DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

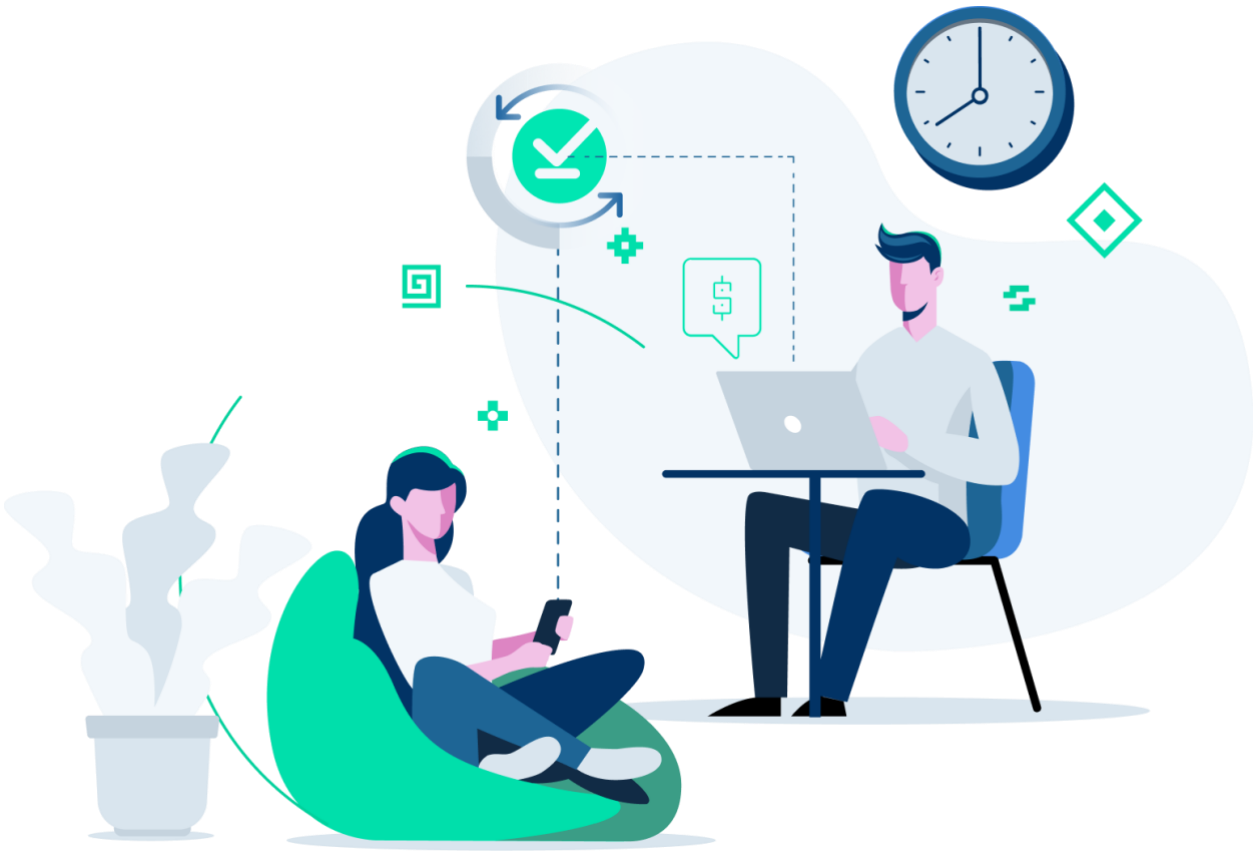
MANUAL DE PREVENCIÓN DE LAVADO DE ACTIVOS

Manual

GGC-MA-0101-KU

Versión 7

Julio 2023



Fecha	Elaborado por	Revisado por		Aprobado por	Firma del aprobador
26/07/2023	Director de Cumplimiento Liliana Carvajal	Chief Governance & Compliance Officer Eduardo Cantón	DS EC	Presidente Ejecutivo Sebastián Castro	DocuSigned by: 138A4B5AC97F4F7...
	Oficial de Cumplimiento Fabián Durán			Chief Executive Officer Aron Schwarzkopf	DocuSigned by: Aron Schwarzkopf 0BC028A8CBC7426...
	Director de Gobierno Corporativo Marisol Vera				

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

CONTENIDO

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

Figuras

Tablas

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

1 INTRODUCCIÓN

Como respuesta a la creciente preocupación de la comunidad global por el problema del lavado de activos y financiación de actividades terroristas en adelante lavado de activos y financiamiento de delitos, como el terrorismo, la Alta Gerencia de Kushki está comprometida con la responsabilidad que tiene frente a estos cumplimientos, de esta manera ha adoptado el presente documento que reúne las políticas y procesos encaminados a fin de prevenir y mitigar las consecuencias que pueden ocasionar estas conductas delictivas a la compañía.

2 MARCO NORMATIVO

Kushki y todas sus subsidiarias (en adelante, la “Compañía”, “Kushki” o la “Sociedad”) ha basado su sistema de prevención de lavado de activos, financiamiento del terrorismo y la proliferación de armas de destrucción masiva en la buenas prácticas internacionales, como las recomendaciones del Grupo de Acción Financiera Internacional (GAFI), las diferentes UIF y las normas locales según la regulación de cada país donde opera Kushki.

El presente manual contiene los lineamiento corporativos que apliquen a Kushki en sus diferentes países de operación o de apertura. Asimismo, en el capítulo 17 Documentos relacionados se listan los documentos que complementan el marco legal de cada país.

3 ALCANCE

El presente manual contiene los procedimientos, lineamientos y medidas de prevención del Lavado de Activos (LA), Financiamiento del Terrorismo (FT), Proliferación de Armas de Destrucción Masiva (PADM) y los delitos precedentes de estos. El alcance del actual documento es para todos los productos y servicios que ofrece la Compañía y todas sus subsidiarias, aplicable a clientes, accionistas, proveedores y colaboradores, así como para las personas naturales y jurídicas con quienes la compañía mantiene relaciones contractuales.

4 DEFINICIONES

Actividades de alto riesgo: son aquellas actividades que por sus características particulares representan un mayor riesgo para las entidades controladas de ser utilizadas en el cometimiento de los delitos de lavado de activos y financiamiento de delitos, como el terrorismo.

Administración del riesgo de lavado de activos y del financiamiento de delitos, como el terrorismo (PLA): es el conjunto de acciones adoptadas por la entidad, con el fin de disminuir la probabilidad de materializar un riesgo y/o su impacto. Las medidas de tratamiento establecidas para el programa de la administración del riesgo de lavado de activos y de la financiación del terrorismo consisten en mitigar y prevenir el riesgo de lavado de activos y financiación del terrorismo.

Alta Gerencia: es el nivel jerárquico dentro de la organización que cuenta con autonomía para tomar decisiones. La integran los representantes legales, presidentes y vicepresidentes ejecutivos, gerentes generales, vicepresidentes o gerentes departamentales y otros profesionales responsables de ejecutar las decisiones del Directorio u organismo que haga sus

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

veces, de acuerdo con las funciones asignadas y la estructura organizacional definida en cada institución.

Bancos pantalla: es aquel que no tiene una presencia física en el país en el que está constituido y recibe una licencia de operación, y no es parte de un grupo financiero regulado que esté sujeto a una supervisión de forma permanente por alguna autoridad regulatoria. Se entiende por "presencia física" cuando dentro de un país existe una estructura gerencial y de personal que permita la operación ordinaria del banco. La existencia simplemente de un agente local o personal de bajo nivel no constituye una presencia física.

Beneficiario final: se refiere a las personas naturales que poseen o controlan un cliente y/o persona natural en cuyo nombre se realiza la transacción o se beneficia de ella, directa o indirectamente. También incluye a las personas que ejercen el control efectivo final sobre una persona jurídica o acuerdo legal.

Canales de distribución: medios por los cuales se brinda productos y servicios financieros como los siguientes: oficinas, cajeros automáticos (ATM), terminal de puntos de venta (POS), sistemas de audio respuesta (IVR), centro de atención telefónica (call center, contact center), corresponsales no bancarios, sistemas de acceso remoto para clientes (RAS), Internet, Banca Móvil, entre otros.

Cliente: toda persona natural o jurídica con que la procesadora de pagos establece o mantiene una relación contractual, a fin de obtener la prestación de un servicio, ofrecido dentro del marco propio del giro o complementario a éste, conforme al marco legal y/o reglamentario, pudiendo ser dicha prestación de servicios de carácter ocasional, esporádico, único, reiterado, frecuente o permanente.

Cohecho: el delito de cohecho es la conducta activa o pasiva ejecutada por un empleado público, cuya finalidad es recibir una retribución no debida en el ejercicio de su cargo, para sí o para un tercero.

Colaboradores cercanos: incluye a aquellas personas que se benefician del hecho de ser cercanos a la persona políticamente expuesta, tales como, sus colaboradores de trabajo, asesores, consultores y socios personales.

Corresponsal: entidad financiera nacional o del exterior con la cual se mantiene relaciones comerciales o bancarias, previa firma de un convenio.

Comercio activo: es aquel establecimiento de comercio que transa independiente de la frecuencia y monto.

Comercio inactivo: es aquel establecimiento de comercio que durante tres meses consecutivos no realiza transacciones.

Contraparte: es cualquier persona natural o jurídica con la que la Empresa tenga vínculos comerciales, de negocios, contractuales o jurídicos de cualquier orden. Entre otros, son contrapartes los asociados, empleados, clientes, contratistas y proveedores de Productos de la Empresa.

Debida diligencia intensificada: es el conjunto de políticas, procesos y procedimientos más exigentes y razonablemente diseñados, aplicados a clientes internos y externos, que en función

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

de su mayor exposición al riesgo y de los casos descritos en la normativa, aplica la entidad para mitigar el riesgo de lavado de activos y financiamiento de delitos, como el terrorismo.

Debida diligencia simplificada: es el conjunto de políticas, procesos y procedimientos menos exigentes, que faculta a la entidad controlada a aplicar cuando ha identificado un bajo riesgo de exposición al delito de lavado de activos y financiamiento de delitos, como el terrorismo.

Elementos de administración de riesgo de prevención de lavado de activos y financiamiento de delitos, como el terrorismo (PLA): son un conjunto de componentes a través de los cuales se instrumenta de forma organizada, sistemática y metódica la administración del riesgo de lavado de activos y financiamiento de delitos, como el terrorismo en las entidades controladas. Se considera como elementos a las políticas, estructura organizacional, manual e información, procedimientos, reportes, auditoría, infraestructura tecnológica, cultura organizacional y capacitación orientados a mitigar el riesgo de lavado de activos y financiamiento de delitos, como el terrorismo.

Empresa pantalla: es la compañía constituida legalmente, que no realiza las actividades establecidas en su totalidad o las ejecuta parcialmente y que es utilizada para encubrir otras actividades.

Etapas de administración del riesgo de prevención del lavado de activos y financiamiento de delitos, como el terrorismo (PLA): se refiere a la identificación, medición, control y monitoreo del riesgo de lavado de activos y financiamiento de delitos, como el terrorismo.

Exposición de riesgo: nivel de riesgo que la entidad posee ante la materialización de eventos asociados al lavado de activos y financiamiento de delitos, como el terrorismo y se expresa a través del riesgo residual.

Factores de riesgo: son los agentes generadores del riesgo o parámetros que permiten evaluar las circunstancias particulares de clientes, productos y servicios, canales y situación geográfica.

Financiamiento del terrorismo: el financiamiento del terrorismo (FT) es cualquier forma de acción económica, ayuda o mediación que proporcione apoyo financiero a las actividades de elementos o grupos terroristas. Aunque el objetivo principal de los grupos terroristas no es financiero, requieren fondos para llevar a cabo sus actividades, cuyo origen puede provenir de fuentes legítimas, actividades delictivas, o ambas.

Jurisdicción: ubicación geográfica en la que se ejecuta una actividad, operación o transacción económica.

Lavado de activos: es la acción realizada que en cualquier forma tenga como objetivo ocultar y/o disimular el origen ilícito de determinados bienes, a sabiendas de que provienen, directa o indirectamente, de la perpetración de hechos constitutivos de delitos como tráfico ilícito de drogas, terrorismo, tráfico de armas, fraude a los estados financieros, malversación de caudales públicos, fraude al fisco y cohecho, entre otros; o bien que a sabiendas de dicho origen, oculte y/o disimule estos bienes.

Matriz de riesgos: es una herramienta de control y gestión, que mediante la identificación y medición de eventos de riesgos asociados a las líneas de negocio y procesos de la entidad y relacionados al lavado de activos y financiamiento de delitos como el terrorismo, permite

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

determinar el riesgo inherente e implementar los controles y acciones de debida diligencia que correspondan, obteniéndose el riesgo residual resultante.

