EL PRESENTE DOCUMENTO ES UNA VERSIÓN PÚBLICA DEL

MANUAL DE POLÍTICAS DE PROTECCIÓN DE DATOS PERSONALES (PO -PDP) DE MMG BANK CORPORATION Y SUBSIDIARIAS

MMG BANK

2022

CONTENIDO

1. INTRODUCCIÓN

MMG Bank Corporation y subsidiarias, en adelante MMG Bank, en cumplimiento de lo dispuesto en la Ley 81 de 2019, que desarrolla el artículo 42 de la Constitución Política, ha desarrollado una Política Organizacional de Protección de Datos Personales, en adelante PO-PDP, y la aplica en el tratamiento de los Datos Personales obtenidos como consecuencia de la activad comercial que realiza y de los servicios y productos que ofrece a clientes y público en general.

MMG Bank, expresa su interés en la protección de la intimidad y de la privacidad de sus colaboradores y clientes y toda aquella persona cuyos datos hayan sido suministrados directa o indirectamente a MMG Bank durante en el desarrollo de sus actividades comerciales, en particular durante las actividades de tratamiento a las que dichos datos son sometidos y las cuales se realizan en respeto de los principios acceso, legalidad, equidad, confidencialidad, seguridad y lealtad.

MMG Bank se compromete a proteger la integridad de toda la información personal a la que tiene acceso y protegerla del uso y/o accesos indebidos, de acuerdo con las normas de la Ley 81 de 2019, sobre Protección de Datos Personales y las reglamentaciones que emitan las autoridades competentes y aplicando las mejores prácticas de seguridad sobre la materia, e informará a los propietarios de los datos personales de cualquier tratamiento realizado por terceros que se considere pueda ser contrario a la normativa vigente en la República de Panamá y en consecuencia, pudiese representar un riesgo para los datos personales.

MMG Bank por este medio declara que toda la información personal que se encuentra en nuestras bases de datos ha sido obtenida de forma lícita en el desarrollo de nuestra actividad comercial, que su recopilación se ha hecho y se hará siempre en atención al interés legítimo y a criterios de cumplimiento normativo y que de forma periódica se realiza una verificación de las autorizaciones de tratamiento que hemos recibido de los propietarios de dicha información.

En todo caso y en cumplimiento de la legislación vigente en materia de PDP, MMG Bank conservará la prueba de la autorización otorgada por los titulares de los Datos Personales para su tratamiento, utilizando mecanismos digitales y políticas de seguridad que garanticen la verificación de la forma y fecha en la que se realizó la autorización.

2. INFORMACIÓN GENERAL SOBRE LA PO-PDP

2.1 Responsable del Tratamiento de Datos Personales

MMG Bank es el responsable del tratamiento de Datos Personales. Sus oficinas principales se encuentran ubicadas en Ave. Paseo del Mar, Costa del Este, MMG Tower, Piso 22, Ciudad Panamá, República de Panamá. Teléfono 265-7600. Para temas relacionados con el ejercicio de los Derechos ARCOP, escribir a pdp@mmgbank.com o acceder a los formularios que están disponibles en la página www.mmgbank.com/pdp.

2.2 Definiciones

- Almacenamiento de datos. Conservación o custodia de datos en una base de datos establecida en cualquier medio provisto, incluido el de las Tecnologías de la Información y la Comunicación (TICs).
- Base de datos. Conjunto ordenado de datos de cualquier naturaleza, cualquiera que sea la forma o modalidad de su creación, organización o almacenamiento, que permite relacionar los datos entre sí, así como realizar cualquier tipo de tratamiento o transmisión de estos por parte de su custodio.
- Bloqueo de datos. Restricción temporal de cualquier acceso o tratamiento de los datos almacenados.
- Base de Datos. Conjunto ordenado de datos de cualquier naturaleza, cualquiera que sea la forma o modalidad de su creación, organización o almacenamiento, que permite relacionar los datos entre sí, así como realizar cualquier tipo de tratamiento o transmisión de estos por parte de su custodio
- Consentimiento. Manifestación de la voluntad del titular de los datos, mediante la cual se efectúa el tratamiento de estos.
- Custodio de la base de datos. Persona natural o jurídica, de derecho público o privado, lucrativa o no, que actúa a nombre y por cuenta del responsable del tratamiento y le compete la custodia y conservación de la base de datos.
- Datos confidenciales. Aquellos datos que por su naturaleza no deben ser de conocimiento público o de terceros no autorizados, incluyendo aquellos que estén protegidos por ley, por acuerdos de confidencialidad o no divulgación, a fin de salvaguardar información. En los

