PAGOS NACIONALES S.A.C.
Noviembre 2023

POLÍTICA PARA LA PREVENCIÓN DE LAVADO DE ACTIVOS

Propósito

El presente documento establece los principios y normas de cumplimiento y gestión de los riesgos asociados a los delitos financieros en PAGOS NACIONALES S.A.C. La finalidad de este documento es evitar que PAGOS NACIONALES S.A.C. sea utilizada para cometer delitos financieros, cumplir con todos los requisitos legales aplicables y garantizar que PAGOS NACIONALES S.A.C. adopte las medidas más adecuadas para mitigar los riesgos asociados a los delitos financieros.

El presente documento describe los requisitos legales aplicables en materia de delitos financieros a los que PAGOS NACIONALES S.A.C. debe adherirse, así como las medidas internas que PAGOS NACIONALES S.A.C. establece para garantizar el cumplimiento de dichos requisitos legales. Este documento se denomina Política para la Prevención de Lavado de Activos (*Anti-Money Laundering, AML*), Contra el Financiamiento del Terrorismo (*Counter-Terrorist Financing, CTF*), Contra el Financiamiento de la Proliferación (*Counter Proliferation Financing, CPF*) y de Sanciones (la "Política") y establece los parámetros para PAGOS NACIONALES S.A.C. en relación con el marco *AML*, *CTF*, *CPF* y de sanciones.

Ámbito de aplicación

La Política se aplica a todos los empleados de PAGOS NACIONALES S.A.C., a todas las unidades de PAGOS NACIONALES S.A.C., a la alta dirección, a los corresponsales extranjeros, a los contratistas y a los terceros con los que PAGOS NACIONALES S.A.C. pueda contratar.

El objetivo de PAGOS NACIONALES S.A.C. no es sólo cumplir con los requisitos legales pertinentes, sino también mitigar y reducir el riesgo potencial para PAGOS NACIONALES S.A.C. de que nuestros clientes utilicen nuestros productos, servicios y canales de entrega para blanquear el producto de actividades ilegales, financiar actividades terroristas o llevar a cabo actividades prohibidas por sanciones financieras.

La Política se actualiza al menos una vez al año, o con mayor frecuencia en función de los requisitos internacionales y los cambios legislativos, la Ley No. 27693 sobre el Sistema de Prevención del Lavado de Activos y Financiamiento del Terorismo (SPLAFT), la Resolución SBS No. 789-2018, su reglamentación y toda regulación, modificación y actualización en la materia.

Definiciones

En general, el blanqueo de capitales se define como la realización de actos destinados a ocultar o encubrir el verdadero origen de las ganancias obtenidas mediante actividades delictivas, de modo que parezca que las ganancias ilícitas proceden de orígenes legítimos o constituyen activos legítimos. Generalmente, el blanqueo de capitales se produce en tres etapas:

- Colocación: El efectivo generado por las actividades delictivas se convierte en instrumentos monetarios, como giros postales o cheques de viaje, o se deposita en cuentas de entidades financieras.

- Estratificación: Los fondos se transfieren o trasladan a otras cuentas u otras instituciones financieras para separar aún más el dinero de su origen delictivo.
- Integración: Los fondos se reintroducen en la economía y se utilizan para adquirir activos legítimos o para financiar otras actividades delictivas o negocios legítimos.

También cubre el dinero, independientemente de cómo se adquiera, que se utilice para financiar el terrorismo. La financiación del terrorismo puede no implicar el producto de una conducta delictiva, sino más bien un intento de ocultar el origen o el uso previsto de los fondos, que posteriormente se utilizarán con fines delictivos.

La financiación del terrorismo se refiere a la recaudación o tenencia de fondos (directa o indirectamente) con la intención de que esos fondos se utilicen para llevar a cabo actividades definidas como actos de terrorismo o con la intención de disponer de esos fondos para un grupo terrorista o un terrorista distinto.

La financiación de la proliferación se refiere al acto de proporcionar fondos o servicios financieros que se utilizan, en su totalidad o en parte, para la fabricación, adquisición, posesión, desarrollo, exportación, transbordo, corretaje, transporte, transferencia, almacenamiento o uso de armas nucleares, químicas o biológicas y sus sistemas vectores y materiales relacionados (incluidas tanto las tecnologías como los bienes de doble uso utilizados para fines no legítimos), contraviniendo las leyes nacionales o, en su caso, las obligaciones internacionales.

Los bienes de origen delictivo son el producto de una conducta delictiva. Esto incluye cualquier tipo de conducta, dondequiera que tenga lugar, que constituiría un delito si se cometiera en PAGOS NACIONALES S.A.C. Incluye el narcotráfico, la actividad terrorista, la evasión fiscal, la corrupción, el fraude, la falsificación, el robo, la falsificación, el correo negro y la extorsión. También incluye cualquier otro delito que se cometa con ánimo de lucro.

Las sanciones son decisiones políticas y económicas que forman parte de los esfuerzos diplomáticos de los países y las organizaciones multilaterales o regionales contra Estados u organizaciones, bien para proteger los intereses de seguridad nacional, bien para proteger el derecho internacional y defenderse de las amenazas a la paz y la seguridad internacionales. Las sanciones pueden ser:

a) Específicas, es decir, relacionadas con listas específicas de personas, entidades jurídicas, organizaciones, buques, etc. (por ejemplo, el Departamento del Tesoro de EE.UU. se refiere a algunas de estas entidades como *Specially Designated Nationals* (Nacionales Especialmente Designados)).

b) General, es decir, cubrir todas las transacciones con determinados países o jurisdicciones; determinadas transacciones con países o jurisdicciones, como exportaciones, importaciones o nuevas inversiones, o todas las transacciones dentro de un determinado ámbito de actividad/productos (por ejemplo, venta de armas a un país concreto).

c) Sectoriales, es decir, cubren a determinadas partes en sectores específicos (por ejemplo, la OFAC designa a las partes en una Lista de Identificación de Sanciones Sectoriales (*Sectoral Sanctions Identifications (SSI) List*), pero sólo restringen determinadas transacciones de estas partes designadas.

<u>Ley No. 27693 sobre el Sistema de Prevención del Lavado de Activos y Financiamiento del Terorismo (SPLAFT)</u>

En virtud de la Ley No. 27693 sobre el Sistema de Prevención del Lavado de Activos y Financiamiento del Terorismo (SPLAFT) y la Resolución SBS No. 789-2018, se debe establecer un programa de cumplimiento de las normas PLD/FT acorde a los siguientes requisitos, incluyendo:

- el nombramiento de una persona responsable del programa de cumplimiento;
- el desarrollo y la aplicación de políticas y procedimientos de cumplimiento actualizados y aprobados por un alto cargo;
- un programa para evaluar el riesgo de que se cometa un delito de lavado de activos o de financiación del terrorismo a través de la empresa, y la aplicación de medidas para mitigar las situaciones de alto riesgo;
- un programa escrito de formación continua en materia de cumplimiento para los empleados de PAGOS NACIONALES S.A.C.;
- una revisión de las políticas y procedimientos para comprobar su eficacia, que realizará cada dos años un auditor interno o externo;

La regulación local y la última redacción de las recomendaciones del GAFI establecen el requisito de que las empresas pertinentes establezcan y mantengan políticas y procedimientos adecuados y sensibles al riesgo en relación con:

- Diligencia debida con respecto al cliente
- Informes
- Mantenimiento de registros
- Control interno
- Evaluación y gestión de riesgos (enfoque basado en el riesgo)
- El control y la gestión del cumplimiento, y
- La comunicación interna de dichas políticas y procedimientos, con el fin de prevenir las actividades relacionadas con el blanqueo de capitales y la financiación del terrorismo y la proliferación.

Estas políticas y procedimientos deben:

- Identificar y examinar
  - Transacciones complejas o inusualmente grandes
  - Patrones inusuales de transacciones que no tienen un propósito económico aparente o lícito visible.
  - Cualquier otra actividad que pueda considerarse relacionada con el blanqueo de capitales, la financiación del terrorismo o la financiación de la proliferación.
- Especificar las medidas adicionales que se adoptarán para impedir la utilización de productos y transacciones que favorezcan el anonimato para el blanqueo de capitales o la financiación del terrorismo.
- Determinar si un cliente es una persona del medio político (véase el anexo 2 para la definición y otras orientaciones).
- Designar a una persona de la organización para que cumpla y reciba información en virtud de la Ley sobre el Blanqueo de Capitales y la Financiación del Terrorismo (PCMLTFA) y los Reglamentos asociados.
- Asegurarse de que los empleados informan de cualquier actividad sospechosa al funcionario designado, y

- Garantizar que el Responsable designado examine dichos informes internos a la luz de la información disponible y determine si dan lugar a conocimiento o sospecha o a motivos razonables para conocer o sospechar de blanqueo de capitales o financiación del terrorismo.

Los principios fundamentales de la Ley y los reglamentos conexos pueden describirse como enfoque basado en el riesgo (RBA). El RBA exige que se tomen varias medidas para determinar la forma más rentable y proporcionada de gestionar y mitigar los riesgos de blanqueo de capitales, financiación del terrorismo, financiación de la proliferación y violación de sanciones a los que se enfrenta la empresa. Los pasos son:

- Identificar los riesgos de lavado de activos, financiación del terrorismo, financiación de la proliferación y violación de sanciones que afectan a la empresa.
- Evaluar los riesgos que presenta el particular:
  - Clientes: tipos y comportamiento;
  - Productos y servicios;
  - Canales de entrega, por ejemplo, efectivo en ventanilla, electrónico, transferencia bancaria o cheque;
  - Zonas geográficas de operación, por ejemplo, ubicación de los locales comerciales, origen o destino de los fondos de los clientes;
  - Complejidad y volumen de las transacciones;
- Diseñar y aplicar controles para gestionar y mitigar estos riesgos evaluados.
- Supervisar y mejorar el funcionamiento eficaz de estos controles y
- Registrar adecuadamente lo que se ha hecho y por qué

Véase el Anexo 1 para una explicación detallada del Enfoque Basado en el Riesgo.

¿Dónde puedo encontrar más información?

Consulte la siguiente página web, que contiene información detallada sobre las distintas cuestiones tratadas en este documento y puede resultarle útil durante su estancia con nosotros:

1. La Unidad de Información Financiera del Perú (UIF): https://www.sbs.gob.pe/prevencion-de-lavado-activos
2. Grupo de Acción Financiera Internacional (GAFI): www.fatf-gafi.org
3. Oficina de Control de Activos Extranjeros (OFAC): www.treasury.gov/ofac
4. Lista consultiva de la Red para la represión de los delitos financieros (FinCEN): www.fincen.gov

<u>Términos</u>

Son términos con los que debe estar familiarizado.

Términos/Acrónimos	Definición
Funcionario designado	Un Nominated Officer (también conocido como MLR officer o AML Compliance Officer) es el punto focal dentro de la empresa para la supervisión de toda la actividad relacionada con cuestiones de lucha contra la delincuencia financiera.