Mercado: es el conjunto de personas y/u organizaciones que participan de alguna forma en la compra y venta de los bienes y servicios o en la utilización de estos. Para definir el mercado en el sentido más específico, hay que relacionarlo con otras variables, como el producto, los ciclos, las ventas, las jurisdicciones, o una zona determinada.

Metodologías: constituye la forma en la que se definen y tratan cada uno de los procedimientos que deben utilizar las entidades controladas; es la sucesión de pasos lógicos, documentados, ligados entre sí por un propósito verificable, comprobable, operativo y fidedigno, que en función de sus clientes, productos y servicios, canales y jurisdicción entre otros, las entidades controladas deben usar para desarrollar y evaluar la PLA, identificando a los clientes y sus riesgos, estableciendo perfiles transaccionales, de comportamiento y de riesgo, aplicando procesos de detección de inusualidades y gestionando los reportes.

Monitoreo y/o seguimiento: es el proceso continuo y sistemático mediante el cual se verifica la eficiencia y eficacia de una política o de un proceso, mediante la identificación de sus logros y debilidades para recomendar medidas correctivas tendientes a optimizar los resultados esperados.

Oficial de Cumplimiento: es el funcionario responsable de controlar el cumplimiento de la administración de riesgo de lavado de activos y financiamiento de delitos como el terrorismo, proponiendo a controlar que el riesgo residual se ubique en niveles apropiados, mediante la aplicación de políticas, procesos y procedimientos preventivos y la detección de operaciones inusuales e injustificadas.

Operación en efectivo: toda operación en efectivo superior a diez mil dólares (U$10.000) de los Estados Unidos de América, o su equivalente en moneada local según el valor del dólar observado el día en que se realizó la operación.

Operación financiera: es un acuerdo o contrato en el que participan dos o más sujetos económicos, intercambiando capitales, de tal manera, que el sujeto que presta el capital adquiere el papel de acreedor, mientras que, el otro, actuará de deudor, además, los bienes que se intercambian tendrán que ser equivalentes en cada momento del tiempo.

Operación inusual: es aquella operación cuya cuantía o características particulares no guardan relación con la actividad económica del cliente o clientes que la realizan, o que, por su frecuencia, o por la cantidad transada se sale de los parámetros de normalidad establecidos para un determinado mercado, o sobre la que existan dudas en cuanto a su razonabilidad o justificación.

Operación sospechosa: es aquella operación que por su número, cantidad o características no se enmarca en el sistema y prácticas normales del negocio, de una industria o de un sector determinado y, además que de acuerdo con los usos y costumbres de la actividad que se trate, no ha podido ser razonablemente justificada.

Perfil del comportamiento del cliente: son todas aquellas características propias y habituales del sujeto de análisis, asociadas con su información general y con el modo de utilización de los servicios y productos que ofrece la entidad.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

Perfil de riesgo: es la condición de riesgo que presenta el cliente tanto por su comportamiento como por transaccionalidad que pueden exponer a la entidad a la ocurrencia de eventos con implicaciones en lavado de activos y financiamiento de delitos, como el terrorismo.

Perfil transaccional del cliente: es el parámetro que indica la capacidad máxima que tiene un cliente para transaccionar con la entidad. El cálculo de su valor o rango se efectúa mediante metodologías de reconocido valor técnico, que consideren variables como sus ingresos, patrimonio, actividad económica, transaccionalidad histórica, entre otros.

Personas Expuestas Políticamente (PEP): son aquellas personas naturales nacionales o extranjeras, que desempeñan o han desempeñado funciones públicas destacadas en el país o en el extranjero en representación del país, sus familiares y colaboradores cercanos. (Esta categoría estará definida de acuerdo con la normativa o mejor práctica de cada país donde Kushki opera).

PLA (Prevención de Lavado de Activos que comprende): LA/FT/FPADM (Lavado de Activos, Financiamiento del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva). Para todos los efectos de la implementación en cada región donde tiene presencia Kushki.

Potencial cliente: persona natural o jurídica que ha consultado y manifiesta interés por acceder a los servicios o productos que ofrece la entidad controlada.

Productos: son mecanismos o instrumentos financieros que, de conformidad con la ley, ofertan las entidades de los sectores financieros público y privado.

Proveedor: es toda persona natural o jurídica de carácter público o privado que desarrolle actividades de producción, fabricación, importación, construcción, distribución.

Proveedor de bienes y servicios estratégicos: persona natural o jurídica que entrega productos o servicios necesarios para que la entidad financiera cumpla con procesos críticos inherentes a su objeto social y cuya deficiencia, debilidad o suspensión podría afectar el normal desenvolvimiento operativo de la entidad, con mayor énfasis en los bienes y servicios relacionados al control y a la prevención de lavado de activos y financiamiento de delitos como el terrorismo.

Políticas: son los lineamientos, orientaciones o aspectos que fundamentan la prevención y el control del riesgo lavado de activos y financiamiento de delitos como el terrorismo.

Riesgos asociados al lavado de activos y financiamiento de delitos como el terrorismo: se refiere a las consecuencias para Kushki derivadas de la materialización de los riesgos tales como:

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

- **Riesgo legal:** es la posibilidad de que una entidad controlada sufra pérdidas directas o indirectas; de que sus activos se encuentren expuestos a situaciones de mayor vulnerabilidad; de que sus pasivos y contingentes puedan verse incrementados más allá de los niveles esperados, o de que en el desarrollo de sus operaciones enfrente la eventualidad de ser afectado negativamente debido a error, negligencia, impericia, imprudencia o dolo, que deriven de la inobservancia, incorrecta o inoportuna aplicación de disposiciones legales o normativas, así como de instrucciones de carácter general o particular emanadas de los organismos de control, dentro de sus respectivas competencias; o, en sentencias o resoluciones jurisdiccionales o administrativas adversas, o de la deficiente redacción de los textos, formalización o ejecución de actos, contratos o transacciones, inclusive distintos a los de su giro ordinario de negocio, o porque los derechos de las partes contratantes no han sido claramente estipuladas.
- **Riesgo reputacional**: es la posibilidad de afectación del prestigio de una entidad controlada por cualquier evento, externo, fallas internas hechas públicas, o al estar involucrada en transacciones o relaciones con negocios ilícitos, que puedan generar pérdidas y ocasionar un deterioro del prestigio de la entidad.
- **Riesgo operativo:** es la posibilidad de que se produzcan pérdidas en las entidades controladas debido a eventos originados en fallas o insuficiencia de procesos, personas, tecnología de la información y en eventos externos imprevistos. Incluye el riesgo legal, pero excluye los riesgos sistémicos y de reputación Agrupa una variedad de riesgos relacionados con deficiencias de control interno que afectan la capacidad de la entidad para responder por sus compromisos de manera oportuna o comprometen sus intereses.
- **Riesgo de contagio:** es la posibilidad de pérdida que puede sufrir una entidad directa o indirectamente, por una acción o experiencia de un tercero.

Riesgo de lavado de activos, financiamiento de delitos como el terrorismo y proliferación de armas de destrucción masiva: es la posibilidad de pérdida o daño que puede sufrir una entidad controlada por su exposición a ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades delictivas incluida el terrorismo, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades. Este riesgo se materializa a través de los riesgos asociados (legal, reputacional, operativo y de contagio) con el consecuente efecto económico negativo que puede representar para su estabilidad financiera cuando es utilizada para tales actividades.

Riesgo inherente: es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles implementados.

Riesgo residual o neto: nivel resultante del riesgo después de aplicar los controles.

ROS (reporte de operación sospechosa): no implica una denuncia, sino que solo constituye información útil y pertinente para que las UIF o UAF puedan realizar inteligencia financiera y, con ello, detectar señales indiciarias de lavado de activos y/o financiamiento del terrorismo.

Segmentación: proceso por medio del cual se lleva a cabo la separación de los factores de riesgos en grupos homogéneos al interior de ellos y heterogéneos entre ellos. La separación se fundamenta en el reconocimiento de diferencias significativas en sus características.

Señales de alerta: son aquellos comportamientos de los clientes o las características de ciertas operaciones financieras o de otro carácter que, según la experiencia nacional o internacional, son indiciarias de operaciones sospechosas o de tipologías de lavado de activos o financiamiento

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

del terrorismo, y nos podrían conducir a detectar oportuna y/o prospectivamente la posible existencia de un riesgo de lavado de activos y financiamiento de delitos como el terrorismo.

Servicios: son todas aquellas interacciones de las entidades controladas con sus clientes y usuarios.

Soborno: el delito de soborno es la conducta de un sujeto, que de forma activa o pasiva, es destinada a dar a un empleado o funcionario público una retribución no debido a su cargo.

Sujetos obligados: son los sectores económicos obligados a reportar y cumplir con las normativas de prevención de lavado de activos, financiamiento del terrorismo y proliferación de armas de destrucción masivas, conforme los señalan marco regulatorio de cada país.

Transacción: movimiento económico con el cual se realiza el perfeccionamiento de la operación financiera entre deudor y el acreedor a través de pagos o ingresos realizados con instrumentos monetarios.

Transacción u operación económica inusual e Injustificada: movimientos económicos realizados por personas naturales o jurídicas, que no guardan correspondencia con el perfil transaccional y de comportamiento establecido por la entidad y que no pueden ser sustentados o cuando aun siendo concordantes con el giro y perfil del cliente parecen desmedidos e inusuales por su monto, frecuencia o destinatarios.

Transferencia: es la transacción efectuada por una persona natural o jurídica denominada ordenante, a través de una entidad autorizada en la respectiva jurisdicción, para realizar operaciones de envío de recursos nacionales y/o internacionales, con el fin de que una suma de dinero se ponga a disposición de una persona natural o jurídica denominada beneficiaria, en la misma u otra entidad autorizada para realizar este tipo de operaciones.

Usuario: es la persona natural o jurídica que, sin ser cliente de la entidad controlada, recibe de esta un servicio.

Vinculado: el vinculado es aquella persona natural o jurídica, relacionada o asociada a la entidad controlada por propiedad, administración o por presunción, que tiene posibilidad de ejercer influencia sobre ella.

UIF (Unidad de Inteligencia Financiera): es una unidad técnica responsable de la recopilación de información, realización de reportes, ejecución de las políticas y estrategias nacionales de prevención y erradicación del lavado de activos y financiamiento de delitos.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

5 ESTRUCTURA ORGANIZACIONAL

Kushki ha establecido la siguiente estructura para la integración de las diferentes áreas de trabajo en la aplicación de las políticas y procedimientos frente al PLA.

Figura 5.1
Estructura organizacional

6 FUNCIONES Y RESPONSABILIDADES

6.1 Funciones del Board Directors

El Board Director esta encargado de:

- Aprobar el manual de PLA, así como sus actualizaciones.
- Designar un colaborador como Oficial de Cumplimiento, para que sea el responsable de velar por la implementación, seguimiento y verificación del cumplimiento de la prevención del lavado de activos y financiamiento de delitos, como el terrorismo de los países y grupo empresarial donde tenga presencia.
- Aprobar los informes presentados por el Chief Risk Officer / Head Risk & Compliance sobre los resultados de la evaluación y análisis de la eficiencia y efectividad del Programa de Compliance, junto con las propuestas de mejora a que haya lugar.
- Disponer las medidas operativas, económicas, físicas, tecnológicas y de recursos que sean necesarias y requeridas para que los Oficiales de Cumplimiento de cada país donde tenga operación y sus empresas relacionadas pueda desarrollar sus labores.
- Aprobar el programa de capacitación para prevenir el lavado de activos y financiamiento de delitos, como el terrorismo.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

- Aprobar las metodologías, modelos, indicadores cualitativos, cuantitativos, matrices y más instrumentos o herramientas para prevenir el riesgo de lavado de activos y financiamiento de delitos como el terrorismo.
- Prestar eficiente y oportuno apoyo al equipo de Cumplimiento mediante el acceso a todos los procesos e información que este funcionario solicite.
- Imponer en el ámbito de su competencia, con sujeción al debido proceso y de conformidad con la ley, las sanciones internas dispuestas por quienes incumplan las disposiciones contenidas en el presente manual.

6.2 Funciones del Chief Risk Officer /Head Risk & Compliance

- Vigilar el estricto cumplimiento de todas las disposiciones relacionadas a la prevención de lavado de activos en las leyes, reglamentos, normativas, manuales e instructivos a nivel regional.
- Reportar al Directorio sobre todos los temas relacionados con cumplimiento desde desarrollo y monitoreo de políticas hasta la aplicación de sanciones por incumplimiento.