casos de la Administración Pública, son aquellos datos cuyo tratamiento está limitado para fines de esta Administración o si se cuenta con el consentimiento expreso del titular, sin perjuicio de lo dispuesto por leyes especiales o por las normativas que las desarrollen. Los datos confidenciales siempre serán de acceso restringido.

- Dato anónimo. Aquel dato cuya identidad no puede ser establecida por medios razonables o el nexo entre este y la persona natural a la que se refiere.
- Dato caduco. Aquel dato que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiera norma expresa, por el cambio de los hechos o circunstancias que consigna.
- Dato personal. Cualquier información concerniente a personas naturales, que las identifica o las hace identificables.
- Dato disociado. Aquel dato que no puede asociarse al titular ni permitir por su estructura, contenido o grado de desagregación la identificación de la persona, sea esta natural.
- Dato sensible. Aquel que se refiera a la esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, a la preferencia u orientación sexual, datos genéticos o datos biométricos, entre otros, sujetos a regulación y dirigidos a identificar de manera unívoca a una persona natural.
- Eliminación o cancelación de datos. Suprimir o borrar de forma permanente los datos almacenados en bases de datos, cualquiera que sea el procedimiento empleado para ello.
- Información de Identificación Personal (IIP). Toda información que por sí sola no puede asociarse al titular ni permitir la identificación de una persona natural, pero que asociada a otra información permite identificar o individualizar a una persona natural.
- Modificación de datos. Todo cambio en el contenido de los datos almacenados en bases de datos.

- Procedimiento de disociación o anonimización. Todo tratamiento de datos que impide que la información disponible en la base de datos pueda asociarse a persona natural determinada o determinable.
- Responsable del tratamiento de los datos. Persona natural o jurídica, de derecho público o privado, lucrativa o no; que le corresponde las decisiones relacionadas con el tratamiento de los datos y que determina los fines, medios y alcance, así como cuestiones relacionadas a estos.
- Titular de los datos. Persona natural a la que se refieren los datos.
- Transferencia de datos. Dar a conocer, divulgar, comunicar, intercambiar y/o transmitir, de cualquier forma y por cualquier medio, de un punto a otro, intra o extrafronterizo, los datos a personas naturales o jurídicas distintas del titular, ya sean determinadas o indeterminadas.
- Tratamiento de datos. Cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permita recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, asociar, disociar, comunicar, ceder, intercambiar, transferir, transmitir o cancelar datos, o utilizarlos en cualquier otra forma.

2.3 REGULADORES Y MARCO LEGAL Y NORMATIVO.

2.3.1 Entidades Reguladoras (encargadas de Supervisión y Control):

2.3.1.1 Superintendencia de Bancos

La Superintendencia de Bancos de Panamá es el órgano máximo del Estado en materia de regulación y supervisión de todos los bancos y empresas fiduciarias. Tiene competencia en todo el territorio nacional, con independencia política, autonomía patrimonial y administrativa.

La Superintendencia de Bancos fue creada mediante Decreto Ley 9 de 26 de febrero de 1998 e inició operaciones a partir del 13 de junio de 1998. El Decreto Ley 2 de 2008 vigente a partir del 25 de agosto de 2008, por el cual se reforma el régimen bancario regulado por el Decreto Ley 9 de 1998.

La Ley 1 de 5 de enero de 1984 que regula el Fideicomiso en Panamá y adopta otras disposiciones, y que conforme lo dispone el artículo 36 de la Ley 1 de 5 de enero de 1984, corresponde al Órgano Ejecutivo a través del Ministerio de Planificación y Política Económica, reglamentar el ejercicio del negocio de Fideicomiso.