Oficial de apoyo	Persona o personas designadas para actuar en nombre del funcionario designado.
AML	Lucha contra el blanqueo de capitales
KYB	Conozca su negocio
KYC	Conozca a su cliente
CDD	Diligencia debida sobre el cliente
EDD	Diligencia debida reforzada
SPLAFT	Ley No. 27693 sobre el Sistema de Prevención del Lavado de Activos y Financiamiento del Terorismo
PEP	Personas políticamente expuestas
ROS	Reporte de Operaciones Sospechosas
SWIFT	Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales
OFAC	Oficina de Control de Activos Extranjeros
GAFI	Grupo de Acción Financiera Internacional
FinCEN	Red para la represión de los delitos financieros
UBO	Propietario beneficiario final
UE	La Unión Europea
ONU	Naciones Unidas
RBA	Enfoque basado en el riesgo
CTF	Lucha contra la financiación del terrorismo
CPF	Financiación de la lucha contra la proliferación
CRA	Agencia Tributaria
UIF	Unidad de Información Financiera

Nuestros productos y servicios

PAGOS NACIONALES S.A.C. se centra en la prestación de servicios comerciales o servicios de procesamiento de tarjetas de pago para varios comerciantes de comercio electrónico incorporados en todo el mundo y que hacen negocios en todo el mundo en el cumplimiento del Código de Conducta para la Industria de Tarjetas de Crédito y Débito en PAGOS NACIONALES S.A.C. y otros

requisitos legales. Para gestionar nuestro riesgo de manera efectiva y cumplir con las listas de cumplimiento y sanciones, todos los clientes y sus negocios serán verificados en las sanciones de la ONU, la Lista de Sanciones de la OFAC, las listas y programas de Visa Inc. y MasterCard Worldwide, etc.

Servicios comerciales

Los servicios a comercios o el procesamiento de tarjetas de pago es la gestión de transacciones de pago electrónico para comercios. Las actividades de procesamiento para comerciantes implican obtener información de ventas del comerciante, recibir autorización para la transacción, recaudar fondos del banco emisor de la tarjeta de pago y enviar el pago al comerciante.

La transferencia real de fondos al comerciante o la liquidación se realizarán de forma posterior. Al final de cada día, el comerciante generalmente revisará las ventas, créditos y anulaciones del día. Una vez verificado esto, el comerciante cerrará su lote, o el lote se cerrará automáticamente. Esto implica cerrar las ventas del día y transmitir la información para su depósito en la plataforma de PAGOS NACIONALES S.A.C., y luego al banco. El banco adquirente encamina la transacción a través del sistema de liquidación correspondiente contra el banco emisor de la tarjeta correspondiente.

A continuación, el banco emisor de la tarjeta devuelve el dinero a través del sistema de liquidación (Visa, MasterCard, etc.) por el importe del giro de venta, menos la correspondiente "tasa de intercambio", a la cuenta del banco adquirente. A continuación, el banco adquirente ingresa el importe, menos la "comisión de descuento", en la cuenta bancaria segregada de clientes de PAGOS NACIONALES S.A.C.

PAGOS NACIONALES S.A.C. entonces deposita la cantidad menos la "comisión de descuento" a la cuenta del Comerciante una vez cada 2-7 días hábiles. Generalmente, dentro de 24-72 horas, los comerciantes tendrán su dinero. PAGOS NACIONALES S.A.C. puede ofrecer a algunos Comerciantes de bajo riesgo "financiación al día siguiente".

El procedimiento de liquidación varía en la fase inicial en función del programa en el que esté inscrito el comerciante. Una agencia de hoteles, viajes o alquiler de coches puede querer obtener una pre-aprobación antes de que el cliente se registre o utilice el servicio. En PAGOS NACIONALES S.A.C., tenemos muchos programas pre-construidos que cualquier comerciante puede solicitar en función de su tipo de negocio.

Vales electrónicos

Un vale electrónico es un vale electrónico de valor almacenado que puede generarse en tiempo real desde un sitio web. El usuario puede canjearlo a través de las interfaces de los comercios. Una vez canjeado, el valor del vale electrónico se transfiere a la cuenta del comerciante y los fondos están disponibles al instante para su uso.

Los vales electrónicos pueden ser utilizados por los comerciantes en cualquier situación que requiera que sus clientes carguen valor en su cuenta, lo que permite cargar efectivo en esa cuenta en forma de vale comprado. Pueden utilizarse para cargar tarjetas de pago, transferir dinero a un monedero electrónico, recargar una cuenta de juego en línea o cualquier otro tipo de cuenta que esté integrada en la plataforma.

Controles internos y comunicación

La ey No. 27693 sobre el Sistema de Prevención del Lavado de Activos y Financiamiento del Terorismo (SPLAFT) exige que las empresas dispongan de sistemas adecuados de control interno y comunicación para prevenir las actividades relacionadas con el lavado de activos y el financiamiento del terrorismo. En términos sencillos, esto significa que las empresas deben asegurarse de que se establezcan controles de gestión que alerten a las personas pertinentes de la empresa sobre la posibilidad de que los delincuentes puedan estar intentando utilizar la empresa para blanquear dinero o financiar el terrorismo o financiar la proliferación o violar sanciones, a fin de permitirles tomar las medidas adecuadas para evitarlo o denunciarlo.

Los sistemas de control interno y comunicación deben ser capaces de identificar transacciones o actividades de clientes inusuales o sospechosas, de identificar transacciones y relaciones comerciales especificadas en una dirección emitida por el regulador. PAGOS NACIONALES S.A.C. debe informar de las transacciones sospechosas en virtud de la Ley y los reglamentos conexos.

La naturaleza y el alcance de los sistemas y controles que la empresa necesita implantar dependen de diversos factores, entre ellos:

- Grado de riesgo asociado a cada área de su actividad
- Naturaleza, escala y complejidad de la empresa
- Tipo de productos, clientes y actividades
- Diversidad de operaciones, incluida la diversidad geográfica
- Volumen y tamaño de las transacciones
- Canales de distribución.

Por ello, PAGOS NACIONALES S.A.C. ha establecido un procedimiento de control interno. La base del proceso de control interno son las autorizaciones bien definidas, la segregación de funciones, la identificación de clientes, la diligencia debida permanente, la notificación de sospechas, etc. PAGOS NACIONALES S.A.C. no dispone de una unidad de auditoría interna, sin embargo PAGOS NACIONALES S.A.C. tiene previsto realizar una auditoría no menos de una vez cada dos años, formando un grupo de tres empleados que trabajen en departamentos no relacionados, a menos que PAGOS NACIONALES S.A.C. considere apropiado un ciclo de rotación más largo. La decisión de los participantes del grupo formado y de la auditoría es tomada por el directorio de la empresa.

PAGOS NACIONALES S.A.C. supervisa regularmente los cambios y el cumplimiento de la legislación pertinente y otros requisitos legales con el fin de mitigar los riesgos de blanqueo de capitales y financiación del terrorismo y de financiación de la proliferación y violación de sanciones, así como para hacer más eficientes los procedimientos de control interno.

El Responsable de Información sobre Blanqueo de Capitales (Responsable designado)

Un funcionario designado es la persona dentro de una organización que se encarga de supervisar todas las actividades relacionadas con la lucha contra el lavado de activos Familiarícese con el personal que figura a continuación, ya que deberá trabajar en estrecha colaboración con él.

El directivo designado por la empresa es Candela Gutiérrez.

En ausencia del Responsable designado, los Responsables designados de apoyo ocuparán su lugar.

El directivo designado de apoyo de la empresa es Candela Gutierrez.

Los Funcionarios Designados de PAGOS NACIONALES S.A.C. deben mantenerse al día con las normas y riesgos ALD/CFT. Si los Funcionarios Designados se ocupan de cuestiones regulatorias cotidianas, los cambios en los requisitos ALD/ATF, pueden no tener tiempo suficiente para mantener los conocimientos necesarios para supervisar un régimen ALD/ATF eficaz. Si este es el caso, PAGOS NACIONALES S.A.C. puede considerar la designación de un individuo calificado diferente como Oficial Nominado.

Entre sus responsabilidades se incluyen las siguientes:

- Recepción de comunicaciones de los empleados (también conocidas como transacciones sospechosas)
  Informe - STR's).
- Revisar todas las nuevas leyes y decidir cómo repercuten en el proceso operativo de la empresa.
- Preparar un manual de procedimientos por escrito y ponerlo a disposición de todo el personal y otras partes interesadas.
- Asegurarse de que se lleva a cabo la diligencia debida con los clientes y socios comerciales.
- Recepción de informes internos sobre transacciones sospechosas (ROS) por parte del personal
- Decidir qué ROS internos deben notificarse a la UIF, RCMP o CSIS.
- Registrar adecuadamente todas las decisiones relativas a los ROS.
- Garantizar que el personal reciba formación contra la delincuencia financiera en el momento de su incorporación y que reciba formación periódica de reciclaje.
- Seguimiento de las relaciones comerciales y registro de las revisiones y decisiones adoptadas
- Tomar decisiones sobre la continuación o el cese de la actividad comercial con determinados clientes.
- Asegurarse de que todos los registros comerciales se conservan durante al menos cinco años a partir de la fecha de la última transacción con el cliente, de acuerdo con la normativa UIF.

El Responsable designado es una persona con autoridad y autonomía suficientes para tomar las decisiones requeridas anteriormente. El Responsable designado de apoyo sustituirá al Responsable designado cuando éste no esté disponible.

Formación del personal e informes

PAGOS NACIONALES S.A.C. mantiene un programa de formación continua de los empleados para que el personal esté adecuadamente formado en los procedimientos KYC y para que el personal sea consciente de los diferentes patrones y técnicas posibles de blanqueo de capitales que pueden darse en su actividad diaria. Los requisitos de formación deben tener un enfoque diferente para el personal nuevo, el personal de primera línea, el personal de cumplimiento o el personal que trata con nuevos clientes/comerciantes. El personal nuevo recibe formación sobre la importancia de las políticas KYC y los requisitos básicos de la empresa. La formación se imparte a todos los miembros del personal al comienzo de la toma de posesión del cargo en PAGOS NACIONALES S.A.C. y en ocasiones regulares posteriormente (al menos una vez al año).

Los miembros del personal que tratan directamente con los clientes reciben formación para verificar la identidad de los nuevos clientes, ejercer la diligencia debida en el manejo de las cuentas de los clientes existentes de forma continua y detectar patrones de actividad sospechosa. La formación también abarca las obligaciones generales derivadas de los requisitos externos (legales y reglamentarios) e internos aplicables y las obligaciones individuales resultantes que deben cumplirse en la actividad cotidiana, así como tipologías para reconocer actividades de blanqueo de capitales o delitos financieros o tipologías de infracción de sanciones.