6.3 Funciones del Chief Governance & Compliance Officer (CCO)

- Asegurar la implementación de políticas en materia de (PLA) a nivel regional.
- Asegurar que la empresa cuente con una política de gestión de riesgos.
- Establecer una cultura dentro de la organización que enfatice su compromiso con los controles internos, la gestión de riesgos y altos estándares éticos.
- Asegurar que existan canales apropiados para reportar problemas de cumplimiento.
- Medir y evaluar el nivel de cumplimiento de todos los requisitos reglamentarios a través de toda la organización.
- Reportar al Directorio sobre todos los temas relacionados con cumplimiento desde desarrollo y monitoreo de políticas hasta la aplicación de sanciones por incumplimiento.

6.4 Funciones del Oficial de Cumplimiento o quién lo supla en ausencias

El Oficial de Cumplimiento, es de nivel gerencial con capacidad decisoria de todo lo que conlleva la implementación para la prevención y control de lavado de activos y financiamiento de delitos como el terrorismo; para el desarrollo de ésta será encargado de:

- Vigilar el estricto cumplimiento de todas las disposiciones o mejores prácticas relacionadas a la prevención de lavado de activos en las leyes, reglamentos, normativas, manuales e instructivos.
- Presentar informes, conforme la obligatoriedad regulatoria de cada región como consta en los documentos de cada país, sobre los resultados de la evaluación y análisis de la eficiencia y efectividad del programa, junto con las propuestas de mejora a que haya lugar.
- Elaborar el Manual de PLA y presentar para la aprobación, así mismo proponer las actualizaciones que correspondan y velar por su socialización a los colaboradores.
- Controlar permanentemente el cumplimiento de las políticas de conocimiento de cliente, coordinando y verificando los procesos de debida diligencia mediante la instrumentación de procedimientos, mecanismos y metodologías establecidos en el presente manual.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

- Evaluar los informes presentados por la auditoría interna/externa o quién ejecute funciones similares o haga sus veces, si es el caso, y adoptar las medidas razonables frente a las deficiencias informadas. Si las medidas que deben ser adoptadas requieren de una autorización de otros órganos, debe promover que estos asuntos sean puestos en conocimiento de los órganos competentes.
- Verificar el cumplimiento de los procedimientos de debida diligencia y debida diligencia intensificada, aplicables a la Compañía.
- Realizar la evaluación del Riesgo LA/FT/FPADM a los que se encuentra expuesta la Compañía.
- Informar al CCO acerca de posibles fallas u omisiones en los controles establecidos para mitigar las situaciones de riesgo identificadas, que comprometan la responsabilidad de los colaboradores y de Kushki.
- Administrar las etapas y elementos de PLA con el propósito de prevenir el riesgo de lavado de activos y financiamiento de delitos como el terrorismo y detectar las operaciones y transacciones inusuales e injustificadas, determinando el riesgo y proponiendo acciones para su mitigación.
- Establecer y difundir los criterios para la clasificación de los clientes, en función de su grado de riesgo.
- Desarrollar junto con el área de Riesgos, los procedimientos específicos, metodologías, modelos, indicadores cualitativos y cuantitativos, matrices y más instrumentos de administración del riesgo de lavado de activos y financiamiento de delitos, como el terrorismo para la aprobación del representante legal.
- Reportar a la Unidad de Inteligencia Financiera de cada país sujeto a esta obligatoriedad, o a la entidad que haga sus veces, los reportes como sujeto obligado entre estos cualquier operación sospechosa de la que tenga conocimiento, acompañando los antecedentes que sean necesarios para su acertada revisión.
- Certificar ante terceros cada vez que sea requerido por algún procesador, adquirente, banco, la existencia del sistema de prevención del lavado de activos y financiación del terrorismo.
- Atender y coordinar cualquier requerimiento, solicitud o diligencia de autoridad judicial o administrativa en materia de prevención y control de actividades delictivas.
- Dar respuesta a consultas de clientes internos y externos sobre materia de prevención de lavado de activos y financiamiento de delitos, como el terrorismo.
- Coordinar tanto las actividades de seguimiento de operaciones, como las investigaciones que deban llevarse a cabo a nivel institucional en materia de lavado de activos y financiamiento de delitos, como el terrorismo.
- Adoptar de manera oportuna las medidas de corrección frente a las observaciones emitidas por la auditoría interna, auditoría externa, las superintendencias u órganos de control y vigilancia de cada país.
- Coordinar y diseñar el programa de capacitación y sensibilización anual y de inducción para todos los colaboradores, así mismo, comunicar oportunamente al Chief Governance & Compliance Officer, los aspectos relativos a capacitación, en coordinación con el área de Recursos Humanos.
- Adoptar las medidas conducentes a conservar los documentos relativos a la prevención de lavado de activos y del financiamiento de delitos, como el terrorismo, de manera confidencial y segura, conforme a los procedimientos establecidos en las disposiciones legales.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

6.4.1 Incompatibilidades e inhabilidades del Oficial de Cumplimiento o quién lo supla en ausencias

- Pertenecer a órganos de control o a áreas directamente relacionadas con las actividades previstas en el objeto social principal.
- Ser empleado tercerizado de la entidad.

6.5 Funciones del Jefe de Monitoreo Transaccional

- Estructurar el proceso de gestión y monitoreo transaccional de compliance a nivel regional.
- Gestionar (identificar, analizar, escalar, entre otras) las operaciones que presenten señales de alerta relacionados a situaciones de LAFT.
- Automatizar el proceso de monitoreo transaccional, mediante la implementación herramientas y modelos basados en maching learning e inteligencia artificial.
- Mantener actualizado el sistema de monitoreo transaccional para que este permita identificar, gestionar y documentar en tiempo real las señales de alerta, operaciones inusuales y/o sospechosas (operaciones que no mantienen relación con la actividad económica del cliente o sobrepasan los parámetros establecidos, a través del análisis automático.
- Apoyar el proceso de identificación, medición, control y monitoreo de los riesgos en temas de PLA y compliance a nivel regional.
- Apoyar el proceso de análisis de los clientes considerados de mayor riesgo.
- Apoyar los procesos relacionados con PLA y proyectos de área de Compliance.
- Realizar la segmentación de los factores de riesgos definido por la entidad.

6.6 Funciones del Especialista de Compliance

- Apoyar al Oficial de Cumplimiento en la implementación de metodologías, modelos, indicadores cualitativos y cuantitativos, matrices y más instrumentos de administración del riesgo de lavado de activos y financiamiento de delitos, como el terrorismo.
- Preparar la documentación relacionada de los diferentes procesos y procedimientos para una adecuada administración del riesgo de lavado de activos y financiamiento del terrorismo.
- Apoyar en el desarrollo de programas internos en materia de capacitación para colaboradores, proveedores y establecimientos de comercio.
- En general todas las funciones inherentes al cargo o las asignadas por el Oficial de Cumplimiento.

6.7 Funciones del Auxiliar de Monitoreo Transaccional

- Apoyar el proceso de identificación, medición, control y monitoreo de los riesgos en temas de AML y compliance a nivel regional.
- Apoyar en la implementación de los diferentes proyectos a nivel regional.
- Realizar el análisis de las alertas generadas por el aplicativo de monitoreo transaccional.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

- Apoyo en la segmentación de factores de riesgos de acuerdo con el nivel individual de riesgo de los clientes.
- Analizar y gestionar alertas en listas restrictivas internacionales (GAFI, OFAC, ONU, entre otras).

6.8 Funciones de la Auditoría Interna o Externa

- Realizar una evaluación anual al Programa de Prevención del Lavado de Activos y Financiación del Terrorismo, a fin de verificar la efectividad de los controles existentes de acuerdo con el plan de trabajo definido.

6.9 Funciones del Comité Interno de Compliance

- Evaluar las operaciones inusuales presentadas por el Jefe de Monitoreo para determinar su reporte ante las diferentes UIF en los países regulados.
- Revisar mensualmente en la herramienta de monitoreo transaccional las alertas generadas a través de una muestra seleccionada.
- Realizar permanentemente el seguimiento de cada una de las etapas y elementos del Sistema en especial sobre la matriz de riesgos, enfatizando en las acciones adoptadas para la mitigación del riesgo de la entidad.

7 POLÍTICAS PARA PLA

Kushki provee servicios de pagos en línea y ofrece soluciones integrales para el procesamiento de pagos que tiene como pilar clave garantizar la seguridad en las transacciones que se realizan mediante su plataforma tecnológica. De la mano con esta promesa de servicio, la compañía está comprometida en mitigar el riesgo de que por su plataforma o por su actividad propia fluyan transacciones monetarias de origen ilícito o cuya finalidad pretenda financiar actos criminales relacionados con el lavado de activos y financiamiento de delitos, como el terrorismo. Por lo tanto, tendrá cero tolerancias a este riesgo y para ello impulsa internamente un abierto rechazo hacia cualquier actividad delictiva.

En este sentido, la Compañía ha definido las siguientes políticas internas:

- Kushki se compromete a adoptar el marco regulatorio legal local y buenas prácticas nacionales e internacionales de acuerdo con el tamaño y complejidad de sus operaciones y al análisis del nivel de riesgo inherente.
- Kushki no provee su servicio a comercios, proveedores, accionistas, beneficiarios finales (personas naturales o jurídicas), que se encuentren en listas OFAC, ONU o UNIÓN EUROPEA. La coincidencia con otras listas o información negativa de carácter público relacionada con el lavado de activos, financiamiento del terrorismo o cualquier delito precedente de estos.
- Kushki, en cumplimiento con sus términos y condiciones de servicio, se reserva el derecho de bloquear, cancelar y/o inhabilitar la operación transaccional de cualquiera de sus clientes para quienes se detecte transacciones inusuales y para las cuales no se haya presentado justificación razonable.
- Kushki no acepta la vinculación de un comercio que no haya diligenciado en su integridad el formulario digital y adjuntando los documentos necesarios para su vinculación.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

- Kushki se compromete en realizar un adecuado proceso de selección de proveedores y colaboradores con los que establecerá una relación legal o contractual para el giro de sus negocios.
- Kushki realiza negocios con personas naturales y jurídicas que desarrollen actividades lícitas. Identificando industrias o rubros que, por la naturaleza de sus actividades comerciales, pudieran ser consideradas como riesgosas y con una mayor probabilidad en la materialización de delitos de lavado de activos, financiamiento del terrorismo y proliferación de armas de destrucción masiva y cualquier delito precedente de estos.
- Kushki establece mecanismos de identificación y corroboración de información entregada por sus terceros (clientes, proveedores, empleados, entre otros), con la finalidad de establecer si estos cuentan con la categoría de PEP directos o por vínculo hasta el 2do grado de consanguinidad, estableciendo los protocolos exigidos en los distintos países donde tenemos presencia.
- Kushki no establece relaciones comerciales con personas que no puedan demostrar licitud del origen de los recursos con los cuales adquiere los productos o servicios.
- Kushki no establece relaciones comerciales con clientes que lleven a cabo transacciones derivadas de campañas políticas y/o partidos políticos.
- Kushki reportará a las autoridades correspondientes sobre operaciones sospechosas, identificadas en cualquier etapa del flujo de relación, brindando todos los respaldos y ayuda solicitada por dichas autoridades según dictamine la ley vigente aplicable en cada país.
- Kushki fomenta la cultura en materia de prevención del lavado de activos y financiamiento de delitos, como el terrorismo, para lo cual mantiene planes permanentes de divulgación y capacitación.
- Kushki vela porque sus colaboradores conozcan el contenido de este manual, sus políticas, procedimientos y sus respectivas actualizaciones para protegerse de estos riesgos, así mismo los colaboradores de Kushki deben anteponer el cumplimiento de las normas en materia de administración de riesgo de lavado de activos y financiamiento de delitos, como el terrorismo y la observancia de los principios éticos al logro de las metas comerciales.
- Kushki estableció una metodología para identificar los factores de riesgo y los eventos que puedan generar éstos con relación al de lavado de activos y financiamiento de delitos, como el terrorismo. Diseña controles que puedan ser preventivos, de detección o correctivos, así mismo establece actividades de monitoreo que permitan asegurar que los controles son integrales y funcionan de manera oportuna, efectiva y eficientemente.
- Kushki no realiza transacciones desde y hacia países que no han tomado medidas adecuadas para mitigar el riesgo de lavado de activos y financiamiento de delitos, como el terrorismo y los cuales están identificados por organismos internacionales como GAFI por ser de alto riesgo.
- Kushki conserva digitalmente los documentos que soporten la implementación de prevención de lavado de activos y financiamiento de delitos, como el terrorismo.
- Kushki cooperará cuando la legislación lo autorice y/u obligue con las autoridades, supervisores, agencias gubernamentales, judiciales y policiales en la investigación de situaciones que puedan involucrar actividades ilícitas, en general, pero especialmente aquellas relacionadas con el lavado de activos, financiamiento del terrorismo o cohecho.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

- Kushki cuenta con un procedimiento para la salida de nuevos productos donde se evalúan los potenciales riesgos estableciendo los controles apropiados.
- Kushki, mediante el Oficial de Cumplimiento, reporta de inmediato a las diferentes Unidades de Información y análisis financiero o de quien haga sus veces en cada país donde aplique, en el evento en que se identifique o verifique cualquier bien, activo, producto, fondo o derecho de titularidad a nombre o bajo la administración o control de cualquier país, persona o entidad incluida en listas vinculantes.
- Kushki no entrará en relaciones comerciales con clientes que tengan relación con bancos pantalla ni entablará relaciones directas con estos bancos ni con instituciones que permitan que sus cuentas sean utilizadas a través de ellos.

