Bagrícola
Más que un banco, un aliado

RESOLUCION DE

Resolución No. 0038
Sesión No. 1792
Fecha: 20 ENE 2022

APROBACIÓN DE PRESENTACION DEL INFORME ANALISIS DE EVALUACION DE RIESGOS LAVADO DE ACTIVOS A LOS QUE SE EXPONDRÁ LA INSTITUCION, ANTE POTENCIALES CLIENTES QUE UTILICEN CANALES DIGITALES DE ESTE BANCO PARA FINES DE CONOCIMIENTO DE LOS SEÑORES MIEMBROS DEL DIRECTORIO EJECUTIVO.

El Presidente del Comité de Cumplimiento y Prevención Lavado de Activos, el **Sr. Salomón Rodríguez Santos**, junto a la Oficial de Cumplimiento, la Sra. **Naty Sabel Abreu**, le presenta a los señores miembros del Directorio Ejecutivo, un informe **ANALISIS DE EVALUACION DE RIESGOS LAVADO DE ACTIVOS A LOS QUE SE EXPONDRÁ LA INSTITUCION, ANTE POTENCIALES CLIENTES QUE UTILICEN CANALES DIGITALES**, con la finalidad de que el máximo organismo de Dirección de la Institución tenga conocimiento y emita su no objeción a la ejecución de dichos trabajos.

El **Sr. Rodríguez Santos**, presentó un resumen contentivo de los aspectos esenciales contenidos en los informes conocidos por el Comité de Cumplimiento y Prevención Lavado de Activos; así como, las recomendaciones realizadas, indicando que, dichos informes forman parte del paquete de documentación que el Banco Agrícola de la República Dominicana está asumiendo conjuntamente con toda la reglamentación requerida para la implementación de los Canales Digitales, las cuales están siendo sometidas al Organismos Superior para fines de conocimiento evaluación y aprobación

Visto el informe presentado, el cual es parte integral de la presente resolución y se encuentra en anexo.

Visto y escuchado lo indicado anteriormente, los señores miembros del Directorio Ejecutivo, por la presente, dan constancia del conocimiento y haber sido informados del contenido del **INFORME DE ANALISIS DE EVALUACION DE RIESGOS LAVADO DE ACTIVOS A LOS QUE SE EXPONDRÁ LA INSTITUCION, ANTE POTENCIALES CLIENTES QUE UTILICEN CANALES DIGITALES**, dejando como constancia la presente resolución.

Fernando Durán
Administrador General

SECRETARÍA GENERAL
Banco Agrícola

Limber Cruz
Miembro Titular

Persio Cruz Pichardo
Miembro Titular

Francisco L. Fernández Onofre
Miembro Titular

Héctor Radhamés González Medina
Miembro Titular

Arismendy Almonte
Miembro Titular

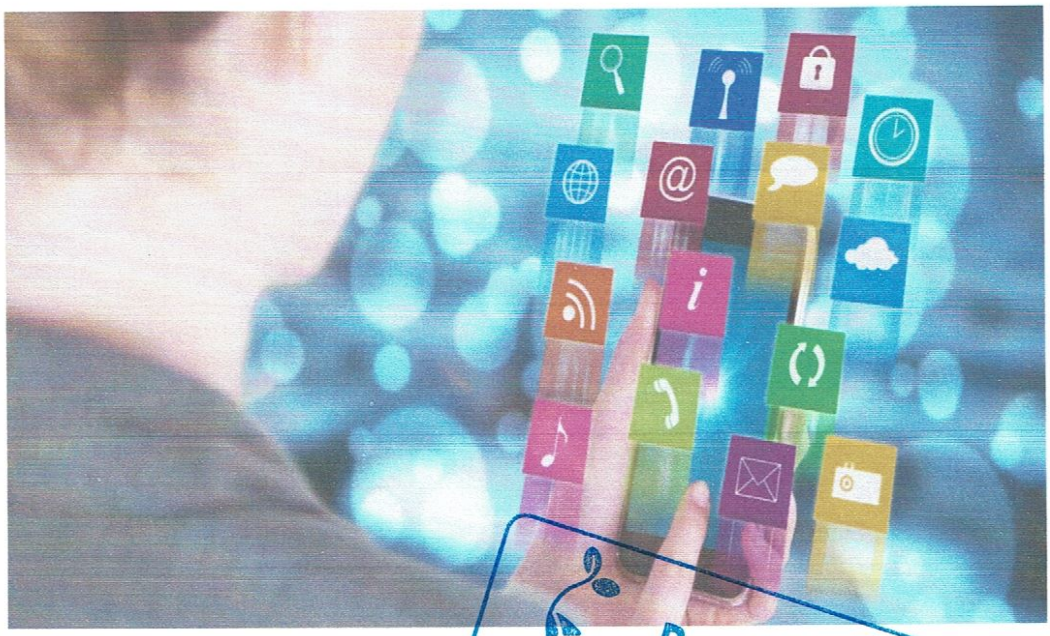
Bernardo Sánchez Rosario
Miembro Titular

ANALISIS DE EVALUACION DE RIESGOS LAVADO DE ACTIVOS A LOS QUE SE EXPONDRA LA INSTITUCION, ANTE POTENCIALES CLIENTES QUE UTILICEN

CANALES DIGITALES:

INTERNET BANKING

APP MOVIL BANKING



BancoAgrícola ¡Cosechando esperanza!
APROBADO
CONDICIONES PLANTEADAS

BancoAgrícola

Departamento de Cumplimiento

Diciembre 2021

CONTENIDO

INTRODUCCIÓN

INTRODUCCIÓN

Los avances tecnológicos y el uso de los canales digitales han significado el progreso y desarrollo de una parte de la humanidad, así como de las Instituciones financieras. En la actualidad, el Banco Agrícola de la República Dominicana, se encuentra en un proceso de modernización y busca estar al alcance de sus clientes, a través de un clic. Esto implica, una fuerte inversión no sólo desde el punto de vista de desarrollo tecnológico, si no, desde la perspectiva de administración de riesgos, pues son herramientas que están al alcance de todo el mundo incluyendo grupos delictivos. La Institución también ha visto en los dispositivos móviles y canales digitales una forma de seguir haciendo negocio y prestar un mejor servicio a nuestros clientes. Sin embargo, al momento de implementar los canales digitales, debemos tener en consideración los riesgos que los mismos representan, ya que estos se pueden convertir en un medio preferido por los delincuentes para lavar dinero y financiar al terrorismo.

Como parte de los requerimientos establecidos por las normas y regulaciones aplicables a las entidades de intermediación financieras y con base a los lineamientos aprobados por el Directorio Ejecutivo del Banco Agrícola, se estará realizando un análisis de los riesgos de lavado de activos a los que se expondrá la Institución ante potenciales clientes que utilicen los canales digitales.

