento.
- Línea de negocio: Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios especializados para atender un segmento del mercado objetivo, definido en la planificación estratégica de la entidad.
- Mapa de calor: Es una herramienta que permite visualizar de una manera rápida la probabilidad de los riesgos y su intensidad, en caso de que estos se materialicen.
- Mapa de procesos: Diagrama que presenta la visión global de la estructura de la entidad, donde se presentan todos los procesos que forman parte de la organización y sus principales relaciones.
- Medios electrónicos: Son los elementos de la tecnología que tienen características digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares.
- Nivel de riesgo: Representa el grado de exposición de riesgo al que podría encontrarse expuesta una entidad de ocurrir un evento identificado.
- Pista de auditoría: Es el registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos, bases de datos, sistemas operativos y demás elementos tecnológicos, con el propósito de mantener información histórica para fines de control, supervisión y auditoría.
- Plan de continuidad del negocio: Es el conjunto de procedimientos que orientan a las entidades a mantener su operatividad en el caso de que ocurran interrupciones que afecten sus servicios.
- POS y PIN Pad: Son dispositivos de hardware y/o software fijos o móviles ubicados en puntos de venta que permiten realizar transacciones con tarjetas.
- Probabilidad: Es la posibilidad de que ocurra un evento de riesgo en un determinado período de tiempo.
- Procedimiento: Es el método específico y estandarizado para llevar a cabo una actividad o un proceso.
- Procesos: Es el conjunto de actividades estandarizadas que transforman insumos en productos o servicios.

- Proceso crítico: Es el conjunto de procedimientos indispensables para la sostenibilidad y continuidad de las operaciones de la entidad, y cuya falta de identificación o aplicación deficiente puede generarle un impacto negativo.
- Propietario de la información: Es la persona encargada de cuidar la integridad, confidencialidad y disponibilidad de la información; debe tener autoridad para especificar y exigir las medidas de seguridad necesarias para cumplir con sus responsabilidades.
- Protección de datos personales: Es un conjunto de prácticas de seguridad para evitar el uso indebido e ilegal de datos personales, para salvaguardarlos contra filtraciones, pérdida o compromiso de los datos.
- Punto de recuperación objetivo (RPO): Es la cantidad máxima aceptable de pérdida de los datos medidos en el tiempo.
- Resiliencia Operativa: Capacidad de una entidad para seguir entregando los servicios críticos durante eventos disruptivos; esta capacidad le permite a la entidad identificar y protegerse de amenazas y potenciales fallas, respondiendo y adaptándose a ellas; así como, recuperarse y aprender de los eventos disruptivos con la finalidad de minimizar su impacto hacia el futuro en la entrega de los servicios críticos.
- Riesgo inherente: Es el nivel de riesgos propio de la actividad con los controles existentes en el momento de la evaluación del riesgo.
- Riesgo residual: Nivel de riesgo esperado después de aplicar los controles.
- Riesgo operativo: Es la posibilidad de que se produzcan pérdidas para la entidad, debido a fallas o insuficiencias originadas en procesos, personas, tecnología de información y eventos externos. El riesgo operativo no incluye los originados por el entorno político, económico y social, los riesgos: sistémico, estratégico y de reputación.
- Seguridad de la información: Es el conjunto de medidas y técnicas que permiten la preservación de la confidencialidad, integridad y disponibilidad de la información; incluyen aspectos relacionados con la seguridad informática y la ciberseguridad.
- Sistemas internos de control integral: Son el conjunto integrado de políticas, procesos, procedimientos y niveles de control formalmente establecidos y validados periódicamente, tendientes a evitar la ocurrencia de eventos de riesgo o mitigar su impacto.
- Sistema de audio respuesta (IVR): Es un sistema automatizado de respuesta interactiva, orientado a entregar o recibir información a través del teléfono.
- Tarea: Es el conjunto de pasos que conducen a un resultado final visible y mesurable.
- Tarjeta con chip: Es la tarjeta que posee circuitos integrados (chip) que permiten la ejecución de cierta lógica programada, contiene memoria y microprocesadores.
- Tarjeta contactless: Es la tarjeta que dispone de una tecnología NFC (Near Field Communication) que permite, a través de una comunicación inalámbrica de corto alcance y alta frecuencia, transaccionar al usuario con tan solo acercar la tarjeta a un terminal o lector.

- Tecnología de la información: Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes y comunicaciones, entre otros.
- TIER III: Certificación o clasificación de los centros de datos que permite el mantenimiento concurrente, con una disponibilidad de 99.982% al año, y un tiempo de parada de 1.6 horas, e incluye redundancia en sus componentes de infraestructura, así como fuentes alternativas de electricidad y refrigeración en caso de emergencia.
- Tipo de evento: Identificación de los eventos de riesgo operativo de acuerdo a su origen.
- Transacciones: Son movimientos que realizan los clientes y/o usuarios a través de los canales que brindan las entidades; y pueden ser monetarias y no monetarias.
    - Transacciones monetarias: Son las que implican movimiento de dinero y son realizadas por los clientes a través de canales presenciales o canales electrónicos, tales como: transferencias, depósitos, retiros, operaciones de crédito, pagos, recargas de telefonía móvil, entre otras.
    - Transacciones no monetarias: Son las que no implican movimiento de dinero y son realizadas por los clientes a través de canales presenciales o canales electrónicos, tales como: consultas, cambios de clave, personalización de condiciones para realizar transacciones, actualización de datos, entre otras.
- Transferencia electrónica de información: Es la forma de enviar, recibir o transferir en forma electrónica datos, información, archivos, mensajes, entre otros.

5. METODOLOGÍA PARA IDENTIFICACIÓN, CUANTIFICACIÓN, MITIGACIÓN Y MONITOREO DEL RIESGO OPERACIONAL: MATRIZ DE RIESGOS

El perfil de Riesgo Integral y Operacional que resulte exclusivamente de datos de pérdidas históricas puede no ser tan adecuado y veraz ya que se podría haber incluido ya controles y acciones correctivas con la finalidad de evitar que vuelvan a ocurrir. Es por esta razón que la evaluación de riesgos Cualitativa es de gran importancia a la hora de estimar riesgos operativos.

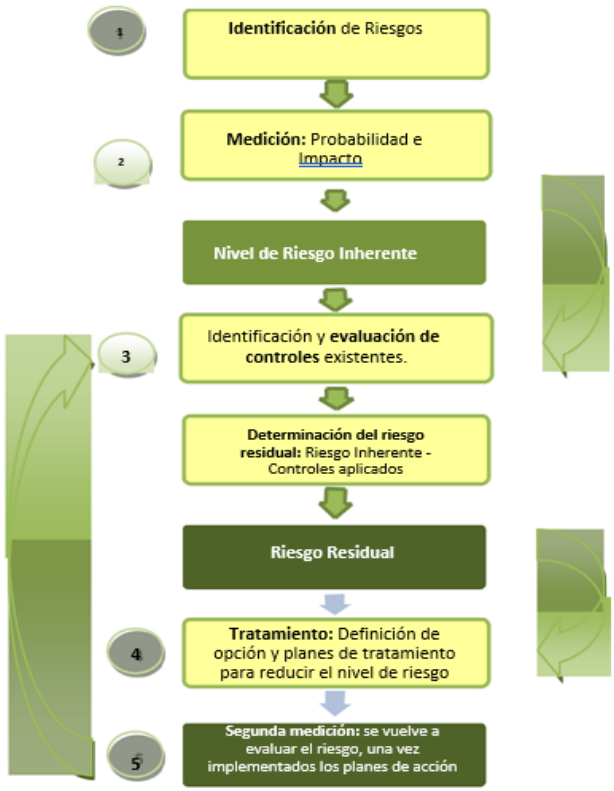
Dentro de las herramientas para evaluar los riesgos cualitativamente se encuentra la “Matriz de Riesgos” donde se inicia desde el mapa de procesos de la institución. Con esta información se puede determinar en cada uno de los subprocesos en qué etapa o en qué actividad puede existir la posibilidad de una pérdida y así poder medirla según los criterios propios establecidos en dicha matriz, este trabajo se lo debe realizar conjuntamente con el dueño de cada proceso ya que ellos son quienes conocen a fondo las actividades y pueden contribuir a la identificación eficaz de debilidades y omisiones que pueda tener el proceso.

La Matriz de Riesgos es la herramienta que permite identificar y evaluar los riesgos, considerando factores internos como el tipo de organización estructural y externos como los cambios en las regulaciones que puedan afectar el normal desarrollo de cada actividad dentro de los procesos. Luego de identificarlos se debe dar un seguimiento al riesgo que permita controlarlo o mitigarlo.

Con la finalidad de identificar correctamente las fallas e insuficiencias en los factores: personas, procesos, tecnología de la información y eventos externos, la Entidad ha diseñado una metodología cualitativa, esto es, la matriz de riesgo operativo, la cual permitirá identificar, medir, controlar y monitorear los riesgos a los que la Institución se encuentra expuesta en el normal desarrollo de sus operaciones y asegure la continuidad del negocio en el corto, mediano y largo plazo.

5.1 FASES DE LA GESTIÓN INTEGRAL DE RIESGOS

Para la elaboración de la matriz de riesgo integral y operativo, se han definido 5 fases con el objetivo de compilar de manera concisa y directa como se observa en el siguiente gráfico:



5.1.1 IDENTIFICACIÓN DE RIESGOS

La identificación del riesgo se lo efectúa mediante la construcción de la bitácora de eventos, es importante que el Administrador de Riesgos conozca el proceso de levantamiento y exista divulgación a nivel de toda la organización, para lo cual se deben aplicar diferentes procedimientos y tomar información de diferentes fuentes tales como:

- **Inventario de procesos actualizado.** Este detalla los macro procesos, procesos y subprocesos que transforman insumos en productos o servicios financieros con valor para el socio y cliente de las diferentes áreas, así como, los dueños de proceso.
- **Priorizar procesos.** Para el análisis e identificación de los riesgos en los procesos se priorizará aquellos procesos calificados como críticos, y luego se continuará con los procesos de más alto riesgo para la institución, conforme los criterios de calificación establecidos por ELTHON CEO.
- **Análisis de procesos e identificación de riesgos.** El Administrador de Riesgos en conjunto con los dueños de los procesos, realizarán el análisis de los riesgos en los diferentes procesos priorizados, a través de observaciones directas y talleres de trabajo con los involucrados, cuestionarios, entrevistas, flujogramas e identificarán los eventos de riesgo reales y potenciales que hayan afectado y puedan afectar a dichos procesos.
- **Análisis de informes de auditoría.** Auditoría interna debe remitir al Administrador de Riesgos los informes de los exámenes de auditoría aplicados a los procesos institucionales a fin de identificar vulnerabilidades o deficiencias, así como la eficacia de los controles y nuevos que puedan estar asociados a los eventos de riesgo y registrarlos en la bitácora de eventos a partir de la fecha de recepción del informe.