Se imparten cursos de actualización periódicos para garantizar que los empleados recuerden sus responsabilidades y se mantengan informados de las novedades. Es crucial que todo el personal pertinente comprenda plenamente la necesidad de las políticas KYC y las aplique de forma coherente. Una cultura dentro de los servicios que promueva dicha comprensión es la clave de una aplicación satisfactoria.

La formación abarca las siguientes cuestiones:

- La legislación relativa a los delitos financieros;
- Riesgos asociados a la amenaza de la delincuencia financiera para la empresa (véase, por ejemplo, www.egmont group.org);
- Identidad y responsabilidades del funcionario designado;
- Establecimiento de políticas y procedimientos internos;
- Diligencia debida sobre el cliente/Medidas reforzadas de supervisión de la diligencia debida;
- Actividad sospechosa: qué hay que tener en cuenta;
- Cómo presentar un informe interno sobre transacciones sospechosas al funcionario designado;
- Requisitos de registro;
- Posible infracción de sanciones: qué hay que tener en cuenta;

El Responsable designado llevará un registro de toda la formación impartida a los miembros del personal.

Todo el personal deberá firmar el registro de formación cuando sea necesario para confirmar que ha recibido la formación.

El Responsable designado distribuirá a todo el personal otro material para aumentar la concienciación sobre las cuestiones relativas a la lucha contra la delincuencia financiera. Este material deberá colocarse en el tablón de anuncios de la empresa, que deberá estar disponible en todas las sedes de la empresa.

El Funcionario Designado será responsable de incluir en su Informe Anual la información relativa a su(s) programa(s) de educación y formación a los que haya asistido durante el año.

PAGOS NACIONALES S.A.C. utilizará las posibilidades de aprendizaje ofrecidas por organizaciones conocidas y acreditadas (por ejemplo ACCP, ACAMS, ICA).

Papel del empleado

En caso de que un empleado tenga sospechas sobre un cliente o una transacción, debe asegurarse de que el Responsable designado por la empresa sea informado de sus sospechas lo antes posible.

El personal debe utilizar el ROS interno (véase el Anexo).

El ROS debe contener como mínimo la siguiente información:

- Fecha/hora de la transacción
- Importe
- Nombre del cliente/información de identificación del cliente (por ejemplo, número de pasaporte, etc.)
- Número de transacción
- Motivo de sospecha de la transacción

En caso de duda, el miembro del personal debe llamar al funcionario designado para discutir las razones de su sospecha, pero debe tener cuidado de no hacerlo mientras el cliente está de pie delante de él (de lo contrario podría "avisar" al cliente, véase más abajo).

El momento oportuno para presentar el ROS interno es importante. La ley establece que una persona que trabaje en el sector regulado debe presentar una denuncia en cuanto tenga sospechas. Esto puede significar antes de que se produzca la transacción o inmediatamente después.

No obstante, el personal puede decidir que, si solicita el consentimiento para una transacción concreta (es decir, antes de que se realice la transacción), existe el riesgo de que el cliente reciba un "advertencia". Más adelante encontrará más información sobre advertencias.

Todos los miembros del personal habrán cumplido plenamente sus obligaciones, y gozarán de la plena protección de la ley, una vez que hayan comunicado sus sospechas al Responsable designado de la empresa.

Una vez que el funcionario designado recibe el ROS interno del funcionario, tiene dos opciones:

- Informar del ROS a UIF.
- Presentar una nota interna indicando por qué, sobre la base de la revisión de las circunstancias en torno a la transacción, se considera que no es necesario hacer un informe a UIF. El funcionario designado debe rellenar el formulario de resolución de ROS del funcionario designado en caso de que decida no presentar una denuncia.

<u>Preguntas más frecuentes (FAQ)</u>

¿En qué circunstancias podría cometer una infracción?

En caso de que un empleado tenga sospechas sobre un cliente o una transacción, debe asegurarse de que el Responsable designado por la empresa sea informado de sus sospechas lo antes posible.

Se puede cometer una infracción:

- si el empleado no sigue los procedimientos KYC aceptados por el funcionario designado
- si se detecta una violación flagrante de los procedimientos AML, KYC ¿Qué

quiere decir con "sospecha"?

La sospecha puede darse en circunstancias que sugieran a una persona razonable que una persona podría estar blanqueando dinero o financiando el terrorismo o la proliferación de la financiación o violar el régimen de sanciones. La sospecha debe ser algo más que una simple corazonada. Cualquier

actividad que no se ajuste al curso normal de los negocios o que no sea normal para un cliente concreto debe considerarse sospechosa.

¿Qué entiende por transacción?

Una transacción es cualquier cosa que se realiza a modo de negocio.

Los indicadores de sospecha para nuevos clientes pueden incluir:

- Comprobar su identidad está resultando difícil;
- El cliente es reacio a facilitar datos sobre su identidad;
- No hay ninguna razón real para que el cliente utilice los servicios de un comerciante;
- Cuando las transacciones implican transferencias internacionales o divisas, la explicación del negocio y el importe implicado no son razonables;

Los indicadores de sospecha para los clientes habituales y establecidos incluyen los:

- La transacción es diferente de la actividad normal del cliente;
- El tamaño y la frecuencia de la transacción no son coherentes con las actividades normales del cliente;
- El patrón de transacciones ha cambiado desde que se estableció la relación comercial;

¿Cómo comunico mi sospecha al funcionario designado?

Deberá comunicar los motivos de su sospecha a su responsable designado de acuerdo con los procedimientos internos de su empresa. Deberá incluir todos los datos de identificación que posea y cualquier otra información sobre el cliente de que disponga.

¿Cuándo debo comunicar mi conocimiento o sospecha al funcionario designado?

Debe hacerlo en cuanto tenga motivos razonables para sospechar. Si no lo hace, puede estar cometiendo un delito.

¿Qué significa "tan pronto como sea posible"?

Es decir, tan pronto como sea razonablemente posible. Las líneas internas de información a su Responsable designado deben ser cortas para evitar retrasos.

¿Qué pasa si sospecho antes de completar la transacción?

Debe realizar un informe interno antes de completar la transacción y esperar el consentimiento de su Responsable designado antes de completar la transacción.

¿Qué debo decir para retrasar la transacción sin advertir al cliente?

Da al cliente una excusa que se ajuste a las circunstancias. En los casos difíciles, habla con tu Responsable designado o tu jefe.

Si creo que retrasar la transacción podría "delatar" al cliente, ¿puedo seguir adelante?

Pregunte a su funcionario designado. Puede que le permitan continuar con la transacción, pero esto no debe hacerse de forma rutinaria. Debe incluir en su informe la razón por la que cree que retrasar la transacción podría "alertar" al cliente.

¿Qué debo hacer si el cliente me pide que le devuelva el dinero antes de obtener el consentimiento del funcionario designado?

Pida consejo urgentemente al funcionario designado.

¿Qué pasa si sospecho después de que se haya realizado la transacción?

Haga un informe interno a su Oficial Designado tan pronto como pueda.

¿Y si rechazo el negocio?

Si rechaza el negocio porque tiene sospechas, debe informar de ello al funcionario designado. Debe obtener pruebas y mantener registros de la identificación del cliente tan pronto como sospeche.

Identificar al cliente

¿Qué significa "conozca a su cliente" (*KYC*)?

KYC significa obtener información sobre un cliente más allá de la identificación requerida.

PAGOS NACIONALES S.A.C. ha implementado un programa KYC para asegurar que todo tipo de clientes (personas naturales o jurídicas o estructuras legales) estén sujetos a medidas adecuadas de identificación, calificación de riesgo y monitoreo. Este programa ha sido implementado en todas las divisiones de PAGOS NACIONALES S.A.C. Con ello se pretende reducir el riesgo de que PAGOS NACIONALES S.A.C. sea utilizada para el blanqueo de capitales y la financiación del terrorismo.

Se utilizan múltiples directorios en línea de información sobre particulares y empresas para comprobar todos los datos de identificación de los clientes antes de activar una cuenta electrónica completa para particulares o empresas.

En el caso de los clientes empresariales, también comprobamos sus datos en los registros públicos de empresas.

Los siguientes procedimientos de KYC serán útiles para identificar a posibles clientes presenciales o no presenciales que puedan presentar riesgos de blanqueo de capitales y financiación del terrorismo y financiación de la proliferación. PAGOS NACIONALES S.A.C. aplica un enfoque basado en el riesgo para KYC con referencia a los vínculos geográficos del cliente, los productos y/o servicios elegidos. El enfoque basado en el riesgo se aplica como bajo, medio o alto. Este enfoque basado en el riesgo indica el riesgo de que un cliente determinado pueda utilizar o vaya a utilizar los servicios y/o productos de PAGOS NACIONALES S.A.C. para cometer delitos financieros.

En todos los casos, antes de aceptar a un nuevo cliente o de realizar una transacción con un cliente con el que no tenemos una relación bien establecida, PAGOS NACIONALES S.A.C. lleva a cabo la diligencia debida suficiente para tener confianza en la integridad de los clientes y en la legalidad de la transacción propuesta mediante las siguientes acciones:

1. Realice esfuerzos razonables para determinar la verdadera identidad de todos los clientes y la titularidad legal y efectiva de todas las cuentas.

2. Determine la nacionalidad del cliente, la dirección de su domicilio y de su empresa, su ocupación o el tipo de negocio. Si procede, obtenga documentación acreditativa.

3. Averigüe si el cliente será el único interesado en la cuenta o si habrá otras personas que tendrán acceso a ella. Verifique la identidad de todas esas personas y actúe con la diligencia debida en relación con ellas.

4. Si el cliente no es un particular;

a. Determinar el estatuto jurídico (por ejemplo, sociedad anónima, sociedad colectiva u otra forma de entidad).

b. Determinar si el cliente está regulado.

c. Determinar todas las personas principales del cliente, tales como funcionarios y directores, o personas que tengan un interés beneficiario sustancial (es decir, que posean una participación igual o superior al 25% en la empresa). De conformidad con la Ley, PAGOS NACIONALES S.A.C. se asegurará de que las empresas y otras personas jurídicas constituidas en su territorio estén obligadas a obtener y mantener información adecuada, precisa y actualizada sobre su titularidad real. Esto incluye los detalles de los usufructos poseídos.

d. Obtenga copias de todos los documentos organizativos pertinentes.

5. Identificar el origen de los fondos del cliente.

6. Examinar al cliente:

a. Coincidencias con la lista OFAC;

b. Los titulares de cuentas de países incluidos en la lista del Grupo de Acción Financiera Internacional ("GAFI"), la lista de PTNC y la lista consultiva de la FinCEN;

c. Las personas con participaciones significativas, que posean más del 25% o más del capital de una empresa sujetas a AML/CTF;

d. partido de sanciones;

e. Listas y programas de riesgo de Visa Inc. y MasterCard Worldwide;

7. Cuando proceda, obtenga información sobre la frecuencia con la que el cliente prevé transferir fondos a o desde la cuenta, es decir, mensual, trimestral, o la naturaleza de los pagos de terceros a o desde la cuenta;

8. Cuando proceda, obtenga y póngase en contacto con referencias acreditadas, como profesionales y otros miembros del sector financiero, bancos, sociedades de valores, etc.