En virtud de lo establecido en la Ley 81 de 2019, la Superintendencia de Bancos de Panamá, en su calidad de Regulador de una actividad regulada por ley especial, pasa a ser el Regulador en materia de PDP para todos los sujetos que se dedican a la actividad Bancaria y al Fideicomiso.

2.3.1.2 Superintendencia del Mercado de Valores

Superintendencia del Mercado de Valores es el organismo autónomo del Estado con personería jurídica y patrimonio propio, cuya atribución principal es el fomentar y fortalecer las condiciones propicias para el desarrollo del mercado de valores en la República de Panamá. Tiene ámbito en toda la República de Panamá.

Fue creada mediante el Decreto Ley No.1 de 8 de julio de 1999, publicado en la Gaceta Oficial No. 23,837, de 10 de julio de 1999. Mediante la Ley 67 de 2011, mediante la cual la Superintendencia del Mercado de Valores cambió su nombre a Superintendencia del Mercado de Valores y se establece el Sistema de Coordinación y Cooperación interinstitucional entre los Entes de Fiscalización financiera.

En virtud de lo establecido en la Ley 81 de 2019, la Superintendencia del Mercado de Valores de Panamá, en su calidad de Regulador de una actividad regulada por ley especial, pasa a ser el Regulador en materia de PDP para todos los sujetos que se dedican a la actividad de inversión en el mercado de valores.

2.3.1.3 Unidad de Análisis Financiero para la prevención del blanqueo de capitales y el financiamiento del terrorismo – UAF

Es el centro nacional para la recopilación y análisis de información financiera relacionada con los delitos del blanqueo de capitales, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva, así como para la comunicación de los resultados de ese análisis a las autoridades de investigación y represión del país.

Fue creada mediante Decreto Ejecutivo No. 136 de 1995 como Unidad de Análisis Financiero para la Prevención del Lavado de Dinero.

2.3.1.4 Autoridad Nacional de Transparencia y Acceso a la Información - ANTAI

La ANTAI fue creada mediante la Ley 33, de 25 de abril de 2013, es el organismo de la administración pública responsable de supervisar, implementar y controlar el cumplimiento de la Ley 81 de 2019. A través de la Dirección de Protección de Datos Personales, es el organismo rector en materia de protección de datos personales. Contará con el apoyo de la Autoridad Nacional para la Innovación Gubernamental, cuando se trate de aspectos relacionados con las Tecnologías de la Información y las Comunicaciones.

Sin embargo, en virtud de lo establecido en la Ley 81 de 2019, sólo tendrá competencia de Regulador PDP para el sector bancario, en caso de que el regulador bancario no emita las reglamentaciones sobre protección de datos personales. La Dirección de Protección de Datos Personales, resolverá, las quejas y peticiones presentadas a la ANTAI. Sus decisiones pueden ser impugnadas mediante recurso de reconsideración ante la misma o de la apelación que se interpondrá ante el Director General de ANTAI.

2.4 MARCO LEGAL Y NORMATIVO:

El tratamiento de datos asociado al cumplimiento regulatorio de MMG Bank se basa en la normativa enunciada a continuación:

2.4.1 Leyes.

Ley 46 de 17 de noviembre de 1995	Ley 45 del 4 de junio de 2003
Ley 50 de 2 de julio de 2003	Ley 14 del 18 de mayo de 2007
Ley 1 del 5 de enero de 1984	Ley 1 del 5 de enero de 1984
Ley 67 del 1 de septiembre de 2011	Ley 11 del 31 de marzo de 2015
Ley 11 del 31 de marzo de 2015	Ley 34 del 8 de mayo del 2015
Ley 47 de 24 de octubre de 2016	Ley 51 de 27 de octubre de 2016
Ley 66 de 9 de diciembre de 2016	Ley 5 de 21 de febrero de 2017
Ley 21 de 10 de mayo de 2017	Ley 47 del 6 de agosto de 2013
Ley 31 del 6 de enero de 2019	Ley 81 de 26 de marzo de 2019