  Los principales campos a registrar en la bitácora de eventos (**Anexo 3 "Matriz de eventos de riesgos"**) serán los siguientes:
  - Número. Representa la línea del evento de riesgo operativo y legal para mantener un listado numerado.
  - Fecha. Representa la fecha que ocurrió el evento de riesgo operativo.
  - Macroproceso. Definido en el portafolio de procesos interno de la institución al que hace referencia el evento de riesgo operativo.
  - Proceso. Definido en el portafolio de procesos interno de la institución al que hace referencia el evento de riesgo operativo.
  - Subproceso. Definido en el portafolio de procesos interno de la institución al que hace referencia el evento de riesgo operativo.

5.1.1.1 ELEMENTOS PARA IDENTIFICAR RIESGOS

Los elementos para la identificación de riesgos se consideran según lo descrito a continuación:

Herramientas para Identificación de Riesgos

Esta actividad la realiza la persona encargada del manejo de riesgos en coordinación con los dueños o responsables de cada proceso. Consiste en reconocer e identificar las fallas o insuficiencias que puedan generar pérdidas financieras para la institución. Esta tarea se puede realizar mediante: Talleres de trabajo y entrevistas, Diagramas de flujo, Evaluación de organigramas funcionales y Cuantificación de eventos de pérdida donde será necesario tener los datos históricos.

Se pueden utilizar, entre otras, las siguientes herramientas:

- Talleres de trabajo y entrevistas. Actividades que se realizan con los dueños y/o responsables de cada proceso, a fin de entender a detalle los procesos y analizar las vulnerabilidades a las que puede estar expuesto.
- Evaluación de organigramas funcionales. Permiten entender la naturaleza y el campo de acción de las operaciones de la Entidad y a su vez detectar la existencia de segregación de funciones y controles por oposición.
- Diagramas de flujo. Permiten identificar e ilustrar los diferentes procesos que se realizan en la institución, a fin de detectar los potenciales riesgos operativos en base a cada una de sus actividades.

Determinación de Riesgos Tangibles e Intangibles

Como parte del proceso de identificación de eventos, se considera la determinación de riesgos tangibles e intangibles, con ello se puede establecer un nivel de afectación en las operaciones o activos de la organización. ELTHON CEO determina riesgos tangibles e intangibles a los siguientes:

- Tangibles: que afectan a los activos tangibles de la organización, por ejemplo activos tecnológicos y personal.
- Intangibles: que afectan a los activos intangibles de la organización, por ejemplo Software ELTHON, base de conocimientos, reputación de la organización, entre otros.

Identificación de la Causa y Consecuencia del Riesgo

Se registra la causa y consecuencia del evento de riesgo con la finalidad de dimensionar el factor que originó el evento y el impacto que éste puede generar de manera negativa en la organización; lo cual es registrado en el **Anexo 3 "Matriz de eventos de riesgos".**

DETALLE DEL EVENTO					
Descripción del Evento	Factor de Riesgo	Origen	Causa	Consecuencia	Tratamiento a Riesgo
as políticas, procesos, procedimientos y metodologías de Captaciones hallan actualizados en todas sus fases, se ajustan a la normativa gente, han sido conocidas y aprobadas por la instancia de decisión rrespondiente y se han difundido y socializado al interior de la ntidad	Procesos	Interno	a,a,c	ab	Compartir
resentación de documentos incompletos e información esactualizada por parte del solicitante al aperturar una cuenta	Procesos	Interno	a,a,c	ab	Compartir

Identificación de Amenazas, Oportunidades, Vulnerabilidades y Capacidades

En la identificación de los eventos se podrán considerar las amenazas que pueden impactar negativamente las operaciones, las posibles oportunidades de mejora que se pueden generar, las debilidades desglosadas en vulnerabilidades que la organización puede tener por la presencia de un evento de riesgo, y finalmente el nivel de capacidad que la organización dispone para la gestión del evento de riesgo.

Cambios en el Contexto de la Organización y Partes Interesadas

Los eventos de riesgo podrían generarse debido a las variaciones existentes en el contexto interno y externo de la organización, por ejemplo cambios en el mercado, en la normativa, en los objetivos estratégicos y las responsabilidades, entre otros. Así como también en los cambios de las necesidades de las partes interesadas debido a la presencia de nuevos factores que pueden generar sesgos en el servicio y expectativas de las entidades.

Disponibilidad de Recursos

La identificación de eventos de riesgos es directamente relacionado a la naturaleza y magnitud de las operaciones de la organización, y con factores vinculados con la disponibilidad de los recursos, el valor de los activos relevantes y necesarios para la ejecución de las actividades relacionadas a la gestión de riesgos; la disponibilidad y confiabilidad de información requerida para la operatividad y toma de decisiones y el nivel de conocimiento del personal interno quienes ejecutan los proceso de ELTHON CEO.

Ante la presencia de un suceso crítico se podrían establecer indicadores de riesgos emergentes en los cuales permite la identificación de un evento de riesgo. Al considerar los

factores relacionados con el tiempo en la identificación de riesgos, se puede obtener una visión de los posibles eventos inciertos que podrían afectar el cumplimiento de objetivos.

5.1.1.2 TIPO DE PROCESO

Para la identificación del riesgo se parte de la estructura de procesos, los mismos que se clasifican en:

- **Procesos gobernantes o estratégicos.** Se considerarán a aquellos que proporcionan directrices y políticas a los demás procesos cuya responsabilidad compete al representante legal, con el fin de cumplir con los objetivos y políticas institucionales. Se refieren a la planificación estratégica, los lineamientos de acción básicos, definición de estructura organizacional, la administración integral de riesgos, entre otros.
- **Procesos productivos, fundamentales u operativos.** Son los procesos propios del giro del negocio, que permiten ejecutar efectivamente las políticas y estrategias relacionadas con la calidad de los productos o servicios que ofrecen a sus socios, clientes o usuarios.
- **Procesos habilitantes, de soporte o apoyo.** Son los procesos administrativos, financieros, tecnología de información, contabilidad, control interno y talento humano, que apoyan a los procesos gobernantes y productivos.

Un proceso crítico o no crítico, se define de acuerdo a la metodología interna de acuerdo al indicador de riesgo del proceso y su nivel de incidencia en la operatividad de la institución. Consta en el portafolio de procesos.

Los procesos productivos se asignarán a las líneas de negocio de acuerdo con los productos y servicios que generan, de forma que, a cada uno de los procesos le corresponda una línea de negocio y que ningún proceso permanezca sin asignar.

5.1.1.3 LÍNEA DE NEGOCIO

Para una adecuada administración del riesgo operativo se deberá agrupar justificada y documentalmente los procesos por líneas de negocio de acuerdo a la siguiente clasificación:

- **Línea minorista.** Contempla las actividades operativas
- **Línea de microfinanzas.** Incluye operaciones financieras como préstamos
- **Línea de tarjetas.** Contempla las actividades y servicios relacionados con tarjetas de crédito, débito, pago y prepago.

- **Línea Comercial.** Incluye las operaciones de crédito comercial de primer piso, operaciones financieras de segundo piso.
- **Línea Inmobiliaria.** Corresponde a la planificación, construcción y comercialización de proyectos orientados al desarrollo de la vivienda y construcción sean estos propios o de terceros.
- **Línea de compensación de pagos.** Contempla todas las actividades relacionadas con la gestión de pagos, transferencias y compensación de acuerdo a lo establecido en el artículo 470 del Código Orgánico Monetario y Financiero.
- **Línea de tesorería tradicional.** Representan actividades cotidianas de la gestión de liquidez y administración de flujo de fondos.

5.1.1.4 FORMALIZACIÓN DE LA IDENTIFICACIÓN DE RIESGOS

El Administrador de riesgos realizará una reunión en la que se registran y aceptan los riesgos identificados, para lo cual se procede a levantar el Acta de Riesgo Integral y Operativo haciendo uso del **Anexo 2 Acta Reunión Riesgo Operativo.**

5.1.2 ANÁLISIS DE LOS RIESGOS

El análisis del riesgo considera factores como:

Probabilidad de los Eventos y las Consecuencias

Se multiplica la probabilidad y el impacto para determinar el nivel de riesgo, los resultados se clasifican y se visualizan en la matriz de riesgo. Esto ayuda a obtener una comprensión completa de los riesgos y su impacto potencial en las operaciones y determinar aquellos riesgos que requieren de una atención inmediata y priorizar acciones de mitigación a través de controles o planes de acción según aplique.

La Naturaleza y la Magnitud de las Consecuencias

La naturaleza implica comprender el tipo de impacto que podría tener un evento de riesgo, para lo cual se reconoce las escalas de categoría para determinar la magnitud y clasificar las consecuencias; esto permite comprender la importancia relativa de los riesgos y priorizar acciones de mitigación.

CATEGORÍA	VALOR	CRITERIOS			
		Repercusiones para la entidad	Repercusiones sobre los clientes	Acciones del Regulador	Posible pérdida económica
Catastrófico	**5**	Riesgo cuya materialización influye directamente en el cumplimiento de la misión, pérdida patrimonial o deterioro de la imagen, dejando además sin funcionar totalmente o por un período importante de tiempo, los servicios o productos que entrega la entidad	Afecta a un número grandes de clientes	Multas significativas	Catastrófica
Mayor	**4**	Riesgo cuya materialización dañaría significativamente el patrimonio, imagen o logro de los objetivos sociales. Además se requerirá una cantidad importante de tiempo de la alta dirección en investigar y corregir los daños	Suspensión prolongada de servicios	Multas medianas	Mayor
Moderado	**3**	Riesgo cuya materialización causaría ya sea una pérdida importante en el Patrimonio o un deterioro significativo de la imagen. Además, se requerirá una cantidad de tiempo importante de la alta dirección en investigar y corregir los daños	Repercusiones significativas sobre los clientes	Acciones por parte del regulador que pueden incluir multas	Moderado
Menor	**2**	Riesgo que causa un daño en el patrimonio o imagen, que se puede corregir en el corto tiempo y que no afecta en el cumplimiento de los objetivos estratégicos	Posibilidades de suspensión de servicios pero el impacto sobre los clientes es insignificante	Comentarios adversos pero no interviene	Menor
Insignificante	**1**	Riesgo que puede tener un pequeño o nulo efecto en la institución	No impacta a los clientes	No interviene	Insignificante

Complejidad y la Interconexión

El Administrador de riesgos realizará el análisis cualitativo considerando distintos grados de detalle y complejidad en función del propósito, características de la información y los recursos disponibles; así como la dependencia y relación que existe entre los riesgos y sus procesos vinculados.