En cumplimiento con estos requerimientos, el informe que presentamos a continuación, contiene la evaluación de los riesgos de lavado de activos a los que se impondrá la Institución ante potenciales clientes que utilicen los productos y canales "INTERNET BANKING Y APP MOVIL BANKING", así como los controles, alertas y monitoreo que tenemos establecidos para mitigar estos riesgos y que las operaciones se hagan de una manera segura para los clientes y la Institución.

- **MARCO REGULATORIO APLICABLE**

Las normas específicas que contemplan responsabilidades de cumplimiento para estas iniciativas son las siguientes:

A. Reglamento sobre lineamientos para la Gestión Integral de Riesgos
B. Reglamento sobre Riesgo Operacional e instructivos de aplicación.
C. Reglamento de Seguridad Cibernética y de la Información e instructivos de aplicación.
D. Instructivo sobre Prevención del Lavado de Activos, Financiamiento del Terrorismo y de la Proliferación de Armas de Destrucción Masiva (circular 003-18)

1. RESUMEN EJECUTIVO

1. RESUMEN EJECUTIVO - EVALUACIÓN DE RIESGOS DE LAVADO DE ACTIVOS: INTERNET BANKING Y APP MOVIL BANKING

Los avances tecnológicos que se nos presentan actualmente, han permitido u obligado al sistema financiero a evolucionar también, para retener a los clientes actuales y cautivar nuevos clientes a través de un mejor servicio y productos versátiles e innovadores y las nuevas tecnologías nos ayudan a lograrlo y así cubrir las necesidades del público y a la vez mantenernos competitivos.

El Proyecto de Internet Banking y App Móvil Banking, como parte de la estrategia de transformación tecnológica del Banco Agrícola, busca crear una nueva experiencia digital para todos sus clientes, adquiriendo los servicios y herramientas tecnológicas necesarias para la implementación de un canal digital vía un portal web amigable e interactivo: Internet Banking y a su vez, implementar un segundo canal interactivo de tipo aplicación móvil, para ser accedido mediante los dispositivos móviles de los clientes: App Móvil Banking.

Conforme a lo establecido en el ordinal V, secciones A, numeral 3, B, E y N, numeral 5 de la citada Circular (SIB: No. 003/18 y el numeral 12 de la Circular SIB No. 008/20 del 21 de abril del 2020, sobre Gestión y Monitoreo de Riesgos de Lavado de Activos, Financiamiento del Terrorismo y de la Proliferación de Armas de Destrucción Masiva, relacionadas con la contingencia sanitaria generada por el coronavirus (COVID-19); esta entidad realiza una evaluación de Riesgos de Lavado de Activos a los que se expondrá la Institución ante potenciales clientes que utilicen los canales digitales a implementar (Internet Banking y APP Movil).

Para la realización de esta evaluación se aplicó la metodología descrita a nivel de detalle en el Manual de Gestión de Riesgos de Lavado de Activos, Financiamiento del Terrorismo y proliferación de Armas de Destrucción Masiva. Este informe está conformado por los resultados de la Evaluación de la Matriz de Gestión de Riesgos de Eventos Potenciales LAFTPADM, para la implementación de los canales digitales (Internet Banking y APP Movil).

1.1 DESCRIPCION DE PRODUTOS Y SERVICIOS

El Internet Banking, es banca virtual, en la cual se puede realizar transacciones en línea, sin la necesidad de desplazarse a una entidad financiera. Estas se hacen a través de la Web (Dispositivos móviles, PC, Tablet, etc.)

La banca móvil es un servicio proporcionado por un banco u otra institución financiera, que permite a sus clientes realizar unas series de transacciones financieras, las cuales están disponibles las 24 horas al día.

El Proyecto de Internet Banking y App Móvil Banking (en lo adelante IBanking y App Móvil), contempla el desarrollo integral de procesos y herramientas que permitan la autenticación, consultas, transferencias y pago de productos de forma digital a través de ambos canales digitales.

El alcance específico de este proyecto está dividido en 2 FASES. Fase 1 en Q22021 y la Fase 2 en Q42021:

En la primera fase que estamos implementando, tenemos:

Consultas de Productos:

- Préstamos
- Cuentas de Ahorro
- Líneas de Crédito
- Depósitos a Plazo

Operaciones de Transferencias:

- Transferencias entre cuentas propias
- Transferencias hacia cuentas de terceros
- Transferencias a otras instituciones - ACH
- Transferencias agendadas (recurrentes)
- Transferencias Frecuentes
- Histórico de transferencias
- Transferencias masivas

Pago de Productos:

- Pagos de préstamos
- Pagos agendados (recurrentes)
- Histórico de pagos

Operaciones de Depósitos a plazos:

- Adelanto de efectivo

El Internet Banking y el uso de la APP Móvil, a pesar de que brindan comodidad y rapidez a los usuarios, pueden presentar los siguientes riesgos:

- No se agotan todos los procesos de actualización de debida diligencia a los clientes.
- Facilitan el ingreso de dinero proveniente de actos ilícitos.
- Producto financiero desde el que se realizan transacciones desde direcciones IP relacionadas en casos de fraude.
- Producto financiero desde el que se realizan transferencias desde una dirección IP diferente a la registrada en los históricos de transacciones
- Producto financiero desde el que se realizan transferencias electrónicas recibidas a favor u ordenadas desde un producto, cuyo dinero es retirado inmediatamente o en muy poco tiempo o transferencias a otros beneficiarios.
- El cliente realiza múltiples transferencias a diferentes beneficiarios, sin justificación aparente.
- Producto financiero desde el que se realizan transferencias con montos continuos, a cuentas de una persona física o jurídica externa, no acordes a su comportamiento habitual.

- Clientes que hacen depósitos de grandes cantidades de efectivo y seguidamente efectúan transferencias a otras cuentas, sin justificación razonable.

Para la identificación y evaluación de los riesgos a los que estaria expuesto la Institución en virtud de los potenciales clientes a los que se les ofreceran los servicios a través de los canales digitales, Cumplimiento realizó las siguientes actividades:

- Revisión de los Eventos Potenciales de Riesgos identificados en la **Matriz de Gestión Eventos Potenciales de Riesgos de LAFT-PADM- Implementación Internet Banking y APP Movil,** para cada Factor de Riesgo (Base de Clientes, Productos y Servicios, Área Geográfica (Jurisdicciones) y Canales de distribución).

- Los principales controles existentes para la mitigación de los riesgos identificados y la evaluación de la efectividad de los controles.

- Las señales de alerta automáticas y manuales que permitan el seguimiento a los eventos que se presenten.

- El sistema de monitoreo automatizado y manual que tiene el sistema para dar seguimiento a las alertas.

- Revisión de manuales de políticas y procedimientos documentados, y de la opinión experta del personal de la entidad.

2. OBJETIVO DEL INFOME - EVALUACIÓN DE RIESGOS DE LAVADO DE ACTIVOS: INTERNET BANKING Y APP MOVIL BANKING

Objetivo general y específico

Objetivo general:

Identificar los principales riesgos de lavado de activos y financiamiento del terrorismo, que presenta la Institución, al implementar el uso de los canales digitales, Internet Banking y App Móvil Banking por parte de los clientes, a través de una matriz de riesgo, con la finalidad de proponer acciones de gestión y control para estos riesgos.