8 METODOLOGÍA PARA EVALUACIÓN DE RIESGOS DE LA/FT

El soporte metodológico para la implementación y administración del riesgo de Kushki está basado en la norma para Gestión de Riesgos ISO 31000, las cuales proporcionan una guía genérica para el desarrollo del proceso de a la administración de riesgo de LA/FT para Kushki a nivel regional.

El presente documento contiene la metodología establecida por Kushki para la administración del riesgo de LA/FT, el cual involucra el establecimiento del contexto interno y externo, la identificación de riesgos, evaluación de probabilidad y el impacto del riesgo inherente y el impacto del riesgo residual y el monitoreo del riesgo de lavado de activos y de la financiación del terrorismo, así como el establecimiento de planes de tratamiento en caso de ser necesario.

8.1 Objetivos

8.1.1 Objetivo general

Realizar la evaluación del sistema de administración de los riesgos de LA/FT en los diferentes procesos de la Compañía, teniendo en cuenta el desarrollo de los elementos y etapas del programa para la administración del riesgo de lavado de activos y de la financiación del terrorismo.

8.1.2 Objetivos específicos

- Impedir que Kushki sea utilizado como instrumento para el lavado de activos o el financiamiento del terrorismo.
- Mitigar el riesgo de incumplimiento normativo relacionado con la prevención de LA/FT.
- Impedir vínculos de cualquier tipo con personas naturales o jurídicas con alguna coincidencia en listados ONU, OFAC, GAFI, Al-Qaida, etc.
- Desarrollar procesos de seguimiento y monitoreo continuo que permitan la detección oportuna de operaciones sospechosas o inusuales.
- Mantener la buena imagen corporativa de Kushki, empresa éticamente correcta siempre preocupada por las buenas prácticas y la prevención de LA/FT.

8.2 Marco de referencia

Para el desarrollo del proceso de la administración de del riesgo de LA/FT en los procesos de la entidad, se tienen en cuenta los siguientes aspectos:

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

- Se identifican los procesos que pueden ser vulnerables al riesgo de LA/FT o procesos relacionados con el programa para la administración del riesgo de Lavado de activos y de la financiación del terrorismo.
- Se realizan reuniones con los colaboradores responsables de los procesos evaluados y el área de Compliance, con el fin de conformar un equipo de trabajo para aplicar la metodología.
- Se identifican los eventos de riesgo inherente y sus causas, así como el factor de riesgo y factor asociado, se evalúa conforme al proceso de medición del riesgo.
- Se identifican y evalúan los controles que mitigan los riesgos identificados, se eliminan los controles que ya no se aplican de ser necesario y/o se proponen controles para su mitigación, según el proceso de la calificación de los controles.
- Se calcula el riesgo residual del proceso.

8.3 Proceso de la gestión del riesgo

8.3.1 Establecimiento del contexto

Para definir los parámetros básicos dentro de los cuales los riesgos deben ser administrados y para proveer una guía en la toma de decisiones cuando realicen estudios más detallados del manejo del riesgo, se hace necesario establecer el contexto o el entorno de la entidad.

8.3.2 Contexto externo

- Entorno regulatorio respecto del riesgo de LA/FT.
- Normatividad vigente y aplicable al negocio de acuerdo con las recomendaciones de cada país donde Kushki tiene presencia.
- Otros entes externos:
  - Recomendaciones del GAFI.
  - Tipologías de lavado de activos y financiación del terrorismo publicados por las UIF o UAF correspondientes.

Otros factores que influyen en el contexto externo son: situaciones del entorno político, geográfico, sectores económicos, situaciones de orden nacional o internacional, que pueden afectar los procesos de la entidad respecto a LA/FT, como, por ejemplo, la incursión en un nuevo mercado, un nuevo producto, canal de atención o jurisdicción.

El equipo de trabajo debe considerar el cumplimiento de la normatividad vigente en materia del riesgo de LA/FT, así como la identificación de nuevas tipologías para la evaluación del riesgo en el proceso.

8.3.3 Contexto interno

Kushki es una sociedad con una trayectoria en el sector de los medios de pago, ofreciendo a sus afiliados la posibilidad de acepte pagos a nivel mundial y recibir dinero en su moneda local. Conecta diferentes métodos de pago en cada país bajo una única integración. Entendiendo la importancia de cada negocio, así las cosas, busca siempre adaptar el servicio de acuerdo con las necesidades del cliente, creando experiencias de pago de clase mundial.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

Aumentado la efectividad de los procesos de pagos y a su vez proporcionando un proceso de pago simple y sin inconvenientes. Contando con facilidad de manejo de todos los métodos de pago en un solo lugar: tarjetas de crédito y débito, transferencias bancarias y efectivo.

La entidad cuenta con un equipo de trabajo calificado, con un gran compromiso de servicio hacia sus clientes, apoyados por una plataforma operativa y tecnológica altamente eficiente, su modelo de negocio se enmarca en los sistemas administrativos de riesgo, auditando los procesos y buscando siempre su optimización.

Entorno normativo

Se debe dar cumplimiento al Manual programa para la administración del riesgo de lavado de activos y de la financiación del terrorismo de cada jurisdicción, así como al código de ética, código de gobierno, política antifraude y anticorrupción, y demás políticas establecidas por la compañía.

El equipo de trabajo debe considerar la normativa interna vigente en materia de riesgo de LA/FT, según el proceso evaluado. Es decir que se debe buscar siempre la norma de procedimiento de los procesos a evaluar las cuales encuentran publicadas la herramienta de procesos.

8.4 Identificación del riesgo de lavado de activos y financiación del terrorismo

- El proceso de identificación del riesgo debe ser permanente y debe responder las preguntas: que puede suceder, cómo y por qué se pueden originar hechos o situaciones que afectan el cumplimiento de los objetivos de la entidad por su exposición al riesgo de lavado de activos y la financiación del terrorismo, para lo cual se puede tomar como referencia el cuestionario para la identificación de riesgos de LA/FT.
- En la etapa de identificación de riesgos se deben tener en cuenta cada uno de los factores que generan el riesgo y crear una lista de posibles eventos a través desde los cuales se puede materializar el riesgo de LA/FT afectando el cumplimiento de los objetivos de Kushki en materia de LA/FT.
- La técnica que se utiliza para la aplicación de la metodología en esa etapa son las entrevistas estructuradas con los expertos de los procesos, cuya evaluación se realiza utilizando cuestionario para la identificación del riesgo de LA/FT.
- Consulta de las fuentes de información existentes sobre los eventos que podrían generar riesgos para la entidad. Estas fuentes incluyen:
    - Reportes de operaciones sospechosas (ROS) efectuados por la entidad.
    - Tipologías elaboradas por las unidades de inteligencia financiera.
    - Señales de alerta publicadas por GAFI.
    - Información de prensa.
    - Opinión de expertos de la entidad, responsable de los procesos.
    - Segmentación de los factores de riesgo.
- Teniendo en cuenta lo anterior se definen los posibles escenarios que exponen a la entidad a riesgos de LA/FT:
    - Surgir en la relación con un cliente.
    - Surgir por el incumplimiento de la norma.
    - Estar relacionado con el ingreso de recursos económicos a la entidad.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

  - Estar relacionado con el destino de los recursos comercio o usuario.
  - Tener relación con la reputación de la entidad.
  - Estar asociados a la presencia de la entidad en países sancionados.
- Una vez definidos los riesgos, estos deben ser asociados a los siguientes factores de riesgo definidos por la entidad correspondiente de cada región:
  - Clientes
  - Productos
  - Canales
  - Jurisdicción
- El Especialista del área de Compliance junto con el responsable del proceso o los colaboradores designados por el mismo, son los responsables de la identificación de riesgos de LA/FT, y sus riesgos asociados, así como los factores de riesgo, identificando las causas que lo originan o que podrían generar la materialización del riesgo y que finalmente se relacionan en la matriz de riesgo, de acuerdo con el procedimiento descrito en el Manual del programa para la administración del riesgo de lavado de activos y de la financiación del terrorismo.
- Para lograr una aproximación a la realidad del proceso en la identificación de riesgos, se debe tener presente NO considerar como riesgos las siguientes situaciones:
  - Las causas asociadas a los riesgos
  - La ausencia de un control
  - La falla de un control
  - La pérdida o impacto esperado por un evento
  - El opuesto al objetivo definido en el proceso
- Finalmente, en los procesos que se encuentran tercerizados o incluyen la participación de un outsourcing, el riesgo debe ser identificado y valorado por el líder del proceso responsable o quienes hagan las funciones de supervisor del tercero.

8.5 Medición o evaluación del riesgo inherente de lavado de activos y financiación del terrorismo

Una vez concluida la etapa de identificación del riesgo se procede a medir probabilidad de ocurrencia del riesgo inherente (sin controles) frente a cada uno de los factores de riesgo, teniendo en cuenta los criterios de frecuencia y/o probabilidad de ocurrencia del riesgo y la magnitud del impacto en caso de materializarse.

8.5.1 Evaluación de la probabilidad de ocurrencia

Es una aproximación cualitativa y/o cuantitativa que describe si una situación de riesgo es susceptible a ocurrir. Esta puede ser medida por la posibilidad de ocurrencia de un evento de lavado de activos o financiación del terrorismo. Teniendo en cuenta la presencia de factores que pueden propiciar el riesgo, aunque este no se haya presentado con anterioridad.

La escala utilizada por Kushki para la medición de la probabilidad de ocurrencia en términos de frecuencia se detalla en la Tabla 8.1.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

Tabla 8.1
Medición de la probabilidad

FRECUENCIA			
CLASIFICACIÓN	**NIVEL**	**DESCRIPCIÓN**	
Muy Alto	5	El evento sucede en mas del 25% de las operaciones.	El número de eventos expuesto es mas de 25 veces al año.
Alto	4	El evento sucede entre el 15% y 25% de las operaciones del año.	El número de eventos expuesto es máximo 25 veces al año.
Medio	3	El evento sucede entre el 5% y 15% de las operaciones del año.	El número de eventos expuesto es máximo 15 veces al año.
Bajo	2	El evento sucede entre el 2% y 5% de las operaciones del año.	El número de eventos expuesto es máximo 5 veces al año.
Muy Bajo	1	El evento sucede en el 2% de operaciones al año.	El número de eventos expuesto es máximo 2 veces al año.

8.5.2 Estimación de la magnitud del impacto

Hace referencia a las consecuencias o resultados en caso de materializarse el riesgo de lavado de activos y financiación del terrorismo. Para efectos de la valoración del impacto se establece la tabla de clasificación del impacto y consiste en una escala de cinco (5) niveles determinados en la Tabla 8.2.