Factores Relacionados con el Tiempo y la Volatilidad

Se analiza la escalabilidad en el tiempo con relación a los niveles aceptables de la probabilidad, para lo cual se verifica que los eventos identificados sean consistentes con la probabilidad asignada y evitar la presencia de volatilidad en la frecuencia de ocurrencia y así mantener eventos con tiempos constantes para un mejor manejo del riesgo.

Eficacia de los Controles Existentes

Se contempla el análisis de los controles que actualmente se ejecutan en los procesos en los cuales se identificaron los eventos de riesgo, de esta manera se podría determinar el nivel de riesgo y la necesidad de la aplicación de nuevos controles con mayor eficacia.

Niveles de Sensibilidad y de Confianza.

Se evalúa los niveles de sensibilidad de los eventos identificados para reconocer si el nivel de impacto es significativo o de menor importancia en los resultados y objetivos de los procesos. Y también es importante definir el nivel de confianza del impacto esperado para que la respuesta a este sea idónea y no ocurran eventos de afectaciones inesperadas.

Influencias en el Análisis de Riesgo

El análisis de riesgos puede estar distorsionado por la presencia de influencias internas y externas que pueden incluir, pero no limitarse a opiniones, prejuicios, el origen de los datos y la calidad de éstos. Estas influencias pueden afectar el resultado del análisis generando contingencias que no generan valor y no mitigan el impacto de los riesgos. Por ello es importante comunicar al personal involucrado en el análisis de riesgos la posible presencia de estas influencias, por medio de la aprobación y publicación de la Metodología Administración de Riesgo Operativo en el repositorio documental de ELTHON CEO.

EL personal involucrado en el análisis de riesgo debe comprender y conocer las posibles influencias presentadas en el análisis de riesgo, para lo cual se describe a continuación el detalle de cada una de ellas:

- Opiniones: la existencia de diferentes ideas puede causar discrepancias en la percepción sobre el evento.
- Prejuicio: La presencia de una idea preconcebida generando un impacto negativo en la comprensión del evento.
- Calidad de los datos: Información recolectada bajo una metodología no acorde al método de evaluación puede resultar en una medición errónea en el impacto del riesgo.

- Limitaciones de las técnicas: intentar aplicar métodos de evaluación sin los conocimientos técnicos adecuados o las herramientas necesarias para su ejecución pueden generar inconsistencias en la gestión del evento.

5.1.3 VALORACIÓN DEL RIESGO

Esta actividad es realizada por el Administrador de Riesgos, e implica la evaluación de los riesgos identificados de acuerdo a los siguientes componentes: línea de negocio, tipo de proceso, factor y tipo de evento. Los campos de la Matriz de Riesgos se definen a continuación:

- **ID**: Código único de identificación del riesgo, compuesto por caracteres alfanuméricos.
- **Macroproceso**: Nombre del macroproceso al que se encuentra atado el riesgo, en base al Mapa de Procesos.
- **Proceso**: Nombre del proceso al que se encuentra atado el riesgo, en base al Inventario de Procesos.
- **Línea del Negocio**: Indicar la Línea de Negocio a la que se encuentra asociado el **proceso** en el que se está identificando el riesgo.
- **Riesgo**: Descripción del riesgo operativo identificado, se debe tener mucha audacia para describir el evento de riesgo ya que debe ser relevante y no debe tomarse como una observación a la persona dueña del proceso.
- **Tipo de riesgo**: Se detalla si el riesgo es operativo o de orden legal.
- **Factor**: Indica la causa primaria o de origen del riesgo. Son los siguientes:
  - Procesos
  - Personas
  - Tecnología de la Información
  - Eventos Externos
- **Tratamiento de riesgos**: acciones a tomar para el manejo del evento de riesgo.
  - asumir
  - compartir
  - mitigar
  - transferir

5.1.4 LÍMITES DE EXPOSICIÓN

A fin de lograr una adecuada administración del Riesgo Operativo, se ha definido un límite de exposición considerado como “aceptable” para aquellos riesgos de nivel 1 (Bajo), 2 (Medio), mientras que aquellos con nivel 3 (Alto) y 4 (Muy alto) son considerados como no aceptables, ya que se encuentran por encima del límite establecido.

5.1.5 FACTORES DE RIESGO OPERACIONAL

Personas

ELTHON CEO debe contar con una estructura orgánico-funcional acorde al tamaño, complejidad de sus operaciones y normativa vigente que le aplica según su segmento. Además, deben identificar las fallas o insuficiencias asociadas al factor "personas", tales como: falta de personal adecuado, negligencia, error humano, conflicto de intereses, falta de segregación de funciones, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros

Procesos

Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, tomando como referencia el estándar ISO 9001, ELTHON CEO define el Mapa de Procesos que cuenta con procesos definidos, documentados, aprobados, actualizados y socializados que se encuentren alineados con la estrategia institucional y con las políticas adoptadas, definiendo formalmente procesos, políticas y procedimientos que aseguren una apropiada planificación, administración y cumplimiento de los objetivos institucionales; en concordancia, principalmente, con los factores de riesgo personas y tecnología de la información. Los procesos se agrupan según su clasificación en gobernantes, productivos y habilitantes.

Se asigna los procesos productivos a la línea de negocio minorista, de acuerdo con los módulos del Software ELTHON, si algún proceso productivo interviene en más de una línea de negocio, se sigue lo descrito en la Metodología BIA para determinar los procesos críticos.

ELTHON CEO deberá adoptar una metodología que les permita identificar y evaluar los procesos críticos, aún en los provistos por terceros, previo a la elaboración del plan de continuidad del negocio; así como realizar un análisis de riesgos y equilibrar el costo de la implementación o no del plan de continuidad, dependiendo de la criticidad de cada proceso.

Tecnología de Información

ELTHON CEO debe contar y mantener tecnología de información acorde a su segmento, naturaleza y perfil de riesgo de sus operaciones, que garantice la captura, procesamiento,

almacenamiento y transmisión de manera oportuna y confiable de la información para la toma de decisiones, incluyendo aquella que está bajo la modalidad de servicios provistos por terceros.

Eventos Externos

En la administración del riesgo operativo, ELTHON CEO debe considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como: incidentes con proveedores, fallas en los servicios públicos, ocurrencia de desastres naturales, atentados, fraudes externos y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades. Para el efecto, deben contar con planes de contingencia y de continuidad del negocio.

5.1.6 TIPOS DE EVENTOS DE RIESGO OPERATIVO

Los tipos de eventos son los siguientes:

a) **Fraude interno.** Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o eludir regulaciones, leyes o políticas, infidelidades de empleados o uso de información privilegiada para beneficio propio;
b) **Fraude externo.** Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes o recursos indebidamente o eludir la legislación, por parte un tercero, incluyendo daños ocasionados por individuos, grupos u organizaciones externas que buscan explorar la dependencia de la institución en recursos tecnológico;
c) **Prácticas laborales y seguridad del ambiente de trabajo.** Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, pago de reclamaciones por daños personales, casos relacionados con la diversidad o discriminación y por responsabilidades generales en el trabajo;
d) **Prácticas relacionadas con los clientes, los productos y el negocio**. Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a socios, clientes o usuarios, o de la naturaleza o diseño de un producto;
e) **Daños a los activos físicos.** Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales o por terrorismo, vandalismo, incendio o inundaciones;
f) **Interrupción del negocio por fallas en la tecnología de la información**. Pérdidas derivadas por la ocurrencia de problemas de telecomunicaciones, servicios públicos y apagones; y,
g) **Deficiencias en la ejecución de procesos, en el procesamiento de operaciones; y en las relaciones con proveedores y terceros.** Pérdidas derivadas de errores en el

procesamiento de operaciones, en la gestión de procesos y en relaciones con contrapartes comerciales y proveedores.

Se considera la siguiente clasificación:

TIPO DE EVENTO NIVEL 1	TIPO DE EVENTO NIVEL 2	FALLA O INSUFICIENCIA NIVEL 3
Fraude interno	Actividades no autorizadas	Operaciones no reveladas/registradas (intencionalmente)
		Operaciones no autorizadas (con pérdidas pecuniarias)
		Inapropiada utilización de información confidencial
	Hurto y fraude	Fraude
		Hurto/extorsión/malversación/robo
		Apropiación indebida de activos
		Destrucción dolosa de activos
		Falsificación (Fuente interna)
		Utilización de cheques sin fondos (Fuente interna
		Contrabando
		Incumplimiento /evasión de impuestos (intencional)
		Soborno/cohecho
		Destrucción maliciosa de activos
Fraude externo	Hurto y fraude	Hurto/robo (fuente externa)
		Falsificación (Fuente externa)
		Utilización de cheques sin fondos (Fuente externa)
	Seguridad de los sistemas	Daños por ataques informáticos
		Robo de información
Prácticas laborales y seguridad del ambiente de trabajo	Relaciones laborales	Inadecuada contratación del personal
		Falta de difusión y comunicación de políticas
		Inadecuada política de administración del personal
	Higiene y seguridad en el trabajo	Casos relacionados con las normas de higiene y seguridad en el trabajo
		Indemnización laboral
	Diversidad y discriminación	Todo tipo de discriminación
Prácticas relacionadas con los clientes, los productos y el negocio	Adecuación, divulgación de información y confianza	Quebrantamiento de la privacidad de información, sobre socios, clientes y usuarios
		Incursión en nuevas actividades sin considerar riesgos
		Actividades no autorizadas
		Prácticas inadecuadas de negociación, prácticas contrarias a la competencia
		Abuso de información privilegiada (en favor de la entidad)
Daños a los activos físicos	Desastes y otros acontecimientos	Pérdidas por desastres naturales, terrorismo, vandalismo, etc.
Interrupción del negocio por fallas en la tecnología de la información	Sistemas	Fallas en el hardware
		Fallas en el software
		Problemas de telecomunicaciones
		Cortes en los servicios públicos
Deficiencias en la ejecución de procesos, en el procesamiento de operaciones; y en las relaciones con proveedores y terceros	Recepción, ejecución y mantenimiento de operaciones	Errores en introducción de datos, mantenimiento o descarga
		Incumplimiento en la entrega de información hacia terceros
		Fallas en la entrega de información
	Aceptación de socios o clientes y documentación	Inexistencia de autorizaciones
		Documentos jurídicos incompletos/inexistentes
		Falla en la administración de colaterales
	Gestión de cuentas de clientes	Acceso no autorizado a cuentas
		Registros incorrectos de socios y clientes
	Contrapartes comerciales	Fallos de contrapartes (proveedores)
		Otros litigios con contrapartes (proveedores)

5.1.6.1 RIESGO INHERENTE

Probabilidad: La probabilidad puede ser medida con criterios de frecuencia o teniendo en cuenta la presencia de factores internos y externos que puedan propiciar el riesgo, aunque este no se haya presentado nunca.

