Empresa de Servicios
Financieros Auxiliares

MANUAL DE RIESGO OPERATIVO

Historial de modificaciones

Fecha	Versión	Descripción de la modificación
04/05/2023	1.0	Documento Original
31/10/2023	2.0	Corrección y ajuste a los cuatro niveles de riesgo. El tipo de información cambia a uso público.
16/02/2024	3.0	- Se actualiza formato control de documentación. - Se incluye cuadro para evidenciar la creación, revisión y aprobación de documentos.
15/08/2025	4.0	– Se da de baja el Anexo 4 Plan para implementación del sistema de gestión de riesgos. – El Anexo 5 Informe de Riesgo Operativo pasa a ser el Anexo 4. – Se incluye la sección Planes de acción. – Actualización integral del manual – Actualización del 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

Las actividades operacionales dentro del desempeño de las organizaciones y las recomendaciones bajo el criterio de mejores prácticas de administración; son aspectos que deben ser considerados al momento de diseñar e implementar un sistema de gestión de riesgo operacional. El mismo que permita mitigar las pérdidas debido a fallas o insuficiencias originadas en personas, procesos, tecnologías de la información y eventos externos.

En términos generales, para la clasificación del riesgo operacional, se consideran siete categorías de riesgo operacional que potencialmente impactan negativamente a cada una de esas líneas (fraude interno, fraude externo, daños en activos físicos, prácticas de los empleados, prácticas del negocio, interrupción del negocio, gestión del proceso).

Hay dos formas de considerar el riesgo legal; así:

1) Cuando el riesgo legal procede de la institución o de sus objetivos; así, por ejemplo, sería el riesgo en el que se encuentra la institución que es sorprendida actuando ilegalmente (no se aseguró de que sus contratos reflejaran de forma adecuada sus objetivos comerciales, se encontró con demandas judiciales, realizó actos ilícitos, etc.). En este caso se puede considerar al riesgo legal como una forma de riesgo operativo porque los controles sobre este tipo de riesgo fueron inadecuados para posibilitar una respuesta a los temas legales, y 2) Cuando el riesgo legal surge debido a que un cambio en la legislación provoca un resultado imprevisto y desagradable. Puede deberse a: alteraciones en la legislación; que una ley difusa se vuelve clara; o que una ley clara es ampliamente ignorada o mal comprendida.

Con la finalidad de gestionar los riesgos operativo y legal, y con el propósito de minimizar la probabilidad de incurrir en pérdidas por este tipo de riesgos, ELTHON CEO identificará, medirá, controlará, mitigará y monitoreará los eventos que podrían ocasionar la materialización del riesgo de acuerdo con su propia percepción y perfil de riesgos.

2. IMPORTANCIA DEL RIESGO OPERATIVO

La Gestión tradicional de riesgos, tanto a nivel nacional cuanto, a nivel internacional, ha relegado el tratamiento de Riesgo Operativo a un plano secundario, no por el hecho de que éste no sea considerado relevante, sino por la heterogeneidad y dificultad para cuantificar y predecir los factores de pérdidas, que abarcan elementos a los cuales no se puede establecer con certeza su ocurrencia y las posibles pérdidas que ellos generarían.

Bajo el marco planteado, el enfoque que pretende la gestión del riesgo operacional es el de minimizar (eliminar) los costos (pérdidas) que asume la Entidad como consecuencia de

factores externos y deficiencias de los sistemas y recursos humanos, a través de la introducción de mecanismos y controles que reduzca la posibilidad de fallas y subjetividad en la ejecución operativa.; para lo cual se podría establecer un esquema de implementación que contempla las siguientes fases:

1. Identificación de los riesgos operacionales más relevantes
2. Jerarquización de los riesgos operacionales (matriz)
3. Determinación de los procedimientos de mitigación y control
4. Generación de las bases de datos de eventos de riesgo operacional
5. Cuantificación de los Riesgos operacionales
6. Determinación de la cobertura patrimonial (dotación de capital)

3. OBJETIVOS

- Establecer una metodología y procedimientos de administración de riesgo operativo, en el cual se incorpore la identificación, medición, priorización, control, monitoreo y comunicación de los riesgos a los cuales se encuentra expuesta la entidad, que permitan asegurar el cumplimiento de las políticas y la consecución de los objetivos institucionales.
- Definir un esquema de administración de los factores de riesgo operativo que son: procesos, personas, tecnología de información y eventos externos.
- Delimitar claramente funciones y responsabilidades en la administración del 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 por cualquier medio, independientemente del medio que se utilice; ya sea impreso, escrito, almacenado electrónicamente, transmitido por correo o por medios electrónicos o presentado en imágenes
- **Administrador del convenio de asociación:** Es la entidad que proporciona el mayor aporte de servicios a los intervinientes del convenio de asociación y que se encarga de la representación y correcta implementación del mismo.
- **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.
- **Autorización de accesos:** Controla el acceso de los usuarios a zonas restringidas; a distintos equipos y servicios después de haber superado el proceso de autenticación.
- **Autenticar:** Proceso, dispositivo o sistema utilizado para la comprobación de credenciales de acceso y la verificación de la identidad de un usuario.
- **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.
- **Base de datos:** Sistema formado por un conjunto de datos almacenados en discos o cualquier otro medio magnético que permite el acceso directo a ellos, estructurados de manera fiable y homogénea, organizados independientemente, accesibles en tiempo real.
- **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 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 fortuito o de fuerza mayor:** Se refieren a aquellos eventos tales como huelgas o paros, actos de vandalismo, terrorismo, manifestaciones o conmoción civil; y, terremotos, incendios, inundaciones u otros similares.
- **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.

- **Información:** Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado y distribuido.
- **Integridad:** Es la garantía de mantener la calidad y exactitud de la información.
- **Información crítica**: Es la considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones.
- **Impacto:** Es la afectación financiera que podría tener la entidad, en el caso de que ocurra un evento de riesgo.
- **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 contingencia:** Es el conjunto de procedimientos alternativos para el funcionamiento normal de los procesos críticos y de aquellos definidos por la entidad que permitan su operatividad, a fin minimizar el impacto operativo y

financiero que pueda ocasionar cualquier evento inesperado específico. El plan de contingencia se ejecuta en el momento que se produce dicho evento.

- **Plan de continuidad:** Es el conjunto de procesos y procedimientos orientados a mantener la operatividad de la entidad ante eventos inesperados.
- **Plan de recuperación de desastres de tecnología de información:** Es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que una entidad pueda comenzar de nuevo sus operaciones ante eventos de caso fortuito o fuerza mayor.
- **Plataforma tecnológica:** Conjunto de equipos, aplicaciones y sistemas interconectados destinados a ofrecer productos y servicios a través del uso de los recursos tecnológicos disponibles, a socios, clientes y/o usuarios.
- **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 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 actual:** 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.
- **Sistema de audio respuesta (IVR):** Es un sistema automatizado de respuesta interactiva, orientado a entregar o recibir información a través del teléfono.
- **Sistemas internos de control integral:** Son el conjunto integrado de políticas, procesos, procedimientos y niveles de control formalmente establecidos y validados periódicamente.
- **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, multimedia, servicios asociados, entre otros.
- **Tiempo de recuperación objetivo (RTO):** Es el período de tiempo transcurrido después de un incidente, para reanudar una actividad o recuperar los recursos antes de que la entidad controlada genere pérdidas significativas.
- **Tiempo real:** Se refiere a las transacciones que se ejecutan de manera inmediata y que sus resultados de ejecución son visualizados en el instante que se realizan.
- **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. CONTEXTO NORMATIVO