Objetivos específicos:

1. Identificar las características de los Canales Digitales y los métodos utilizados para legitimar fondos de origen ilícito a través de ellos.

2. Analizar y cumplir con los establecido en la regulación sobre la Circular 003-18 correspondiente al Instructivo Sobre Prevención de Lavado de Activos, Financiamiento del Terrorismo y de la Proliferación de Armas de Destrucción Masiva, específicamente lo establecido en el ordinal V, secciones A, numeral 3, B, E y N, numeral 5, sobre Gestión y Monitoreo de Riesgos de Lavado de Activos, Financiamiento del Terrorismo y de la Proliferación de Armas de Destrucción Masiva.

3. Identificar, medir, controlar y monitorear los riesgos de LA/FT al implementar el uso por parte de los clientes, de los canales digitales de la institución, a través de una matriz de riesgos, para determinar las principales medidas que se deberían tomar para mitigar estos riesgos, a través de la aplicación de controles eficaces, producto de la evaluación de los Factores de Riesgos (Base de Clientes, Productos y Servicios, Canales de Distribución y Área Geográfica).

3. INFORME DE CUMPLIMIENTO

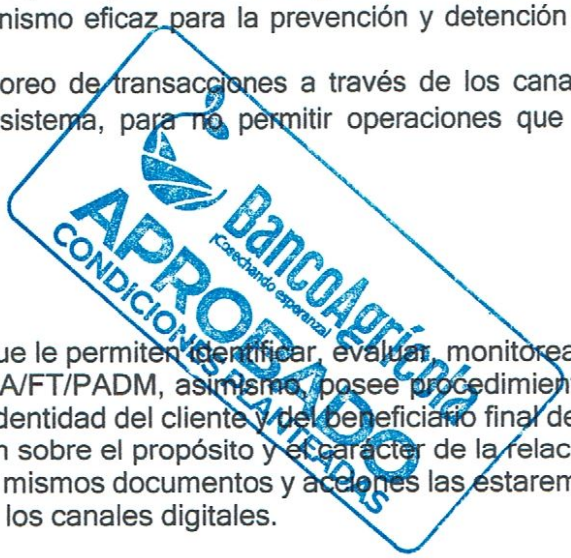
3. INFORME DE CUMPLIMIENTO - EVALUACIÓN DE RIESGOS DE LAVADO DE ACTIVOS: INTERNET BANKING Y APP MOVIL BANKING

El informe de Cumplimiento, sobre la evaluación de Riegos de Lavado de activos para la implementación de los canales digitales: Internet Banking y APP Móvil, considera los aspectos de debida diligencia que realiza la Institución relativos a:

1. **La aceptación de clientes,** que van a utilizar los Canales Digitales (Internet Banking y APP Móvil), sus reglas, controles políticas y procedimientos que existen en la Institución para aceptar un cliente.
2. **Identificación de Clientes, Beneficiarios Finales y Debida Diligencia,** en este proceso se identifica al cliente, y se le hace la debida diligencia al momento de captar al cliente y la debida diligencia continua a todos los clientes actuales, para conocer el perfil transaccional de estos e identificar alguna transacción que se salga de los parámetros habituales.
3. **Segmentación de los Clientes:** Con la Segmentación de los clientes, la Institución tiene un entendimiento más completo del perfil transaccional de estos, y así poder detectar operaciones inusuales. Nos permite saber cuándo aplicar una debida diligencia simplifica o una debida diligencia ampliada.

   Otros aspectos que incluye el informe son:

4. **Actividades del Comité de Cumplimiento,** evaluar los riesgos y mantener informado al Directorio Ejecutivo.
5. **Respuestas a Requerimientos de Información,** aquí mostramos como el Banco Agrícola como sujeto obligado considera de alta prioridad, la relación y comunicación con las autoridades del Sistema Financiero Nacional, en lo que tiene que ver con el cumplimiento de las medidas preventivas y correctivas.
6. **Reportes de Operaciones Sospechosas**, se muestra el cumplimiento de la Institución en caso de que se detecten operaciones sospechosas y se reportaría a los Organismos regulatorios.
7. **Señales de Alerta,** contamos con un mecanismo eficaz para la prevención y detención de operaciones de LA/FT/PADM.
8. **Monitoreo de transacciones**, para el monitoreo de transacciones a través de los canales digitales, existe la parametrización en el sistema, para no permitir operaciones que no cumplan con las regulaciones vigentes.
9. **Otros controles**



1. Aceptación de Clientes

El Banco cuenta con políticas y procedimientos que le permiten identificar, evaluar, monitorear y tomar acción eficaz para mitigar los riesgos de LA/FT/PADM, asimismo, posee procedimientos de debida diligencia para identificar y verificar la identidad del cliente y del beneficiario final de la operación, con la finalidad de obtener información sobre el propósito y el carácter de la relación comercial durante la vigencia de la misma. Estos mismos documentos y acciones las estaremos aplicando para los clientes que estarán utilizando los canales digitales.

Actualmente tenemos la política de **"debida diligencia y aceptación de clientes"** que establece los siguientes aspectos para aceptar los clientes:

1- No serán aceptados como Clientes para las aperturas de cuentas y otros productos y servicios financieros del Banco Agrícola, los siguientes:

a) Los que no cumplan con los requisitos exigidos en los "lineamientos generales de debida diligencia" establecidos en la política de **"debida diligencia y aceptación de clientes".**

b) Quienes evadan las regulaciones establecidas internas y los señalados en las listas de las resoluciones del consejo de seguridad de las Naciones Unidas (ONU) y en la lista de la Oficina de Control de Activos Extranjeros (Office of Foreign Assets Control, (OFAC).

c) Los que dificulten su identificación o que susciten serias dudas sobre la veracidad de sus datos y fuente de los recursos (dinero).

d) Los que no entreguen en forma fehaciente y oportuna, la información y documentación solicitada, así como los que se nieguen a proporcionarlas.

e) Aquellos cuya integridad y honestidad sean dudosas o si se tuviera algún indicio de vinculación al narcotráfico u otras de las infracciones graves señaladas en la ley 155-17, y al financiamiento del terrorismo.

f) Quienes capten dinero del público en forma masiva y habitual sin contar con la previa autorización de las autoridades competentes.

g) Las personas y empresas que se dediquen a la intermediación cambiaria sin la autorización de lugar para actuar como tales por las autoridades correspondientes.

h) Los comerciantes que distribuyan, intermedien o posean mercancías ingresadas o sacadas del país de manera irregular, o producida de forma ilegal.

i) Los que tengan negocios o realicen transacciones cuya naturaleza sea difícil o imposible para la institución, verificar la legalidad de sus operaciones o la procedencia de los fondos.

j) Los insolventes.

k) Los que hayan sido condenados por delitos de naturaleza económica o por lavado de activos y/o acción, el financiamiento del terrorismo y la proliferación de armas de destrucción masiva.

l) Las personas legalmente incapaces o que hayan sido objeto de remoción de sus cargos en la Administración Monetaria y Financiera, a causa de una actividad ilícita en el ejercicio de sus funciones.

m) Quienes hayan sido sancionado por infracción grave a las normas vigentes con la separación del cargo e inhabilitación para desempeño.

n) La persona física o jurídica que no cumpla con los requisitos establecidos por la Superintendencia de Bancos en la Circular SB NO.011-09 del 30 de noviembre del 2009.