La probabilidad de ocurrencia es el nivel de repetición del factor de riesgo analizado, es decir, con qué frecuencia el evento de riesgo se origina en el caso de ser real o potencial. Se han definido 5 niveles de probabilidad, los cuales se muestran a continuación:

CATEGORÍA	VALOR	CRITERIOS DE CALIFICACIÓN	
		DESCRIPCIÓN	OCURRENCIA EN TIEMPO
Muy Alto	**5**	Probabilidad de ocurrencia es **muy alta**	Riesgo cuya ocurrencia es al menos una vez cada **15 días (24 veces)**
Alto	**4**	Probabilidad de ocurrencia es **alta**	Riesgo cuya ocurrencia al menos una vez cada **mes (12 veces)**
Medio	**3**	Probabilidad de ocurrencia es **media**	Riesgo cuya ocurrencia es al menos una vez cada **tres meses (4 veces)**
Bajo	**2**	Probabilidad de ocurrencia es **baja**	Riesgo cuya ocurrencia es al menos una vez cada **seis meses (2 veces)**
Muy Bajo	**1**	Probabilidad de ocurrencia es **muy baja**	Riesgo cuya ocurrencia es al menos una vez al **año (1 vez)**

Impacto: se debe evaluar la consecuencia potencial del evento de riesgo si este llegara a suscitarse, es decir, cual es el efecto directo o indirecto en la institución. La matriz define 5 niveles de impacto, los cuales se muestran a continuación:

CATEGORÍA	VALOR	CRITERIOS			
		Repercusiones para la entidad	Repercusiones sobre los clientes	Acciones del Regulador	Posible pérdida económica
Catastrófico	**5**	Riesgo cuya materialización influye directamente en el cumplimiento de la misión, pérdida patrimonial o deterioro de la imagen, dejando además sin funcionar totalmente o por un período importante de tiempo, los servicios o productos que entrega la entidad	Afecta a un número grandes de clientes	Multas significativas	Catastrófica
Mayor	**4**	Riesgo cuya materialización dañaría significativamente el patrimonio, imagen o logro de los objetivos sociales. Además, se requerirá una cantidad importante de tiempo de la alta dirección en investigar y corregir los daños	Suspensión prolongada de servicios	Multas medianas	Mayor

CATEGORÍA	VALOR	CRITERIOS			
		Repercusiones para la entidad	Repercusiones sobre los clientes	Acciones del Regulador	Posible pérdida económica
Moderado	**3**	Riesgo cuya materialización causaría ya sea una pérdida importante en el Patrimonio o un deterioro significativo de la imagen. Además, se requerirá una cantidad de tiempo importante de la alta dirección en investigar y corregir los daños	Repercusiones significativas sobre los clientes	Acciones por parte del regulador que pueden incluir multas	Moderado
Menor	**2**	Riesgo que causa un daño en el patrimonio o imagen, que se puede corregir en el corto tiempo y que no afecta en el cumplimiento de los objetivos estratégicos	Posibilidades de suspensión de servicios pero el impacto sobre los clientes es insignificante	Comentarios adversos pero no interviene	Menor
Insignificante	**1**	Riesgo que puede tener un pequeño o nulo efecto en la institución	No impacta a los clientes	No interviene	Insignificante

ELTHON CEO categoriza en una escala cualitativa el nivel de exposición que tiene un determinado riesgo, a través del resultado del producto matemático entre impacto y probabilidad, el cual está representado en 4 niveles:

Rango Riesgo Residual		Nivel Riesgo Residual	
Mínimo	Máximo		
1	3	1	Bajo
4	8	2	Medio
9	16	3	Alto
17	25	4	Muy Alto

Conforme el límite de exposición establecido por la administración se buscarán las opciones más óptimas de tratamiento, siendo prioridad la gestión de los riesgos calificados en los niveles Alto y Muy alto, en tanto que, para los dos siguientes niveles Medio y Bajo se buscarán diferentes alternativas para su gestión, en todos los casos se debe realizar el análisis de costo beneficio, entre la severidad del riesgo y la implementación de la medida de acción.

5.1.7 MAPA DE CALOR

Constituye una herramienta gerencial que brinda criterios de decisión a la alta dirección frente a los cambios que deben ser realizados en la organización para controlar los riesgos existentes y prevenir su materialización.

Una vez determinado el nivel de riesgo inherente, se genera el mapa de calor, mismo que es una representación gráfica en un plano cartesiano en el que convergen la escala de probabilidad e impacto del riesgo.

			IMPACTO				
PROBABILIDAD / IMPACTO			Muy bajo	Bajo	Medio	Alto	Muy alto
			1	2	3	4	5
PROBABILIDAD	Muy alta	5	5	10	15	20	25
	Alta	4	4	8	12	16	20
	Media	3	3	6	9	12	15
	Baja	2	2	4	6	8	10
	Muy baja	1	1	2	3	4	5

Los niveles de riesgo inherentes se presentan a continuación:

Riesgo Inherente							
Escala	Escala	Escala Riesgo Inherente		Rango Riesgo Inherente		Nivel Riesgo Inherente	
Impacto	Probabilidad	Impacto x Probabilidad	Nivel Riesgo Inherente	Mínimo	Máximo		
1	1	Imp:1 Prob:1	1	1	3	1	Bajo
1	2	Imp:1 Prob:2	2				
1	3	Imp:1 Prob:3	3	4	8	2	Medio
1	4	Imp:1 Prob:4	4	9	16	3	Alto
1	5	Imp:1 Prob:5	5	17	25	4	Muy Alto
2	1	Imp:2 Prob:1	2				
2	2	Imp:2 Prob:2	4				
2	3	Imp:2 Prob:3	6				
2	4	Imp:2 Prob:4	8				
2	5	Imp:2 Prob:5	10				
3	1	Imp:3 Prob:1	3				
3	2	Imp:3 Prob:2	6				
3	3	Imp:3 Prob:3	9				
3	4	Imp:3 Prob:4	12				
3	5	Imp:3 Prob:5	15				
4	1	Imp:4 Prob:1	4				
4	2	Imp:4 Prob:2	8				
4	3	Imp:4 Prob:3	12				
4	4	Imp:4 Prob:4	16				
4	5	Imp:4 Prob:5	20				
5	1	Imp:5 Prob:1	5				
5	2	Imp:5 Prob:2	10				
5	3	Imp:5 Prob:3	15				
5	4	Imp:5 Prob:4	20				
5	5	Imp:5 Prob:5	25				

5.1.8 ACCIONES DE VALORACIÓN DE RIESGO

Se presenta un esquema acciones para valorar el riesgo, el cual consiste en el establecimiento de actividades que conllevan a decisión de la aplicación de acciones o controles adicionales para la mitigación del nivel de riesgo. Esto puede conducir a una decisión de:

- **Asumir el riesgo (no hacer nada más):** La entidad asumirá el riesgo cuando los eventos sean de nivel de riesgo bajo.
- **Considerar opciones para el tratamiento de riesgo:**
    - **Compartir el riesgo.** Acuerdos contractuales que permiten traspasar parcialmente parte del riesgo a un tercero
    - **Mitigar:** Tomar medidas encaminadas a impedir la materialización de los eventos de riesgo Ej. Rediseño de procesos, implementación de nuevos controles.

- **Transferir.** Es el traspaso total del riesgo identificado a otras entidades Ej. Contratación de seguros, empresas transportadoras de valores, entre otros.

- **Realizar un análisis adicional para comprender mejor el riesgo y reconsiderar los objetivos:** El Administrador de riesgos junto con el Administrador abordan una revisión adicional de la valoración del riesgo en el cual se confirma que los niveles de probabilidad e impacto fueron asignados correctamente.
- **Mantener los controles existentes:** se acepta el nivel de riesgo del evento debido a que los controles existentes coadyuvan con la respuesta al evento de riesgo manteniendo un impacto controlado para la organización dentro de los parámetros esperados.

Una vez identificado, analizado y valorado el evento de riesgo, esta información deberá constar en la **Anexo 1 Matriz de Eventos de Riesgos** de ELTHON CEO, la cual contempla los siguientes campos:

- **Descripción del evento.** Los responsables de cada área realizarán un levantamiento preliminar, en el campo Descripción identificarán los riesgos operacionales potenciales en los diferentes procesos, que pueden derivar en pérdidas financieras, suspensión de operaciones o de información para la entidad, en base a la experiencia de los responsables de los mismos. Para luego efectuar una revisión y levantamiento final de los procesos y riesgos levantados con el Administrador de Riesgos en conjunto con los responsables de cada área.
- **Tipo de factor.** Representa si el evento es interno o externo.
- **Factor de riesgo operativo.** Se define el factor del hecho generador de pérdida puede ser: Personas, procesos, tecnología de información o eventos externos.
- **Calificación del riesgo inherente.** Se calificará la probabilidad e impacto de cada evento para determinar el nivel de riesgo inherente.
- **Calificación de los controles existentes.** Son las políticas y procedimientos que se implementan para ayudar a asegurar que las respuestas a los riesgos se llevan a cabo eficazmente. El proceso de control se inicia a través de un levantamiento de los procesos operativos durante el cual se debe centrar la atención en aquellos controles que minimizan los factores de riesgo ya identificados.