Tabla 8.2
Medición del impacto

NIVEL	LEGAL	REPUTACIONAL	OPERATIVO	CONTAGIO
MUY ALTO	pérdidas por sanciones administrativas mayor que 0,5% del patrimonio de la compañía.	Las consecuencias reputacionales son de conocimiento del público. Impacto que afecta la imagen de la entidad relacionado con prácticas inseguras que generan perdida de confianza, intervención y sanciones. Consecuencias reputacionales alcanzan el nivel regional.	Insuficiencia en procesos, recursos, infraestructura, tecnología o incumplimiento de normas internas con impacto grave que acarrea daños cuyo costo operativo afecta el patrimonio de la entidad.	El evento se considera grave por la participación del vinculado en delitos de la vado de activos que comprometen a la entidad.
ALTO	pérdidas por sanciones administrativas menores que el 0,5% y mayores a 0,36% del patrimonio de la compañía.	Las consecuencias reputacionales son de conocimiento del sector financiero, procesadores y demás relacionados, divulgación de fallas y/o investigación por parte del órgano regulador. Impacto que afecta la imagen de la entidad relacionado con prácticas inseguras.	Insuficiencia de procesos, recursos, infraestructura, tecnología o incumplimiento de normas o internas con impacto importante que acarrea daños, cuyo costo operativo es mayor.	El evento de riesgo implica la participación de una persona vinculada laboral o contractualmente con la entidad que puede ser participe del delito de LA/FT.
MODERADO	pérdidas por sanciones administrativas menores 0.36% del patrimonio de la compañía.	Las consecuencias reputacionales son de conocimiento de la alta gerencia y de los órganos de control. Consecuencias reputacionales alcanzan el nivel nacional.	Insuficiencia de procesos, recursos, infraestructura, tecnología o incumplimiento de normas o internas con impacto moderado en el desarrollo de los procesos de gestión.	El evento de riesgo supone la participación de una persona vinculada con la entidad que pueda afectar la situación económica y administrativa de la misma.
BAJO	Sin impacto económico. La ocurrencia del riesgo no genera un costo o sanción por el incumplimiento de normas.	Las consecuencias reputacionales no exceden de la entidad. No se produce daño a la reputación a la entidad; la situación es de conocimiento de la alta gerencia.	Insuficiencia de procesos, recursos, infraestructura, tecnología con impacto menor y que no afectan los procesos de gestión.	La posibilidad de contagio para la entidad es menor. No hay interrelaciones importantes que afecten la entidad en relación con el mercado, los clientes o vinculados.
MUY BAJO	Sin impacto económico. La ocurrencia del riesgo no genera un costo o sanción por el incumplimiento de normas.	Sin efectos externos. La imagen y buen nombre de la entidad no se ven afectados.	Deficiencias en los procesos por reestructuración del recursos humano o tecnológico de la entidad.	Otros relacionados involucrados en el lavado de activos que no tienen efectos colaterales que perjudiquen a la entidad.

Los riesgos identificados deben ser relacionados a un riesgo asociado (reputacional, legal, operacional o contagio), teniendo en cuenta el impacto que pueda generar en caso de materializarse.

De acuerdo con la tabla de clasificación del impacto y según el riesgo asociado, se establece el impacto del riesgo si se materializa.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

8.5.3 Evaluación del nivel de riesgo inherente

Después de determinar la probabilidad y el impacto inherente para cada causa de riesgo, se estima el perfil inherente (sin controles), medido de acuerdo con los criterios de probabilidad de impacto y se ubica en el mapa de riesgos de la entidad.

El nivel de riesgo se determina como un valor numérico, que se obtiene como resultado del producto de los valores asignados a la probabilidad de ocurrencia y el impacto, en caso de materializarse a través de los riesgos asociados.

Riesgo Inherente = Valor Asociado Frecuencia x Valor Asociado Impacto

Escala para el perfil del riesgo inherente

Para tal efecto se utiliza una escala clasificada en 4 rangos, ver Tabla 8.3.

Tabla 8.3
Escala riesgo inherente

Nivel	Clasificación
1 - 4.99	BAJO
5 - 9.99	TOLERABLE
10 - 14.99	GRAVE
15 - 25	CRÍTICO

8.6 Construcción del mapa de riesgos

- De acuerdo con los lineamientos de la entidad respecto de la gestión de riesgos, Kushki realiza la construcción de mapas de riesgos, tomando como marco de referencia la metodología COSO ERM (Enterprise Risks Management), con el fin de implementar estándares internacionales en la gestión de riesgos de la entidad.
- Los mapas de riesgos constituyen para Kushki, una herramienta eficaz para identificar de forma gráfica los eventos de riesgo que se encuentran más expuestos, permitiendo la asignación de prioridades para su atención, ante cualquier vulnerabilidad que se enfrente y que requiera una toma de decisiones oportuna.
- Los riesgos de lavado de activos y de la financiación del terrorismo se grafican en el siguiente modelo de riesgo, con el fin de facilitar la gestión de estos.
    - El resultado de la combinación de la probabilidad y el impacto determina el nivel de riesgo inherente o exposición al riesgo de LA/FT del riesgo identificado.
    - El nivel de riesgo se determina como un valor numérico, que se obtiene como resultado de la concatenación de los valores asignados al impacto y a la probabilidad de ocurrencia, en caso de materialización a través de los riesgos asociados.
    - Como producto de lo anterior, lo niveles de riesgo establecido para Kushki se encuentran definidos en la siguiente matriz de cuantificación de severidad del riesgo.
    - Con el resultado de nivel inherente de cada una de las causas, se constituye el mapa de riesgos consolidado por proceso, y el consolidado de la entidad, en el cual se observa la exposición de los eventos de riesgos sin controles.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

Tabla 8.4
Mapa de calor

		IMPACTO				
		Muy Bajo	Bajo	Moderado	Alto	Muy Alto
PROBABILIDAD	Muy Alta	0	0	0	0	0
	Alta	0	0	0	0	0
	Media	0	0	0	0	0
	Baja	0	0	0	0	0
	Muy Baja	0	0	0	0	0

8.7 Control de riesgo de lavado de activo y financiación del terrorismo

Es el conjunto de acciones adoptadas por la entidad, con el fin de disminuir la probabilidad de materializar un riesgo y/o su impacto. Las medidas de tratamiento establecidas para el programa de la administración del riesgo de lavado de activos y de la financiación del terrorismo consisten en mitigar y prevenir el riesgo de lavado de activos y financiación del terrorismo.

En esta etapa, se identifican y evalúan los controles para determinar la efectividad de estos sobre los riesgos identificados, cuya finalidad es reducir la probabilidad o el impacto del riesgo en caso de materializarse.

A continuación, se describen los criterios definidos para la evaluación de la efectividad de controles establecidos para la mitigación del riesgo de lavado de activos y financiación del terrorismo.

8.7.1 Criterios de evaluación de controles

La clasificación y evaluación de los controles se determina a través de cuatro (4) atributos esenciales del control que son: OPORTUNIDAD, AUTOMATIZACIÓN, APLICACIÓN e IMPLEMENTACIÓN. A cada uno de ellos se le ha asignado un peso máximo de 25 puntos sobre 100 como se detalla en la Tabla 8.5.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

Tabla 8.5
Clasificación de controles

VARIABLE	CRITERIO	VALOR	CONCEPTO	MAX. PUNTAJE
OPORTUNIDAD	PREVENTIVO	25	El Control previene la ocurrencia del riesgo	25
	DETECTIVO	15	El Control detecta la materialización del riesgo	
	CORRECTIVO	5	El Control corrige el impacto de la ocurrencia del riesgo	
	INEXISTENTE	0	No existe un control asociado a la ocurrencia del riesgo	
AUTOMATIZACIÓN	AUTOMATICO	25	El Control es ejecutado de forma automática por el software	25
	COMBINADO	15	El Control es ejecutado en el sistema con un componente manual	
	MANUAL	5	El Control es operado netamente por el recurso humano	
	INEXISTENTE	0	No existe un control asociado a la ocurrencia del riesgo	
APLICACIÓN	PERMANENTE	25	El Control se aplica de forma permanente y cíclica	25
	PERIODICA	15	El Control se aplica solamente cuando es necesario	
	OCASIONAL	5	El Control se aplica en algunas ocasiones a discreción del responsable	
	INEXISTENTE	0	No existe un control asociado a la ocurrencia del riesgo	
IMPLEMENTACIÓN	TOTAL	25	El control esta documentado, divulgado e incorporado al proceso	25
	PARCIAL	15	El Control esta implementado pero no documentado o viceversa	
	NULA	5	El Control no esta documentado, ni divulgado, ni incorporado al proceso	
	INEXISTENTE	0	No existe un control asociado a la ocurrencia del riesgo	

- Oportunidad: hace referencia al momento en el cual opera el control en la ejecución de una actividad.
- Automatización: hace referencia al grado de sistematización del control al momento de su aplicación, buscando disminuir la operatividad manual del mismo.
- Aplicación: hace referencia a la frecuencia con la que se aplica el control, a fin de mitigar la materialización del riesgo.
- Implementación: hace referencia al grado de oficialidad y divulgación del control dentro del sistema documental de la Compañía.

Posteriormente, la sumatoria de las calificaciones de estos criterios arroja el puntaje máximo de cada control por causa de riesgo. El cual dependiendo de su valoración se ubica en la siguiente escala para determinar su calificación y el efecto de mitigación individual que tiene sobre cada causa.

Tabla 8.6
Calificación y efecto de mitigación

Rango	Calificación	Efecto de mitigación
90 a 100	FUERTE	75%
65 a 89	BUENO	55%
35 a 64	NORMAL	40%
11 a 34	MODERADO	25%
1 a 10	INSUFICIENTE	10%
0	INEXISTENTE	0%

Finalmente, se ponderan los efectos de mitigación individuales para obtener la mitigación promedio de los controles asociados a cada riesgo. Este porcentaje es el que refleja la efectividad que tiene el control en la mitigación del impacto y la frecuencia del riesgo, el cual una vez aplicado al riesgo inherente permite obtener la valoración del riesgo en forma residual.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

8.8 Evaluación del riesgo residual

8.8.1 Perfil de riesgo residual

El perfil de riesgo residual es el resultado consolidado de la medición de los riesgos a los que se ve expuesta **Kushki**, donde se utiliza la siguiente fórmula para el cálculo del perfil de riesgo:

PR = ∑ (R (R/ ∑R)) Es decir: **PR** = (a x (a/R)) + (b x (b/R)) +... (n x (n/R))

PR: Perfil de Riesgo

a: Riesgo 1

b: Riesgo 2

n: Riesgo n

R: Sumatoria de los niveles de riesgos (a + b +...n)

La fórmula permite determinar un perfil de riesgo consolidado, teniendo en cuenta el perfil de riesgo representado por el porcentaje de cada uno de sus riesgos individuales. El resultado de este cálculo se ajusta al método de redondeo simple.

8.8.2 Nivel de aceptación al riesgo de LA/FT

El Directorio de Kushki ha definido que su nivel máximo de aceptación del riesgo residual, dentro de la clasificación es Bajo, es decir el resultado de la exposición teniendo en cuenta el efecto de los controles sobre los riesgos inherentes identificados.

8.8.3 Tratamiento del riesgo residual

Una vez evaluada la acción de los controles frente al riesgo inherente, el resultado de la valoración final será ubicado en la Tabla 8.7 de acuerdo con su criticidad, con el objetivo de definir el tratamiento del riesgo residual.

Tabla 8.7
Clasificación del riesgo residual

Nivel	Clasificación	Descripción
1 - 4.99	BAJO	Si el riesgo se encuentra en este nivel, se debe realizar monitoreo periódico para asegurar el cumplimiento de los controles.
5 - 9.99	TOLERABLE	Cuando el riesgo se ubique dentro de este nivel, se requieren planes de acción y/o controles específicos para tratarlo.
10 - 14.99	GRAVE	Para este nivel se requiere fortalecer controles o definir planes de acción a corto plazo, adicionalmente se informa al Comité de Riesgos para su seguimiento.
15 - 25	CRÍTICO	En este caso, el Comité de Riesgos debe intervenir de forma directa y debe informar inmediatamente al Directorio de la compañía.

Los riesgos residuales clasificados como BAJO y TOLERABLES deben ser evaluados anualmente por los líderes de proceso con el apoyo del área de Compliance, garantizando la eficacia de los controles en el tiempo, ya sea mejorándolos o definiendo nuevos controles cuando haya lugar. Si se percibe un incremento en el nivel del riesgo debe ser informado inmediatamente

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

al Comité SRCC (Security, Risk and Compliance Committe) con el fin de realizar la respectiva reclasificación.

Para los riesgos residuales clasificados como GRAVES o CRÍTICOS, el líder de proceso debe establecer planes de acción que busquen reducir la exposición de la Compañía a través de la creación de nuevos controles o la implementación de modificaciones a los controles existentes.

A dichos planes se les hará seguimiento de forma trimestral, reportando su avance al Comité SRCC (Security, Risk and Compliance Committe) y al Directorio, con el fin de tomar las decisiones respectivas para su tratamiento y mitigación. Las medidas adoptadas por Kushki para mitigar o tratar los riesgos residuales son las siguientes:

- **Eliminar el riesgo:** se opta por suspender el producto o proceso por una decisión administrativa.
- **Mitigar el riesgo:** se deben generar cambios sustanciales al interior de los procesos por mejoramiento de controles, rediseño o eliminación de actividades, orientados a la disminución del impacto, la distribución de la frecuencia o la disminución de las dos.
- **Dispersar o atomizar el riesgo:** se logra mediante la distribución o localización del riesgo en diversos lugares, procesos o personas.
- **Transferir el riesgo:** buscar respaldo y/o compartir el riesgo con una contraparte.
- **Asumir el riesgo:** luego que el riesgo ha sido reducido o transferido, puede quedar un riesgo residual que se mantiene, en este caso el Directorio acepta la pérdida residual tolerable y debe definir tratamientos específicos para gestionar estos riesgos.