5.1. INTERNACIONAL

- Basilea III: Finalización de las reformas poscrisis (actualizado a Dic 2017)
- Disposiciones transitorias de Basilea III, 2017-2027
- Finalización de Basilea III - En pocas palabras (actualizado a Dic 2017)
- ISO 31000:2018 “Sistema de gestión de riesgos”
- Norma ISO 9001:2015 “Sistema de gestión de la calidad”
- Norma ISO 22301: 2019 “Sistema de continuidad del negocio”
- Norma ISO 27001:2022 “Sistema de Gestión de Seguridad de la Información”

Específicamente, en lo que respecta al Riesgo Operativo, el Comité de Basilea frente a la crisis financiera puso de relieve dos importantes limitaciones del actual marco de riesgo operacional. Primero, los requerimientos de capital por riesgo operacional resultaron insuficientes para cubrir las pérdidas por riesgo operacional incurridas por algunos bancos. Segundo, la naturaleza de dichas pérdidas, a raíz de faltas de conducta o de sistemas y controles inadecuados, resaltó la dificultad asociada con el uso de modelos internos para estimar los requerimientos de capital por riesgo operacional.

5.2. NACIONAL

- Codificación de Resoluciones de la Superintendencia de Bancos, CAPÍTULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO:
- NORMA DE CONTROL PARA LA ADMINISTRACIÓN DEL RIESGO OPERATIVO EN LAS ENTIDADES DEL SECTOR FINANCIERO POPULAR Y SOLIDARIO RESOLUCIÓN Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-IGJ-0116

6. ESTRUCTURA, ROLES Y RESPONSABILIDADES PARA EL RIESGO OPERATIVO

Las disposiciones emitidas en el presente manual son de cumplimiento obligatorio para todo el personal involucrado en el proceso de la Administración, gestión y control de los riesgos operativo y legal de ELTHON CEO.

- ELTHON CEO tiene una estructura jerárquica, dinámica en comunicación y acorde a las operaciones que desempeña la organización; de esta manera todo el personal mantiene la responsabilidad de identificar y velar el cumplimiento del proceso de gestión de riesgos.
- Las estructuras de ELTHON CEO tiene los componentes que se describen a continuación:

6.1. ESTRUCTURA ADMINISTRATIVA

6.1.1. ADMINISTRADOR

a. Crear una cultura organizacional con principios y valores de comportamiento ético que priorice la gestión eficaz del riesgo operativo;
b. Alinear los objetivos del sistema de gestión de riesgos a las operaciones de la organización.
c. Aprobar las políticas, estrategias y metodologías
d. Aprobar el manual de gestión de riesgo operativo
e. Conocer los principales riesgos operativos afrontados por la entidad, estableciendo cuando ello sea posible, adecuados niveles de tolerancia.
f. Comunicar la importancia de la implementación y monitoreo del Sistema de Gestión de Riesgos a todos los niveles de la organización.
g. Asignar los líderes de los procesos los cuales serán de igual manera responsables de la gestión de riesgos, su implementación y seguimiento para lograr resultados alineados con los objetivos estratégicos de la organización.

6.1.2. COMITÉ DE RIESGOS, TECNOLOGÍA Y SEGURIDAD

a. Está conformado por el Administrador, el Administrador de Riesgo y el Jefe de TI quienes serán responsables de evaluar y supervisar las actividades estratégicas de carácter tecnológico y actividades relacionadas al sistema de gestión de la seguridad.
b. Evaluar y proponer al Administrador, las políticas, los manuales y metodologías de administración del riesgo operativo para su aprobación;
c. Aprobar los procesos y procedimientos de administración de riesgo operativo;
d. Evaluar la aplicación de manuales y metodologías de gestión de riesgo previo a la aprobación del Administrador;
e. Definir los mecanismos para monitorear y evaluar la exposición a riesgos;

f. Someter a aprobación del Administrador el plan de recuperación de desastres de tecnología de información.
g. Expedir un reglamento en donde se establece el objetivo, funciones y responsabilidades.
h. Mantener una reunión de forma trimestral o cuando la situación lo amerite, dejando evidencia de las decisiones adoptadas haciendo uso del Registro de Asistencia, además mantendrá informado permanentemente a la Alta Dirección.

6.2. ESTRUCTURA DE CONTROL

6.2.1. AUDITOR INTERNO

a. Realizar anualmente un proceso de auditoría independiente al Sistema de Gestión del Riesgo Operativo, con la finalidad de comprobar su adecuado funcionamiento.
b. Verificar el cumplimiento de las responsabilidades en materia de riesgo operativo del gobierno corporativo, alta gerencia, dueños de procesos.
c. Verificación que las medidas de acción para la mitigación de riesgos se hayan implementado.
d. Verificar el cumplimiento de la declaración de apetito de riesgo.
e. Compartir los hallazgos de auditoría que involucren riesgos operativos potenciales o materializados.

6.3. ESTRUCTURA OPERATIVA

6.3.1. ADMINISTRADOR DE RIESGOS

a. Proponer políticas para la gestión del riesgo operativo;
b. Participar en el diseño y permanente actualización del manual de gestión del riesgo operativo;
c. Desarrollar la(s) metodología(s) para la gestión del riesgo operativo;
d. Apoyar y asistir a las demás unidades de la entidad para la aplicación de la(s) metodología(s) de gestión del riesgo operativo integral;
e. Evaluar el riesgo operativo integral, de forma previa al lanzamiento de nuevos productos y ante cambios importantes en el ambiente operativo o informático en base a los informes de las áreas que corresponda;
f. Consolidar y desarrollar reportes e informes sobre la gestión del riesgo operativo y legal por unidades, factores;
g. Identificar las necesidades de capacitación y difusión para una adecuada gestión del riesgo operativo;
h. Elaborar y liderar la ejecución del plan de recuperación de desastres de tecnología de información;

i. Otras necesarias para el desarrollo de la función.

6.3.2. JEFE DE GESTIÓN DE LA CALIDAD

a. Mantener los respaldos de los documentos asociados, y
b. Difundir los cambios y actualizaciones de los documentos junto con el Administrador de Riesgos a todo el personal.

6.3.3. LÍDER DEL PROCESO

a. Mantener vigente y actualizados los procesos a su cargo,
b. Asegurar que los procesos mantengan los controles para mitigar posibles eventos de riesgo.
c. Capacitar y comunicar al personal interno de ELTHON CEO los procesos a su cargo.
d. Realizar las actividades vinculadas para la mitigación de riesgos, por medio de controles y planes de acción.

6.3.4. JEFE DE TECNOLOGÍA DE LA INFORMACIÓN

a. Garantizar que las operaciones de tecnología de la información satisfagan los requerimientos de los Órganos de control que supervisan a las entidades.
b. Implementar y documentar políticas, metodologías y procesos dentro del Macroproceso de Tecnología de la Información, mismas que se encuentran en el Repositorio Documental y que consideran:
    i. Seguridad de la información, con referencia a la documentación normativa de la ISO 27001:2022
    ii. Gestión de incidentes, con referencia al Subproceso de Gestión de Incidentes y la Política de Gestión de Incidentes descrita en la Política de la Seguridad de la Información.
    iii. Respaldo de la información, con referencia el documento interno de Especificaciones Técnicas de los Sistemas de ELTHON.
    iv. Continuidad del negocio, con referencia a la documentación normativa de la ISO 22301: y los Subprocesos de Continuidad del negocio.
    v. Pruebas técnicas y funcionales, con referencia al Subproceso Gestión de Pruebas del Plan de Continuidad del Negocio.