5.1.9 TRATAMIENTO DEL RIESGO

El proceso del tratamiento de los eventos implica la decisión de la aplicación de actividades adicionales relacionadas con controles o planes de acción, para lo cual se considerará los siguientes aspectos para la formulación del tratamiento de los eventos:

- **Formular y seleccionar opciones para el tratamiento del riesgo**: se establecerán diferentes tipos de opciones para mitigar el evento dependiendo el nivel de riesgo inherente obtenido. Las opciones pueden formularse tomando en cuenta la aceptación del nivel de riesgo, la aplicación de controles reforzados y la elaboración de planes de acción.
- **Planificar e implementar el tratamiento del riesgo**: de acuerdo a la opción seleccionada se realiza una planificación de la implementación en conjunto con el líder del proceso que definirán los lineamientos, responsabilidades, tiempos de cumplimiento y actividades a ejecutar en caso de que la opción corresponda una aplicación de control o plan de acción.
- **Evaluar la eficacia de ese tratamiento**: una vez aplicada la opción para el tratamiento de un evento de riesgo (control o plan de acción) se verifica se haya reducido el nivel de riesgo, obteniendo así un riesgo residual.
- **Decidir si el riesgo residual es aceptable:** los resultados de los niveles de riesgo residuales deben estar dentro de los límites de riesgo aceptable (muy bajo, bajo y medio), por lo que si un evento no mantiene estos niveles se deberá realizar acciones adicionales.
- **Si no es aceptable, efectuar tratamiento adiciona**l: se podrá reformular planes de acción que conlleven a actividades y responsabilidades reforzadas que contengan diferentes alternativas para cubrir el nivel de riesgo residual no aceptable.

Una vez tratado los eventos de riesgo se registra la información en la Matriz de Eventos de Riesgos de ELTHON CEO, la cual contendrá la siguiente información:

- **Descripción del control:** Se detalla una breve descripción del control identificado.
- **Automatización del control:** Se refiere al uso de sistemas o elementos computarizados y electromecánicos para establecer controles.
- **Oportunidad del control:** Se debe hacer un balance entre los tipos de controles siempre teniendo en cuenta que es preferible prevenir pérdidas a detectarlas. Los controles podrán ser de carácter preventivo, detectivo o correctivo.
- **Periodicidad del control**: Se refiere a la frecuencia con que se aplica el control implementado; éste puede ser Permanente, Periódico u Ocasional.
- **Documental del control:** Se refiere a si el control está constando en procesos documentados debidamente aprobados o no.
- **Responsable:** Indica si existe o no un responsable del llevar a cabo el control.
- **Eficacia:** Indica si al aplicar el control se presentan o no eventos de riesgo.
- **Calificación del Control:** Es la multiplicación del valor de las categorías escogidas en periodicidad, oportunidad y automatización. La escala puede ir desde el valor de 1 hasta 125.

- **Efectividad del Control:** Es la multiplicación del valor de las categorías escogidas en Documental, Responsable y eficacia. La escala puede ir desde el valor de 1 hasta 125.
- **Riesgo residual.** Es el riesgo resultante una vez que se han implementado los controles pertinentes para su tratamiento. Es el resultado de la diferencia entre el riesgo inherente menos la efectividad del control.

5.1.10 EVALUACIÓN DE CONTROLES Y SU EFICACIA

El proceso de control se centra en la atención en aquellos controles que minimizan los factores de riesgo ya identificados. Adicionalmente, en esta fase se identifica si existe un control para el riesgo identificado, y se procede a evaluar su nivel de efectividad:

- **Descripción del control:** Se detalla una breve descripción del control identificado.
- **Implementación:** Se detalla si es que el control se encuentra implementado o en proceso de implementación.
- **Responsable:** Gerencia responsable de ejecutar el control.
- **Normado:** En este campo se detalla si es que el control se encuentra documentado o no a fin de definir su nivel de formalidad.
- **Periodicidad del control**: Se refiere a la frecuencia con que se aplica el control implementado; éste puede ser Permanente, Periódico u Ocasional.
- **Oportunidad del control:** Se debe hacer un balance entre los tipos de controles siempre teniendo en cuenta que es preferible prevenir pérdidas a detectarlas. Los controles podrán ser de carácter preventivo, detectivo y correctivo.
- **Automatización del control:** Se refiere al uso de sistemas o elementos computarizados y electromecánicos para establecer controles.
- **Calificación del Control:** Es la multiplicación del valor de las categorías escogidas en periodicidad, oportunidad y automatización. La escala puede ir desde el valor de 1 hasta 125.
- **Efectividad del Control:** Es el indicador del nivel de relevancia y pertinencia del control, así como de que su aplicación es oportuna, correcta y consistente.
- **Riesgo residual:** Es el riesgo resultante una vez que se han implementado los controles pertinentes para su tratamiento. Es el resultado de la diferencia entre el riesgo inherente menos la efectividad del control.

Control Evaluación del Impacto					
Escala	**Categoría Automatización**	**Escala**	**Categoría Oportunidad**	**Escala**	**Categoría Documental**
1	Manual	1	Registro	1	No existen procesos
2	Hoja Electrónica Simple	2	Correctivo (ExPost)	2	Existen procesos NO documentados definidos personal operativo

Control					
Evaluación del Impacto					
3	Hoja Electrónica Macros	3	Detectivo	3	Existen procesos NO documentados definidos por el supervisor operativo
4	Automatizado Sistema Externo	4	Preventivo	4	Existen procesos y procedimientos NO aprobados, definidos por el dueño del proceso
5	Automatizado Nativo Core	5	Mitigación Integral	5	Existen procesos y procedimientos debidamente aprobados y documentados

	Categoría Automatización	Detalle
1	Manual	El control es manual, se registra y administra en documentos físicos
2	Hoja Electrónica Simple	El control se realiza en una hoja electrónica, los datos de cada evento de riesgo se ingresan, registran y gestionan mediante el ingreso manual a la hoja
3	Hoja Electrónica Macros	El control se realiza en una hoja electrónica, los datos de cada evento de riesgo se ingresan, registran y gestionan mediante la carga a través de macros/archivo plano de una fuente informática
4	Automatizado Sistema Externo	El control se realiza en un sistema informático que no es nativo del core transaccional, se cargan archivos e información de formato txt o digitando al sistema
5	Automatizado Nativo Core	El control se realiza en un sistema informático que es nativo del core transaccional, los datos y análisis se realiza sin la participación manual de los funcionarios de la entidad, los reportes no pueden alterarse ni modificarse por terceros

	Categoría Oportunidad	Detalle
1	Registro	La entidad se limita a registrar e inventariar los eventos de riesgo, no implementa medidas de mitigación
2	Correctivo (ExPost)	El control es de carácter correctivo (expost), se toman medidas de mitigación luego de la presencia del evento particular, la acción de la entidad es reactiva. Permiten, después de ser detectado el evento, el restablecimiento de la actividad y mitigación del impacto/frecuencia
3	Detectivo	La entidad se esfuerza por implementar controles sobre eventos que ya se han presentado, sin que exista ningún caso o evento presente particular. Se registra un evento después presentado; sirven para descubrir resultados no previstos y alertar sobre la presencia de pérdidas reales
4	Preventivo	Los controles se implementan a través de la identificación de eventos que se han presentado o pueden presentarse, con criterios de jerarquización y asignación de recursos a través de una matriz de riesgos debidamente estructurada
5	Integral	Los controles han sido implementados de manera integral, con un protocolo de registro de los eventos, se procede con una respuesta a la presencia real de un evento (correctivo), se encuentran debidamente inventariados (detectivo) e incluso se gestionan de carácter preventivo mediante una matriz de riesgos debidamente estructurada. Se orientan a eliminar las causas del riesgo, para prevenir su ocurrencia o materialización

	Categoría Documental	Detalle
1	No existen procesos	No existen procesos ni procedimientos documentados o verbales
2	Existen procesos NO documentados definidos personal operativo	Existen procesos y procedimientos no documentados (verbales), definidos por el propio personal operativo
3	Existen procesos NO documentados definidos por el supervisor operativo	Existen procesos y procedimientos no documentados (verbales), definidos por el supervisor operativo

Control Evaluación del Impacto		
4	Existen procesos y procedimientos NO aprobados, definidos por el dueño del proceso	Existen procesos y procedimientos no aprobados, pero si documentados en los que se detalla el control definidos por el dueño del proceso
5	Existen procesos y procedimientos debidamente aprobados y documentados	Existen procesos y procedimientos debidamente aprobados por la instancia de decisión y documentados en los que se detalla el control

Control Evaluación de la Probabilidad					
Escala	**Categoría Perioricidad**	**Escala**	**Categoría Responsable**	**Escala**	**Categoría Eficacia**
1	Excepcional/Respuesta a Evento	1	No Existe Responsable Visible	1	Aún se presentan eventos repetitivos
2	Esporádico/Sorpresa	2	Asignación Puntual del Responsable	2	Aún se presentan eventos esporádicos
3	Ocasional/Bajo Solicitud	3	Asignación Verbal del Responsable	3	Se presentan eventos ocasionales
4	Periódico	4	Asignación Mail del Responsable	4	Se presentan eventos esporádicos
5	Permanente/Diario	5	Asignación Funcional del Responsable	5	No se ha presentado ningún evento

	Categoría Perioricidad	**Detalle**
1	Excepcional/Respuesta a Evento	El control implementado solo se ejcuta luego de la presencia de un evento generador de pérdida
2	Esporádico/Sorpresa	El control implementado se ejecuta esporádicamente, mediante un proceso aleatorio (sorpresa)
3	Ocasional/Bajo Solicitud	El control implementado se ejecuta ocasionalmente. Al menos una vez por trimestre
4	Periódico	El control implementado se ejecuta frecuentemente. Al menos una vez por mes
5	Permanente/Diario	El control se ejecuta en forma permanente, con una frecuencia diaria

	Categoría Reponsable	**Detalle**
1	No Existe Responsable Visible	No se observa reponsable visible de implementar y ejcutar el control
2	Asignación Puntual del Responsable	El responsable del control se asigna al momento de presentarse un evento, la realiza el responsable del área (proceso) sin disponer de un procedimiento específico
3	Asignación Verbal del Responsable	El responsable del control lo asigna verbalmente por el responsable del área (proceso), bajo su criterio discresional
4	Asignación Mail del Responsable	El responsable del control lo asigna por mail por el responsable del área (proceso), bajo su criterio discresional
5	Asignación Funcional del Responsable	El responsable del control se encuentra asignado en el Manual Orgánico Funcional de la entidad, dentro de las especificaciones del cargo / puesto

	Categoría Eficacia	**Detalle**
1	Aún se presentan eventos repetitivos	Se ha presentado al menos UN evento de riesgo (hecho generador) semanal

Control		
Evaluación del Impacto		
2	Aún se presentan eventos esporádicos	Se ha presentado al menos UN evento de riesgo (hecho generador) mensual
3	Se presentan eventos ocasionales	Se ha presentado al menos UN evento de riesgo (hecho generador) semestral
4	Se presentan eventos esporádicos	Se ha presentado al menos UN evento de riesgo (hecho generador) anual
5	No se ha presentado ningún evento	No se ha presentado ningún evento