8.9 Monitoreo del riesgo de lavado de activos y financiación del terrorismo

El monitoreo busca evaluar la evolución del riesgo de la entidad tanto inherente como residual y su variación, así como la efectividad de los controles con el fin de determinar las medidas correctivas a que haya lugar.

8.9.1 Monitoreo con relación a la administración de Kushki

- El monitoreo con relación a la administración del riesgo de LA/FT en las áreas o procesos de la compañía tiene como propósito realizar el seguimiento a los perfiles de riesgo inherente y residual, y a las etapas del programa para la administración del riesgo de lavado de activos y de la financiación del terrorismo, con el fin de realizar las acciones correctivas, preventivas y de mejora al sistema.
- La evolución individual y consolidada de los perfiles de riesgo de los factores de riesgo y los controles adoptados, así como de los riesgos asociados se realiza de manera semestral.
- Así mismo, la auditoría en el seguimiento a las áreas realiza la correspondiente evaluación de los controles conforme al plan de trabajo diseñado para el seguimiento al programa para la administración del riesgo de lavado de activos y de la financiación del terrorismo de la Compañía.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

9 SEGMENTACIÓN DE FACTORES DE RIESGO

El soporte metodológico para segmentación por factores de riesgo de Kushki está basado en la metodología CRISP-DM, que son las siglas de Cross-Industry Standard Process for Data Mining, es un método probado para orientar trabajos de minería de datos, bajo las siguientes fases:

- Comprensión del negocio
- Comprensión de los datos
- Recopilación de los datos iniciales
- Descripción de los datos
- Exploración de datos
- Verificación de la calidad de los datos
- Preparación de los datos
- Modelado
- Evaluación
- Despliegue

Kushki con una herramienta de reconocido valor estadístico determina las características de las transacciones usuales y las compara con aquellas que realicen los clientes, a efectos de detectar las operaciones inusuales y/o sospechosas de forma oportuna.

9.1 Factores de riesgo para Kushki

De acuerdo con nuestro modelo de negocio en el ofrecimiento, venta y suministro de nuestros productos y servicios nos enfrentamos a los siguientes cuatro (4) factores de riesgo distintos que nos exponen en mayor o menor medida al riesgo de LA/FT:

- Nuestras contrapartes
- Nuestros productos
- Los canales
- Jurisdicciones

Para identificar el riesgo de LA/FT de Kushki es preciso comprender cada uno de los factores de riesgo. Para esto y conforme la herramienta obtenida por Kushki, se agrupan de acuerdo con las características homogéneas de cada factor de riesgo.

10 PROCEDIMIENTOS

10.1 Procedimiento conocimiento de contrapartes

10.1.1 Procedimiento de conocimiento de comercios

Este pilar incluye la correcta identificación de los clientes a quienes Kushki presta su servicio de pagos. El comercio o establecimiento que desea usar nuestros productos tecnológicos debe completar una afiliación que inicia en nuestra página web y cargar los documentos requeridos.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

Una vez completados los formularios de afiliación en el sitio web, se disipa una serie de actividades que deben completarse por varias áreas dentro de Kushki antes de que el cliente pueda empezar a operar con el servicio.

La primera actividad del proceso de afiliación consiste con la validación de perfil de riesgo, donde este proceso busca conocer a profundidad al cliente mediante la consulta en listas de control, restrictivas, nacionales e internacionales a través de las herramientas designadas, incluyendo el perfil crediticio. Para generar un criterio de aceptación con los resultados de las consultas hechas al comercio, se hace uso de una matriz de decisiones, este resultado es el producto de varias ponderaciones y permite marcar un límite mínimo para la aceptación del comercio en la afiliación del modelo Gateway, de encontrarse alguna coincidencia en las consultas y conforme a nuestras políticas, no se procederá con el enrolamiento del cliente deteniendo el proceso en dicha instancia.

Toda esta debida diligencia que se detalla en sus procesos tiene como principal objetivo, evitar que los productos o servicios ofrecidos por Kushki, sean utilizados como instrumentos para ocultar, manejar, invertir o desviar dineros u otros valores cuya procedencia o destino sean producto de actividades delictivas. Es por ello por lo que los canales comerciales están en la obligación de tener un adecuado conocimiento de los clientes, siendo ésta la estructura fundamental en materia de prevención del riesgo de lavado de activos y financiamiento de delitos, como el terrorismo.

En el marco de la debida diligencia, se deben ejecutar las siguientes medidas orientadas al conocimiento del cliente:

- Identificar al cliente y verificar la identidad de éste a través de los documentos expedidos por las autoridades de cada país para dicho propósito.
- Identificar al beneficiario final de los comercios, de manera tal que Kushki esté convencido de quién se trata.
- Entender y, cuando corresponda, obtener información sobre el propósito y el carácter que se pretende dar a la relación comercial.

Para efectos de mitigar el riesgo legal y reputacional que puede conllevar tener relaciones con personas naturales y jurídicas en listas OFAC, ONU, UNIÓN EUROPEA y locales, luego de su vinculación, el sistema realiza un monitoreo continúo de las personas físicas y jurídicas.

Kushki mantiene un proceso de actualización de datos de acuerdo con el nivel de riesgo de cada comercio activo, para los comercios inactivos aplica su actualización cuando dejen de tener tal condición.

Como parte de este pilar se tienen considerados algunos negocios riesgosos y prohibidos como como consta en el documento **GGC-IN-0104-KU** Mapeo de negocios riesgosos y prohibidos, es de anotar que los negocios considerados de mayor riesgo deben pasar al área de Compliance para su revisión y concepto, en este análisis según el caso se requiere información o documentación adicional, donde se informe las políticas o medidas que adoptan para prevenir el lavado de activos y financiamiento de delitos como el terrorismo.

10.1.2 Procedimiento de conocimiento de colaboradores

- Para realizar el proceso de reclutamiento, selección y contratación se debe gestionar y solicitar a los candidatos participantes los documentos descritos en el proceso de reclutamiento y selección del área de Recursos Humanos.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

- El área de Recursos Humanos antes de realizar la oferta laboral debe hacer un adecuado conocimiento del candidato y demás normas definidas para dicho fin, así mismo debe consultar el candidato en listas restrictivas a través del aplicativo interno dispuesto por el área de Compliance para prevenir el riesgo de contagio de LA/FT. El resultado de la consulta en listas, la hoja de vida del candidato, concepto de seguridad (cuando aplique) y demás documentos requeridos durante el proceso de selección, deben ser archivados en la carpeta del colaborador.
- La consulta en listas restrictivas se debe realizar posterior a la vinculación para validar que no existe ningún cambio en la información y que no han sido reportados en alguna lista restrictiva, por tanto, desde el área de Compliance se realiza validación anual de todos los colaboradores activos de la compañía, dejando la evidencia de la consulta en una carpeta compartida de Compliance.
- En caso de que el reporte sea positivo, debe informarse inmediatamente a los Oficiales de Cumplimiento de cada país donde se tienen operación al correo electrónico compliance@kushki.com / compliance@billpoket.com.
- Anualmente se gestiona la actualización de los datos personales de los colaboradores activos de la compañía.

10.1.3 Procedimiento de conocimiento de proveedores

De la mano con la promesa de valor de la Compañía, comprometida en trabajar única y exclusivamente con proveedores y/o aliados que se alineen a los ideales de Kushki. Se cuenta con lineamientos clave para la selección y evaluación de los proveedores de bienes y servicios que Kushki requiera contratar, aplicado para todos los proveedores tanto locales como extranjeros de bienes y servicios que buscan trabajar con Kushki en cualquiera de sus filiales y cuyo servicio afecta directamente la prestación del servicio de Kushki.

- Para la selección de un proveedor en específico, se realiza la respectiva evaluación usando los criterios que se encuentran en el procedimiento selección y evaluación de proveedores.
- Kushki consulta previa a su vinculación los datos del proveedor en listas restrictivas/vinculantes.
- Kushki NO trabaja con proveedores (personas naturales o jurídicas) con antecedentes u obligaciones penales, judiciales, fiscales y/o que se encuentren en algunas listas vinculantes o restrictivas.
- La consulta en listas restrictivas se debe realizar posterior a la vinculación para validar que no existe ningún cambio en la información y que no han sido reportados en alguna lista restrictiva, por tanto, desde el área de Compliance se realiza validación anual de todos los proveedores activos de la Compañía, dejando la evidencia de la consulta en una carpeta compartida de Compliance.
- Kushki cancelará cualquier relación contractual si evidencia alguna coincidencia en listas vinculantes y restrictivas tanto nacionales e internacionales de cara al lavado de activos y financiación del terrorismo.
- Kushki, se reserva el derecho de bloquear, cancelar y/o inhabilitar la relación de servicio con algún proveedor tercero si el mismo incumple con lo estipulado contractualmente.
- Kushki solicita actualización anual de los proveedores recurrentes a través de los mecanismos dispuestos para este fin.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

10.1.4 Procedimiento de conocimiento de accionistas

- En ningún caso Kushki deja de identificar y conocer la información básica de todos sus accionistas, incluyendo a las personas naturales finales o beneficiarias efectivas de una persona jurídica.
- Kushki verifica anualmente que los accionistas no consten en listas vinculantes, restrictivas, incluida la condición de personas PEP, en el caso de presentarse coincidencias deben tomarse las acciones que correspondan.

10.1.5 Beneficiario final

Kushki en aras de dar cumplimiento a las normativas de cada país y con base en los estándares internacionales como el GAFI, ha implementado diferentes mecanismos para capturar la información de los beneficiarios finales de los comercios afiliados, entre estos la declaración expresa del comercio al momento de diligenciar la información del formulario virtual o en el formato **GGC-FO-0107-KU** Formulario de declaración beneficiario finalel cual cuenta con campos para registro de los socios o accionistas de los países regulados de cada empresa que hace parte del proceso de Afiliaciones de Kushki.

10.2 Procedimientos para personas expuestas políticamente

El Oficial de Cumplimiento se apoya para identificar a los PEP a través de las bases de datos suministradas por el proveedor de listas.

Para aquellos clientes que se hayan identificado en esta categoría, debe ser aprobada la vinculación por la instancia superior de Sales en las regiones donde tiene presencia Kushki, y en general se debe surtir las acciones establecidas en el procedimiento **GGC-PD-0103-KU** Debida diligencia intensificada.

Monitorear periódicamente las operaciones de los clientes considerados PEP, a fin de determinar que éstas se encuentren dentro de los parámetros de normalidad frente al perfil del segmento al que pertenecen.

Periódicamente Compliance realiza revisiones, de la base de datos de clientes, con el fin de determinar si alguno ha adquirido la condición de PEP luego de su proceso de afiliación.

10.3 Procedimientos para personas naturales y jurídicas que ya tengan relación con Kushki y se encuentren en listas vinculantes, impedidos o en otras listas o noticias

Una vez se detecte en el proceso de monitoreo continúo en listas que alguna persona física o jurídica ingresó en una lista vinculante o con un proceso fiscal en listas locales, se debe terminar la relación contractual conforme lo establecido en los términos y condiciones, el Oficial de Cumplimiento, lo reporta ante la Unidad de Inteligencia del país sujeto regulado donde aplique, así mismo se reporta al área de Operaciones para cancelar al cliente y el área Comercial, KAM o Soporte informa al cliente la decisición.

El Oficial de Cumplimiento en su proceso de monitoreo que haya identificado alguna noticia con las personas físicas o jurídicas con las cuáles se tiene establecida una relación contractual debe informar a Alta Gerencia, el tratamiento que se le dará, dependiendo del riesgo reputacional o legal que pueda representar para Kushki, se podrá solicitarles explicación de la situación y de esta manera tomar las acciones respectivas.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

10.4 Procedimiento de monitoreo transaccional de comercios

De la mano con el pilar de conocimiento del cliente, Kushki maneja el proceso de monitoreo transaccional para riesgo de lavado de activos y financiamiento de delitos como el terrorismo, a través de la información registrada de las transacciones de los comercios en la Consola de Monitoreo y a partir de ello se definieron alertas con base en el comportamiento, naturaleza y características de cada comercio. Las alertas se generan a partir de la parametrización desarrollada con fundamentos estadísticos y éstas son revisadas por el Especialista de Compliance, ante cualquier comportamiento atípico se notifica al área Comercial quién debe emitir el concepto de acuerdo con la debida diligencia realizada y posteriormente notificarla a Compliance quién determinará el cierre de la operación inusual.