7. ADMINISTRACIÓN DEL RIESGO OPERATIVO

ELTHON CEO adopta un modelo basado en 3 líneas de defensa para la administración del riesgo operativo:

1. **Primera línea de defensa:**
    a. El Jefe de TI en conjunto con el Administrador realizan el diseño y evaluación de sus controles y la implementación de acciones preventivas para hacer frente a deficiencias que podrían presentarse en procesos y tecnología de la información, mientras que el Jefe de Gestión de Calidad en conjunto con el Administrador evalúan e implementan controles para hacer frente a las deficiencias de personas.
2. **Segunda línea de defensa:**
    a. El equipo de TI liderado por el Jefe de TI, tienen la función de monitorear y hacer contraposición de los controles diseñados y evaluados en la primera línea y el monitoreo de la evolución de los riesgos operativos.
3. **Tercera línea de defensa.**
    a. El Jefe de Gestión de la Calidad o su delegado realizará la auditoría interna para verificar la eficacia de los controles implementados para mitigar el riesgo operativo en cada uno de sus factores y generará los informes respectivos que evidencien dicha labor. Asimismo, verificará que se cumplan con los lineamientos establecidos en la normativa.

- El Administrador confirma las prácticas del gobierno y de la administración de riesgos operativos en cada línea de defensa.

8. ETAPAS DE LA GESTIÓN DE RIESGOS

- El Administrador deberá velar por el cumplimiento del proceso de la gestión del riesgo, el cual implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo.
- El proceso de la gestión del riesgo deberá ser una parte integral de la gestión y de la toma de decisiones, por lo que el Administrador deberá integrarlo en la estructura, las operaciones y los procesos de ELTHON CEO. Puede aplicarse a nivel estratégico, operacional o de apoyo.
- Las etapas de la gestión de riesgos que ELTHON CEO aplica son las siguientes:

- **Identificación**: reconocer los riesgos existentes en cada operación, producto, proceso y línea de negocio que desarrolla la organización, para lo cual se identifican y clasifican los eventos adversos según el tipo de riesgo al que corresponden;
- **Medición:** los riesgos deberán ser cuantificados con el objeto de medir el posible impacto económico en los resultados financieros de la organización. Las metodologías y herramientas para medir el riesgo deben estar de conformidad con el tamaño, la naturaleza de sus operaciones y los niveles de riesgo asumidos por la organización;
- **Priorización:** una vez identificados los eventos de nesgas y su impacto, la organización deberá priorizar aquellos en los cuales enfocará sus acciones de control;
- **Control**: es el conjunto de actividades que se realizan con la finalidad de disminuir la probabilidad de ocurrencia de un evento adverso, que pueda originar pérdidas a la organización;
- **Mitigación**: corresponde a la definición de las acciones para reducir el impacto de un evento de riesgo y minimizar las pérdidas;
- **Monitoreo:** consiste en el seguimiento que permite detectar y corregir oportunamente deficiencias y/o incumplimientos en las políticas, procesos y procedimientos para cada uno de los riesgos a los cuales se encuentra expuesta la organización; y,
- **Comunicación:** acción orientada a establecer y desarrollar un plan de comunicación que asegure de forma periódica la distribución de información apropiada, veraz y oportuna, relacionada con la organización y su proceso de administración integral de riesgos. Esta etapa debe coadyuvar a promover un proceso de empoderamiento y mejora continua en la administración integral de riesgos.

9. POLÍTICAS PARA LA GESTIÓN DE RIESGO OPERATIVO

El riesgo operativo se entenderá como la posibilidad de que se ocasionen pérdidas por eventos derivados de fallas o insuficiencias en los factores de: procesos, personas, tecnología de la información y por eventos externos.

9.1. POLÍTICAS GENERALES

- El Administrador nombrará el responsable de la administración de riesgos de ELTHON CEO, para lo cual asumirá el rol de Administrador de Riesgos.
- ELTHON CEO identifica y gestiona los riesgos operativos para proteger los activos e información de las entidades, para lo cual desarrolla e implementa controles y planes de acción para mitigarlos.
- El Administrador de riesgos, determinará la aplicación de los planes de acción, en el caso que los eventos de riesgos no se mitiguen y permanezcan como riesgos altos o críticos.
- El Administrador deberá asegurar que la gestión del riesgo de ELTHON CEO se encuentra integrada en los procesos y servicios suministrados para las entidades, de manera que se considere el marco de referencia, el cual conlleva: integración, diseño, implementación, valoración y mejora.
- El Administrador deberá proveer los recursos necesarios vinculados a la tecnología, procedimientos y conocimiento; así como el apoyo al sistema de gestión de riesgos operativos.
- Para la asignación del personal en la gestión de riesgos se considerará las habilidades, la experiencia, desarrollo profesional, necesidades de formación y las competencias, lo cual se encuentra descrito en el Manual Descriptivo de Cargos.
- La gestión de riesgos de ELHTON CEO se realizará con base a los requerimientos obligatorios estipulados en las normativas vigentes en el país, así como la aplicación del estándar internacional de administración de riesgos.
- El Administrador de riesgos deberá considerar el nivel de impacto y el tipo de riesgo para el proceso de gestión de riesgos, cuyos resultados serán comunicados a la organización y a sus partes interesadas, según aplique.
- ELTHON CEO designara las atribuciones formales para la gestión del riesgo legal y asesoría jurídica a las áreas pertinentes para este fin, estas áreas contarán con el personal capacitado y con la debida experiencia, con relación al tamaño y complejidad de las operaciones de la entidad.

9.2. DECLARATORIA DE LA POLÍTICA DE RIESGOS DE ELTHON CEO

ELTHON CEO dedicado al desarrollo de software de riesgos y gestión gerencial para el sector financiero se compromete a mantener un sistema de gestión de riesgo para identificar,

medir, priorizar y controlar los eventos de riesgos que puedan presentarse, considerando los objetivos organizacionales, normativa y regulaciones de los Organismos de Control a los cuales ELTHON CEO precautela su cumplimiento con base en las responsabilidades aplicables de acuerdo a los servicios de la organización. Para la gestión de riesgos se considera los factores asociados en la operatividad de la organización:

- personas
- procesos
- tecnología de la información
- eventos externos

De la misma forma, se desarrollan estrategias para mitigar los riesgos identificados, asignando recursos necesarios y responsabilidades al personal involucrado en los Planes de Acción que se requieran implementar, precautelando el liderazgo y compromiso de la alta dirección en las actividades principales del negocio y la toma de decisiones.

Finalmente, se realiza un monitoreo constante del desempeño de los indicadores relacionados a la medición del riesgo en la organización y se mantiene una comunicación del desempeño del Sistema de Gestión de Riesgos al personal interno y a las partes interesadas de ELTHON CEO, con la finalidad de fomentar una cultura de gestión de riesgo, y así identificar oportunidades de mejora para garantizar los niveles de calidad de servicio y protección de datos de las entidades que usan los servicios de ELTHON CEO para cumplir sus necesidades del mercado y requerimientos de los Órganos de Control.