Evaluación de la Calidad de Control IMPACTO

Calidad Control									
Evaluación de Impacto									
Categoría Automatización	Categoría Oportunidad	Categoría Documental	Aut * Opo*Doc	Escala	Escala Ordenado	Rango		Calidad Control	
						Inferior	Superior		
1	1	1	Imp: 1 Ocu: 1 Doc: 1	1	1	0	0	Sin Control	0
1	1	2	Imp: 1 Ocu: 1 Doc: 2	2	2	1	10	Deficiente	-1
1	1	3	Imp: 1 Ocu: 1 Doc: 3	3	2	11	20	Débil	1
1	1	4	Imp: 1 Ocu: 1 Doc: 4	4	2	21	40	Regular	2
1	1	5	Imp: 1 Ocu: 1 Doc: 5	5	3	41	60	Bueno	3
1	2	1	Imp: 1 Ocu: 2 Doc: 1	2	3	61	90	Adecuado	4
1	2	2	Imp: 1 Ocu: 2 Doc: 2	4	3	91	125	Optimo	5
1	2	3	Imp: 1 Ocu: 2 Doc: 3	6	4				
1	2	4	Imp: 1 Ocu: 2 Doc: 4	8	4				
1	2	5	Imp: 1 Ocu: 2 Doc: 5	10	4				
1	3	1	Imp: 1 Ocu: 3 Doc: 1	3	4				
1	3	2	Imp: 1 Ocu: 3 Doc: 2	6	4				
1	3	3	Imp: 1 Ocu: 3 Doc: 3	9	4				
1	3	4	Imp: 1 Ocu: 3 Doc: 4	12	5				
1	3	5	Imp: 1 Ocu: 3 Doc: 5	15	5				
1	4	1	Imp: 1 Ocu: 4 Doc: 1	4	5				
1	4	2	Imp: 1 Ocu: 4 Doc: 2	8	6				
1	4	3	Imp: 1 Ocu: 4 Doc: 3	12	6				
1	4	4	Imp: 1 Ocu: 4 Doc: 4	16	6				
1	4	5	Imp: 1 Ocu: 4 Doc: 5	20	6				
1	5	1	Imp: 1 Ocu: 5 Doc: 1	5	6				
1	5	2	Imp: 1 Ocu: 5 Doc: 2	10	6				
1	5	3	Imp: 1 Ocu: 5 Doc: 3	15	8				
1	5	4	Imp: 1 Ocu: 5 Doc: 4	20	8				
1	5	5	Imp: 1 Ocu: 5 Doc: 5	25	8				
2	1	1	Imp: 2 Ocu: 1 Doc: 1	2	8				
2	1	2	Imp: 2 Ocu: 1 Doc: 2	4	8				
2	1	3	Imp: 2 Ocu: 1 Doc: 3	6	8				
2	1	4	Imp: 2 Ocu: 1 Doc: 4	8	8				
2	1	5	Imp: 2 Ocu: 1 Doc: 5	10	9				
2	2	1	Imp: 2 Ocu: 2 Doc: 1	4	9				
2	2	2	Imp: 2 Ocu: 2 Doc: 2	8	9				
2	2	3	Imp: 2 Ocu: 2 Doc: 3	12	10				
2	2	4	Imp: 2 Ocu: 2 Doc: 4	16	10				
2	2	5	Imp: 2 Ocu: 2 Doc: 5	20	10				
2	3	1	Imp: 2 Ocu: 3 Doc: 1	6	10				
2	3	2	Imp: 2 Ocu: 3 Doc: 2	12	10				
2	3	3	Imp: 2 Ocu: 3 Doc: 3	18	10				
2	3	4	Imp: 2 Ocu: 3 Doc: 4	24	12				

2	3	5	Imp:2 Ocu:3 Doc:5	30	12
2	4	1	Imp:2 Ocu:4 Doc:1	8	12
2	4	2	Imp:2 Ocu:4 Doc:2	16	12
2	4	3	Imp:2 Ocu:4 Doc:3	24	12
2	4	4	Imp:2 Ocu:4 Doc:4	32	12
2	4	5	Imp:2 Ocu:4 Doc:5	40	12
2	5	1	Imp:2 Ocu:5 Doc:1	10	12
2	5	2	Imp:2 Ocu:5 Doc:2	20	12
2	5	3	Imp:2 Ocu:5 Doc:3	30	15
2	5	4	Imp:2 Ocu:5 Doc:4	40	15
2	5	5	Imp:2 Ocu:5 Doc:5	50	15
3	1	1	Imp:3 Ocu:1 Doc:1	3	15
3	1	2	Imp:3 Ocu:1 Doc:2	6	15
3	1	3	Imp:3 Ocu:1 Doc:3	9	15
3	1	4	Imp:3 Ocu:1 Doc:4	12	16
3	1	5	Imp:3 Ocu:1 Doc:5	15	16
3	2	1	Imp:3 Ocu:2 Doc:1	6	16
3	2	2	Imp:3 Ocu:2 Doc:2	12	16
3	2	3	Imp:3 Ocu:2 Doc:3	18	16
3	2	4	Imp:3 Ocu:2 Doc:4	24	16
3	2	5	Imp:3 Ocu:2 Doc:5	30	18
3	3	1	Imp:3 Ocu:3 Doc:1	9	18
3	3	2	Imp:3 Ocu:3 Doc:2	18	18
3	3	3	Imp:3 Ocu:3 Doc:3	27	20
3	3	4	Imp:3 Ocu:3 Doc:4	36	20
3	3	5	Imp:3 Ocu:3 Doc:5	45	20
3	4	1	Imp:3 Ocu:4 Doc:1	12	20
3	4	2	Imp:3 Ocu:4 Doc:2	24	20
3	4	3	Imp:3 Ocu:4 Doc:3	36	20
3	4	4	Imp:3 Ocu:4 Doc:4	48	20
3	4	5	Imp:3 Ocu:4 Doc:5	60	20
3	5	1	Imp:3 Ocu:5 Doc:1	15	20
3	5	2	Imp:3 Ocu:5 Doc:2	30	24
3	5	3	Imp:3 Ocu:5 Doc:3	45	24
3	5	4	Imp:3 Ocu:5 Doc:4	60	24
3	5	5	Imp:3 Ocu:5 Doc:5	75	24
4	1	1	Imp:4 Ocu:1 Doc:1	4	24
4	1	2	Imp:4 Ocu:1 Doc:2	8	24
4	1	3	Imp:4 Ocu:1 Doc:3	12	25
4	1	4	Imp:4 Ocu:1 Doc:4	16	25
4	1	5	Imp:4 Ocu:1 Doc:5	20	25
4	2	1	Imp:4 Ocu:2 Doc:1	8	27
4	2	2	Imp:4 Ocu:2 Doc:2	16	30
4	2	3	Imp:4 Ocu:2 Doc:3	24	30
4	2	4	Imp:4 Ocu:2 Doc:4	32	30
4	2	5	Imp:4 Ocu:2 Doc:5	40	30
4	3	1	Imp:4 Ocu:3 Doc:1	12	30
4	3	2	Imp:4 Ocu:3 Doc:2	24	30
4	3	3	Imp:4 Ocu:3 Doc:3	36	32
4	3	4	Imp:4 Ocu:3 Doc:4	48	32

4	3	5	Imp:4 Ocu:3 Doc:5	60	32
4	4	1	Imp:4 Ocu:4 Doc:1	16	36
4	4	2	Imp:4 Ocu:4 Doc:2	32	36
4	4	3	Imp:4 Ocu:4 Doc:3	48	36
4	4	4	Imp:4 Ocu:4 Doc:4	64	40
4	4	5	Imp:4 Ocu:4 Doc:5	80	40
4	5	1	Imp:4 Ocu:5 Doc:1	20	40
4	5	2	Imp:4 Ocu:5 Doc:2	40	40
4	5	3	Imp:4 Ocu:5 Doc:3	60	40
4	5	4	Imp:4 Ocu:5 Doc:4	80	40
4	5	5	Imp:4 Ocu:5 Doc:5	100	45
5	1	1	Imp:5 Ocu:1 Doc:1	5	45
5	1	2	Imp:5 Ocu:1 Doc:2	10	45
5	1	3	Imp:5 Ocu:1 Doc:3	15	48
5	1	4	Imp:5 Ocu:1 Doc:4	20	48
5	1	5	Imp:5 Ocu:1 Doc:5	25	48
5	2	1	Imp:5 Ocu:2 Doc:1	10	50
5	2	2	Imp:5 Ocu:2 Doc:2	20	50
5	2	3	Imp:5 Ocu:2 Doc:3	30	50
5	2	4	Imp:5 Ocu:2 Doc:4	40	60
5	2	5	Imp:5 Ocu:2 Doc:5	50	60
5	3	1	Imp:5 Ocu:3 Doc:1	15	60
5	3	2	Imp:5 Ocu:3 Doc:2	30	60
5	3	3	Imp:5 Ocu:3 Doc:3	45	60
5	3	4	Imp:5 Ocu:3 Doc:4	60	60
5	3	5	Imp:5 Ocu:3 Doc:5	75	64
5	4	1	Imp:5 Ocu:4 Doc:1	20	75
5	4	2	Imp:5 Ocu:4 Doc:2	40	75
5	4	3	Imp:5 Ocu:4 Doc:3	60	75
5	4	4	Imp:5 Ocu:4 Doc:4	80	80
5	4	5	Imp:5 Ocu:4 Doc:5	100	80
5	5	1	Imp:5 Ocu:5 Doc:1	25	80
5	5	2	Imp:5 Ocu:5 Doc:2	50	100
5	5	3	Imp:5 Ocu:5 Doc:3	75	100
5	5	4	Imp:5 Ocu:5 Doc:4	100	100
5	5	5	Imp:5 Ocu:5 Doc:5	125	125