Para determinar si una operación es o no sospechosa se debe presentar al Comité Interno de Compliance, junto con los soportes de análisis y según aplique concepto del área Comercial, donde se determinará el ROS de los países donde aplique. Por ningún motivo se tendrá en consideración criterios de índole subjetivo, el análisis debe estar debidamente sustentado y documentado.

10.5 Procedimiento de determinación o utilización de señales de alerta

Son aquellos hechos, situaciones, eventos, cuantías o indicadores financieros que se salen de los parámetros particulares de los clientes o los mercados, a partir de las cuales se puede inferir la posible existencia de un hecho o situación que se escapa en el giro ordinario de las operaciones que realizan en Kushki.

Las siguientes señales de alerta son de carácter general y toman como guía las que entrega la UAF en su página web, o autoridad por país considerando los hechos y situaciones que se derivan de la propia actividad de Kushki, así como de su relación con sus clientes y la información que se obtenga de los mismos. Es de obligatorio cumplimiento que todo colaborador de Kushki reporte de manera inmediata al Oficial de Cumplimiento a través de Slack, canal de denuncia o a los correos electrónicos de compliance@kushki.com / compliance@billpocket.com, si dentro de sus funciones diarias identifica alguna de ellas o las que considere sujetas a reportar:

- Cuando el cliente entrega información insuficiente o inconsistente, argumentando que en los próximos días la misma se complementará o se aclarará.
- Cuando las transacciones de los clientes no son consistentes con sus actividades económicas y su perfil transaccional.
- Cuando el cliente se niega a entregar información que permita verificar el origen de los recursos.
- Cuando los clientes demuestran escaso conocimiento acerca de su negocio.
- Cuando los documentos presentados por el cliente generan duda en cuanto a la existencia del establecimiento.
- Cuando se muestran renuentes o molestos a completar los formularios de afiliación o aclaración de los datos consignados en ellos.
- Cuando un empleado tiene un estilo de vida que no corresponde con el monto de su salario.
- Cuando un empleado sea renuente a disfrutar de vacaciones, a aceptar cambios de su actividad o promociones que impliquen no continuar ejecutando las mismas actividades.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

- Cliente indica una dirección que coincide con el domicilio de otro negocio diferente al que declaró desarrollar, o no se ajusta a la ocupación declarada.
- Cliente que realiza transacciones de elevado monto y no declara un empleo remunerado o actividad acorde que justifique los montos involucrados.
- Clientes cuya dirección para envío de correspondencia y estados de cuenta se encuentra en el extranjero o corresponde a una casilla de correos.
- Incremento inusual e injustificado de la facturación del negocio de un cliente, observado a partir de la actividad económica consignada en sus cuentas y perfil.
- Cliente que en un corto período aparece como dueño de nuevos negocios o empresas, constituidas con capitales iniciales relevantes.
- Cliente que realiza reiteradas operaciones a nombre de terceras personas.
- Cliente que con frecuencia envía o recibe transferencias de dinero hacia o desde países considerados no cooperantes por el Grupo de Acción Financiera Internacional (GAFI), o territorios catalogados por la Organización para la Cooperación y el Desarrollo Económicos (OCDE) como regímenes fiscales preferenciales, sin contar con una justificación económica aparente.
- Constitución de empresas con capitales o socios provenientes de países considerados no cooperantes por GAFI, o regímenes fiscales preferenciales nocivos según clasificación de la OCDE (paraísos fiscales).
- Cambio repentino en la propiedad de una sociedad, cuyos nuevos socios presentan un perfil comercial que no se ajusta a la información histórica de la entidad, o que se muestran reacios a presentar información personal o financiera.
- Cliente que se rehúsa o suspende una transacción al momento de ser requerido para que aporte información acerca del origen de los fondos involucrados.
- Apertura de múltiples comercios con una persona en común a todas ellas.
- Clientes cuyas sociedades tienen como directivos a personas que no se ajustan al perfil de los cargos.
- Clientes cuyas sociedades presentan ingresos no operacionales superiores a los operacionales en el momento del ingreso y/o en su actualización.
- Clientes cuyos estados financieros reflejan resultados que no se coinciden con el promedio de la industria o sector.
- Que se tome conocimiento por los medios de difusión pública u otro, según sea el caso, que un cliente está siendo investigado o procesado por el delito de lavado de activos, delitos precedentes o financiamiento del terrorismo.
- Transferencias solicitadas por un cliente a varias personas sin relación aparente.
- Transferencias remitidas a diferentes países, con un mismo beneficiario y en un corto período.
- Transferencias realizadas a varias personas, respecto de las cuales se detectan datos en común (dirección, teléfono, entre otros).
- Recepción de fondos provenientes de distintos remitentes, respecto de los cuales se detectan datos en común (dirección, teléfono, entre otros).
- Recepción de transferencias por altos montos, remitidas por empresas procesadoras de pagos en línea (PayPal, Money bookers, etc.), las cuales no aportan información acerca del remisor.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

- Clientes que realizan transacciones en jurisdicciones que no tienen relación con el objeto social a la jurisdicción habitual.
- Empresas que tienen un capital muy bajo y/o un objeto social muy amplio.
- Clientes que cambian en períodos muy cortos sus cuentas bancarias y/o sus beneficiarios finales.
- Existencia de una o más cuentas comerciales a través de la(s) cual(es) se realiza un gran número de transferencias hacia y desde el exterior, y para la cual no parece existir un propósito comercial o económico suficientemente justificado, particularmente cuando esta actividad se realiza desde o hacia países, territorios o jurisdicciones sometidos a especial seguimiento (países designados por las autoridades nacionales, o países y territorios denominados como no cooperadores por el GAFI o la OCDE).
- Utilización de enlaces virtuales de transferencias entre cuentas bancarias tradicionales y servicios de pagos anónimos (Money Services Business, monedas virtuales, intercambiadores de divisas digitales o canales de pago alternativos como e-cash, e-wallet), con la finalidad de estratificar los fondos de la fuente original e integrarlos en una o más cuentas mediante transferencias desde o hacia lugares que generan preocupación.
- Creación y funcionamiento de organizaciones no gubernamentales (ONG) u organizaciones sin fines de lucro (OSFL) cuya actividad u objeto social no resulta justificado con las características del medio o lugar en donde opera, la recepción y el envío frecuente de dinero desde o hacia el exterior, el uso de los fondos no justificado en relación con el propósito para que fue creada, inexistencia de la infraestructura necesaria para desarrollar sus actividades, recepción de aportes en dinero en efectivo para financiar sus operaciones internas, o se vincula a personas externas que recepcionan o reenvían dinero a terceros.
- Organismos sin fines de lucro (OSFL) que basan su existencia en la recepción de aportes provenientes de países considerados de elevado riesgo terrorista.
- La transacción no coincide con el perfil del cliente o de los negocios que actúan como contraparte, o la información del usuario final no coincide con el perfil de su negocio.
- Un cliente o contraparte, declarado como actividad comercial, realiza operaciones que sugieren que está actuando como negocio de envío de dinero o como cuenta de pago. Estas cuentas implican un movimiento rápido de operaciones de gran volumen y un pequeño saldo al final del día sin razones comerciales claras. En algunos casos, la actividad asociada a los ordenantes parece ser la de entidades que pueden estar relacionadas con un programa de proliferación patrocinado por un estado (como sociedades ficticias que operan cerca de países con problemas de proliferación o desvío), y los beneficiarios parecen estar asociados a fabricantes o expedidores sujetos a controles de exportación.
- Participación de una pequeña empresa comercial, de corretaje/intermediaria, que podría estar llevando a cabo actividades inconsistentes con su negocio usual.
- El patrón de transacciones de un cliente o su contraparte, el cual declara ser negocio comercial, sugiere que está actuando como una empresa de remesa de dinero.

10.6 Procedimientos para nuevos productos

Siempre que un nuevo producto sea diseñado y previo a su ofrecimiento al público, el área de Compliance debe realizar la evaluación del riesgo de lavado de activos y financiación del

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

terrorismo al que está expuesto este producto y establecer en cada caso los controles adecuados para mitigar estos riesgos.

Cada ficha técnica de producto debe ser remitida al área de Compliance para que esta área evalúe si cada producto implementó los controles adecuados y en caso contrario, solicitar al área encargada la implementación y puesta en práctica de estos.

10.7 Medidas de debida diligencia[1]

Atendido el perfil de riesgo de cada cliente, Kushki puede aplicar una o más de las siguientes medidas:

- **Para perfiles de alto riesgo** se deben ejecutar las medidas de debida diligencia intensificada contempladas en el procedimiento **GGC-PD-0103-KU** Debida diligencia intensificada. Todos los potenciales clientes que se encuentren enmarcados en algunas de las siguientes categorías, deben surtir ser direccionados a través Kiss Flow al área de Compliance:
  - Los PEP nacionales y extranjeros.
  - Organizaciones no gubernamentales ONG u organizaciones benéficas.
  - Clientes que efectúan transacciones comerciales transfronterizas con países de alto riesgo, en los que Kushki no mantiene operaciones.
  - Negocios riesgosos y prohibidos (**GGC-IN-0104-KU**).
  - Clientes con operaciones inusuales que determine Compliance.
  - Clientes con antecedentes negativos.
- **Para perfiles de bajo riesgo** pueden (facultativamente) aplicarse siguientes medidas de debida diligencia simplificada:
  - Completar los datos de debida diligencia simplificada mediante la utilización de terceras fuentes de información.
  - Postergación de la obligación de verificar la información de identificación del cliente y beneficiario final al momento en que se realice un acto, operación y/ o transacción por sobre un umbral monetario determinado.
  - Reducción en la frecuencia de la actualización de los datos de identificación del cliente.
    - Actualización de los datos de Debida Diligencia Intensificada (DDI) en función de información obtenida de terceras fuentes.
    - Reducción en la intensidad de la DDI continua del cliente. Esta menor intensidad puede estar determinada por un umbral monetario establecido.
    - Exención de la solicitud de antecedentes sobre el propósito de la relación legal o contractual, o de la transacción ocasional.

Sin perjuicio de lo anterior, las medidas de debida diligencia simplificada no serán aplicables cuando existan sospechas de LA/FT respecto de un cliente.

[1] Remitirse al procedimiento GGC-PD-0103-KU Debida diligencia intensificada, para conocer el detalle de esta actividad.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

11 PROGRAMA DE CAPACITACIÓN

El objetivo de la capacitación es difundir, impulsar y fomentar una cultura de prevención de lavado de activos y financiamiento de delitos, como el terrorismo para la protección tanto de los colaboradores como de la empresa.

La capacitación se desarrolla de manera obligatoria para los colaboradores en el programa de inducción y una vez al año se realiza las actualizaciones necesarias del programa y pueden ser adelantados por los medios virtuales y/o presenciales definidos para tal efecto.

El programa de capacitación durante el proceso esta enfocado en comprender el funcionamiento de las actividades criminales del lavado de activos y financiación del terrorismo, así como sus diferentes etapas, modalidades y tipologías relacionadas con la actividad económica de Kushki., así mismo se enfatiza en la importancia de las señales de alerta, sanciones internas administrativas y externas penales, reforzar contenido del presente manual de prevención de LA/FT, el procedimiento a ejecutar frente a una operación de carácter sospechosa y mecanismos de reporte o denuncia interna garantizando en todo momento la confidencialidad y anonimato del denunciante.

Adicionalmente, a través de los medios de comunicación internos de Kushki (Slack, o correo electrónico), se envían boletines, videos, noticias, blog con temas y actualizaciones relacionados con la prevención de lavado de activos y financiamiento de delitos como el terrorismo.

En la inducción y cada año en la actualización, los colaboradores se registran en la Academia Kushki, donde desarrollan el programa de LA/FT, es responsabilidad del área de Recursos Humanos llevar los indicadores de control y asistencia.

De otra parte, como mecanismo para determinar la eficacia de la capacitación realizada a los colaboradores, la plataforma E-Learning contiene la evaluación de conocimientos que consta de 5 preguntas, el porcentaje de aprobación de la evaluación es del 80%. Para aquellos colaboradores que obtengan una calificación inferior a este porcentaje de aprobación, se les dará una retroalimentación y volverán a presentar la evaluación con una aprobación de aceptación del 100%.

Kushki realiza una capacitación a los terceros conforme su naturaleza, ejecutará un listado de asistencia y unas preguntas para evaluar la participación de éstos. Siendo la responsabilidad de la empresa demostrar la gestión realizada.

12 DOCUMENTACIÓN Y DIVULGACIÓN

El presente manual y sus respectivos documentos relacionados deben reposar en la herramienta de gestión documental; así mismo el área de Procesos es el encargado de divulgar las respectivas actualizaciones.