Los instrumentos de que dispone el banco para asegurar la aceptación de clientes son:

- Manual de Control Interno, para la prevención del lavado de activos, financiamiento del terrorismo y la proliferación de armas de destrucción masiva.
- Política de debida diligencia y aceptación de clientes.
- Procedimiento creación y afiliación de clientes.

Adicional se fortalece el entrenamiento y la capacitación al personal de Negocios sobre Debida Diligencia, para que estén atentos a las señales de alerta al momento de aceptar un cliente. (**Ver Matriz de Gestión de eventos potenciales de riesgos de LAFT-PADM- Implementación Internet Banking y APP Móvil). En la actividad de afiliación de clientes tanto para personas físicas, jurídica, PEP, ONG).**

2. Identificación de Clientes, Beneficiarios Finales y Debida Diligencia

Mediante la formal identificación del cliente y el conocimiento de sus negocios y actividades, podemos evitar el LA/FT/PADM en la Institución. La debida diligencia al momento de captar al cliente y la debida diligencia continua a todos los clientes actuales, nos permiten conocer el perfil transaccional de estos e identificar alguna transacción que se salga de los parámetros habituales.

Estos controles contemplan que toda persona física o jurídica debe presentar una serie de documentos que comprueben la validez de las informaciones suministradas, si estos documentos resultan ser insuficientes, la Institución no aceptará el vínculo con el cliente y para esto tiene definida en su política de **"debida diligencia y aceptación de clientes"** los siguientes lineamientos de Debida Diligencia:

Dando cumplimiento a lo establecido en el artículo 38 de la ley 155-17, la entidad realiza una debida diligencia a sus actuales y potenciales clientes a fin de:

- ✓ Obtener la formal identificación y registro del cliente, y el conocimiento de sus negocios y actividades, al momento de iniciar la relación comercial con el Banco y durante la vigencia de la misma, confirmándolas a través de documentos suministrados, visitas, consultas y llamadas;
- ✓ Requerir en los casos de que una persona actúe en nombre de otro (cliente) para realizar transacciones en nombre del titular, la autorización o el poder que le otorga a éste para realizar la operación. De igual modo se deberá identificar y verificar la identidad de esa persona, así como, al beneficiario final. A tales fines, se deberá tomar las medidas adecuadas para verificar la identidad del beneficiario final requiriendo la información correspondiente;
- ✓ Identificar al beneficiario final y tomar las medidas razonables para verificar la identidad del beneficiario final usando la información pertinente o los datos obtenidos mediante fuentes confiables, de tal manera que se obtenga el conocimiento adecuado de quien es el beneficiario final;
- ✓ Obtener información sobre el propósito y el carácter que se pretende dar a la relación comercial y financiera;
- ✓ Aplicar los requisitos de la Debida Diligencia a los clientes (DDC) existentes, en base a la materialidad y el riesgo; así como deben considerar si se han tomado las medidas de

debida diligencia previamente y si los datos obtenidos son adecuados y actualizados según el riesgo.

En caso de que no se pueda realizar una Debida Diligencia satisfactoriamente, el Banco toma la decisión de no tener las relaciones con el cliente o relacionado o no realizar determinada transacción; en este caso se realiza un reporte de operación sospechosa.

Los registros de las operaciones con clientes, tanto nacionales como internacionales, son conservados en la Institución durante al menos diez (10) años después de finalizada la transacción o después de la fecha de la transacción ocasional, según corresponda. Esto incluye, todos los registros obtenidos a través de medidas de Debida Diligencia, como son los archivos de las operaciones activas y pasivas, así como, los resultados de los análisis realizados. Dichos registros deben ser suficiente para permitir la reconstrucción de cada una de las transacciones, a fin de que se puedan suministrar pruebas, si fuera necesario, para entablar un juicio por actividades delictivas.

Los documentos, datos o informaciones recopiladas en virtud de un proceso de Debida Diligencia se mantienen actualizados, mediante la revisión de los registros existentes.

Las transacciones que se efectúen a lo largo de esa relación son examinadas tanto por la Sucursal como por Cumplimiento, para asegurar que las mismas se correspondan con el conocimiento que se tiene del cliente, su actividad comercial y perfil de riesgo, así como, el origen de los fondos cuando corresponda.

La entidad ha adoptado el proceso de conocer al cliente de acuerdo a su naturaleza, tenemos las personas físicas y jurídicas que pueden ser nacionales o extranjeras. Para aquellas personas físicas que tengan doble nacionalidad se realiza el proceso de Debida Diligencia, para cada nacionalidad.

Los instrumentos que utiliza el banco para asegurar la Identificación de Clientes, Beneficiarios Finales y Debida Diligencia, son:

- Manual de Control Interno, para la prevención del lavado de activos, financiamiento del terrorismo y la proliferación de armas de destrucción masiva.
- Política de debida diligencia y aceptación de clientes.
- Sistema de Alerta manual, revisando las propias listas que hemos elaborado en la Institución, con las informaciones que obtenemos por publicaciones en la prensa; oficios de requerimiento de información que nos han solicitado las autoridades competentes y clientes con operaciones que recurrentemente son calificadas como sospechosas, o personas físicas y jurídicas que tenemos conocimiento que están siendo investigadas o procesadas por la comisión de delitos que generan ganancias ilícitas.
- Adicional revisamos la lista de personas y empresas relacionadas con el terrorismo y el narcotráfico (Specially Designated Nationals List-SDN) emitida por la "Office of Foreign Assets Control (OFAC)"; la lista y resoluciones sobre personas involucradas en actividades terroristas emitidas por el Comité del Consejo de Seguridad de las Naciones Unidas (ONU) y la lista de países y territorios no cooperantes con el GAFI, a fin de poner especial atención a las personas físicas o jurídicas citadas en las mismas y constantemente estamos actualizando las mismas.
- Realizamos un monitoreo constante de la aplicación e implementación de las políticas y procedimientos para la prevención de lavado de activos y el financiamiento del terrorismo.

- Mediante envío de emails, damos seguimiento desde Cumplimiento a las áreas encargadas de aplicar las políticas de "Conozca su Cliente" y verificar que las informaciones y datos suministrados por estos se revisan y actualizan periódicamente.

- Al momento del cliente solicitar el acceso a los canales digitales, el departamento de Operaciones, responsable de darle acceso al cliente, no lo ejecutará hasta que Cumplimiento confirme que se han realizado las revisiones correspondientes del cliente y el mismo puede ser aceptado.