9. Funcionarios públicos y cuentas bancarias en el extranjero.

Se aplican procedimientos especiales a las cuentas en beneficio de personas políticamente expuestas (PEP), incluidas altas personalidades gubernamentales y políticas, en particular de determinados países, y a las cuentas abiertas por o a través de bancos extranjeros y por clientes de países o sectores considerados de alto riesgo. PAGOS NACIONALES S.A.C. aplica medidas reforzadas de diligencia debida y diligencia debida permanente proporcionales al riesgo del cliente. Por lo tanto, los clientes de alto riesgo estarán sujetos a una diligencia debida reforzada y a una diligencia debida continua. Los procesos de diligencia debida continuada se aplicarán a todos los clientes existentes

dentro de un periodo específico que se determinará en función de si se definen como de riesgo alto, medio o bajo.

En la medida en que no se trata de una actividad habitual de la Empresa, debe consultar al Responsable de Cumplimiento antes de abrir una cuenta de este tipo.

10. Cuentas a través de un intermediario;

Cuando las cuentas llegan a través de un intermediario, el Agente debe realizar la diligencia debida con respecto a la cuenta o asegurarse de que el intermediario ha realizado el tipo de diligencia debida con respecto a la cuenta que satisfaría la política de "Conozca a su cliente" del Agente.

a. El alcance de esta diligencia debida variará en función de la relación histórica de los Agentes con el intermediario, de si el intermediario es a su vez una entidad regulada y de la jurisdicción en la que se encuentre el intermediario. Se debe consultar al Responsable de Cumplimiento sobre el tipo de diligencia debida necesaria para un intermediario específico.

b. Como mínimo, la diligencia debida de un intermediario debe incluir una revisión de sus procedimientos contra el blanqueo de capitales y la financiación del terrorismo. En su caso, podrán obtenerse declaraciones del intermediario sobre el cumplimiento de sus procedimientos.

c. En términos generales, salvo en el caso de intermediarios que estén regulados en una jurisdicción adecuada o que el Agente tenga constancia de que cuentan con procedimientos adecuados contra el blanqueo de capitales y la financiación del terrorismo, debe realizar comprobaciones de referencias a través de fuentes publicadas y otras.

11. Contrapartidas;

Las mismas normas establecidas en el punto 10 anterior se aplican también a las operaciones con contrapartes por cuenta de nuestros clientes. A estos efectos, las contrapartes incluyen contrapartes de transacciones privadas y bancos y otros operadores, agentes e intermediarios. Aunque se exigirá un nivel relativamente bajo de diligencia debida a las contrapartes que estén reguladas en un país del que se sepa que cuenta con una normativa adecuada y bien aplicada contra el blanqueo de capitales y la financiación del terrorismo, las demás contrapartes requerirán el mismo nivel de diligencia debida que los clientes.

<u>Proceso de establecimiento de relaciones comerciales</u>

Bono electrónico individual

Todos los titulares de vales electrónicos deberán presentar un documento de identidad con fotografía y una prueba de residencia (por ejemplo, una factura de servicios públicos) para que sus cuentas se activen y entren en funcionamiento. Los titulares de E-Vocher deberán enviar a PAGOS NACIONALES S.A.C. una copia de su documento de identidad con fotografía certificada, es decir, Pasaporte Internacional, DNI, Permiso de Conducir, Permiso de Residencia, Permiso de Trabajo Visa u otro documento de identidad de verificación y una copia de su prueba de residencia en función de determinados límites. El cliente también es sometido a un control de sanciones AML/CTF/CPF.

A los solicitantes seleccionados se les notificará por correo electrónico o en gabinete personal que su cupón electrónico ha pasado a ser plenamente funcional.

Tenga en cuenta que, en caso necesario, PAGOS NACIONALES S.A.C. podrá solicitar información adicional sobre los detalles relativos a la naturaleza de determinadas transacciones.

Todas las copias impresas y en papel de la documentación de los clientes individuales se conservarán durante un mínimo de cinco años. Todos los documentos verificados se revisarán anualmente para garantizar que: a) siguen siendo pertinentes para la actividad que realiza el cliente y b) siguen siendo válidos (es decir, que los documentos de identidad facilitados no han caducado).

Cuenta electrónica empresarial

Servicios comerciales

Los servicios para comerciantes han sido concebidos para las empresas que desean crear una cuenta de servicios para empresas. Antes de establecer relaciones comerciales, el cliente potencial debe proporcionar ciertos detalles de información.

Los detalles deben incluir:

- Un formulario de solicitud cumplimentado con las condiciones generales firmadas,
- Documentos de constitución; certificado, memorándum de acuerdo y estatutos, factura de servicios públicos de la empresa (comprobante de domicilio);
- Detalles de la propiedad (aquellas personas o entidades que posean el 25% o más de las acciones), directores y personal que operará en nombre de la empresa, incluida copia del pasaporte y factura de servicios públicos,
- Información relativa a la naturaleza de su negocio; incluyendo las cantidades de dinero involucradas y la frecuencia esperada de las transacciones. Durante esta etapa, se debe aclarar y anotar el motivo por el cual se utilizan los servicios de PAGOS NACIONALES S.A.C., la naturaleza y el nivel de la actividad a realizar y el origen y destino de los fondos.
- Cualquier certificación relacionada con la empresa
- Cualquier otra información pertinente sobre las operaciones comerciales relacionadas con el uso de nuestros servicios/interfaz/plataforma,
- En caso necesario, PAGOS NACIONALES S.A.C. podrá solicitar información adicional sobre los detalles relativos a la naturaleza de determinadas transacciones.

Si lo considera necesario, solicite que un abogado certifique que toda la información de Business KYC, o una parte de ella, es una copia fiel del original.

Esta información debe enviarse por correo electrónico o por correo postal a PAGOS NACIONALES S.A.C.

Los candidatos seleccionados serán notificados por correo electrónico por un empleado de PAGOS NACIONALES S.A.C. sobre la necesidad de firmar un acuerdo de cooperación.

Todas las copias impresas y en papel de la documentación de los clientes empresariales se conservarán durante un mínimo de cinco años. Todos los documentos verificados deberán revisarse anualmente para garantizar que: a) siguen siendo pertinentes para la actividad que desarrolla el cliente empresarial y b) siguen siendo válidos (es decir, que los datos registrados de la empresa y los datos del personal clave de la empresa siguen siendo los mismos).

Mantener actualizada la información sobre los clientes

La regulación exige mantener actualizada la información CDD y KYC. Las regulaciones requieren que PAGOS NACIONALES S.A.C. tome medidas razonables para mantener actualizada la información de identificación del cliente. PAGOS NACIONALES S.A.C. debe actualizar esta información cada vez que se produzca un cambio material en las circunstancias del cliente. A estos efectos, PAGOS NACIONALES

S.A.C. realiza una CDD continua para todos los clientes con una regularidad que depende del nivel de riesgo del cliente.

Preguntas frecuentes (FAQ)

¿Qué es una relación comercial?

Una relación comercial es aquella que:

- Ayuda a la realización de transacciones de forma frecuente, habitual o regular y
- Cuando el importe total de cualquier pago que deba efectuarse no se conozca, o no pueda conocerse, desde el principio.

Que su cliente sea una empresa no significa que tenga una relación comercial con él. Una relación comercial es cuando tratas a un cliente de forma diferente a como tratas a tus clientes puntuales.

¿Cómo sabré si el cliente desea establecer una relación comercial?

Debe asegurarse de obtener información suficiente sobre la naturaleza de cualquier nuevo negocio con el que trate, incluidas las cantidades de dinero implicadas y la frecuencia prevista de las transacciones. En la primera transacción, debe establecer el:

- Motivo para establecer el negocio con usted,
- Naturaleza y nivel de la actividad a realizar y
- Origen y destino de los fondos.

También debe tener en cuenta por qué el cliente utiliza sus servicios.

¿Por qué son importantes las pruebas de identidad?

Para seguir el rastro del dinero blanqueado, las autoridades policiales necesitan conocer los nombres de las personas implicadas.

¿Cuándo es necesaria la identificación?

Debe confirmar y conservar la identificación de cualquier cliente que:

- Desea establecer una relación comercial con usted que implique transacciones frecuentes o regulares y el valor total de las transacciones no se conoce al principio,
- Como se ha mencionado anteriormente, la CDD debe llevarse a cabo no sólo con todos los nuevos clientes, sino también en el momento oportuno con los clientes existentes en función del riesgo, o cuando se produzca un cambio de cliente relevante, o cuando la entidad obligada tenga alguna obligación legal.
- Realiza cualquier transacción que sabe o sospecha que puede implicar el producto de un delito o que se va a destinar a un uso delictivo o terrorista.

¿Es necesario comprobar el DNI en las transacciones de poco valor?

Está obligado a comprobar el documento de identidad en las transacciones de escaso valor o limitadas, a menos que se trate de una relación comercial, siempre que no se sospeche de blanqueo de capitales.

¿A quién debo pedir una prueba de identificación?

Normalmente, debe obtener esta prueba de su cliente. En los casos en que su cliente actúe o parezca actuar en nombre de otra persona, deberá obtener pruebas de identificación de todos los integrantes de la cadena.

¿Qué debo hacer cuando un cliente quiere realizar una transacción que requiere identificación?

Deberías:

- Comprobar el documento de identidad en la primera transacción,
- Siempre que sea posible, conserve una fotocopia de las pruebas o, como mínimo, registre y conserve la información que permita obtener una copia,
- Compruébelo periódicamente y asegúrese de que el cliente es quien dice ser.

¿Cuáles son las mejores pruebas de identificación?

La ley establece que debe asegurarse de que la persona es quien dice ser. El documento de identidad debe haber sido expedido por una autoridad gubernamental federal, provincial, territorial o estatal y debe ser válido (no estar caducado):

- nombre
- fecha de nacimiento
- foto
- firma.

Algunas combinaciones de identificación son:

- pasaporte
- permiso de conducir
- documento nacional de identidad
- tarjeta sanitaria

Tenga en cuenta que todas las pruebas de identificación deben incluir las fotografías

individuales

¿Y si aún no estoy satisfecho?

Cuando no disponga de pruebas suficientes, puede decidir realizar comprobaciones adicionales, por ejemplo, llamando por teléfono a un tercero tras pedir a su cliente que designe a alguien que responda por él. El número de teléfono del tercero debe figurar en la guía telefónica.

Si sigue sin estar totalmente satisfecho con la identificación que le han presentado, debe rechazar el negocio e informar a su funcionario designado, quien decidirá si lo transmite a UIF..

¿Qué debo comprobar de las pruebas documentales que se me entregan?

Deberías:

- Comprobar la fecha de nacimiento comparándola con la apariencia del cliente en el documento de identidad con fotografía y
- Compare la ortografía de los nombres y direcciones en cada documento.