Adicionalmente se relacionan los documentos:

- Acta donde conste la aprobación del manual diseñado para la prevención del lavado de activos y financiación del terrorismo.
- Los documentos y registros que soportan el diseño, desarrollo e implementación de las metodologías en materia de prevención de lavado de activos y financiamiento de delitos, como el terrorismo.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

- Los documentos que soportan las operaciones inusuales y sospechosas en los países donde aplique la normativa.
- Los informes trimestrales realizados por el Oficial de Cumplimiento donde la regulación lo exija.
- Toda la documentación adicional que soporte la implementación y actualización del programa.

Kushki conserva, de acuerdo con las condiciones establecidas en las normas locales, los siguientes documentos durante al menos diez (10) años, salvo que la legislación local de cada país o la política de Kushki sobre conservación de documentos especifiquen un periodo más largo:

- Los formularios de vinculación de los comercios afiliados cuando sea aplicable.
- Los informes presentados ante las autoridades gubernamentales sobre actividades sospechosas de un cliente relacionadas con un posible caso de lavado de dinero u otra conducta delictiva, junto con la documentación que respalde tales suposiciones.
- Registros de todos los cursos impartidos sobre el lavado de dinero incluidos los nombres, niveles y unidades de los negocios de los participantes, así como las fechas y lugares en que se impartió la formación.
- Registro debida diligencia y conocimiento del cliente contiene la información que los clientes entreguen por medio del proceso de afiliación y se especificará si dicho cliente es de alto o bajo riesgo para efectos de tomar medidas de debida diligencia intensificada.
- Registro de operaciones realizadas por Personas Expuestas Políticamente (PEP): contiene la información relativa a toda operación llevada a cabo por alguna persona que se incluya dentro de la definición de PEP.
- Cualquier otro documento que sea necesario conservar en virtud de las leyes aplicables contra el lavado de dinero, en cada país.

13 REPORTES

Un componente clave del Programa para la prevención del lavado de activos y la financiación del terrorismo de Kushki es la presentación de los reportes regulatorios en los países donde la normativa lo exija. Por lo tanto, todos los empleados, oficiales y directores son responsables de comunicar oportuna y adecuadamente el conocimiento que tengan de cualquier incidencia de incumplimiento o de operaciones inusuales a través de los canales oficiales dispuestos por la compañía.

Además, son responsables de notificar oportuna y adecuadamente cualquier problema o deficiencia que se perciba en las políticas, procedimientos, prácticas o sistemas y pueda conducir al incumplimiento de las políticas de Kushki o las disposiciones legales.

13.1 Canal de denuncia

Kushki cuenta con canales de denuncia donde se le garantiza el anonimato, facilitando el reporte de situaciones sospechosas, donde se pueda ver involucrado un empleado, proveedor, cliente y/o cualquier tercero que se relacione de forma directa o indirecta con la empresa. El denunciante puede elegir cualquiera de las siguientes alternativas para ejecutar una eventual denuncia.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

13.1.1 Vía correo electrónico

La primera alternativa es escribiendo al correo lineaetica@kushkipagos.com, en el asunto del correo se solicita que se escriba cuál es la conducta que se quiere reportar. En el cuerpo del correo es necesario que se describa de manera detallada los hechos que se suscitaron y no olvidar los siguientes aspectos fundamentales:

- Quien realizó la conducta.
- Área y cargo de la persona relacionada en la conducta a reportar (de no contar con esta información, favor de incluir algún otro dato que permita identificar a la persona en cuestión).
- Fechas de los hechos y si es posible también la hora aproximada en que sucedieron.
- Si se tiene alguna evidencia favor de adjuntarla en el correo.
- En el evento que se requieran mayores antecedentes desde la denuncia el Oficial de Cumplimiento se contactará con usted, garantizando la confidencialidad y anonimato del denunciante.

13.1.2 Vía web

La segunda forma del reporte es ingresando al siguiente link: https://www.kushki.com/gobcorp/. En este portal se puede realizar la denuncia deseada, siguiendo una serie de pasos que la propia página de forma intuitiva va indicando.

Figura 13.1
Reporte vía web

13.2 Responsabilidad

La responsabilidad de asegurar que se elaboren y presenten los informes sobre asuntos relativos al lavado de activos y la financiación del terrorismo recae en el Jefe o Director de la Alta Dirección, área o unidad. Siguiendo atentamente las normas e instrucciones señaladas en este Manual junto con las políticas y los procedimientos que se detallan en otros manuales y la documentación

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

de operaciones, los empleados estarán protegidos de cualquier responsabilidad civil y criminal cuando se informe alguna operación a las autoridades reguladoras.

La presentación de informes tiene como propósito:

- Mantener al Consejo Directivo informado sobre los asuntos y riesgos significativos.
- Mantener al área de Compliance en conocimiento de los asuntos que existan en torno al lavado de activos y el financiamiento de actividades terroristas, de modo que puedan adoptar las medidas correctivas convenientes, según se requiera.
- Concentrar la atención y fomentar la disciplina con respecto al cumplimiento continuo de las normas preventivas contra el lavado de activos y la financiación del terrorismo dentro de Kushki.
- Cumplir con las disposiciones reglamentarias de notificar las actividades inusuales (p. ej. La sospecha de lavado de activos o de financiamiento de actividades terroristas).

13.3 Reporte de operaciones sospechosas (ROS)

Corresponde a Kushki reportar a las unidades de Inteligencia Financiera en forma inmediata las operaciones que se determinen como sospechosas, de acuerdo con las normativas locales de cada país.

13.4 Reportes internos

Todos los empleados de Kushki se encuentran obligados a realizar los siguientes reportes internos:

- Reporte internos sobre operaciones inusuales: a través de los canales dispuestos para este fin (Slack, correo electrónico compliance@kushki.com y/o la línea ética).
- Reporte interno sobre operaciones sospechosas.
- Reportes de la etapa de monitoreo: como resultado del monitoreo, el Especialista de Cumplimiento elabora un informe mensual sobre este tema.
- Reportes mensual compliance: el Oficial de Cumplimiento mensualmente dirige un reporte al Chief Governance & Compliance Officer con la gestión.
- Reporte trimestral al Consejo Directivo.
- Reporte anual de gestión a la Asamblea General de Accionistas.

13.5 Confidencialidad de la información

Toda la información que Kushki mantenga de sus clientes y operaciones en las bases de datos, o en cualquier registro, es estrictamente confidencial. De esta forma, Kushki vela para que los funcionarios que tengan acceso a esta información sean solamente aquellos que, debido a su cargo o posición, tengan los permisos necesarios para acceder a la misma.

Kushki, sus colaboradores, socios y gerentes, tienen la prohibición de informar al afectado o a terceras personas acerca de la circunstancia de haberse requerido o remitido información a la Unidad de Análisis Financiero como, asimismo proporcionarle cualquier otro antecedente al respecto.

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

14 INFRAESTRUCTURA TECNOLÓGICA

Kushki vela porque las áreas involucradas en el proceso de administración del riesgo de lavado de activos y financiamiento de delitos, como el terrorismo, cuenten con las herramientas tecnológicas necesarias, en aras de velar por el estricto cumplimiento de lo estipulado en el presente manual.

15 CONSECUENCIAS DEL INCUMPLIMIENTO

El incumplimiento de las políticas, procesos y controles establecidos en el presente manual y en general en las normas relacionadas con la prevención del riesgo de lavado de activos y financiamiento de delitos, como el terrorismo, puede generar sanciones indicadas en el **GRH-CO-0101-KU** Código de ética y conducta para todos los colaboradores, socios o terceros que las incumplan dentro del rol que desempeñan en la entidad.

A continuación, se detallan algunas consecuencias derivadas del incumplimiento a procesos establecidos en esta materia:

- Sanciones penales, multas y penas privativas de la libertad de acuerdo con lo establecido en el código penal y leyes vigentes de cada país donde Kushki tiene presencia, aplicables tanto a personas naturales como jurídicas, cuando éstas incumplan las obligaciones legales para prevenir el lavado de activos y el financiamiento del terrorismo.
- Sanciones laborales, las cuales podrían ir incluso hasta la terminación del contrato de trabajo, si se demuestra, después de la respectiva investigación que el empleado incurrió en cualquier de las siguientes faltas:
  - Incumplimiento de las políticas y procesos contenidos en el presente documento o al código de ética y conducta.
  - Revelar al establecimiento de comercio sobre gestiones administrativas o judiciales que adelanten en su contra.
  - Desatender requerimientos de las autoridades competentes.
  - Permitir el ocultamiento de dineros provenientes de actividades ilícitas.

16 REFERENCIAS

- GGC-PL-0401-KU Política para la gestión de riesgos corporativos

17 DOCUMENTOS RELACIONADOS

- GRH-CO-0101-KU Código de ética y conducta
- GGC-PD-0103-KU Debida diligencia intensificada
- GGC-IN-0104-KU Mapeo de negocios riesgosos y prohibidos
- GGC-FO-0107-KU Formulario de declaración beneficiario final
- GGC-DG-0102-CO PLA regional Colombia
- GGC-DG-0103-EC PLA regional Ecuador
- GGC-DG-0104-CL PLA regional Chile
- GGC-DG-0105-PE PLA regional Perú

DocuSign Envelope ID: 9781BF50-3317-4394-BE93-22942EDDC703

- GGC-DG-0106-MX PLA regional México
- GGC-DG-0107-BR PLA regional Brasil

18 CONTROL DE CAMBIOS

Versión	Fecha	Cambios realizados
V4	16/02/2021	*Ajustes en cumplimiento de la normatividad chilena en materia de prevención de Lavado de activos y Financiación del terrorismo. *Ajustes conforme recomendaciones dadas por la Auditoría Externa BDO.
V5	20/12/2021	3. Se actualiza el código del procedimiento DDC. 10.1.5. Se especifica las consideraciones de beneficiario final en Chile y Colombia. 10.5. Se indica que las señales de alerta toman como guía lo especificado por la UAF. 13.1. Se agrega el capítulo del canal de denuncia en Kushki. 13.3. Se complementa el segundo párrafo referente a requisitos de Chile. 13.4. Se agrega los pasos para rectificar un ROE. 16. Se actualiza la lista de documentos referenciados.
V6	02/06/2022	2. El marco normativo se amplía a todas las subsidiarias de Kushki. Se incluye dentro del sistema de PLA la proliferación de armas de destrucción masiva y se indica que el sistema se basa también en recomendaciones de las UIF. Se elimina la tabla con el marco regulatorio por país. 3. Se amplía el alcance a todas las subsidiarias de Kushki. 4. Se elimina el concepto de DDC, Encargado de prevención de delitos, países con régimen tributario preferente, ROE y UAF. Se actualiza la definición de lavado de activos y operación sospechosa. 5. Se modifica la Figura 5.1. 6. Se actualiza las funciones y responsabilidades del Board Directors, CCO, Oficial de Cumplimiento, Especialista de Compliance y del Comité Interno de Compliance. Se agregan las funciones del Chief Risk Officer /Head Risk & Compliance, Jefe de Monitoreo Transaccional y Auxiliar de Monitoreo Transaccional. Comité interno de Compliance. Se eliminan las funciones del representante legal, Encargado de Prevención de Delito, Revisor Fiscal y los requisitos para el Oficial de Cumplimiento. 7. Se indica que Kushki no establece relaciones comerciales con clientes que lleven a cabo transacciones derivadas de campañas políticas y/o partidos políticos 8.8.3. Se actualiza el nombre del Comité de Riesgos a Comité SRCC. 10.1.2. Se actualiza la periodicidad de la consulta de los colaboradores en listas de semestral a anual. Se agrega el correo de Billpocket. 10.1.3. Se indica que las consultas en listas de los proveedores se realizar previo y posterior a su vinculación. 10.1.4. Se actualiza la periodicidad de la consulta de los accionistas en listas de semestral a anual. 10.1.5. Se actualiza el procedimiento para beneficiario final. 10.2. La aprobación de PEP la da la instancia superior de Sales. 10.3. Se indica que el KAM y área de Soporte también podrían comunicar la cancelación de servicios al cliente. 10.5 Se agrega el correo para denuncias y una instancia para situaciones particulares inusuales. Se agrega como señal de alerta cambios en cuentas bancarias en periodos cortos. 10. Se elimina el capítulo de procedimientos para el registro de transacciones de clientes, específicos para Chile. 11. Se incluye la capacitación a terceros. 12. La gestión documental es responsabilidad del área de Procesos. 13.1. Se indica que el canal de denuncia garantiza el anonimato. 13.3 Se actualiza el reporte de operaciones sospechosas. 15. Se eliminan las sanciones que aplican en Chile