Evaluación de la Calidad de Control PROBABILIDAD

Calidad Control									
Evaluación de Probabilidad									
Categoría Responsable	Categoría Periodicidad	Categoría Eficacia	Res*Per*Efi	Escala	Escala Ordenado	Rango		Calidad Control	
						Inferior	Superior		
1	1	1	Per:1 Res:1 Efi:1	1	1	0	0	Sin Control	0
1	1	2	Per:1 Res:1 Efi:2	2	2	1	10	Deficiente	-1
1	1	3	Per:1 Res:1 Efi:3	3	2	11	20	Débil	1
1	1	4	Per:1 Res:1 Efi:4	4	2	21	40	Regular	2
1	1	5	Per:1 Res:1 Efi:5	5	3	41	60	Bueno	3
2	1	1	Per:1 Res:2 Efi:1	2	3	61	90	Adecuado	4
2	1	2	Per:1 Res:2 Efi:2	4	3	91	125	Optimo	5
2	1	3	Per:1 Res:2 Efi:3	6	4				
2	1	4	Per:1 Res:2 Efi:4	8	4				
2	1	5	Per:1 Res:2 Efi:5	10	4				
3	1	1	Per:1 Res:3 Efi:1	3	4				
3	1	2	Per:1 Res:3 Efi:2	6	4				
3	1	3	Per:1 Res:3 Efi:3	9	4				
3	1	4	Per:1 Res:3 Efi:4	12	5				
3	1	5	Per:1 Res:3 Efi:5	15	5				
4	1	1	Per:1 Res:4 Efi:1	4	5				
4	1	2	Per:1 Res:4 Efi:2	8	6				
4	1	3	Per:1 Res:4 Efi:3	12	6				
4	1	4	Per:1 Res:4 Efi:4	16	6				
4	1	5	Per:1 Res:4 Efi:5	20	6				
5	1	1	Per:1 Res:5 Efi:1	5	6				
5	1	2	Per:1 Res:5 Efi:2	10	6				
5	1	3	Per:1 Res:5 Efi:3	15	8				
5	1	4	Per:1 Res:5 Efi:4	20	8				
5	1	5	Per:1 Res:5 Efi:5	25	8				
1	2	1	Per:2 Res:1 Efi:1	2	8				
1	2	2	Per:2 Res:1 Efi:2	4	8				
1	2	3	Per:2 Res:1 Efi:3	6	8				
1	2	4	Per:2 Res:1 Efi:4	8	8				
1	2	5	Per:2 Res:1 Efi:5	10	9				
2	2	1	Per:2 Res:2 Efi:1	4	9				
2	2	2	Per:2 Res:2 Efi:2	8	9				
2	2	3	Per:2 Res:2 Efi:3	12	10				
2	2	4	Per:2 Res:2 Efi:4	16	10				
2	2	5	Per:2 Res:2 Efi:5	20	10				
3	2	1	Per:2 Res:3 Efi:1	6	10				
3	2	2	Per:2 Res:3 Efi:2	12	10				
3	2	3	Per:2 Res:3 Efi:3	18	10				
3	2	4	Per:2 Res:3 Efi:4	24	12				
3	2	5	Per:2 Res:3 Efi:5	30	12				

4	2	1	Per:2 Res:4 Efi:1	8	12
4	2	2	Per:2 Res:4 Efi:2	16	12
4	2	3	Per:2 Res:4 Efi:3	24	12
4	2	4	Per:2 Res:4 Efi:4	32	12
4	2	5	Per:2 Res:4 Efi:5	40	12
5	2	1	Per:2 Res:5 Efi:1	10	12
5	2	2	Per:2 Res:5 Efi:2	20	12
5	2	3	Per:2 Res:5 Efi:3	30	15
5	2	4	Per:2 Res:5 Efi:4	40	15
5	2	5	Per:2 Res:5 Efi:5	50	15
1	3	1	Per:3 Res:1 Efi:1	3	15
1	3	2	Per:3 Res:1 Efi:2	6	15
1	3	3	Per:3 Res:1 Efi:3	9	15
1	3	4	Per:3 Res:1 Efi:4	12	16
1	3	5	Per:3 Res:1 Efi:5	15	16
2	3	1	Per:3 Res:2 Efi:1	6	16
2	3	2	Per:3 Res:2 Efi:2	12	16
2	3	3	Per:3 Res:2 Efi:3	18	16
2	3	4	Per:3 Res:2 Efi:4	24	16
2	3	5	Per:3 Res:2 Efi:5	30	18
3	3	1	Per:3 Res:3 Efi:1	9	18
3	3	2	Per:3 Res:3 Efi:2	18	18
3	3	3	Per:3 Res:3 Efi:3	27	20
3	3	4	Per:3 Res:3 Efi:4	36	20
3	3	5	Per:3 Res:3 Efi:5	45	20
4	3	1	Per:3 Res:4 Efi:1	12	20
4	3	2	Per:3 Res:4 Efi:2	24	20
4	3	3	Per:3 Res:4 Efi:3	36	20
4	3	4	Per:3 Res:4 Efi:4	48	20
4	3	5	Per:3 Res:4 Efi:5	60	20
5	3	1	Per:3 Res:5 Efi:1	15	20
5	3	2	Per:3 Res:5 Efi:2	30	24
5	3	3	Per:3 Res:5 Efi:3	45	24
5	3	4	Per:3 Res:5 Efi:4	60	24
5	3	5	Per:3 Res:5 Efi:5	75	24
1	4	1	Per:4 Res:1 Efi:1	4	24
1	4	2	Per:4 Res:1 Efi:2	8	24
1	4	3	Per:4 Res:1 Efi:3	12	25
1	4	4	Per:4 Res:1 Efi:4	16	25
1	4	5	Per:4 Res:1 Efi:5	20	25
2	4	1	Per:4 Res:2 Efi:1	8	27
2	4	2	Per:4 Res:2 Efi:2	16	30
2	4	3	Per:4 Res:2 Efi:3	24	30
2	4	4	Per:4 Res:2 Efi:4	32	30
2	4	5	Per:4 Res:2 Efi:5	40	30
3	4	1	Per:4 Res:3 Efi:1	12	30
3	4	2	Per:4 Res:3 Efi:2	24	30
3	4	3	Per:4 Res:3 Efi:3	36	32
3	4	4	Per:4 Res:3 Efi:4	48	32

3		4	5	Per:4 Res:3 Efi:5	60	32
4		4	1	Per:4 Res:4 Efi:1	16	36
4		4	2	Per:4 Res:4 Efi:2	32	36
4		4	3	Per:4 Res:4 Efi:3	48	36
4		4	4	Per:4 Res:4 Efi:4	64	40
4		4	5	Per:4 Res:4 Efi:5	80	40
5		4	1	Per:4 Res:5 Efi:1	20	40
5		4	2	Per:4 Res:5 Efi:2	40	40
5		4	3	Per:4 Res:5 Efi:3	60	40
5		4	4	Per:4 Res:5 Efi:4	80	40
5		4	5	Per:4 Res:5 Efi:5	100	45
1		5	1	Per:5 Res:1 Efi:1	5	45
1		5	2	Per:5 Res:1 Efi:2	10	45
1		5	3	Per:5 Res:1 Efi:3	15	48
1		5	4	Per:5 Res:1 Efi:4	20	48
1		5	5	Per:5 Res:1 Efi:5	25	48
2		5	1	Per:5 Res:2 Efi:1	10	50
2		5	2	Per:5 Res:2 Efi:2	20	50
2		5	3	Per:5 Res:2 Efi:3	30	50
2		5	4	Per:5 Res:2 Efi:4	40	60
2		5	5	Per:5 Res:2 Efi:5	50	60
3		5	1	Per:5 Res:3 Efi:1	15	60
3		5	2	Per:5 Res:3 Efi:2	30	60
3		5	3	Per:5 Res:3 Efi:3	45	60
3		5	4	Per:5 Res:3 Efi:4	60	60
3		5	5	Per:5 Res:3 Efi:5	75	64
4		5	1	Per:5 Res:4 Efi:1	20	75
4		5	2	Per:5 Res:4 Efi:2	40	75
4		5	3	Per:5 Res:4 Efi:3	60	75
4		5	4	Per:5 Res:4 Efi:4	80	80
4		5	5	Per:5 Res:4 Efi:5	100	80
5		5	1	Per:5 Res:5 Efi:1	25	80
5		5	2	Per:5 Res:5 Efi:2	50	100
5		5	3	Per:5 Res:5 Efi:3	75	100
5		5	4	Per:5 Res:5 Efi:4	100	100
5		5	5	Per:5 Res:5 Efi:5	125	125

RIESGO RESIDUAL

IMPACTO / PROBABILIDAD

Riesgo Residual											
Escala				Nivel		Escala				Nivel	
Impacto	Calidad Control Impacto	Riesgo Residual Impacto	Rango Riesgo Residual Impacto	Riesgo Residual Impacto		Probabilidad	Calidad Control Probabilidad	Riesgo Residual Probabilidad	Rango Riesgo Residual Probabilidad	Riesgo Residual Probabilidad	
1	0	1	<=1	1	Insignificante	1	0	1	<=1	1	Muy Bajo
1	1	0	2	2	Menor	1	1	0	2	2	Bajo
1	2	-1	3	3	Moderado	1	2	-1	3	3	Medio
1	3	-2	4	4	Mayor	1	3	-2	4	4	Alto
1	4	-3	5	5	Catastrofico	1	4	-3	5	5	Muy Alto
1	5	-4				1	5	-4			
2	0	2				2	0	2			
2	1	1				2	1	1			
2	2	0				2	2	0			
2	3	-1				2	3	-1			
2	4	-2				2	4	-2			
2	5	-3				2	5	-3			
3	0	3				3	0	3			
3	1	2				3	1	2			
3	2	1				3	2	1			
3	3	0				3	3	0			
3	4	-1				3	4	-1			
3	5	-2				3	5	-2			
4	0	4				4	0	4			
4	1	3				4	1	3			
4	2	2				4	2	2			
4	3	1				4	3	1			
4	4	0				4	4	0			
4	5	-1				4	5	-1			
5	0	5				5	0	5			
5	1	4				5	1	4			
5	2	3				5	2	3			
5	3	2				5	3	2			
5	4	1				5	4	1			
5	5	0				5	5	0			

RIESGO RESIDUAL

Riesgo Residual							
Escala	Escala	Escala Riesgo Residual		Rango Riesgo Residual		Nivel	
Impacto Residual	Probabilidad Residual	Impacto x Probabilidad	Nivel Riesgo Inherente	Mínimo	Máximo	Riesgo Residual	
1	1	Imp:1 Prob:1	1	1	3	1	Bajo
1	2	Imp:1 Prob:2	2				
1	3	Imp:1 Prob:3	3	4	8	2	Medio
1	4	Imp:1 Prob:4	4	9	16	3	Alto
1	5	Imp:1 Prob:5	5	17	25	4	Muy Alto
2	1	Imp:2 Prob:1	2				
2	2	Imp:2 Prob:2	4				
2	3	Imp:2 Prob:3	6				
2	4	Imp:2 Prob:4	8				
2	5	Imp:2 Prob:5	10				
3	1	Imp:3 Prob:1	3				
3	2	Imp:3 Prob:2	6				
3	3	Imp:3 Prob:3	9				
3	4	Imp:3 Prob:4	12				
3	5	Imp:3 Prob:5	15				
4	1	Imp:4 Prob:1	4				
4	2	Imp:4 Prob:2	8				
4	3	Imp:4 Prob:3	12				
4	4	Imp:4 Prob:4	16				
4	5	Imp:4 Prob:5	20				
5	1	Imp:5 Prob:1	5				
5	2	Imp:5 Prob:2	10				
5	3	Imp:5 Prob:3	15				
5	4	Imp:5 Prob:4	20				
5	5	Imp:5 Prob:5	25				

5.1.11 MITIGACIÓN DEL RIESGO

La administración y gestión del riesgo operativo, tendrá un carácter de prioritario puesto que los riesgos o los eventos de riesgo sobre los que se establecerán controles de manera inmediata serán aquellos riesgos identificados como Alto y Extremo, es decir que de materializarse ocasiona un impacto importante en el patrimonio de la entidad.