9.3. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO OPERATIVO

- La administración del riesgo operacional considera a todos y cada uno de los funcionarios de acuerdo a la estructura organizacional, cuyo objetivo es minimizar el impacto y ocurrencia de los eventos de riesgo, que pueden ocasionar pérdidas en el largo plazo.
- El Comité de Riesgos se encuentra conformado por el Administrador, Administrador de riesgos y el Jefe de TI.
- El Administrador de riesgos levantará los eventos de riesgos mediante la formalización del **Anexo 2: Acta Reunión Riesgo Operativo**
- El Jefe de TI mantiene una base de datos centralizada en la nube, donde se registra, la información sobre los riesgos y eventos de riesgo operativo incluidos los de orden legal, de seguridad de la información y de continuidad del negocio, el efecto cuantitativo de pérdida producida y estimada, así como, la frecuencia y probabilidad, y otra información que las entidades controladas consideren necesaria y oportuna, para que se pueda estimar las pérdidas atribuibles a este tipo de riesgo.

- El Administrador de riesgos deberá considerar lo descrito en los subprocesos de la Macro tecnología de la Información, Plan de Contingencia, Plan de Continuidad, Plan de Recuperación de Desastres Informáticos, el Sistema de Continuidad del Negocio para la gestión del riesgo operativo.

9.4. POLÍTICA DE COMUNICACIÓN Y CONSULTA

- En caso de presentarse un evento de riesgo, ELTHON CEO establece un orden de comunicación descrito en el Plan de Continuidad del Negocio.
- El Administrador con base al impacto de la información durante un evento de riesgo definirá qué comunicar en función a su gestión de riesgos.
- ELTHON CEO comunica a sus partes interesadas aspectos relevantes al sistema de gestión de riesgos en cada una de sus etapas, así como el proceso aplicado a través de la Plataforma Virtual.
- El Especialista de Soporte Funcional dará seguimiento a las entidades con el fin de obtener retroalimentación de los servicios prestados por ELTHON CEO con énfasis en la cultura de riesgos y cumplimiento de objetivos. Esto permite establecer controles internos efectivos y tomar decisiones informadas con base en las expectativas de las partes interesadas.
- Las partes interesadas pueden proporcionar retroalimentación para llevar a cabo mejoras a través de encuestas de satisfacción semestrales, las cuales son un medio de apoyo para la consulta de los sistemas de gestión de riesgos.
- El módulo de riesgo operativo del Software ELTHON debe parametrizar los tipos de eventos y factores, bajo un formato de árbol de decisión, asociados a la matriz de riesgos, de acuerdo al formato exigido por el Organismo de Control, lo que le da permeabilidad y facilidad para realizar los controles y seguimientos pertinentes, que permiten a las entidades identificar, medir, controlar, mitigar y monitorear su exposición a posibles riesgos en el desarrollo de sus operaciones.

9.4.1. POLÍTICA PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE RIESGOS

- La implementación del sistema de gestión de riesgos, se realiza en función a lo descrito en el presente Manual que menciona los plazos y recursos, la identificación de dónde, cuándo, cómo y quién toma decisiones en todos los niveles de la organización la modificación de los procesos de toma de decisiones cuando sea necesario para integrar la gestión del riesgo, y el aseguramiento de que las disposiciones adoptadas para gestionar el riesgo sean claramente comprendidas y puestas en práctica por todo el personal involucrado, en la sección de Estructura, roles y responsabilidades.
- El Administrador de Riesgos deberá considerar lo descrito en el Manual de Sistema de Continuidad del Negocio, Plan de Recuperación de Desastres Informáticos, Plan de Contingencia y Plan de Continuidad del negocio para la gestión del riesgo operativo.

- El Administrador de riesgos será quien capacite y difunda al personal interno la importancia y gestión del riesgo en la organización.

9.4.2. POLÍTICA PARA LA VALORACIÓN DEL SISTEMA DE GESTIÓN DE RIESGOS

- ELTHON CEO realiza la valoración efectiva del sistema de gestión de riesgos con una periodicidad anual de acuerdo con las directrices de la norma ISO 31000, se busca identificar, evaluar y tratar los riesgos de manera cuantificable con el fin de tener una referencia para la toma de decisiones que permitan establecer estrategias para mitigar los riesgos según los indicadores descritos en el **Subproceso de Gestión y Evaluación de riesgos** y la **Matriz de indicadores de desempeño.**
- El Administrador de riesgos gestionará el riesgo operativo para cada uno de sus factores, que son: procesos, personas, tecnología de la información y eventos externos.
- El Jefe de TI en conjunto con el Administrador definirán los requisitos y procedimientos de tecnología de la información que garantice la existencia de un apropiado ambiente de gestión de riesgo tecnológico para el procesamiento, almacenamiento y trasmisión de la información.
- Las actualizaciones y propuestas que realicen los líderes de los procesos deberán ser revisados y aprobados por Administrador en representación del Comité de Riesgos y tecnología; posteriormente serán difundidos y comunicados a todo el personal involucrado haciendo uso de los canales provistos para este fin.
- El Jefe de TI en coordinación con el Administrador definirán el **Plan Estratégico de Tecnología de la Información** que establece las actividades a ejecutar, cronograma, personal responsable y presupuesto.

9.4.3. POLÍTICA PARA LA MEJORA DEL SISTEMA DE GESTIÓN DE RIESGOS

- El Administrador de Riesgos junto con el Jefe de Gestión de la Calidad deberá realizar el seguimiento de los resultados generados en la valoración y de acuerdo al desempeño del sistema de gestión de riesgos se determinará la necesidad de adaptarlo en función a los cambios externos e internos de ELTHON CEO, a través del establecimiento de estrategias o planes de acción que conlleven a la mejora del sistema de riesgos.
- Los líderes de procesos en coordinación con el Jefe de Gestión de la Calidad deberán promover la mejora continua considerando los aspectos vinculados al marco de referencia de la gestión de riesgos, así como los procesos asignados a su cargo; en caso que aplique se deberá desarrollar planes que contribuyan con el fortalecimiento del sistema de gestión de riesgos.

9.5. POLÍTICA PARA EL ESTABLECIMIENTO DE CRITERIOS PARA LA MEDICIÓN DEL RIESGO

- El Administrador de Riesgos deberá precautelar que los criterios para la medición del riesgo sean coherentes con las políticas y declaraciones acerca de la gestión del riesgo, así como también deberá considerar las obligaciones de la organización y punto de vista de las partes interesadas con relación a la gestión de riesgos.
- El Administrador de Riesgos podrá reconsiderar los criterios asignados para la medición del riesgo basándose en los resultados de la revisión continua, lo cual puede incluir una actualización, revisión o modificación de los criterios.

9.5.1. INCERTIDUMBRE

- El Administrador de riesgos deberá considerar la presencia de incertidumbre como parte de la identificación y gestión de los eventos de riesgo.
- ELTHON CEO identifica tres tipos principales de incertidumbre que se toman en cuenta en la gestión de riesgos:

  - ✓ Epistémica: relacionada a la falta de conocimiento que conlleva a la ambigüedad de resultados, y se deduce solo después de conocer la fuente de riesgo.
  - ✓ Aleatoria: se caracteriza por la existencia de un rango de la variabilidad de los resultados. Si se aumenta el conocimiento no se reduce el resultado de la aleatoriedad.
  - ✓ Ontológica: es la incertidumbre que no es conicidad y no puede ser conocida ni estudiada.