Le rogamos que comente cualquier anomalía detectada en los resultados con el funcionario designado.

¿Qué debo hacer cuando mi cliente es una empresa?

Si su cliente o proveedor es una sociedad limitada, debe identificar a las personas con las que trata que tienen autoridad dentro de la empresa para mover fondos (no sólo los firmantes de cheques) y obtener los datos de la empresa:

- Número de registro, razón social y nombres comerciales utilizados,
- Domicilio social y, en su caso, domicilio comercial principal,
- Foto ID,
- Comprobación de perfil,
- Los registros públicos mercantiles se comprueban para validar el nombre, la dirección y los administradores de la empresa. Si el cliente registrado no es administrador de esa empresa, PAGOS NACIONALES S.A.C. solicitará a un administrador de esa empresa que firme un formulario de usuario adicional miembro de la empresa. Esto le dará a la persona que se ha registrado la autorización para utilizar y operar en nombre de esa empresa.

¿Con qué frecuencia debo actualizar el registro de identificación de mi cliente?

Sólo tiene que actualizar las pruebas de identidad si algo ha cambiado. Por ejemplo, puede que tenga que actualizar los datos de su dirección si se muda. Es aconsejable revisar anualmente la información para asegurarse de que sigue siendo válida y está actualizada. (para más información, véase el anexo)

<u>Mantenimiento de registros</u>

Deberá conservar todos los registros de las transacciones comerciales durante al menos cinco años a partir de la fecha en que finalice la relación comercial.

¿Por qué debemos conservar los registros durante cinco años desde el final de una relación comercial?

Es la ley. La finalidad de conservar los registros es permitir a las autoridades competentes reconstruir las transacciones comerciales, a menudo mucho después de que haya concluido la actividad original. Al crear y conservar registros, debe tener en cuenta la necesidad de proporcionar una pista de auditoría clara de los negocios que ha llevado a cabo.

Los registros que deben conservarse son:

- Una copia o las referencias a las pruebas de la identidad del cliente obtenidas en virtud de los requisitos de diligencia debida con respecto al cliente de conformidad con la normativa.
- Los registros justificativos de las relaciones comerciales u operaciones ocasionales que son objeto de medidas de diligencia debida con respecto al cliente o de un seguimiento continuo.
- Registro de cuándo tuvo lugar la primera identificación y verificación de clientes, y cómo.
- Documentos que justifiquen la exención de identificación, si procede.

En relación con la prueba de la identidad de un cliente, las empresas deben conservar los siguientes registros:

- Una copia de los documentos de identificación aceptados y de las pruebas de verificación obtenidas, o
- Referencias a las pruebas de identidad del cliente.

Los registros de transacciones y relaciones comerciales (por ejemplo, archivos de cuentas, correspondencia comercial pertinente, libros de registro diario, recibos, cheques, etc.) deben conservarse de forma que pueda compilarse una pista de auditoría satisfactoria y que permita establecer un perfil financiero de cualquier cuenta o cliente sospechoso.

¿Qué es una pista de auditoría?

Una pista de auditoría es un registro paso a paso mediante el cual se pueden rastrear los datos financieros hasta su origen. En el caso del blanqueo de capitales, el objetivo de establecer una pista de auditoría es rastrear los fondos hasta la primera transacción (la colocación) para identificar al blanqueador.

¿Qué registros debo llevar?

Los registros que mantengamos deben ser suficientes para formar una pista de auditoría completa que los funcionarios de aduanas puedan seguir desde el inicio de la transacción hasta el final; esto es especialmente importante en caso de que la transacción forme parte posteriormente de una investigación en curso por parte de las fuerzas de seguridad.

Existen varios tipos de registros que debemos conservar:

- Una copia de la prueba de identificación presentada. Las pruebas fotográficas son especialmente valioso.
- Datos sobre dónde se pueden encontrar las copias de identificación, que deben estar archivadas y ser fácilmente recuperables. Debe conservar estos registros durante al menos cinco años a partir de la fecha en que finalice la relación con su cliente.
- Registros comerciales. Debe conservar durante cinco años un registro de todas las transacciones, independientemente de que haya sido necesario verificar la identidad del cliente.
- Todos los registros de divulgaciones. Las cartas recibidas de UIF o cualquier otra correspondencia con un organismo encargado de hacer cumplir la ley deben conservarse durante al menos cinco años.

Nota: Conservamos los registros de clientes individuales y clientes empresariales durante al menos un periodo de cinco años una vez finalizada la relación comercial.

Identificación de actividades sospechosas

Una vez identificado un cliente y realizada la diligencia debida necesaria, estaremos en buena posición para detectar cualquier cosa inusual con los clientes, sus acciones, inacciones o transacciones.

Esté atento a cualquier acción o actividad sospechosa en cada fase de la negociación con el cliente. Por ejemplo, puede tratarse de una remesa inusual al extranjero o del importe de una transacción que no esté en la línea normal de actividad.

La siguiente lista ofrece varios tipos de comportamiento o actividad que pueden ser sospechosos. La lista no es exhaustiva ni concluyente. Más bien, los empleados que tengan contacto con clientes, intermediarios o contrapartes deben utilizar la lista como guía para la indagación y el seguimiento:

- El cliente desea realizar transacciones que carecen de sentido comercial o son incoherentes con el negocio/estrategia declarada del cliente.
- El cliente muestra una preocupación inusual por el secreto, especialmente en lo que respecta a su identidad, tipo de negocio o relaciones con empresas.
- Cuando se le solicita, el cliente se niega a identificar o no indica una fuente legítima de sus fondos.
- El cliente muestra una inusual despreocupación por los riesgos, comisiones u otros costes de transacción.
- El cliente parece operar como agente de un mandante no revelado, pero se muestra reacio a facilitar información sobre el mandante.
- El cliente tiene dificultades para describir la naturaleza de su negocio. El cliente carece de conocimientos generales sobre su sector.
- Sin motivo aparente, el cliente tiene varias cuentas bajo un mismo nombre o varios nombres, con un gran número de transferencias entre cuentas o a terceros.
- El cliente procede o tiene cuentas en un país identificado como paraíso para el blanqueo de capitales.
- El cliente, o una persona asociada públicamente o conocida por el cliente, tiene antecedentes dudosos, incluidas condenas penales previas.
- La cuenta del cliente presenta una gran actividad inexplicable o repentina, especialmente en cuentas que tenían poca o ninguna actividad previa.
- La cuenta del cliente muestra numerosas divisas o transacciones en efectivo que suman sumas significativas. Sin embargo, esto no es relevante ya que PAGOS NACIONALES S.A.C. no tiene transacciones en efectivo.
- La cuenta del cliente tiene un gran número de transferencias bancarias a terceros no relacionados.
- La cuenta del cliente tiene transferencias electrónicas hacia o desde un país con secreto bancario o un país identificado como riesgo de blanqueo de capitales.
- La cuenta del cliente presenta transacciones inusuales o desproporcionadas en relación con la actividad conocida del cliente.

Asimismo, existen directrices sobre transacciones sospechosas con indicadores más específicos de LA/FT relacionados con el sector de servicios monetarios:

- El cliente solicita una transacción a un tipo de cambio superior al publicado.
- El cliente quiere pagar tasas de transacción superiores a las publicadas.
- El cliente cambia divisas y solicita billetes de la mayor denominación posible en una moneda extranjera.
- El cliente conoce mal la dirección y los datos de contacto del beneficiario, es reacio a revelar esta información o solicita un instrumento al portador.
- El cliente desea que se emita un cheque en la misma divisa para sustituir al que se está cobrando.
- El cliente quiere que le conviertan el efectivo en un cheque y usted normalmente no se dedica a emitir cheques.
- El cliente desea cambiar efectivo por numerosos giros postales de pequeñas cantidades para otras muchas partes.
- El cliente realiza transacciones con contrapartes en lugares poco habituales para él.
- El cliente da instrucciones para que los fondos sean recogidos por un tercero en nombre del beneficiario.
- El cliente realiza grandes compras de cheques de viaje que no coinciden con los planes de viaje conocidos.
- El cliente realiza compras de giros postales en grandes volúmenes.
- El cliente solicita numerosos cheques de pequeño importe y diversos nombres, que suman el importe del canje.
- El cliente solicita que se emita un cheque o giro postal al portador.
- El cliente solicita el cambio de una gran cantidad de divisas a otra moneda extranjera.
- El cliente adquiere un gran volumen de giros postales y cambia el tipo de pago para evitar la obligación de informar.

Si detecta una actividad sospechosa, póngase en contacto con el funcionario designado, que se encargará de emitir un ROS a través del sistema en línea UIF. El Nominated Officer también debe notificarlo a la alta dirección.

Nota: NO plantees ninguna preocupación al cliente ni utilices palabras que sugieran que no estás contento con algo que pueda ponerle sobre aviso.

Notificación de sospechas

Los procesos de lucha contra el blanqueo de capitales requieren un enfoque de equipo. Las cuestiones relacionadas con el blanqueo de capitales son complejas. El Oficial Nominado de PAGOS NACIONALES S.A.C. no debe intentar resolverlos por sí solo y si el oficial tiene conocimiento de cualquier circunstancia sospechosa, o tiene alguna pregunta, debe consultar rápidamente con el Oficial Nominado y el Equipo de Cumplimiento de PAGOS NACIONALES S.A.C.

Informes sobre transacciones sospechosas: proceso interno de la empresa

En el caso de que un empleado (a estos efectos, colectivamente, los miembros del personal) tenga sospechas sobre un cliente y/o transacción, debe asegurarse de que el Responsable designado de la empresa sea notificado sobre sus sospechas lo antes posible.

El personal debe utilizar el "Formulario de notificación de transacciones sospechosas" interno.

El ROS debe contener como mínimo la siguiente información:

- Detalles y datos de identificación de todas las partes de la transacción

- El propietario del dinero en cuestión
- Cómo se verificó la identidad del cliente
- Una descripción completa de la transacción
- Motivo de la sospecha y pruebas
- Detalles de cualquier activo sujeto a sanciones internacionales

En caso de duda, el miembro del personal debe llamar al funcionario designado para discutir las razones de su sospecha - sin embargo, debe tener cuidado de no hacerlo mientras el cliente está de pie delante de él o a través de cualquier comunicación intercambiada con el cliente (de lo contrario, puede "avisar" al cliente, véase más adelante).

El momento oportuno para presentar el ROS interno es importante. La ley establece que una persona que trabaje en el sector regulado debe presentar una denuncia en cuanto sospeche algo. Esto puede significar antes de que se produzca la transacción o inmediatamente después.

Cuando un miembro del personal tiene conocimiento de que un cliente desea realizar una transacción sospechosa y el momento de la transacción lo permite, el miembro del personal debe asegurarse de que se da el "consentimiento" antes de procesar la transacción. “Consentimiento" significa que la empresa ha solicitado y obtenido la aprobación para procesar la transacción. A continuación se ofrece más información sobre la "solicitud de consentimiento".