2.4.2 Decretos.

Decreto Ley No.1 de 8 de julio de 1999	Decreto Ley 14 del 18 de mayo de 2007

Decreto Ejecutivo 947 de 5 de diciembre de 2014	Decreto Ejecutivo N° 241 de 31 de mayo de 2015
Decreto Ejecutivo 363 del 13 de agosto de 2015	Decreto Ejecutivo 587 del 4 de agosto de 2015
Decreto Ejecutivo 10 de 2 de febrero de 2017	Decreto Ejecutivo 126 de 16 de mayo de 2017
Decreto Ejecutivo 124 de 12 de mayo de 2017 – Ministerio de Economía y Finanzas	

2.4.3 Resoluciones.

Resolución General JD SBP-GJD-0009-2014 de 2 de diciembre de 2014
Resolución General SMV JD-001-2014 de 3 de diciembre de 2014
Resolución No. 201-3931 de la Dirección General de Ingresos, Ministerio de Economía y Finanzas de 29 de junio de 2017

2.4.4 Acuerdos.

Superintendencia de Bancos	Superintendencia del Mercado de Valores
Acuerdo 10-2000, de 15 de diciembre de 2000	Acuerdo 5-2003 de 25 de junio de 2003
Acuerdo 9-2001 de 6 de agosto de 2001	Acuerdo 2-2011, de 1 de abril de 2011
Acuerdo 7-2015, de 9 de junio de 2015	Acuerdo 04-2015, de 7 de julio de 2015
Acuerdo 9-2015, de 27 de julio de 2015	Acuerdo 06-2015, de 19 de agosto de 2015
Acuerdo 10-2015, de 27 de julio de 2015	Acuerdo 6-2018, de 10 de octubre de 2018
Acuerdo 6-2016, de 27 de septiembre 2016	
Acuerdo 1-2019, de 2 de abril de 2017, de 18 de abril de 2017	
Acuerdo Fiduciario 1-2017, de 1 de agosto de 2017	
Acuerdo 1-2019, de 2 de abril de 2019	
Acuerdo 1-2019, de 2 de abril de 2019	

2.4.5 Circulares.

Circular 59-2000 de 26 de octubre de 2000	Circular 65-2000 de16 de noviembre de 2000
Circular 70-2000 de 2 de diciembre de 2000	Circular 4-2002 de 9 de enero de 2002
Circular 11-2002, del 8 de febrero de 2002	Circular 19-2004, de 12 de abril de 2004
Circular 21-2004 de 18 de mayo de 2004	Circular 32-2004 de 9 de julio de 2004
Circular 33-2004 de 9 de julio de 2004	Circular 33-2004 de 9 de julio de 2004
Circular 36-2004 de 28 de julio de 2004	Circular 47-2004 del 15 de noviembre de 2004
Circular 1-2005 de 11 de enero de 2005	Circular 37-2005
Circular 26-2006 sobre Fe de Errata - Acuerdo 12-2005	Circular 41-2006 sobre Sitio en Internet de la UAF
Circular 55-2006 sobre Formulario de Reporte de Cuentas Relacionadas	Circular 59-2006 sobre Control de Reporte de Cuentas Relacionadas
Circular 59-2006 sobre Control de Reporte de Cuentas Relacionadas	Circular 10-2007 sobre Formulario de Declaración de Efectivo
Circular 19-2007 sobre Formulario de Declaración de Efectivo	Circular 36-2008 sobre las Reformas al Código Penal
Circular Fiduciaria 44-2012	Circular 34-2015
Circular 35-2015	Circular SMV 02-2019 de 20 de febrero de 2019
Circular SMV 03-2019 de 20 de febrero de 2019	Circular SMV 04-2019 de 31 de mayo de 2019

Circular 51-2019 (Banco) y Circular 52-2018 (Fiduciaria): Que contienen los documentos adoptados por la UAF en la Resolución Administrativa No.5-2019

2.5 ALCANCE, AMBITO DE APLICACIÓN Y FINALIDAD DE LA POLÍTICA DE PDP.

Esta PO-PDP establece los principios y requerimientos mínimos de seguridad establecidos por MMG Bank para la gestión y el tratamiento de todos los Datos Personales y de la Información de Identificación Personal, así como de las bases de datos que contengan Datos Personales y sobre los cuales MMG Bank actúa como Responsable de Datos Personales.