9.5.2. PROBABILIDAD/ FRECUENCIA

- El Administrador de riesgos analizará la probabilidad de ocurrencia de los eventos de riesgo para lo cual se asignará los niveles de las categorías de acuerdo a lo descrito en el **Anexo 1 "Metodología Administración de Riesgo Operativo".** Estos niveles son:

  - ✓ Muy bajo
  - ✓ Bajo
  - ✓ Medio
  - ✓ Alto
  - ✓ Muy alto

- Los parámetros de ocurrencia en el tiempo que se medirán los eventos están comprendidos en días, meses y años según la categoría de probabilidad definida.

9.5.3. IMPACTO

- El Administrador de riesgos analizará el nivel de afectación de un evento de riesgo de acuerdo a lo descrito en el **Anexo 1 "Metodología Administración de Riesgo Operativo".** Estos niveles son:

  - Insignificante
  - Menor
  - Moderado
  - Mayor
  - Catastrófico

9.5.4. COHERENCIA EN EL USO DE LAS MEDICIONES

- El Administrador de riesgos deberá velar por la existencia de coherencia en el uso de las mediciones que implica asegurarse de que las categorías utilizadas para clasificar sean consistentes y aplicables.
- El Administrador de riesgos deberá verificar que la probabilidad e impacto mantengan la misma escala de valores, para mantener una coherencia en la determinación de riesgo inherente.

9.5.5. ESCALA DE RIESGO INHERENTE (COMBINACIONES Y SECUENCIAS MÚLTIPLES RIESGOS)

- ELTHON CEO utiliza diferentes combinaciones y secuencias de múltiples riesgos para poder determinar un nivel de riesgo residual, la escala de riesgo se presenta en el **Anexo 1 "Metodología Administración de Riesgo Operativo".**

9.6. POLÍTICAS PARA LA METODOLOGÍA DE GESTIÓN DE RIESGOS

9.6.1. IDENTIFICACIÓN DEL RIESGO

- El Administrador de riesgos deberá realizar la identificación de los riesgos de manera inicial previo a la implementación de la gestión de riesgos en la organización.
- El Administrador de riesgos en conjunto con el líder del proceso identificará los eventos de riesgo tomando como insumo principal el Inventario de procesos, mismo que deberá contener los procesos vigentes y actualizados.
- Para la identificación de los eventos, el Administrador deberá considerar los procesos determinados como críticos, de acuerdo al resultado del Subproceso Valoración de procesos mediante análisis de impacto al negocio BIA.

- El Administrador de riesgos podrá considerar los resultados de los informes de auditorías internas y externas para la identificación de eventos de riesgo.
- El Administrador de riesgos deberá considerar los tipos de eventos de riesgo operativo que se mencionan a continuación:
    - ✓ Fraude interno
    - ✓ Fraude externo
    - ✓ Prácticas laborales y seguridad del ambiente de trabajo;
    - ✓ Prácticas relacionadas con los clientes, los productos y el negocio;
    - ✓ Daños a los activos físicos;
    - ✓ Interrupción del negocio por fallas en la tecnología de la información; y,
    - ✓ Deficiencias en el diseño y/o la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.
- El Administrador de riesgos identifica los riesgos operativos por línea de negocio, tipo de evento, factor de riesgo operativo y las fallas o insuficiencias, utilizando para el efecto el **Anexo 1 "Metodología Administración de Riesgo Operativo".**
- El Administrador de riesgos deberá identificar los eventos de riesgo vinculados a los procesos considerando la línea de negocio y la clasificación de los tipos de procesos:
    - ✓ Gobernantes
    - ✓ Productivos
    - ✓ Habilitante

9.6.2. ANÁLISIS DEL RIESGO

- El Administrador de riesgos deberá analizar los eventos de riesgos identificados considerando los lineamientos descritos en la etapa de identificación de riesgo.
- Para el análisis de los eventos identificados se utilizarán los elementos detallados en la sección de Análisis de la Metodología Administración Riesgo Operativo, con ello se determinará:

    - ✓ Si la identificación de los eventos fue de forma asertiva con relación a,
        - la probabilidad de los eventos y de las consecuencias
        - la naturaleza y la magnitud de las consecuencias
        - la complejidad y la interconexión
        - los factores relacionados con el tiempo y la volatilidad
        - la eficacia de los controles existentes
        - los niveles de sensibilidad y de confianza
    - ✓ Para aplicar un proceso de mejora en la gestión de los eventos identificados.

- El Administrador de riesgos comunicará al Administrador la presencia de anomalías que pudieran generarse en el proceso de análisis de los riesgos identificados a través del **Anexo 2 Acta de Reunión de Riesgo Operativo.**

9.6.3. VALORACIÓN DEL RIESGO

- El Administrador de riesgos deberá realizar la valoración de los riesgos para comparar los resultados del análisis del riesgo que será de apoyo para la toma de decisiones y la ejecución de una acción adicional cuando es requerida.
- El Administrador de riesgos valorará los riesgos de acuerdo a los siguientes componentes:
  - ✓ línea de negocio,
  - ✓ tipo de proceso,
  - ✓ factor de riesgo operativo
  - ✓ tipo de evento
  - ✓ fallas o insuficiencias.
- El Administrador de riesgos determinará el nivel de riesgo inherente a través de lo descrito en el **Anexo 3 "Metodología Administración de Riesgo Operativo".** El cual consiste en multiplicar el IMPACTO y PROBABILIDAD para obtener el RIESGO INHERENTE mismo que se visualizará en cuatro niveles BAJO, MEDIO, ALTO y MUY ALTO, tal como se visualiza en la siguiente imagen.

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

- El Administrador de riesgos podrá considerar factores adicionales como las consecuencias percibidas por las partes interesadas para ajustar la valoración de los eventos de riesgo.
- El Administrador de riesgos deberá comunicar los resultados de valoración al Administrador con una periodicidad trimestral, a través del **Anexo 2 Acta de Reunión de Riesgo Operativo.**

–

9.6.4. POLÍTICAS DE GESTIÓN POR PERSONAS

- El Jefe de Gestión de la Calidad en conjunto con el Administrador o su delegado definirán políticas y lineamientos para la incorporación, permanencia y desvinculación del personal con el fin de asegurar la planificación y administración del capital humano en la gestión del riesgo operativo. Para lo cual hacen uso de:

  - ✓ Manual de Talento Humano
  - ✓ Subproceso de incorporación del personal
  - ✓ Subproceso capacitación, competencia y concienciación del personal
  - ✓ Subproceso Evaluación al desempeño de trabajadores
  - ✓ Subproceso de desvinculación del personal
  - ✓ Manual descriptivo de cargos
  - ✓ Contrato de trabajo
  - ✓ Acuerdo de confidencialidad

9.6.5. POLÍTICAS DE GESTIÓN POR PROCESOS

- El Jefe de Gestión de la Calidad en conjunto con el Administrador definirá la estructura documental de ELTHON CEO, con la finalidad de estandarizar y estructurar los documentos y registros de la empresa descrita en el **Manual de Gestión por Procesos.**
- El Jefe de gestión de la Calidad establece la **Metodología de Gestión por procesos** para el diseño, control, actualización, seguimiento y medición de los procesos.
- El Jefe de Gestión de la Calidad en conjunto con el Administrador revisarán y determinarán para cada proceso:
  - ✓ las actividades a realizarse de forma ordenada
  - ✓ sus líderes y responsables manteniendo la separación de funciones que evite concentraciones de carácter incompatible.
  - ✓ indicadores que permitan medir la efectividad de los procesos.
- El líder del proceso o su delegado deberá difundir y comunicar el mismo entre los responsables correspondientes buscando garantizar su correcta aplicación, para lo cual hará uso del Registro de Capacitación.
- El Líder del Proceso realizará propuestas de mejora, y en coordinación con el Jefe de Gestión de la Calidad, se gestionarán aquellas que se consideren viables; con el fin de promover una cultura de mejora continua y eficiencia organizacional.
- El Jefe de Gestión de la Calidad deberá mantener actualizado el inventario de los procesos existentes para lo cual hará uso del **Inventario de Procesos.**