Adicional a estas medidas se tiene un programa de cumplimiento que incluye entrenamiento y capacitación continua a Negocios, sobre el tema de debida diligencia y aceptación de clientes. **(Ver Matriz de Gestión de eventos potenciales de riesgos de LAFT-PADM- Implementación Internet Banking y APP Móvil). En la actividad de afiliación de clientes tanto para personas físicas, jurídica, PEP, ONG).**

Igualmente, cuando surgen cambios en las regulaciones que impactan los clientes y los canales digitales, se actualiza a los departamentos involucrados y se capacita nuevamente a Negocios sobre estos cambios.

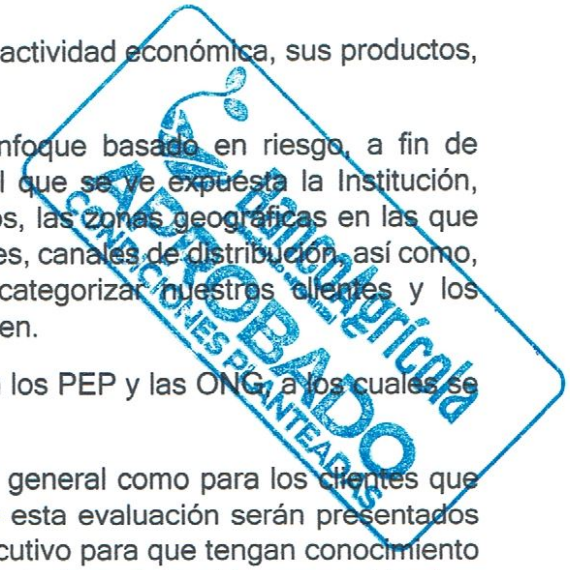
3. Segmentación de los Clientes

La segmentación de los clientes nos permite tener un entendimiento más completo del perfil transaccional de nuestros clientes, mediante ésta, podemos detectar operaciones inusuales. Nos permite saber cuándo aplicar una debida diligencia simplifica o una debida diligencia ampliada.

Si es necesario hace una **Debida Diligencia Ampliada** (DDA), la Institución solicita información adicional al cliente considerado de alto riesgo, como tipo de operaciones que realiza, origen de los fondos, movimientos de sus transacciones, si es un cliente PEP, visita al negocio para ver la actividad y regularidad de sus operaciones, etc.

Los clientes los tenemos segmentados dependiendo de su actividad económica, sus productos, sus canales de distribución y áreas geográficas.

Adicional tenemos las matrices de evaluación con un enfoque basado en riesgo, a fin de identificar, medir y mitigar los riesgos de LA/FT/PADM, al que se ve expuesta la Institución, tomando en cuenta los productos y servicios que ofertamos, las zonas geográficas en las que tenemos presencia, actividades económicas, tipos de clientes, canales de distribución, así como, cualquier otro factor que consideremos relevante para categorizar nuestros clientes y los hacemos en función del nivel de riesgo que estos representen.



Los clientes que representan mayor riesgo en la Matriz son los PEP y las ONG, a los cuales se les hace la debida diligencia ampliadas.

Nuestra matriz fue actualizada recientemente tanto a nivel general como para los clientes que estarían utilizando los canales digitales. Los resultados de esta evaluación serán presentados tanto al comité de Cumplimiento, Riesgo y al Directorio Ejecutivo para que tengan conocimiento de los Riesgos identificados como alto, medio y bajo y los controles establecidos para mitigarlos.

Los instrumentos con que cuenta el banco para asegurar la segmentación de los Clientes, son:

- Matriz de Gestión Eventos Potenciales de Riesgos de LAFT-PADM, segmentada por Base de clientes, canales de distribución, productos y servicios y Área geográfica. Esta matriz incluye los riegos inherentes, los controles y los riesgos residuales.

- Matriz de Gestión Eventos Potenciales de Riesgos de LAFT-PADM- implementación Internet Banking y APP Movil. segmentada por Base de clientes, canales de distribución y Área geográfica. Esta matriz incluye los riegos inherentes, los controles y los riesgos residuales

- El Banco dispone de señales de alerta y un esquema de monitoreo bajo supervisión (manual) que nos permiten identificar eventos potenciales de riesgo.

Adicionalmente, cuando surgen cambios en las regulaciones que impactan los clientes y los canales digitales, se actualiza la base de datos y la segmentación de los clientes, para adecuarla a las nuevas regulaciones, riesgos que se presenten y controles alternos que tengamos que implementar.

4. Actividades del Comité de Cumplimiento para informar al Directorio Ejecutivo:

Internamente, celebramos cada tres meses el Comité de Cumplimiento, con la finalidad de mantener informado a sus Miembros, así como al Directorio Ejecutivo, de los hechos relevantes que puedan estar impactando la Institución, así como los proyectos en curso para asegurar su cumplimiento, por lo que en nuestras presentaciones consideramos siempre:

1. Hechos Relevantes

    - Se presentar los eventos que hayan impactado la Institución y las medidas alternas de control que se han implementado.
    - Notificaciones de Sanciones, si aplican

2. Retrasos en remisión de reportes, si aplican
3. Estadísticas Reportes RTE y ROS
4. Estadísticas Requerimiento de Información de PLAFT SB

    - Certificación de Información (CI)

5. Estadísticas Requerimiento de Información de UAF
6. DDC-Clientes PEP's
7. Seguimiento Hallazgos Inspección SB
8. Circulares Reguladores (SB/BCRD)
9. Se presentan, las disposiciones normativas emitidas por la Administración Monetaria y Financiera y se da seguimiento al cumplimiento de las mismas a todos los niveles de la Institución.

10. Actividades Relevantes Realizadas en el Período (Lanzamiento de nuevos productos o servicios)
11. Seguimiento al Plan de Trabajo anual sobre Prevención de Lavado de Activos
12. Seguimiento del Plan anual de Capacitación
13. Seguimiento de Proyectos (Lanzamiento de nuevos productos o servicios)

- Evaluación de Riesgos Lavado de Activos - Internet Banking y App Móvil Banking

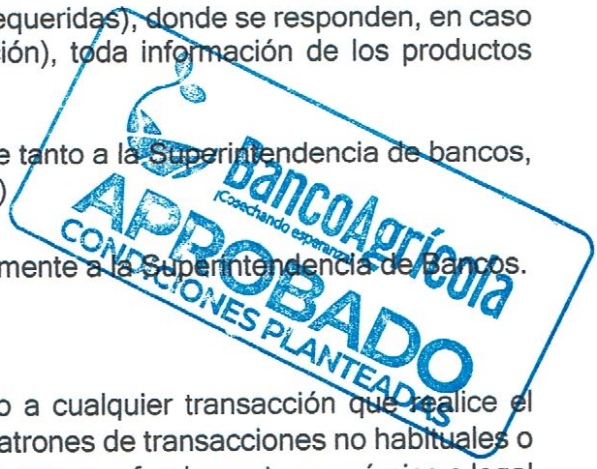
5. Respuestas a Requerimientos de Información

El Banco Agrícola como sujeto obligado considera de alta prioridad, la relación y comunicación con las autoridades del Sistema Financiero Nacional, en lo que tiene que ver con el cumplimiento de las medidas preventivas y correctivas.