En cuanto a los niveles de riesgo medio y bajo también serán gestionados, pero su nivel de prioridad será menor en comparación a los riesgos del nivel superior.

Una vez identificados y medidos los riesgos, la institución debe concentrarse en la calidad de la estructura de control interno, así como también en evaluar la eficiencia de los controles existentes. Las actividades de control deben ser ejecutadas a través de la totalidad de la organización por todos los niveles de su estructura y en cada una de las funciones que se realicen.

Las actividades de control comprenden:

- Evaluación del diseño de los procesos elaborados por los responsables de los controles

- Identificación de controles claves.
- Evaluación de controles generales y de aplicación de tecnología de la información.
- Pruebas para comprobar la efectividad de los controles claves.
- Plan de continuidad del negocio, con estrategias y políticas que permiten actuar de forma oportuna ante diversos eventos de riesgo operativo y las fallas o insuficiencias que los ocasionaron.
- Implementación o modificación de límites de riesgo.

Se deberá proceder a la revisión de todos los controles, incluyendo los pasos automatizados o la utilización de herramientas tecnológicas que aseguren el cumplimiento, exactitud y validez de la información.

El tratamiento de los riesgos identificados involucra las posibles respuestas que pueden implementarse; el análisis de dichas opciones, las cuales no necesariamente son mutuamente excluyentes, incluye la posibilidad de:

- **Evitar:** evitar el riesgo decidiendo no iniciar o continuar con la actividad que genera el riesgo.
- **Aceptar o aumentar:** No se toma ninguna acción que afecte la probabilidad de ocurrencia o el impacto. Ocurre en los casos en que se determina que el costo a incurrir en el intento de reducción es superior al generado por el propio riesgo.
- **Mitigar:** La acción se toma para reducir o modificar la probabilidad de ocurrencia, el impacto o ambos; o eliminar la fuente de riesgo. Corresponde generalmente a la toma de decisiones respecto de actividades comerciales. Reducir un riesgo significa llevarlo a límites de tolerancia admitidos en la política fijada por la dirección de la organización.
- **Controlar:** Se acepta la exposición, pero se toman medidas para que no aumente el nivel de riesgo (mantener el nivel de riesgo).
- **Transferirlos:** La acción es utilizada para reducir el impacto transfiriendo una porción del riesgo involucrado.

Se puede considerar estas medidas de tratamiento recomendadas en función del límite de exposición de cada riesgo en particular, diferenciando eventos POTENCIALES y eventos REALES:

Evento de Riesgo		Opción de Tratamiento de Riesgo			
Nivel	Calificación				
Muy Alto	4			Transferir	Mitigar
Alto	3			Transferir	Mitigar
Medio	2	Asumir	Controlar		
Bajo	1	Asumir			

5.1.13 PLANES DE ACCIÓN

Como parte del proceso de tratamiento de riesgo se puede decidir por la estructuración y ejecución de planes de acción que tendrán como objetivo alcanzar los niveles de mitigación de un evento en específico que mantiene un nivel de riesgo alto o crítico.

El Administrador de Riesgos aplicará los planes de acción, en el caso que los eventos de riesgos no se mitiguen y permanezcan como riesgos altos o críticos.

En la matriz de riesgo operativo debe contener lo siguiente:

- **Definición del plan de acción:** se analizarán diferentes opciones del plan de acción a aplicar, para lo cual se seleccionará el plan de acción adecuado en base a los factores como económicos, recursos disponibles, estructura tecnológica y el personal adecuado.
- **Plan de Acción:** Detalle el conjunto de medidas secuenciales a ser implementado para la mitigación del riesgo, constituye el control a ser implementado.
- **Responsable:** Indica la Gerencia responsable de la implementación del plan.
- **Gerencias involucradas:** Detalla las Gerencias que participarán en la implementación del plan.
- **Fecha inicio:** fecha propuesta para dar inicio con la ejecución del plan de acción.
- **Fecha fin:** fecha propuesta para concluir el plan de acción.
- **Porcentaje de cumplimiento:** Indica el porcentaje de avance en la implementación del plan, a la fecha de monitoreo.
- **Responsable de monitoreo:** Detalla el personal que realizó el último monitoreo a la implementación del plan.
- **Fecha de monitoreo:** Registra la última fecha en la que se ha realizado el seguimiento a la implementación del plan.
- **Actividades:** conjunto de tareas a desarrollar dentro de un plan de acción.

- **Recursos y presupuest**o: insumos utilizados para el desarrollo de las actividades del plan de acción. Se considerarán los recursos necesarios en caso de la presencia de contingencias.
- **Indicador**: corresponde a las medidas del desempeño del plan de acción a través del establecimiento de un indicador.
- **Restricciones:** limitaciones que se hicieron presentes durante la ejecución del plan de acción.
- **Avance esperado**: corresponde al seguimiento del plan de acción a través de la determinación de un porcentaje de avance esperado de cumplimiento.

5.1.14 SEGUIMIENTO Y REVISIÓN DEL RIESGO

El Administrador de Riesgos realizará el seguimiento al cumplimiento de los controles, planes de acción, resultados de indicadores y estadísticas de los riesgos registrados, con el fin de garantizar su mitigación, dando prioridad a los que presentan mayor nivel de probabilidad e impacto, maximizando la posibilidad de que se materialicen.

De igual forma, un monitoreo regular tiene como objetivo detectar rápidamente y corregir deficiencias en la administración de Riesgo Operativo; además, de fomentar la identificación temprana de cambios en el perfil de riesgo.

En este punto, el monitoreo corresponde a:

- Realizar el seguimiento al cumplimiento de los planes de acción y controles.
- Evaluar el perfil de riesgo de la organización
- Evaluar mejoras y avances en cuanto a la identificación, medición, control de eventos de riesgo.

El monitoreo consiste en el seguimiento efectivo a los perfiles de riesgo con los siguientes propósitos:

- Asegurar que los controles estén funcionando de forma oportuna y efectiva
- Asegurar que los riesgos residuales se encuentren en los niveles establecidos por la entidad

Así mismo el monitoreo es una parte integral del plan de tratamiento de la administración de riesgos. Los riesgos y la efectividad de las medidas de control necesitan ser monitoreadas para asegurar que no se registren cambios que alteren las prioridades de los riesgos. A tal fin se deben considerar al menos para efectos de análisis:

- Las técnicas de medición adecuadas para el análisis requerido, que permitan identificar los supuestos y parámetros utilizados en dicha medición.
- Las técnicas de evaluación adecuadas para minimizar la posibilidad de pérdidas financieras relacionadas al diseño inapropiado de los procesos críticos
- Las políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.
- Asimismo, corresponderá controlar que no se afecten las probabilidades de ocurrencia y el impacto sobre los resultados, como también los factores que afectan la conveniencia o costos de las distintas opciones de tratamiento. En consecuencia, es necesario repetir regularmente el ciclo de administración de riesgos.

Las medidas de control adoptadas serán monitoreadas de forma trimestral a menos que los resultados ameriten realizar un monitoreo de menor frecuencia.

1.1. CLASIFICACIÓN DEL MONITOREO

ELTHON CEO define los siguientes mecanismos de monitoreo:

- **Auditoría Interna**: Responsable de evaluar la eficiencia y eficacia de los controles implementados, así como de verificar que se cumplan todas y cada una de las etapas y los elementos del proceso de Administración Integral de Riesgos con el fin de determinar deficiencias y sus posibles soluciones. Los resultados deberán ser comunicados a los responsables de los procesos, Administrador de Riesgo Operativo y al Comité de Riesgos.

- **Revisión de los dueños de los procesos**: Los dueños de los procesos son responsables de identificar los eventos de riesgo operativo y validarlo conjuntamente con el Administrador de Riesgo.

- **Análisis y Evaluación de la Unidad de Riesgos:** El análisis y evaluación de riesgo operativo que debe efectuar la unidad incluirá:
    - La medición del perfil de riesgo operativo inherente y residual para cada proceso de la Institución
    - El análisis de la efectividad de los controles existentes.
    - La planificación de la evaluación en los procesos por parte de los dueños de los procesos.
    - La solicitud de acciones preventivas y correctivas hacia temas relacionados con el riesgo operativo.

5.2 REGISTRO E INFORME DEL RIESGO

El informe de riesgo contempla los siguientes aspectos:

- Las diferentes partes interesadas, sus necesidades y requisitos específicos de información: el informe podría ser entregado a las partes interesadas que el Administrador pueda designar, para lo cual se considerará sus necesidades y requisitos específicos en materia de gestión de riesgo.
- El costo, la frecuencia y los tiempos del informe: el informe será elaborado de manera semestral, el tiempo de vigencia del informe se regirá por las diferentes fechas de aprobación por el Administrador; y no se refleja un costo por ejecución del informe debido a que es realizado con recursos propios de ELTHON CEO.
- Método del informe: el informe es generado de manera automática por el Software ELTHON.
- Pertinencia de la información con respecto a los objetivos de la organización y la toma de decisiones: el informe se encuentra construido con la información de procesos, eventos, controles y planes de acción los cuales son relacionados directamente con los objetivos de la organización, cuya información es un recurso de apoyo para la toma de decisiones.

7. VIGENCIA Y ACTUALIZACIÓN DE DOCUMENTACIÓN

El documento tendrá una vigencia inicial de 1 año a partir de la fecha de implementación. La frecuencia de actualización se realizará de forma anual, a menos que surja la necesidad de una revisión o modificación significativa, en cuyo caso se llevará a cabo de manera inmediata. El Administrador de Riesgos será el responsable de las actualizaciones, y cualquier cambio en la documentación deberá ser notificado al Jefe de Gestión de la Calidad y aprobado por el Administrador antes de su implementación.