9.6.6. POLÍTICAS DE FACTOR TECNOLOGÍA DE LA INFORMACIÓN

- El Administrador en conjunto con el Jefe de TI definirán el área de tecnología de la información en función del tamaño y complejidad de las operaciones. Conformado por el Comité de Riesgos, Tecnología y Seguridad, el Jefe de TI, el Arquitecto de TI y los desarrolladores.
- El Jefe de TI en conjunto con el Administrador elaborarán el Plan Estratégico de Tecnología y el Plan Operativo Anual para garantizar que la administración de la tecnología de la información soporte los requerimientos de operación actuales y futuros de la entidad.
- El Jefe de TI en conjunto con el Administrador establecerán controles y planes de acción para una correcta administración del riesgo operativo que permitan minimizar la ocurrencia de posibles eventos de riesgo y su impacto.
- ELTHON CEO no depende de empresas externas de software, todo es propietario y desarrollado por la organización.
- Los líderes de los procesos deberán seguir lo descrito en el Manual Gestión de Cambios con el fin de asegurar que los cambios a los aplicativos e infraestructura que soportan las operaciones estén debidamente autorizados, documentados, probados, y aprobados por el propietario de la información.
- Con el objeto de garantizar que las operaciones de tecnología de la información satisfagan los requerimientos de las entidades financieras, el Jefe de TI en conjunto con el Jefe de Gestión de la Calidad implementa el **Manual de Tecnología de la Información** y los **Subprocesos de Tecnología de la Información**.

9.7. TRATAMIENTO DEL RIESGO

- El Administrador de riesgos deberá implementar mecanismos de prevención, control o mitigación del riesgo según el nivel del riesgo.
- El Administrador de riesgos deberá priorizar la aplicación de controles en función del nivel de impacto del evento durante la gestión de riesgo. A los eventos identificados como alto y muy alto se aplicarán controles o planes de acción de manera inmediata de acuerdo a lo descrito en el **Anexo 1 Metodología Administración Riesgo Operativo.**
- El Administrador evaluará la eficiencia de los controles aplicados de manera que estos cumplan con su función de mitigación del evento de riesgo.
- ELTHON CEO podrá considerar los valores, las percepciones, el involucrar potencialmente a las partes interesadas para efectuar el tratamiento de riesgos, estos aspectos se podrán recabar mediante canales virtuales directamente con cada parte interesada.
- La definición de los planes de acción deberá realizarse junto al Administrador de Riesgos y líder del Proceso.

- El Administrador de riesgos en conjunto con el líder del proceso deberá realizar un seguimiento permanente de la implementación de los controles o planes de acción ejecutados para así evitar consecuencias no previstas.
- El Administrador de riesgos deberá registrar y mantener una continua revisión a los eventos que persisten en un nivel de riesgo no aceptable, para lo cual será comunicado de manera inmediata al Administrador para la toma de decisiones.
- Los riesgos residuales se podrán visualizar y controlar a través de la matriz de eventos de ELTHON CEO.
- En caso de retrasos en el cumplimiento de planes de tratamiento, el Administrador de Riesgos en conjunto con el Líder del Proceso deberán analizar las causas que generaron dichos desfases.

9.8. SEGUIMIENTO Y CONTROL

- El Administrador de riesgos realizará un continuo seguimiento y evaluación de los niveles de exposición al riesgo, conforme a cada uno de los procesos críticos con el fin de controlar los posibles factores y sus incidencias en la entidad.
- El Administrador de riesgos en conjunto con el Administrador decidirá qué riesgos asumirá, compartirá, mitigará o transferirá.
- Es responsabilidad del Administrador de Riesgos realizar el seguimiento de los eventos de riesgo, en especial a los catalogados como no aceptables, a través de los planes de acción implementados; con el fin de mitigar o evitar una pérdida económica para la entidad.
- El Administrador de riesgos deberá revisar el seguimiento y control de los eventos considerando los diferentes mecanismos que puedan aplicar, los cuales se encuentran detallados en el **Anexo 1 "Metodología Administración Riesgo Operativo".**

9.9. REGISTRO E INFORME DE RIESGOS

- Los resultados del seguimiento y revisión se deberán comunicar por el Administrador de Riesgos trimestralmente al Administrador a través del **Anexo 2 Acta de Reunión Riesgo Operativo**, para que los controles sean mejorados por los líderes de los procesos en caso de existir cambios en los riesgos y que proporcionen información para la toma de decisiones. En caso de aplicar la comunicación se extenderá entre el personal de ELTHON CEO y las partes interesadas a través de reuniones virtuales.
- El Administrador de riesgos presentará informes trimestrales de gestión de los eventos de riesgo en sesiones del Comité de Riesgos con el fin de que se tomen decisiones para su gestión, siempre y cuando el Administrador lo autorice.
- El informe trimestral presentado por el administrador de riesgos deberá incluir los niveles de exposición al riesgo operativo, la evolución de los riesgos reflejados en sus

respectivos indicadores clave de riesgos; la eficiencia y eficacia de las políticas, procesos, procedimientos y metodologías aplicadas; el grado de cumplimiento de los planes de mitigación; y, conclusiones y recomendaciones;

- El informe a utilizar como mecanismo para la comunicación de los resultados de la gestión de eventos de riesgo será a través de:

  - ✓ **Anexo 3: Matriz de Eventos de Riesgos,** mismo que podrá ser obtenido por el software utilizado para la administración del riesgo (Software ELTHON).
  - ✓ **Matriz de indicadores clave de desempeño** que permitan evaluar la eficiencia y eficacia de las políticas, procesos, procedimientos y metodologías aplicadas.
  - ✓ Mapa de calor de los eventos de riesgo operativo.
- La comunicación interna a todos los funcionarios de ELTHON CEO sobre la gestión del riesgo operacional, se ejecutará a través de canales virtuales.
- El Administrador de riesgos mantendrá las bases de datos centralizadas que registren, ordenen, clasifiquen y dispongan de información sobre los riesgos y eventos de riesgo operativo, incluyendo los de orden legal, seguridad de la información y continuidad del negocio. Esto incluye la cuantificación de pérdidas producidas y estimadas, la frecuencia y probabilidad, así como cualquier otra información relevante que las entidades consideren necesaria. La responsabilidad de administrar esta base de datos recae en la unidad de riesgo operativo.