Existen procesos claros y eficientes para las remisiones de las solicitudes de información a los Órganos Reguladores.

Entre los reportes que se remiten regularmente y los que son requeridos por los organismos reguladores tenemos:

- Formulario IF-02 (remisión de informaciones requeridas), donde se responden, en caso de que aplique (si son clientes de la Institución), toda información de los productos financieros, tantos activos, como saldados.
- Formulario IF-01, que se remite mensualmente tanto a la Superintendencia de bancos, como a la Unidad de Análisis Financiero (UAF)
- El reporte de los PEP, que se envía semestralmente a la Superintendencia de Bancos.



6. Reportes de Operaciones Sospechosas

En Cumplimiento como en la Sucursal, se está atento a cualquier transacción que realice el cliente por cualquiera de nuestros canales, que tenga patrones de transacciones no habituales o transacciones no significativas pero periódicas, que no tengan un fundamento económico o legal evidente, o que generen una sospecha de estar involucradas en el lavado de activos, alguna infracción precedente o determinante o en la financiación al terrorismo.

En base a esto, el Oficial de Cumplimiento prepara el Reporte de Operaciones Sospechosas y en este reporta todas las transacciones u operaciones efectuadas o no, que sean complejas, insólitas, significativas frente a todos los patrones de transacciones no habituales. Por lo que se examina, con especial atención, cualquier operación, con independencia de su cuantía, que, por su naturaleza, pueda estar vinculada al lavado de activos, el financiamiento del terrorismo y la proliferación de armas de destrucción masiva o cualquier delito subyacente que pueda dar inicio a considerar una transacción sospechosa. Cuando se han dado estos casos, se requiere mediante un email a través de la Sucursal, información del cliente sobre el origen de los fondos, el propósito de la transacción y la identidad de las partes involucradas en la misma.
Luego en Cumplimiento, cuando se recibe toda la información evalúa e identifica si se trata de una transacción sospechosa para reportarla a los organismos correspondientes.

Los instrumentos con los que cuenta el banco para reportar las actividades sospechosas, son:

- Reporte elaborado en la sucursal y analizado en la Sección de Cumplimiento, los cuales se remiten a la Unidad de Análisis Financiero dentro de los cinco (5) días hábiles después de realizada o intentada la operación, según los artículos 53 y 55, respectivamente de la Ley 155-17 y documentaciones que soporten ésta.

7. Señales de Alerta

Contamos con un mecanismo eficaz para la prevención y detención de operaciones de LA/FT/PADM, con el contacto directo en la sucursal, en el manejo transparente, íntegro y consistente de la información, que se logra con la documentación que soporta las transacciones y las indagaciones relativas a confirmar la veracidad de las informaciones ofrecidas por el cliente y el conocimiento de la naturaleza de sus operaciones.

Cuando determinamos y detectamos operaciones inusuales, realizamos desde Cumplimiento, un análisis con la información de los clientes, que permita conforme a un buen criterio del funcionario, identificar si la firma de un contrato o la realización de un acto se realiza con un cliente que puede presentar operaciones sospechosas.

A continuación, tenemos un catálogo de ejemplos de operaciones con el fin de aumentar el grado de conocimiento de aquellas circunstancias que pueden dar lugar a sospechas, o que configuran la existencia del lavado de activos, el financiamiento del terrorismo y la proliferación de armas de destrucción masiva. El mismo es un mecanismo de control que consiste en identificar prototipos de conductas que ilustran o revelan sobre comportamiento o procedimientos utilizados por individuo(s) o empresa(s), para lavar activos o financiar actividades terroristas, así como comportamiento y situaciones atípicas que presentan operaciones que pueden encubrir tales riesgos, estas informaciones se le suministran a los Gerentes y al equipo de la sucursal, para ampliar sus conocimientos, y que reconozcan estas señales de alerta, como son:

a) Operaciones que no están de acuerdo con la capacidad económica del cliente: Una persona que, sin fundamento, aparece como dueño de importantes negocios.

b) Clientes cuyos estados financieros reflejan resultados muy diferentes frente a las otras empresas del mismo sector o con actividad similar.

c) Depósitos importantes no usuales de dinero en efectivo hechos por una persona o una sociedad, cuyas actividades aparentes de negocio normalmente se generarían utilizando cheques y otros instrumentos.

d) Clientes que se oponen a dar informaciones para los reportes o para proceder con la transacción, una vez que se les informa que el reporte debe ser firmado y presentado.

e) Clientes que no deseen informar antecedentes personales cuando abren una cuenta o realizar una transacción por encima de límite que requiere del reporte.

f) Clientes que por primera vez utilizan nuestros servicios, cuyo teléfono de la casa esta desconectado o el de su trabajo falso.

g) Clientes que solicitan el uso de los Canales digitales, y una vez aprobado, realizan operaciones inusuales.

h) Clientes que declinan facilitar información, que en circunstancias normales les permite acceder a un crédito o a otros servicios bancarios que son sin dudas valiosos.

i) Insuficiente utilización de las ventajas bancarias normales como, por ejemplo, clientes que evitan altos tipos de intereses para grandes depósitos.

j) Resistencia de un cliente a facilitar la información normal requerida al abrir una cuenta, efectuar un depósito o solicitar el uso de los canales digitales, facilitando información mínima o falsa o cuando solicita abrir una cuenta facilita información que es difícil o clara de verificar para la Institución.

Para el tema de las alertas que se puedan presentar con los clientes y que nos permiten identificar transacciones sospechosas tenemos:

- Manual de Control Interno, para la prevención del lavado de activos, financiamiento del terrorismo y la proliferación de armas de destrucción masiva.
- Política de debida diligencia y aceptación de clientes.
- Procedimiento creación y afiliación de clientes.
- Reportes vía email, que envían las Sucursales a Cumplimiento ante señales de alerta de transacción inusual.
- Entrenamientos que se realiza al personal de la Sucursal y personal que está en contacto con los clientes (ver programa anual de capacitación y entrenamiento de Cumplimiento).
- El banco dispone de señales de alerta y un esquema de monitoreo bajo supervisión (manual) que nos permiten identificar eventos potenciales de riesgo. (ver email de seguimiento con las sucursales).

Adicionalmente, ante eventos que puedan surgir en la Institución y que no fueron detectados oportunamente, tenemos como control una actualización continua de las señales de alertas que tenemos identificadas y se actualizan directamente en cumplimiento. Estas nuevas señales de alertas son informadas a negocios para que tengan conocimiento y tomen las acciones correspondientes con los clientes

Igualmente, si el Regulador informa sobre nuevos esquemas de fraude que se estén realizando, se incluyen las señales de alertas referentes a los mismos, como controles adicionales para mitigar los riesgos.