Todo Tratamiento de Datos Personales deberá ser realizado en los términos, condiciones y fines establecidos en los contratos de servicios o en las autorizaciones de tratamiento entregadas a MMG Bank por el titular de los Datos Personales y/o en cumplimiento de la normativa vigente en materia de blanqueo de capitales y demás normas aplicables a la actividad bancaria, fiduciaria y del mercado de valores.

Todas las bases de datos de MMG Bank que gestionen Datos Personales e IIP serán inventariadas y serán registradas de conformidad con lo dispuesto en la ley y sus reglamentos.

La PO-PDP debe ser conocida y aplicada por y para todos los colaboradores, clientes y proveedores de MMG Bank y tiene como finalidad:

1. Dar a conocer los principios y procedimientos de recolección y tratamiento de Datos Personales realizados por MMG Bank y su apego a los requerimientos regulatorios.
2. Proporcionar a los propietarios de los Datos Personales gestionados un instrumento que les permita conocer los derechos reconocidos por MMG Bank y un instructivo para el ejercicio de dichos derechos.

2.6 CONSULTA DE LA PO-PDP Y GARANTIAS DE ACCESO.

La PO-PDP, o en su defecto, un extracto de la PO-PDP, debe ser anunciada, presentada y accesible en todo momento desde el sitio web de MMG Bank “www.mmgbank.com/pdp”.

Esta información deberá ser presentada en un formato que permita una fácil consulta, acceso y comprensión por parte del público en general sobre aspectos relevantes de los tratamientos de Datos Personales realizados, la justificación/interés legítimo que sustenta cada tratamiento, así como los mecanismos y plazos para el ejercicio de los derechos ARCOP.

MMG Bank garantiza al titular de los datos personales el ejercicio de los Derechos ARCOP, a fin de que, con previa acreditación de su identidad, legitimidad y sin costo alguno, tenga completo acceso a sus Datos Personales a través del ejercicio de los Derechos ARCOP. Para facilitar el acceso, MMG Bank ha puesto a disposición los titulares de los datos personales diferentes medios, principalmente electrónicos, que permitan el acceso directo a dichos datos.

2.7 GESTIÓN DE BASES DE DATOS Y DATOS PERSONALES.

A partir de la entrada en vigor de la Ley 81 de 2019, el 28 de marzo de 2021, todos los datos personales y la Información de Identificación Personal son catalogados como información protegida y confidencial dentro de la República de Panamá. Para garantizar el cumplimiento normativo en materia de Protección de Datos Personales, esta Política Organizacional de Protección de Datos Personales (PO-PDP) ha sido alineada con la Ley 81, antes citada y con el Decreto Ejecutivo 285 de 2021.

MMG Bank sólo realiza los tratamientos requeridos para alcanzar los fines establecidos en la relación contractual con sus clientes y procura aplicar las mejores prácticas para garantizar la seguridad de la infraestructura de seguridad informática y la protección de los Datos Personales e IIP y de las bases de datos que contengan Datos personales e IIP.

Los datos personales gestionados son para uso exclusivo de MMG Bank y no serán compartidos para ser utilizados con fines publicitarios sin la previa autorización de sus titulares.
La actualización de los Datos Personales y de la IIP se hará de forma periódica en base a los lineamientos establecidos por los reguladores bancarios y por la regulación para Protección de Datos Personales, establecida a partir de la Ley 81 de 2019.

3. TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES.

3.1 DATOS PERSONALES TRATADOS.

3.1.1 Clientes.

El tratamiento de Datos Personales y de IIP es consecuencia de los servicios y productos propios de la actividad bancaria, fiduciaria y del mercado de valores ejercida por MMG Bank. La información de contacto de los clientes es utilizada en primer lugar, para la identificación de cuentahabientes y beneficiarios finales de los diferentes productos ofrecidos por el banco y en segundo lugar, para remitir

información actualizada de nuestros productos y beneficios de valor agregado, los cuales MMG Bank considera son útiles para la toma de decisión de sus clientes.

Por tratarse del ejercicio de una actividad regulada por varias entidades públicas y en virtud de acuerdos internacionales y de la regulación bancaria, fiduciaria y del mercado de valores nacional, MMG Bank tiene la obligación de realizar tratamientos obligatorios, presentar informes y permitir el acceso de los reguladores a cierta información de los clientes.