No obstante, el personal puede decidir que, si solicita el consentimiento para una transacción concreta (es decir, antes de que se realice la transacción), existe el riesgo de que el cliente sea advertido.

Todos los miembros del personal habrán cumplido plenamente sus obligaciones, y gozarán de la plena protección de la ley, una vez que hayan comunicado sus sospechas al Responsable designado de la empresa.

Una vez que el funcionario designado recibe el ROS interno del funcionario, tiene dos opciones:

- Informar del ROS al regulador (véase el procedimiento a continuación);
- Presentar una nota interna indicando por qué, sobre la base de la revisión de las circunstancias en torno a la transacción, se considera que no es necesario hacer un informe al regulador.

El funcionario designado deberá cumplimentar el formulario de Resolución de ROS (véase el modelo en el apéndice) en caso de que decida no presentar una denuncia al regulador.

<u>Notificación de operaciones sospechosas</u>

En caso de que un empleado tenga sospechas sobre un cliente o una transacción, debe asegurarse de que el Responsable designado por la empresa sea informado de sus sospechas lo antes posible.

El personal debe utilizar el ROS interno (véase el Anexo).

El ROS debe contener como mínimo la siguiente información:

• Fecha/hora de la transacción

• Importe

- Nombre del cliente/información de identificación del cliente (por ejemplo, número de pasaporte, etc.)
- Número de transacción
- Motivo de sospecha de la transacción

En caso de duda, el miembro del personal debe llamar al funcionario designado para discutir las razones de su sospecha, pero debe tener cuidado de no hacerlo mientras el cliente está de pie delante de él (de lo contrario podría "avisar" al cliente, véase más abajo).

El momento de presentar el ROS interno es importante. La ley establece que una persona que trabaje en el sector regulado (es decir, en el sector de servicios monetarios) debe presentar una denuncia en cuanto sospeche algo. Esto puede significar antes de que se produzca la transacción o inmediatamente después.

No obstante, el personal puede decidir que, si solicita el consentimiento para una transacción concreta (es decir, antes de que se realice la transacción), existe el riesgo de que el cliente reciba una alerta.

Todos los miembros del personal habrán cumplido plenamente sus obligaciones, y gozarán de la plena protección de la ley, una vez que hayan comunicado sus sospechas al Responsable designado de la empresa.

Una vez que el funcionario designado recibe el ROS interno del funcionario, tiene dos opciones:

- Informar del ROS al regulador;
- Presentar una nota interna indicando por qué, sobre la base de la revisión de las circunstancias en torno a la transacción, se considera que no es necesario hacer un informe al regulador.

El Funcionario Designado deberá rellenar el formulario de Resolución de ROS en caso de que decida no presentar un informe.

La advertencia

Cualquier miembro del personal debe juzgar si cualquier retraso en la transacción ("solicitud de consentimiento") tendría el efecto de "avisar" al cliente.

Es delito hacer o decir algo que pueda "alertar" a otra persona de que se ha hecho una revelación o perjudicar de algún modo una investigación. Esto significa que las empresas no deben informar a un cliente:

- que se ha retrasado o se está retrasando una transacción porque se ha solicitado el consentimiento del regulador;
- que los detalles de sus transacciones o actividades serán/han sido comunicados al regulador;
- que están siendo investigados por las fuerzas del orden.

En situaciones en las que retrasar una transacción puede conducir inadvertidamente a una advertencia, tendrá sentido procesar la transacción y después asegurarse de que se presenta un ROS al funcionario designado lo antes posible. El miembro del personal gozará de la protección de la ley desde el momento en que se envíe el ROS al funcionario designado.

En caso de duda sobre la conveniencia de realizar una operación, el funcionario deberá ponerse inmediatamente en contacto con el funcionario designado para pedirle consejo.

Documentación

La documentación justificativa es una piedra angular de nuestros procedimientos de lucha contra el blanqueo de capitales y la financiación del terrorismo.

Los pasos no registrados se olvidan pronto. Los registros ayudan a rastrear la información pertinente y a demostrar que la empresa/persona ha llevado a cabo nuestras actividades de forma responsable e íntegra. Todas las entrevistas, búsquedas y actividades emprendidas para verificar la integridad de las transacciones y las personas deben documentarse y almacenarse para que PAGOS NACIONALES S.A.C., el regulador pueda consultarlas en caso necesario.

Todos los registros deben conservarse durante un mínimo de cinco años una vez finalizada la relación comercial con el cliente.

Prevención del blanqueo de capitales para comerciantes

¿Tienen los comerciantes que cumplir la normativa?

La empresa obtiene toda la información necesaria para determinar a su entera satisfacción la identidad de cada nuevo comerciante o persona jurídica, así como la finalidad y la naturaleza prevista de la relación comercial. El alcance y la naturaleza de la información dependen del tipo de solicitante (personal, empresa, etc.) y de los volúmenes de ventas previstos.

Cuando una cuenta de Comerciante ha sido abierta, pero surgen problemas de verificación en la relación de servicio que no pueden ser resueltos, PAGOS NACIONALES S.A.C. puede cerrar la cuenta y transferir el dinero a la cuenta bancaria del Comerciante. Si bien se considerará la transferencia de un saldo inicial desde una cuenta a nombre del cliente en otra organización sujeta al mismo estándar de KYC, PAGOS NACIONALES S.A.C. seguirá sus propios procedimientos de KYC. PAGOS NACIONALES S.A.C. puede considerar la posibilidad de que el anterior gestor de la cuenta haya solicitado la eliminación de la cuenta debido a una preocupación por actividades dudosas.

Naturalmente, los Comerciantes tienen derecho a trasladar sus negocios de una organización a otra. Sin embargo, si PAGOS NACIONALES S.A.C. tiene alguna razón para creer que a un solicitante se le están denegando facilidades de servicio por parte de otra organización, la Compañía tiene el deber de emprender procedimientos reforzados de diligencia debida hacia el cliente.

PAGOS NACIONALES S.A.C. no aceptará abrir una cuenta de comerciante ni realizar operaciones en curso con un cliente que insista en el anonimato o que dé un nombre ficticio. Las cuentas confidenciales numeradas tampoco deben funcionar como cuentas anónimas, sino que deben estar sujetas exactamente a los mismos procedimientos KYC que todas las demás cuentas de clientes, incluso si la prueba la realiza personal seleccionado.

Mientras que una cuenta numerada puede ofrecer protección adicional para la identidad del titular de la cuenta, la identidad debe ser conocida por un número suficiente de personal para operar con la debida diligencia.

Empresas e industrias prohibidas

La empresa se ha fijado la prohibición de la lista de bienes y servicios (industria):

1. Venta de billetes;
2. Drogas y consumo de una droga o sustancia similar;
3. Armas y municiones;
4. Joyería, metales preciosos;
5. Servicios de reaseguro y seguros;
6. Servicios de efectivo (como tesorería corriente, oficinas de cambio de divisas, agentes de transferencia de dinero u otros proveedores de servicios que ofrecen facilidades de transferencia de dinero);
7. 7. Servicios de intermediación en el comercio de divisas (por ejemplo, corredores de divisas), excepto en los casos en que el proveedor esté autorizado o haya emitido un dictamen jurídico y se lleve a cabo bajo la supervisión del proveedor del servicio; 8. Opciones binarias;
9. Marketing multinivel;
10. Comercio de antigüedades y arte;
11. Farmacias y actividad farmacéutica, productos farmacéuticos, especialidades farmacéuticas y comercio farmacéutico;
12. La venta de productos del tabaco;
13. Grabaciones de audio o vídeo ilegales/piratas;
14. Mercancías infractoras (mercancías falsificadas);
15. Servicios sexuales, Adultos;
16. Pirámide financiera;
17. Servicios de cobro de deudas;
18. Aceptar activos de los que se sepa o sospeche que proceden de actividades delictivas;
19. Entablar/mantener relaciones comerciales con personas o entidades de las que se sepa o se sospeche que son terroristas o miembros de organizaciones delictivas o que figuren en listas de sanciones;
20. Mantener cuentas anónimas, cuentas para bancos ficticios o cuentas de pago.

<u>Incorporación de comerciantes</u>

El proceso de Incorporación de Comerciantes se realiza en conjunto con el banco Adquirente, que prestará servicios a PAGOS NACIONALES S.A.C.

1. Comprobación previa

Al principio del proceso de incorporación debe cumplimentarse un formulario específico de solicitud previa.

La comprobación inicial del comerciante no tardará más de 2 días laborables. Se comprobará la página web del comerciante, los contactos con los programas de riesgo de OFAC, MasterCard y VISA, así como el modelo de negocio y se comprobará de acuerdo con las Industrias Internas Prohibidas y Restringidas.

2. Documentos para la diligencia debida

Una vez dada la pre-aprobación para procesar, un empleado recoge vía e-mail y envía al Equipo de Cumplimiento de PAGOS NACIONALES S.A.C. y al Banco Adquirente el paquete completo de documentación:

- Documentos de registro de la empresa expedidos en el país en el que está constituido el comerciante (por ejemplo, certificado de registro, estatutos y escritura de constitución, certificado de domicilio social, certificado de administradores, etc.)
- Documentos que acrediten los derechos de propiedad del beneficiario efectivo final (por ejemplo, certificado de accionista, transferencia de acciones, registro electrónico, etc.)
- Documentos de identificación con la firma del titular (por ejemplo, DNI, pasaporte, permiso de conducir, etc.)
- Documentos que acrediten los derechos de representación de una empresa (por ejemplo, poderes, estatutos, actas de junta, etc.)
- Acuerdos con socios y proveedores, si procede;
- Licencia, si procede;
- Estados financieros
- Historial de procesamiento.

PAGOS NACIONALES S.A.C. en conjunto con los Abogados del Banco Adquirente verificarán la validez de los documentos y listarán los documentos que deberán ser notariados.

3. Firma del acuerdo

Una vez que el negocio es aprobado por PAGOS NACIONALES S.A.C. y el Banco Adquirente, un empleado de PAGOS NACIONALES S.A.C. prepara el acuerdo junto con todos los términos y condiciones.

PAGOS NACIONALES S.A.C. firma el acuerdo y lo envía al Comerciante o se reúne con el Comerciante para firmarlo. Este acuerdo también se envía al banco Adquirente.

Toda la documentación (es decir, los formularios de acuerdo y solicitud) que firme el comerciante deberá estar certificada ante notario o firmada durante la visita in situ.


PAGOS
NACIONALES

Anexo 1: Evaluación basada en el riesgo

La Ley, en su capítulo XI, habla sobre la identificación y evaluación de los riesgos de LA/FT.

Se utiliza un Enfoque Basado en Riesgo (RBA), puede establecerse tanto sobre la base de criterios objetivos como de criterios subjetivos. A cada criterio se le asigna una "calificación de riesgo".