8. Monitoreo de transacciones

En cuanto a los aspectos del monitoreo que se les hará a los clientes que utilicen los Canales digitales de la Institución y con el objetivo de prevenir el uso de nuestros productos financieros a través de los canales digitales, como medio en el cual personas físicas o jurídicas utilicen para

dar apariencia legitima a bienes o activos ilícitos, el sistema tiene parametrizado los siguientes controles para que de manera automática se realice el monitoreo a las transacciones, entre los que tenemos:

Parametro para generar las alertas				
Descripcion de la alerta	**Criterios establecidos**	**Tipos de atertas**	**Tipo de accion**	**Area**
El cliente ha agotado el limite establicido diario para realizar transferencia a terceros	Pago a terceros es igual al monto establecido diario	Proactiva	Enviar correo a operaciones	Operaciones
limite establecido diario	monto establecido diario	Preventiva	cumplimiento	Cumplimiento
Cuentas que pasan de registrar bajas sumas de dinero a cantidades muy altas en poco tiempo	Depósito de mas de un 700% en una semana	Preventiva	Enviar correo a cumplimiento	Cumplimiento
Depósitos de grandes sumas a cuentas que estaban inactivas	Depósito que superen los 500 mil pesos	Preventiva	Enviar correo a cumplimiento	Cumplimiento
El cliente realiza en forma reiterada operaciones fraccionadas	Más de 10 depósitos al dia a un mismo benficiario	Preventiva	Enviar correo a cumplimiento	Cumplimiento
El cliente realiza operaciones complejas sin una finalidad aparente	Depósito que superen los 500 mil pesos y la justificacion sea dudosa	Preventiva	Enviar correo a cumplimiento	Cumplimiento
Transferencias hacia o desde países registrados en las listas de bloqueo	Transferencias a paise en lista de bloqueo	Preventiva	Enviar correo a cumplimiento	Cumplimiento
Pago otros bancos cuyo monto excede al 10 % del balance promedio del cliente	Pago otros bancos cuyo monto excede al 10 % del balance promedio de la cuenta del cliente	Preventiva	Enviar correo a cumplimiento	Cumplimiento
Pago prestamos cuyo monto excede al 10 % del balance promedio del cliente	Pago prestamos cuyo monto excede al 10 % del balance promedio de la cuenta del cliente	Preventiva	Enviar correo a cumplimiento	Cumplimiento
Pago prestamos otros bancos cuyo monto excede al 10 % del balance promedio del cliente	Pago prestamos otros bancos cuyo montoexcede al 10 % del balance promedio de la cuenta del cliente	Preventiva	Enviar correo a cumplimiento	Cumplimiento
Pagos prestamos a tercero cuyo monto excede al 10 % estimado del balance promedio del cliente	Pagos TC cuyo monto excede al 10 % del balance promedio de la cuenta del cliente	Preventiva	Enviar correo a cumplimiento	Cumplimiento
Transferencias cuyo monto excede al 10 % estimado del balance promedio del cliente	Transferencias cuyo monto excede al 10 % del balance promedio de la cuenta del cliente	Preventiva	Enviar correo a cumplimiento	Cumplimiento

9. Otros controles adicionales que tenemos son:

   1. **Parametrización de la Plataforma:**

      - Se han definido <u>límites operativos para los productos y servicios</u> habilitados a través de un BackOffice que gestione el IBanking y App Movil Banking, como:
        a. Cantidad máxima de transacciones
        b. Monto máximo por transacción

2. La Institución cuenta con procesos de monitoreo especializados para operaciones realizadas a través del IBanking y App Móvil Banking:
    a. Monitoreo para la prevención de fraudes
    b. Monitoreo para la prevención de lavado de activos
    c. Monitoreo relacionado a la seguridad cibernética y de la información.
    d. Monitoreo de los componentes tecnológicos.

3. Se han elaborado las políticas y procedimientos que normarán el IBanking y App Móvil Banking, incluyendo reglas de uso, operaciones no aceptadas, responsabilidades, entre otros elementos del proceso, como son:
    a. Política de debida diligencia y aceptación de clientes
    b. Política de gestión y administración de canales digitales
    c. Procedimiento de creación y afiliación de clientes
    d. Procedimiento de gestión de incidentes, parámetros y solicitudes
    e. Manual de Usuario - Internet Banking
    f. Manual de Backoffice
    g. Manual de Políticas y Procedimientos para el manejo de reclamaciones
    h. Política de conservación de Información (en base a normas locales aplicables al sector, para fines de asegurar un adecuado resguardo de las informaciones que surjan de las operaciones realizadas a través del proceso de los canales digitales IBanking y App Móvil Banking).

4. Se han definido controles de transacciones y vinculación de productos y servicios a través de estos canales digitales. Y la plataforma incluye un control adicional, para garantizar y asegurar las siguientes transacciones:
    a. Transferencias entre cuentas de terceros y cuentas a otros Bancos.
    b. Pago de productos de otros Bancos.
    c. Pago de Servicios.
    d. Registro de cuentas de terceros y de otros Bancos.
    e. Registro de productos tarjetas de crédito, débito y préstamo de terceros y de otros Banco.

5. El sistema tiene establecido controles de validación de información que aseguran la integridad y validez de las informaciones de los clientes. Ejemplo: Controles de validación en los sistemas internos sobre datos de clientes.

6. Se ha elaborado y ejecutado un plan de capacitación / entrenamiento, orientado al personal operativo, técnico y de servicio al cliente, sobre el manejo de los elementos asociados a los canales digitales IBanking y App Móvil Banking, su impacto en los procesos y los diferentes elementos de responsabilidad asociados a la gestión operativa y tecnológica de estos servicios.

7. Se ha elaborado un plan de contingencia y continuidad para los procesos y dependencias tecnológicas en la premisa (Banco) y en la plataforma en la nube (proveedor).

8. Procesos A continuación, se listan las consideraciones más relevantes asociadas al factor "procesos" de los canales digitales IBanking y App Móvil Banking:

a. El proceso de autenticación de los canales digitales IBanking y App Móvil Banking es automático y validado internamente con las bases de datos de clientes internos del Banco.

b. El proceso de la plataforma tecnológica, será gestionado por el proveedor Bankingly en integración con el proceso tecnológico interno vía el Core Bancario del Banco.

9. Tecnología de la Información & Seguridad Cibernética y de la Información A continuación, se listan las consideraciones más relevantes asociadas al factor "Tecnología de la Información y Seguridad Cibernética & de la Información" de los canales digitales IBanking y App Móvil Banking:

   a. El proveedor Bankingly, proveerá al banco, la plataforma tecnológica de los canales digitales IBanking y App Móvil Banking en la nube, en modalidad tipo SaaS (Software as a Service, o Software como servicio).

   b. Se utilizarán web services y application programming interface (APIs), para las interconexiones y enlaces entre la cloud y core bancario del Banco.

   c. Todos los servicios de Bankingly, están soportados por la plataforma de la nube de Microsoft, denominada Microsoft Azure, estableciendo relaciones de confianza con los ambientes on-premises para habilitar el intercambio seguro de datos entre los canales digitales y el sistema Core Bancario del Banco.

   d. Se tiene un portal de administración, para administrar todos los canales digitales. El acceso está restringido por el Banco, a sus usuarios administradores.

   e. Todos los servicios consumidos desde las Apps nativas están expuestos mediante HTTPS (protocolo HTTP con SSL/TLS), por lo que toda la comunicación se realiza de forma encriptada. Así como también, Todos los servicios del API están expuestos mediante HTTPS (protocolo HTTP con SSL/TLS), por lo que toda la comunicación se realiza de forma encriptada.