MMG Bank podrá enviar a sus clientes, por diferentes canales como teléfono fijo, teléfono celular, mensajes de texto a su celular, correo electrónico y redes sociales, información sobre servicios/productos, beneficios, eventos y todas aquellas actividades asociadas a los productos e intereses particulares expresados por el cliente al inicio de la relación contractual.

La transferencia de información a entidades públicas (no reguladores) y a otros agentes económicos sólo será realizada si dichas instituciones/agentes económicos tienen autorización expresa del dueño de los Datos Personales para pedir dichos datos y/o por mandato de una autoridad judicial.

3.1.2 Colaboradores.

El tratamiento de Datos Personales de los colaboradores nace a partir de la relación contractual entre MMG Bank y sus colaboradores, e incluye el tratamiento de la información que se suministra en los formularios laborales o CV, pagos de salarios y obligaciones como empleador por la gestión de afiliaciones y aportes a seguridad social y cajas de compensación, tanto de los empleados como de sus familiares y gestión de acciones administrativas de carácter laboral tales como permisos, incapacidades, vacaciones, capacitaciones, viajes de trabajo, controles de acceso y horario de trabajo del colaborador.

Todos los datos suministrados por los colaboradores de MMG Bank serán recolectados, almacenados, compilados, utilizados, compartidos, consultados, transmitidos, intercambiados y transferidos, para dar cumplimiento a las obligaciones derivadas de la relación laboral y al ejercicio de los derechos como empleador.

Toda la información relativa a los colaboradores y/o ex colaboradores de MMG Bank, serán conservados con el fin de que la empresa pueda cumplir sus obligaciones como empleador y ejercer los derechos

que en esa misma condición le corresponden, de acuerdo con la legislación laboral vigente, y serán conservados por el tiempo establecidos en las leyes relacionadas y al vencimiento de dicho plazo, empezará a computarse el plazo establecido en la Ley 81 de 2019, para que MMG Bank descarte de forma segura o disocie dichos datos personales a fin de que no puedan ser asociados de forma efectiva al titular de los mismos.

Al momento iniciar labores en MMG Bank todo colaborador debe firmar un Acuerdo de Confidencialidad que incluye instrucciones para la gestión y protección de Datos Personales, leer la PO-PDP y debe manifestar expresamente y por escrito conocer, aceptar y aplicar los lineamientos de Protección de Datos Personales establecidos en la PO-PDP. Todos colaboradores que iniciaron sus labores con anterioridad a la emisión de esta PO-PDP han firmado un acuerdo de confidencialidad actualizado con las políticas de gestión y protección de Datos Personales y también han debido leer la PO-PDP y manifestar expresamente y por escrito conocer, aceptar y aplicar los lineamientos de Protección de Datos Personales establecidos en la ella.
Adicional a estas declaraciones, todo colaborador de MMG Bank debe participar en un programa de capacitación en gestión y tratamiento de datos personales.

3.1.3 Proveedores.

El tratamiento de Datos Personales de proveedores nace como consecuencia de la relación permanente para solicitud de cotizaciones y/o servicios y de las relaciones comerciales que surjan, con el objeto de adquirir sus productos o servicios como insumos para el funcionamiento de MMG Bank.

MMG Bank tramitará los datos comerciales e información financiera que considere necesaria para el cumplimiento de su objeto social y para toda celebración de contratos con terceros. Los datos personales obtenidos como consecuencia de las relaciones comerciales serán gestionados con elevados niveles de protección de privacidad y confidencialidad, dentro del proceso del tratamiento de Datos Personales, y durante todas las actividades que tendrán los principios de confidencialidad, seguridad, legalidad, acceso, libertad y transparencia

3.1.4 Visitantes a las instalaciones.

MMG Bank es un banco orientado a la inversión, el número de visitantes diarios no es muy elevado. La información que suministran los visitantes para identificarse al momento de ingresar al edificio donde están ubicadas las oficinas de MMG Bank, es solicitada y registrada por parte de la empresa de seguridad

que gestiona los accesos al edificio como medida control frente a posibles incidentes de seguridad. El tratamiento y conservación de estos datos no es responsabilidad de MMG Bank.