9.10. POLÍTICA PARA SERVICIOS PROVISTOS POR TERCEROS

- El Jefe de TI en conjunto con el Administrador seguirán lo descrito en el **Manual para la Gestión de Proveedores** y **los Acuerdos de Nivel de Servicio** con el fin de mantener el control de los servicios provistos por terceros.
- El Jefe de TI deberá gestionar el servidor físico como proveedor alterno de los servicios.
- El Jefe de TI deberá implementar los centros de procesamiento de datos principal y/o alterno siguiendo el estándar TIA-942 o superior y contar como mínimo con la certificación TIER III o su equivalente para diseño, implementación y operación y así garantizar la disponibilidad de los servicios brindados.
- El Jefe de TI deberá confirmar que el proveedor de servicios en la nube cuente con la certificación ISO 27001 en seguridad de la información, así como, la implementación de los controles establecidos en los estándares ISO 27017 (controles de seguridad para servicios en la nube), ISO 27018 (protección de información personal en la nube) y/o aquella que aplique conforme el servicio ofertado.

9.11. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

- El Comité de Tecnología y Seguridad de la Información estará conformado por el Administrador, el Administrador de Riesgo y el Jefe de TI quienes serán responsables de evaluar y supervisar las actividades estratégicas de carácter tecnológico y actividades relacionadas al sistema de gestión de la seguridad
- El Jefe de TI en conjunto con el Administrador definirán y documentarán las Políticas de Seguridad de la Información que satisfaga las necesidades de la entidad y salvaguarde la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas.
- El Jefe de TI es el oficial de seguridad de la información, quien es el responsable del área de seguridad de la información.
- El Jefe de TI en conjunto con el Administrador mejorarán continuamente el Sistema de Gestión de la Seguridad realizando actualizaciones cuando sea necesario en cuanto a su alcance, política, inventario de activos, propietarios de los activos, metodología de gestión de riesgos, pruebas y monitoreo.
- El Administrador, gestionará la ejecución de auditorías externas al menos una vez al año, con el fin de identificar opciones de mejora y mitigar los riesgos que podrían afectar a la preservación de la confidencialidad, integridad y disponibilidad de la información, y seguirán los descrito en el **Manual de Auditoría Interna.**
- El Jefe de TI establecerá un apropiado ambiente de gestión de la seguridad de la información, tomando en cuenta:
    - Inventario y clasificación de activos de la información
    - Subproceso de uso aceptable de activos de la información.
    - Subproceso de eliminación de la base de datos
    - Subproceso para el control de accesos a la información
    - Subproceso para la gestión de perfil y usuarios.
    - Subproceso Gestión de Incidentes de SI
    - Subproceso Mantenimientos del Sistema de Información
    - Manual de Gestión de manejo de contraseñas
    - Resultado de escañero de vulnerabilidades por SonarQube
    - Política de Clasificación de la Información
    - Especificaciones técnicas seguridad APL (Nivel de protección de aplicación)
- El Jefe de TI será el responsable de activos de la información donde se incluye la designación de los propietarios de activos.
- El Jefe de TI en conjunto con el Administrador establecerá una **Metodología de gestión de riesgos de seguridad de la información.**
- El Jefe de Gestión de la Calidad controlará que la información permanezca documentada para verificar el cumplimiento.
- El Auditor Interno realizará una evaluación del desempeño del sistema de gestión de la seguridad de la información. El resultado de estas evaluaciones, así como las acciones de mejora deben ser conocidas y aprobadas por el comité de riesgos, tecnología y seguridad.

- El Administrador o su delegado, en conjunto con el Jefe de Gestión de la Calidad definirán políticas y procesos para la incorporación, permanencia y desvinculación del personal al servicio de la organización, soportados técnicamente y ajustados a las disposiciones legales, de manera que, aseguren la planificación y administración del capital humano, toma como referencia el **Manual de Talento Humano y los Subprocesos vinculados al Proceso de Administración del personal.**
- El Administrador en conjunto con el Jefe de TI implementarán y documentarán políticas y procedimientos para mejorar el Sistema de Continuidad del Negocio para garantizar su capacidad de operar de forma continua y limitar las pérdidas en caso de una interrupción grave, tomando como referencia el Manual de Gestión de Continuidad del Negocio, el Plan de Continuidad, el Plan de Contingencia y el Plan de Recuperación de Desastres informáticos.
- El Administrador en conjunto con el Administrador de Riesgos establecerán en el Plan de Continuidad de Negocio el Análisis de impacto en el negocio (BIA) para el proceso crítico de Tecnología de la Información, así como las estrategias de continuidad y los tiempos de recuperación.
- El Jefe de TI seguirá lo descrito en el Subproceso de Pruebas de Plan de Continuidad del Negocio que permitirán comprobar su efectividad y realizar los ajustes necesarios, cuando existan cambios que afecten la aplicabilidad del Plan de Continuidad, al menos, una vez al año; las pruebas incluirán el alcance y el detalle de los aspectos a probar, así como las conclusiones y recomendaciones obtenidas como resultado de su ejecución.
- El Administrador de riesgos gestionará el riesgo legal y minimizará la probabilidad de incurrir en pérdidas por este tipo de riesgo, para lo cual identificará, medirá, controlará, mitigará y monitoreará los eventos que podrían ocasionar la materialización del riesgo legal de acuerdo con su propia percepción y perfil de riesgos.
- ELTHON no es una entidad transaccional por lo cual no es necesario definir lineamientos para la seguridad de canales electrónicos.
- Las áreas designadas en ELTHON CEO deberán generar planes y programas que permitan dar cumplimiento a las disposiciones emanadas en la Ley Orgánica de Protección de Datos Personales.

9.12. LÍMITES DE EXPOSICIÓN AL RIESGO

- Se deberá fijar los límites de exposición al riesgo, de manera individual y específica. La misma será de conocimiento y aprobación por parte del Administrador y será revisada al menos una vez al año.
- Las categorías de riesgo, bajo y medio son considerados como niveles de riesgo aceptables; por el contrario, las categorías de riesgo alto y muy alto se consideran como niveles de riesgo no aceptables.

VALOR (RI-C)	NIVEL RIESGO RESIDUAL	
4	Extremo	INACEPTABLE
3	Alto	
2	Moderado	
1 - 0	Bajo	ACEPTABLE

9.13. PLANES DE ACCIÓN

- El Administrador de riesgos aplicarán los planes de acción, en el caso que los eventos de riesgos no se mitiguen y permanezcan como riesgos altos o críticos según lo descrito en el **Anexo 1 Metodología para la Administración de Riesgo Operativo.**

9.14. SISTEMAS DE INFORMACIÓN

- El Administrador realizará la gestión de riesgos de ELTHON CEO utilizando el Software ELTHON, el cual es una herramienta que permite consolidar de manera estructurada toda la información.

10. PÉRDIDA ESPERADA E INESPERADA PARA RIESGO OPERATIVO Y LEGAL

10.1. MÉTODO DE DISTRIBUCIÓN DE PÉRDIDAS (LDA)

Los orígenes del LDA se ubican en las aplicaciones actuariales, siendo el principal objetivo proporcionar una estimación de pérdida, tanto por la línea de negocio como por evento, dicha distribución de pérdida se origina por los eventos de riesgo (frecuencia y severidad).

El modelo LDA proporciona estimaciones para la pérdida agregada; una vez que se cuenta con ese valor, se pasa a calcular la pérdida total.