Clasificación de riesgos	Clasificación	Revisión periódica
L	Bajo riesgo	Cada 5 años
M	Riesgo medio	Cada 3 años
H	Alto riesgo	Anualmente
PR	Prohibido	N/A

La Empresa, como parte de su Programa AML, ha llevado a cabo un análisis de riesgos para identificar criterios específicos de riesgos potenciales de blanqueo de capitales. Este enfoque basado en el riesgo incluye la identificación de los riesgos de lavado de activos y financiación del terrorismo (en la medida en que pueda identificarse dicho riesgo) de clientes, categorías de clientes y transacciones que permitan a la Empresa determinar y aplicar medidas y controles proporcionados para mitigar estos riesgos. Si bien la evaluación del riesgo se realiza de forma rutinaria al inicio de la relación con el cliente, en el caso de algunos clientes el perfil de riesgo completo sólo puede hacerse evidente una vez que el cliente ha comenzado a realizar transacciones a través de una cuenta. Por lo tanto, el seguimiento de las transacciones de los clientes y las revisiones continuas son un componente fundamental del enfoque basado en el riesgo de la empresa. Además, este tipo de proceso de evaluación del riesgo también puede ajustarse para un cliente concreto en función de la información recibida de una autoridad competente.

La Sociedad mide los riesgos de blanqueo de capitales y financiación del terrorismo utilizando categorías que proporcionan una estrategia para gestionar los riesgos potenciales al permitir a la Empresa someter a los clientes a controles y supervisión proporcionados. La importancia otorgada a estas categorías de riesgo (individualmente o combinadas) en la evaluación del riesgo global de blanqueo de capitales puede variar en función de las circunstancias específicas de la empresa.

I. Riesgo País o Geográfico.

El riesgo país, junto con otros factores de riesgo, proporciona información útil sobre los riesgos potenciales de blanqueo de capitales y financiación del terrorismo. Entre los factores que pueden dar lugar a la determinación de que un país presenta un riesgo más elevado se incluyen: Países sujetos a sanciones, embargos o medidas similares emitidas por las Naciones Unidas ("ONU") como ejemplo. Además, algunas circunstancias que someten a los países a sanciones o medidas similares a las emitidas por organismos como la ONU, pero que pueden no estar universalmente reconocidas, pueden recibir crédito por parte de la Compañía debido a la posición del emisor y a la naturaleza de las medidas;

Países que, según fuentes fidedignas, carecen de leyes, reglamentos y otras medidas adecuadas en materia de lucha contra el blanqueo de capitales. El término "fuentes fidedignas" se refiere a la

información elaborada por organismos reconocidos que gozan de una reputación general y que ponen dicha información a disposición del público de forma generalizada.

Otras fuentes pueden ser organismos supranacionales o internacionales como la Organización Internacional del Trabajo (OIT), Fondo Monetario Internacional (FMI), el Banco Mundial y el Grupo Egmont de Unidades de Inteligencia Financiera, así como organismos gubernamentales nacionales y organizaciones no gubernamentales pertinentes. La información facilitada por estas fuentes fidedignas no tiene el efecto de una ley o reglamento y no debe considerarse como una determinación automática de que algo es de mayor riesgo;

Países identificados por fuentes fidedignas como proveedores de financiación o apoyo a actividades terroristas que cuentan con organizaciones terroristas designadas que operan en ellos; o Países identificados por fuentes fidedignas como países con niveles significativos de corrupción u otras actividades delictivas.

El riesgo asociado a países y zonas geográficas, PAGOS NACIONALES S.A.C. considera el riesgo relacionado con:

a) las jurisdicciones en las que tienen su sede el cliente y el beneficiario efectivo;

b) las jurisdicciones de los principales centros de actividad del cliente y del beneficiario efectivo; y

c) las jurisdicciones con las que el cliente y el beneficiario efectivo tienen vínculos personales relevantes.

La empresa define una lista de jurisdicciones con las que no coopera, así como una lista de países de alto riesgo basada en las jurisdicciones de alto riesgo del GAFI y otras jurisdicciones vigiladas, el índice AML de Basilea, el índice de Transparencia Internacional, los programas de sanciones de Estados Unidos, etc.

PAGOS NACIONALES S.A.C. no gestiona transacciones ni embarca a ningún cliente de la lista de países no cooperantes.

II. Riesgo para el cliente.

Determinar los riesgos potenciales de blanqueo de capitales o de financiación del terrorismo (en la medida en que pueda identificarse dicho riesgo) que plantea un cliente o una categoría de clientes es un componente crítico. Basándose en sus propios criterios, la empresa es capaz de determinar si un cliente concreto plantea un riesgo mayor y el impacto potencial de cualquier factor atenuante en esa evaluación. La aplicación de variables de riesgo puede atenuar o agravar la evaluación del riesgo. Las categorías de clientes cuyas actividades pueden indicar un mayor riesgo incluyen:

Clientes que llevan a cabo su relación comercial o sus transacciones en circunstancias inusuales, como:

- Distancia geográfica significativa e inexplicable entre la empresa y la ubicación del cliente;
- Movimientos frecuentes e inexplicables de cuentas a diferentes instituciones; y
- Movimientos frecuentes e inexplicables de fondos entre instituciones de diversas ubicaciones geográficas.

La estructura o naturaleza de la entidad o relación dificulta la identificación del verdadero propietario o de los intereses de control del cliente.

Empresas con uso intensivo de efectivo (y equivalentes de efectivo), incluidas:

- Empresas de servicios monetarios (por ejemplo, empresas de envío de remesas, casas de cambio, agentes de transferencia de dinero y comerciantes de billetes de banco u otras empresas que ofrezcan facilidades o servicios de transferencia de dinero);
- Casinos, apuestas y otras actividades relacionadas con el juego; y
- Las empresas que normalmente no hacen un uso intensivo de efectivo generan cantidades sustanciales de efectivo para determinadas transacciones.

Organizaciones benéficas y otras organizaciones "sin ánimo de lucro" que no están sujetas a control o supervisión (especialmente las que operan a escala "transfronteriza").

"Gatekeepers", como contables, abogados u otros profesionales que tengan cuentas en la Empresa, que actúen en nombre de sus clientes/titulares de tarjetas, y cuando la Empresa confíe injustificadamente en el gatekeeper.

Utilización de intermediarios en la relación que no estén sujetos a leyes y medidas adecuadas de lucha contra el blanqueo de capitales y que no estén supervisados adecuadamente.

Clientes que son Personas Expuestas Políticamente (PEP).

III. Riesgo de productos y servicios.

Esta categoría de riesgo incluye la determinación de los riesgos potenciales que presentan los productos y servicios ofrecidos por la empresa, como los riesgos asociados a productos o servicios nuevos o innovadores y los siguientes factores:

- Servicios identificados por las autoridades competentes u otras fuentes creíbles como potencialmente de mayor riesgo, incluidos, por ejemplo:
- Servicios de corresponsalía bancaria internacional que implican transacciones como pagos comerciales para no clientes (por ejemplo, actuando como banco intermediario) y actividades de valija; y
- Servicios internacionales de banca privada
- Servicios relacionados con el comercio y la entrega de billetes de banco y metales preciosos; o
- Servicios que intrínsecamente han proporcionado más anonimato o que pueden cruzar fácilmente las fronteras internacionales, como la banca en línea, las tarjetas de valor almacenado, las transferencias bancarias internacionales, las sociedades de inversión privada y los fideicomisos.

IV. Otras variables de riesgo.

La metodología del enfoque basado en el riesgo de la empresa puede tener en cuenta variables de riesgo específicas de un cliente o transacción concreta. Estas variables pueden aumentar o disminuir el riesgo percibido planteado por un cliente o transacción en particular y pueden incluir:

- Finalidad de una cuenta o relación que puede influir en el riesgo evaluado. Las cuentas abiertas principalmente para facilitar transacciones de consumo tradicionales de baja denominación pueden plantear un riesgo menor que una cuenta abierta para facilitar grandes transacciones en efectivo de una entidad comercial desconocida hasta entonces.
- Nivel de activos que debe depositar un cliente concreto o volumen de las operaciones realizadas. Niveles inusualmente altos de activos o transacciones inusualmente grandes en comparación con lo que podría esperarse razonablemente de clientes con un perfil similar puede indicar que un cliente que de otro modo no se consideraría de mayor riesgo debería

ser tratado como tal. Por el contrario, los bajos niveles de activos o las operaciones de escaso valor en las que participe un cliente que, de otro modo, parecería de mayor riesgo, podrían permitir a la empresa tratar al cliente como de menor riesgo.

- Nivel de regulación u otro régimen de supervisión o gobernanza al que está sujeto un cliente. Un cliente que sea una institución financiera regulada en un país con un régimen ALD satisfactorio plantea menos riesgos desde el punto de vista del blanqueo de capitales que un cliente no regulado o sujeto sólo a una regulación ALD mínima. Además, las empresas y sus filiales al 100% que son de propiedad pública y cotizan en una bolsa reconocida suelen plantear riesgos mínimos de blanqueo de capitales. Estas empresas suelen proceder de países con un régimen normativo adecuado y reconocido, que por lo general plantean menos riesgos debido al tipo de negocio que realizan y al régimen de gobernanza más amplio al que están sujetas. Del mismo modo, estas entidades pueden no estar sujetas a una diligencia debida tan estricta en la apertura de cuentas o en la supervisión de las transacciones durante el transcurso de la relación.
- Regularidad o duración de la relación. Las relaciones duraderas que implican un contacto frecuente con el cliente a lo largo de la relación pueden presentar menos riesgo desde el punto de vista del blanqueo de capitales.
- Familiaridad con un país, incluido el conocimiento de las leyes, reglamentos y normas locales, además de la estructura y el alcance de la supervisión reglamentaria, como resultado de las propias operaciones de la empresa en el país.
- Utilización de vehículos corporativos intermedios u otras estructuras que no tengan una justificación comercial o de otro tipo aparente o que aumenten innecesariamente la complejidad o provoquen una falta de transparencia. El uso de tales vehículos o estructuras, sin una explicación aceptable, aumenta el riesgo.