MMG Bank es responsable de la gestión y tratamiento de los datos obtenidos (incluyendo imágenes) al momento de ingresar a las áreas de uso exclusivo del banco y a las instalaciones de MMG Bank. Se ha identificado de forma adecuada las áreas donde los datos de los visitantes (incluyendo las imágenes) son responsabilidad de MMG Bank.

La información de los visitantes es eliminada a los doce (12) meses de la fecha de la visita a nuestras instalaciones.

3.1.5 Proceso de gestión de Recurso Humano y Gestión de Hojas de Vida.

MMG Bank publica ofertas de empleo en sus canales de comunicación para posiciones dentro de la organización. Este proceso de selección lo realiza el Recursos Humanos, en ocasiones en colaboración con el Departamento de Desarrollo Organizacional de Morgan & Morgan o con empresas dedicadas a la búsqueda de talentos, quienes cuentan con sus propias herramientas de búsqueda. En todo caso, los términos y condiciones de estas colaboraciones se desarrollan en base a nuestra PO-PDP que establece las políticas de tratamiento de la información personal de los aspirantes a iniciar el proceso de selección, incluyendo el plazo para la retención de las hojas de vida de aquellos candidatos o aplicantes que no han sido contratados, en cuyo caso la hoja de vida no podrá ser conservada por un período mayor a seis (6) meses, salvo autorización expresa y por escrito del candidato o aspirante.

Al momento de llenar una vacante o abrir una nueva plaza a concurso, MMG Bank ejecuta procesos previamente establecidos, garantizando que el perfil buscado sea filtrado, preseleccionado y presentado para estudio por el área respectiva, siempre que cada una de las hojas de vida analizadas tengan adjunta una autorización de tratamiento por parte del aspirante y con el más elevado estándar de confidencialidad en el manejo de Datos Personales e IIP.

MMG Bank no es una empresa de reclutamiento de recurso humano. Sin embargo, puede canalizar y contactar posibles candidatos para una vacante en otra de sus compañías subsidiarias. Para tales fines, una vez se tenga conocimiento de una hoja de vida con un perfil profesional que pudiese interesar a otra empresa dentro del grupo, se le pedirá autorización expresa al propietario para compartir su hoja

de vida. Si han transcurrido seis (6) meses desde el momento de la solicitud de autorización para compartir la hoja de vida, MMG Bank asumirá que la persona no está interesada y eliminará la hoja de vida de la base de datos y de sus repositorios.

En caso de que un aspirante haga llegar su hoja de vida de forma electrónica o física por algún medio de contacto, de forma espontánea y sin requerimiento, la oficina de Desarrollo Organizacional estudiará la hoja de vida para determinar si reúne el perfil profesional para ser considerada en algún proceso de preselección o si puede ser retenida para un proceso futuro. Si la hoja de vida no aplica para ninguna de las dos condiciones antes señaladas, se procede a la eliminación inmediata de la hoja de vida de todos los repositorios de MMG Bank, garantizando la protección de sus Datos Personales y evitando que sean utilizados para actividades o procesos de selección en los cuales el candidato no ha expresado su interés en participar.

Si el perfil resulta interesante para la oficina de recursos humanos, se solicitará una autorización de tratamiento para retener la hoja de vida y poder utilizarla en futuros procesos de preselección dentro del banco o para alguna empresa afiliada. Si esa autorización no es recibida dentro de los treinta (30) días siguientes, MMG Bank asumirá que la persona no está interesada y eliminará la hoja de vida de la base de datos y de sus repositorios.

Toda autorización para tratamiento interno y/o externo de una hoja de vida podrá ser revocada en cualquier momento utilizando el formulario disponible en www.mmgbank.com/pdp, que deberá ser enviado a la siguiente dirección pdp@mmgbank.com para el trámite correspondiente.
Una vez recibida la solicitud de revocación de autorización de tratamiento, se correrá traslado a la unidad administrativa correspondiente para que en un plazo no mayor de cinco (5) días hábiles elimine la hoja de vida de los repositorios del MMG Bank. Una vez realizado el procedimiento se le notificará al propietario de la hoja de vida que ésta ha sido eliminada.