Adicional a todos estos controles referentes al monitoreo de las transacciones y de los clientes que utilizaran los Canales Digitales, cuando Regulador informa sobre nuevos esquemas de fraude que se estén realizando, se incluyen las señales de alertas referente a los mismos, como controles adicionales para mitigar los riesgos y estas son incorporadas en los monitoreos que tenemos establecidos. **(Ver Matriz de Gestión de eventos potenciales de riesgos de LAFT-PADM-Implementación Internet Banking y APP Móvil). En la actividad de monitoreo de transacciones).**

10. Uso de Servicios CLOUD

En cumplimiento con el reglamento e instructivo de seguridad cibernética y de la información, y en la evaluación de riesgos de este tipo de servicio tecnológicos a contratar, incluyendo en su alcance los controles de conexión, procesamiento, privacidad de informaciones, capacidades de control y robustez del proveedor a ofrecer el servicio. Se verificaron los componentes asociados al uso de la nube para confirmar que:

a. El proveedor Bankingly ofrece una plataforma de canales digitales en modalidad SaaS (Software as a Service, o Software como servicio) alojadas en la nube de Microsoft Azure.

b. Los canales digitales ofrecidos por el proveedor para este proyecto son: Web y Smartphone Apps, que son los canales digitales IBanking y App Móvil Banking.

c. Toda la información de Bankingly catalogada como sensible, se transmite y almacena encriptada utilizando el estándar de cifrado avanzado AES.

d. Se tiene una conexión cifrada y seguridad entre los ambientes proveedor y banco: Bankingly Microsoft Azure y banco - Plataforma interna Core Bancario.

11. Controles ante Riesgos de eventos eternos

A continuación, se listan las consideraciones más relevantes asociadas al factor "Eventos Externos" de los canales digitales IBanking y App Móvil Banking:

a. El servicio de los canales digitales IBanking y App Móvil Banking tendrá total exposición en el Internet.

b. La plataforma tecnológica de ambos canales digitales IBanking y App Móvil Banking recae sobre el mismo proveedor Bankingly.

c. Dependencias tecnológicas del proveedor Bankingly con otros proveedores (Microsoft Azure), como proveedores de servicio IaaS y PaaS de Bankingly).

Controles establecidos:

a. La plataforma cuenta con la posibilidad de parametrizar IPs válidas y países válidos para acceder a los canales digitales y al portal de administración.

b. Bankingly cuenta con un firewall para aplicaciones web (WAF) con protección avanzada contra bots y los servicios de detección de shell de puerta trasera.

c. Bankingly ejecutan por medio de terceros, ethical hacking (pentesting), para el control de vulnerabilidades, garantizándose la cobertura de OWASP top 10.

4. RESULTADOS DE LA EVALUACION

4. RESULTADOS DE LA EVALUACION - EVALUACIÓN DE RIESGOS DE LAVADO DE ACTIVOS: INTERNET BANKING Y APP MOVIL BANKING

La rapidez con que se envían los datos a través del internet banking y las APP móvil, ha facilitado el lavado de activos y el financiamiento del terrorismo. Motivo por el cual, hoy en día conforme avanza el comercio electrónico y por ende la banca electrónica, se hace más necesario evaluar los riegos de lavado de activos que esta representa, por lo que requerimos el conocimiento pleno del cliente, de la fuente de sus recursos y del uso de los canales a su disposición, que permitan determinar el comportamiento esperado de los clientes y por lo tanto el nivel de riesgo al que está expuesto la institución.

Como resultado de todos los riesgos que se han identificado para los clientes que estarían utilizando los canales digitales, (**Ver Matriz de Gestión Eventos Potenciales de Riesgos de LAFT-PADM- Implementación Internet Banking y APP Móvil**), así como los controles establecidos actualmente, para mitigarlos, adicional a todas la medidas de prevención de lavado de activos y financiamiento de terrorismo que tiene la institución actualmente y que indicamos en el punto No. 3 de ese Informe, donde tenemos:

- Manuales, políticas y procedimientos, los cuales han sido aprobados por el Directorio Ejecutivo.
- Señales de Alerta claramente identificadas.
- Mecanismos de monitoreo parametrizados de manera automática en la herramienta,
- Monitoreo manual, mediante el seguimiento que le hace Cumplimiento, Operaciones y las Sucursales, al momento de que surja alguna alerta de riesgo de lavado.

- En base a todos estos mecanismos de control de que dispone la Institución, podemos indicar que la Institución está preparada para implementar el Internet Banking y la App Móvil para nuestros clientes.

5. OBSERVACIONES FINALES

5. OBSERVACIONES FINALES - EVALUACIÓN DE RIESGOS DE LAVADO DE ACTIVOS: INTERNET BANKING Y APP MOVIL BANKING

Es importante indicar que la Institución está actualmente en un proceso de modernización y adecuación de todas sus estructuras, así como de revisión de sus procesos, los cuales estarán fortaleciendo la gestión y monitoreo del uso de los Canales Digitales por parte de nuestros clientes, entre lo que podemos citar:

a. La reestructuración del departamento de Tecnología de la Información.
b. La creación del departamento de Ciberseguridad, con la elaboración y fortalecimiento de sus políticas y procedimientos..
c. La creación de la Gerencia de Operaciones, la cual estará a cargo dentro de sus funciones, del seguimiento y control de todo lo relativo a los canales digitales y el manejo de las reclamaciones de la Institución.

Por lo que el Banco Agrícola, se compromete, si, a aplicar las disposiciones en materia de prevención de lavado de activos, y financiamiento del terrorismo y de la proliferación de armas de destrucción masiva, previstas por los Organismos Reguladores, las mejores prácticas internacionales y las políticas establecidas por la Institución, así como a fortalecer nuestro programa de cumplimiento basado en riesgos para incorporar ahora el cumplimiento respecto a los Canales digitales.

El programa actual de cumplimiento contempla para el uso de los Canales digitales, sin ser limitativo:

Actual:

a. Políticas y procedimientos para evaluar los riesgos en lavado de activos y financiamiento del terrorismo y mitigarlos.
b. Políticas y procedimientos de gestión de personal.
c. Código de ética.
d. Régimen de sanciones disciplinarias.

Para el 2022:

e. Implementación de un software de Prevención de Lavado, Monitor Plus, que es un avanzado sistema de análisis y monitoreo, que funciona en tiempo real. (estimado para el 2022).

f. Auditoría externa, que se encarga de verificar la efectividad del programa de cumplimiento. (estimada para el 2022).