El riesgo cliente también se ve afectado por la Actividad Inusual que puede ser sospechosa:

- Transacciones fraccionadas: el cliente intenta fraccionar una transacción grande en varias transacciones más pequeñas para evitar la obligación de demostrar el origen de los fondos.
- Nuevos clientes que realizan grandes transacciones (a diferencia de los clientes habituales)
- El cliente habitual está procesando transacciones que sí coinciden con el perfil de transacciones anteriores
- Clientes que procesan transacciones que no parecen ser propietarios legítimos de los fondos (por ejemplo, estudiantes que procesan transacciones grandes).
- Clientes implicados en transacciones que parecen estar vinculadas a transacciones procesadas por otros clientes.
- Clientes que no pueden presentar un documento de identidad cuando se les solicita o que presentan documentos falsos
- Clientes que no pueden justificar el origen de los fondos cuando se les solicita
- El cliente no es local (pero no es turista)
- Transacciones en las que el cliente está acompañado o recibe instrucciones de otra persona que le dice lo que tiene que hacer

<u>Estrategias de mitigación de riesgos</u>

La empresa ha aplicado las siguientes estrategias de mitigación de riesgos:

1. Identificación de clientes, diligencia debida y conocimiento del cliente. La empresa ha puesto en marcha un Programa de Identificación de Clientes (PIC) que permite al personal formarse una

convicción razonable de que conoce la verdadera identidad de cada cliente y, con un grado de confianza adecuado, conoce los tipos de negocios y transacciones que es probable que realice el cliente. En general, este programa

1.1. Identifica y verifica puntualmente la identidad de cada cliente;

1.2. Adopta medidas razonables basadas en el riesgo para identificar y verificar la identidad de cualquier beneficiario efectivo;

1.3. Obtiene la información adicional adecuada para comprender las circunstancias y la actividad del cliente, incluida la naturaleza y el nivel previstos de las transacciones;

1.4. Evalúa los riesgos que puede plantear el cliente teniendo en cuenta las variables de riesgo apropiadas antes de tomar una determinación final. Este proceso de diligencia debida incluye:

1.4.1. Un nivel estándar de diligencia debida que se aplica a todos los clientes al iniciar o proseguir una relación, como:

1.4.1.1. Evaluar la naturaleza de la relación. Por ejemplo, determinar la duración de la relación de un cliente con la empresa, los productos y servicios prestados a un cliente y la forma en que un cliente fue remitido a la empresa. La naturaleza de la relación con un cliente puede servir para mitigar o aumentar los indicadores generales de riesgo que se describen a continuación.

1.4.1.2. Identificación de zonas geográficas de alto riesgo, incluidos los clientes situados en zonas de alto riesgo de blanqueo de capitales y delitos financieros conexos, o que realizan operaciones comerciales en dichas zonas.

1.4.1.3. Identificar las entidades, funciones bancarias y operaciones de alto riesgo (véase el subtema Entidades de alto riesgo más adelante).

1.4.2. El nivel estándar se reduce en escenarios reconocidos de menor riesgo, como:

1.4.2.1. Empresas que cotizan en bolsa sujetas a requisitos reglamentarios de divulgación;

1.4.2.2. Otras instituciones financieras (nacionales o extranjeras) sujetas a un régimen ALD coherente con todas las recomendaciones ALD;

1.4.2.3. Personas cuya principal fuente de fondos proceda de un salario, pensión, prestaciones sociales de una fuente identificada y adecuada y cuyas transacciones sean proporcionales a los fondos.

1.4.2.4. Operaciones que implican los importes mínimos para determinados tipos de operaciones (por ejemplo, pequeñas primas de seguros).

1.4.3. El nivel estándar se incrementa con respecto a los clientes que se consideran de mayor riesgo debido a la naturaleza de sus actividades, que pueden requerir una mayor supervisión. Esto puede ser el resultado de la actividad empresarial del cliente, la estructura de propiedad, el volumen previsto o real o los tipos de transacciones, incluidas las transacciones con países de mayor riesgo o definidas por la legislación o la normativa aplicable como de mayor riesgo, como las relaciones de corresponsalía. Estos procedimientos reforzados de diligencia debida incluyen, entre otros:

1.4.3.1. Mayor conocimiento por parte del personal de la empresa de los clientes y transacciones de mayor riesgo dentro de las líneas de negocio de toda la empresa;

1.4.3.2. Aumento de los niveles de PIC de la empresa, conocimiento del cliente (KYC) y diligencia debida reforzada;

1.4.3.3. Se obtiene la documentación adicional adecuada para confirmar la identidad y las actividades comerciales lícitas de un cliente;

1.4.3.4. Escalada para la aprobación del establecimiento de una cuenta o relación;

1.4.3.5. Comprensión de las transacciones normales y esperadas de un cliente, incluida una mayor supervisión de las transacciones;

1.4.3.6. Mayores niveles de controles permanentes y frecuencia de las revisiones de las relaciones; y

1.4.3.7. Notificación de actividades sospechosas de conformidad con los requisitos de notificación vigentes.

2. Consulte los temas Política del Programa de Identificación de Clientes y Política Conozca a su Cliente de esta política para obtener orientaciones detalladas.

2.1. Supervisión de clientes y transacciones. El grado y la naturaleza de la supervisión que realiza la empresa dependen de su tamaño, de los riesgos de blanqueo de capitales que haya identificado, del método de supervisión utilizado (manual y/o automatizado) y del tipo de actividad que se esté examinando. No todas las transacciones, cuentas o clientes se controlan de la misma manera.

2.2. El grado de supervisión se basa en los riesgos percibidos asociados a un cliente, los productos o servicios que utiliza y la ubicación del cliente y de las transacciones. En cualquier caso, dicha supervisión se documenta adecuadamente. El principal objetivo del sistema de supervisión basado en el riesgo de la empresa es responder a los problemas de toda la empresa basándose en el análisis de sus principales riesgos. La supervisión con arreglo a este enfoque basado en el riesgo permite a la empresa crear umbrales monetarios o de otro tipo por debajo de los cuales no se revisará una actividad. Las situaciones definidas o los umbrales utilizados con este fin se revisan periódicamente para determinar su adecuación a los niveles de riesgo establecidos. Además, la Alta Dirección evalúa periódicamente la adecuación de los sistemas y procesos y los documenta debidamente. Consulte los temas correspondientes de esta política para obtener orientaciones detalladas con respecto a la supervisión de clientes y transacciones.

2.3. Notificación de transacciones sospechosas. La obligación legal y reglamentaria de notificar las transacciones o actividades sospechosas de la empresa ofrece a las autoridades federales la posibilidad de utilizar dicha información financiera para combatir el blanqueo de capitales, la financiación del terrorismo y otros delitos financieros. Cuando un requisito legal o reglamentario obliga a notificar una actividad sospechosa una vez que se ha formado una sospecha, la empresa debe presentar una notificación. Por lo tanto, no es aplicable un enfoque basado en el riesgo para la notificación de actividades sospechosas en estas circunstancias.

2.4. Sin embargo, un enfoque basado en el riesgo es apropiado para identificar actividades sospechosas (como dirigir recursos adicionales a las áreas que la empresa ha identificado como de mayor riesgo). En este mismo sentido, la empresa utiliza la información facilitada por las autoridades estatales y federales.

2.5. mejorar su enfoque para identificar actividades sospechosas. Además, la dirección siempre debe evaluar periódicamente la idoneidad de la formación y evaluación de los empleados del sistema de la empresa para identificar y notificar transacciones sospechosas.

2.6. Formación y sensibilización. La empresa imparte a sus empleados una formación sobre el programa de lucha contra el blanqueo de capitales y la financiación del terrorismo adecuada y proporcional a sus respectivos cargos. Este esfuerzo a nivel de toda la empresa proporciona a todos los empleados pertinentes información general sobre las leyes, reglamentos y políticas internas en materia de lucha contra el blanqueo de capitales:

2.6.1. Adaptado a la responsabilidad del personal correspondiente (por ejemplo, contacto con el cliente u operaciones);

2.6.2. Con el nivel de detalle adecuado (por ejemplo, personal de primera línea, productos complicados o productos gestionados por el cliente);

2.6.3. Con una frecuencia relacionada con el nivel de riesgo de la línea de negocio implicada; y

2.6.4. Prueba para evaluar conocimientos acordes con el detalle de la información facilitada.

Anexo 2: Control de las personas políticamente expuestas A continuación figura la definición de "PEP":

- Desempeña o ha desempeñado, en cualquier momento del año anterior, funciones públicas relevantes,
- Es familiar directo de dicha persona,
- Es un socio conocido de dicha persona,
- Es o ha sido, en cualquier momento del año anterior, encargado de una función pública destacada por cualquier estado;
- Un organismo internacional; o

Nota: Un familiar directo o un allegado conocido de una persona mencionada en el párrafo inmediatamente anterior no se considera necesariamente una PEP sin la correspondiente evaluación de riesgos.

En los casos en que se identifique una PEP:

- Antes de establecer un plan de acción, siempre se debe solicitar la aprobación de la alta dirección.
- Relación comercial con un PEP
- Debe establecerse el origen de los fondos.

La relación comercial debe ser objeto de un seguimiento reforzado y constante.

Establecer el origen de los fondos

Es importante que antes de entablar una relación comercial con una PEP se establezca su origen de fondos y que la empresa esté convencida de que no hay indicios de que los fondos que se utilizarán para las transacciones que se llevarán a cabo procedan de la corrupción (es decir, la recepción de sobornos), el fraude o un intento por parte de la PEP de retirar/ocultar activos de su país de origen. Por lo tanto, el funcionario designado es responsable de enviar una solicitud a una PEP identificada con el fin de establecer su fuente de fondos.

El origen de los fondos de la PEP puede establecerse formulando al individuo en cuestión una serie de preguntas para determinar de dónde recibe su dinero. Estas preguntas podrían incluir la confirmación de la fuente principal de ingresos (es decir, el salario), cualquier interés comercial o inversiones de las que se reciben/recibirán fondos.

Tomar la decisión de realizar transacciones con el PEP

Con el fin de satisfacerse, a continuación se presentan áreas sobre las cuales se pueden hacer preguntas al PEP para determinar si se debe establecer una relación de negocios - la información de esto se puede presentar a la Alta Dirección de PAGOS NACIONALES S.A.C. para que tomen una decisión informada:

- Cuál es el cargo y las funciones del PEP- (tenga en cuenta que un PEP de menor *seniority* es un riesgo menor que el de los jefes de Estado, diputados, miembros del poder judicial y embajadores).

- ¿Hay algún familiar o socio cercano que también sea PEP?
- Identificar al cliente y al beneficiario efectivo de la cuenta.
- Conozca el país de residencia del cliente.
- Conozca el objetivo de la apertura de la cuenta y el volumen y la naturaleza de la actividad prevista para la cuenta.
- Obtener información sobre la ocupación y las demás fuentes de ingresos.
- Obtenga información sobre los familiares directos o asociados que tienen poder para realizar transacciones en la cuenta.

Por favor, tenga en cuenta que actualmente PAGOS NACIONALES S.A.C. no realiza transacciones con ningún PEP.

Nazar Ianko
Gerente General

Anexo 3: Formato de reporte interno sobre operaciones sospechosas (ROS)

Nº SAR: ...../.....

Particulares	Observaciones
Date:	
ID del cliente:	
Nombre/dirección del cliente:	
Teléfono del cliente:	
Naturaleza de la actividad sospechosa:	
Detalle todas las sospechas: [Incluya detalles de las transacciones y comprobaciones de identidad].	
Adjunte los documentos pertinentes: 1. Recibos de transacciones 2. Documento de identidad y dirección 3. Comprobaciones de la lista de sanciones	
Nombre del funcionario informante:	
Firma del funcionario informante:	
Remitirse a UIF: [A cumplimentar por Funcionario designado]	
No haga referencia a UIF: Motivo de la decisión: Detalles	
Firma del funcionario designado:	
Fecha de remisión al funcionario designado Decisión:	