- (Pérdida total). La pérdida total es la suma aleatoria de las distintas pérdidas.

$$L = \sum_{i=1}^{I} \sum_{j=1}^{J} S_{ij},$$

donde Sij es la pérdida total en la celda i, j de la matriz de pérdidas, I representa el número de eventos considerados, y J el número de líneas de negocio de la entidad. Las Sij se calculan como:

$$S_{ij} = \sum_{N=1}^{n} X_{N_{ij}},$$

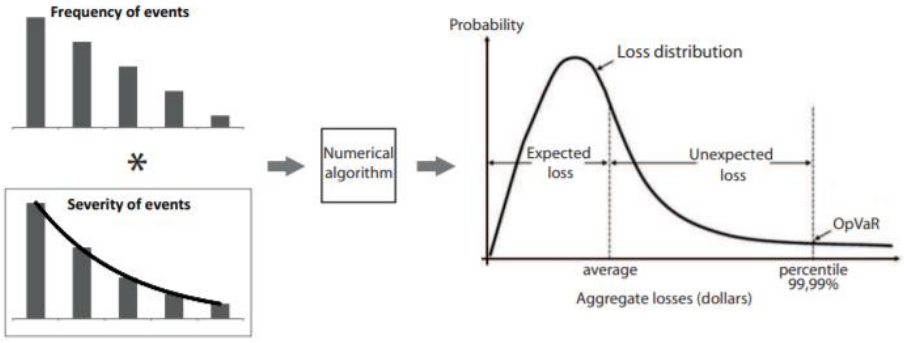
donde, Nij es la variable aleatoria que representa el número de eventos de riesgo en la celda i, j (frecuencia de los eventos) y XN es el monto de la pérdida en la celda i, j (severidad del evento).

En consecuencia, las pérdidas son resultado de por lo menos dos diferentes fuentes de aleatoriedad, la frecuencia y la severidad. Estas estimaciones surgen de combinar, mediante convolución, un proceso estocástico discreto (frecuencia) y un proceso estocástico continuo (severidad). En primer lugar se estima la distribución de frecuencias; luego, la severidad. El siguiente paso es obtener la distribución de las pérdidas totales de riesgo operacional. Para el círculo de capital regulatorio se aplica el concepto de Valor en Riesgo (VaR por sus siglas en inglés) en el contexto del riesgo operativo, se denomina Valor en Riesgo Operacional (OpVar por sus siglas en inglés).

- (Valor en Riesgo Operacional, OpVar). Este representa un percentil de la distribución de probabilidad de pérdidas por lo que es, ante todo, una medición de tipo estadístico.

$$Pr\{L > OpVar\} = p, \; donde \; p = percentil.$$

Un esquema de esta técnica se puede ver en la siguiente figura:



La distribución de frecuencia y severidad se obtienen de la información que se usa para realizar el análisis.

Las dos distribuciones (frecuencia y severidad) se combinan para obtener la distribución de pérdidas agregadas.

El OpVar se obtiene tomando el percentil de la distribución de pérdida agregada en el nivel de confianza deseado.

El OpVar se puede interpretar como una cifra, expresada en unidades monetarias, que nos informan sobre la mínima pérdida potencial en la que podría incurrir una determinada línea de negocio, por tipología de riesgo operacional, dentro de un horizonte temporal de un año y con un nivel de confianza estadístico del 99,9 %.

- La pérdida esperada es la pérdida media que es factible y probable que ocurra en un período determinado. Es decir, las pérdidas esperadas recogerán todas aquellas mermas, previsibles y habituales, intrínsecas a la actividad ordinaria de la entidad.
- La pérdida inesperada consiste en la diferencia entre el OpVaR y la pérdida esperada, es decir, es el monto de capital que la institución debería tener para cubrir las pérdidas no esperadas a sucesos no previstos inicialmente por la entidad que, sin embargo, pueden desencadenar situaciones funestas para la institución dada la magnitud del quebranto, de acuerdo al nivel de confianza deseado. La distribución de las pérdidas agregadas es resultado de una composición entre la variable aleatoria discreta asociada a la frecuencia y la variable aleatoria continua asociada a la severidad de los eventos de riesgo.
- (Distribución de pérdida Agregada). Esta distribución constituye la media ponderada de la n-ésima convolución de la severidad, donde los pesos son las probabilidades de masa de las frecuencias. La n-ésima convolución de la severidad es la probabilidad de ocurrencia del agregado de n pérdidas individuales. Si las pérdidas agregadas para una celda específica están dadas por:

$$S = X_1 + X_2 + \cdots + X_N = \sum_{i=1}^{N} X_i,$$

donde, N es la variable aleatoria de conteo del evento, y Xi es la variable aleatoria de severidad por ocurrencia del evento, donde todas las Xi se asumen independientes y con función de distribución idéntica dada por:

$$F_X(x) = P(X \leq x),$$

entonces, la n-ésima convolución de la distribución de severidad, denotada por $F*n$ X (x), está dada por:

$$P(X_1 + X_2 + \cdots + X_n \leq x) = F * F * \cdots * F = F_X^{*n}(x),$$

por tanto, la función de distribución de las pérdidas agregadas está dada por:

$$G_s(x) = P(S \leq x) = \sum_{n=0}^{\infty} P(N = n) F_X^{*n}(x).$$

El modelo LDA considera los siguientes supuestos dentro de cada clase de riesgo:

a) La variable frecuencia es una variable aleatoria independiente de la variable aleatoria severidad;
b) Las observaciones de tamaño de pérdidas dentro de una misma clase son homogéneas, independientes e idénticamente distribuidas.
La suposición a) admite que la frecuencia y la severidad son dos fuentes aleatorias e independientes. La suposición b) significa que dos diferentes pérdidas dentro de la misma clase son homogéneas, independientes e idénticamente distribuidas.

En general, resulta muy complejo obtener una solución analítica de la igualdad, motivo por lo cual se utilizan métodos numéricos como: simulación Monte Carlo y/o el enfoque recursivo de Panjer. De igual manera, se pueden utilizar métodos analíticos aproximados como la transformada rápida de Fourier, entre otros. Se calculará la distribución de pérdidas agregadas con la simulación Monte Carlo. Este enfoque estima dicha distribución utilizando un número suficiente de escenarios hipotéticos a partir de las distribuciones de severidad y frecuencia, generados aleatoriamente.

- Distribuciones de frecuencia y de severidad. La variable aleatoria frecuencia representa el número de eventos que producen pérdidas en un determinado intervalo de tiempo, y que sigue una distribución de probabilidad de referencia. Se recomienda considerar otras alternativas, tales como la distribución Binomial Negativa, Binomial, Geométrica e Hipergeométrica. La variable aleatoria severidad representa el impacto del evento en términos de pérdidas económicas y que sigue una distribución de probabilidad de referencia. Se recomienda considerar otras alternativas como la distribución Weibull, Pareto y Exponencial.

10.2. REPORTES Y ESTRUCTURAS NORMATIVAS

De acuerdo a la Resolución referente a la Norma de control para la administración del riesgo operativo bajo el control de la Superintendencia de Bancos no establece la remisión de estructuras o reportes normativos.

10.3. POLÍTICA DE INCUMPLIMIENTO

A toda falta u omisión contempladas en la Ley, Código de Ética, Normativa interna y demás normas que regulen el riesgo operacional, incluyendo circulares y resoluciones emitidas por

los Organismos de Control, así como las disposiciones emitidas en este manual, se procederá según la ley.

11. VIGENCIA Y ACTUALIZACIÓN DE DOCUMENTACIÓN

El Manual 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.

12. ANEXOS

Anexo 1	Metodología para la Administración de Riesgo Operativo-Matriz de Riesgo
Anexo 2	Acta Reunión Riesgo Operativo
Anexo 3	Matriz de Eventos de Riesgos
Anexo 4	Informe de riesgo operativo