3.2 TRATAMIENTOS DE DATOS PERSONALES POR MMG BANK

Los Datos Personales y IIP de clientes obtenida y gestionada por MMG Bank serán sometidos a los siguientes tratamientos:

TRATAMIENTOS	
TIPO DE TRATAMIENTO	**INTERÉS LEGÍTIMO**
Acciones propias y necesarias para la gestión de la cuenta y/o productos a título del cliente.	Necesario para la relación contractual
Acciones de debida diligencia y relacionadas a la prevención del uso de los servicios bancarios para cualquier tipo de actividad ilícita.	Necesario para la relación contractual
Acciones propias y necesarias para garantizar la funcionalidad de los servicios/productos ofrecidos por MMG Bank (tarjetas de débito o crédito, monederos electrónicos, etc.), que pueden involucrar transferencia de datos personales con terceras empresas encargadas de dichos servicios	Necesario para la relación contractual
Referir los servicios de las subsidiarias de MMG y compartir la información de contacto, cuando estas ofrezcan soluciones y servicios que respondan a necesidades financieras y/o estratégicas que este haya informado o consultado a MMG durante la relación contractual.	Necesario para la relación contractual
Comunicar cambios normativos que pueden influir en la relación cliente banco.	Necesario para la relación contractual
Comunicar cambios significativos en los procesos y plataformas utilizados por MMG Bank.	Necesario para la relación contractual
Recibir comunicaciones con información de beneficios, eventos y todas aquellas actividades asociadas a la relación comercial, que podrán ser	Requiere consentimiento informado, previo y expreso

de interés para alcanzar objetivos financieros e intereses particulares del cliente.	
Recibir comunicaciones con información sobre tasas vigentes, servicios/productos, que podrán ser de interés para alcanzar objetivos financieros e intereses particulares del cliente.	Requiere consentimiento informado, previo y expreso
Recibir información sobre tasas vigentes, servicios y productos de inversión que podrán ser de interés para alcanzar objetivos financieros e intereses particulares del cliente. – **(aplica a la cuenta de custodia de inversiones)**	Requiere consentimiento informado, previo y expreso
Recibir Información del mercado, análisis y noticias. – **(aplica a la cuenta de custodia de inversiones)**	Requiere consentimiento informado, previo y expreso
Realizar encuestas y estudios de mercado con el fin obtener mediciones de satisfacción respecto de los servicios, desarrollar mejoras y nuevos productos.	Requiere consentimiento informado, previo y expreso

Todos los tratamientos de datos personales realizados por MMG Bank se realizan para cumplir con el rol de asesor de productos financieros establecida con nuestros clientes y de los requerimientos normativos para el intercambio de información con los reguladores y fiscalizadores estatales de la actividad bancaria.

Antes de realizar un nuevo tratamiento a los datos gestionados, ya sea por cambios tecnológicos o regulatorios, MMG Bank realizará una Evaluación de Impacto con la finalidad determinar si el tratamiento se ajusta al alcance establecido en los contratos con nuestros clientes o si es necesario actualizar la autorización de tratamientos contenida en nuestros contratos. (Ver en el Anexo 1. Procedimiento para Autorización de nuevos tratamientos).

MMG Bank comunicará a los titulares de los datos de cualquier tratamiento realizado por una autoridad reguladora o de cualquier tercera parte haya sido realizado de forma contraria a las disposiciones legales y a lo dispuesto en esta política y cuando se tenga conocimiento de cambios legislativos y/o normativos en algunas de las jurisdicciones involucradas en la transferencia internacional de datos que pueda afectar la seguridad e integridad de los datos personales gestionados. (Ver en el Anexo 1. Procedimiento de notificación de cambios normativos – transferencia internacional de datos)

3.3 DEBIDA DILIGENCIA (OBLIGACIÓN DE OBTENER INFORMACIÓN DE LOS CLIENTES).

La República de Panamá ha adoptado lineamientos y regulaciones destinadas a combatir el lavado de dinero y prevenir el financiamiento del terrorismo y armas de destrucción masiva, a través de los servicios de banca, corretaje y/o servicios financieros.

Para este propósito, los lineamientos y regulaciones obligan a las entidades financieras (por ejemplo: bancos y casas de valores) a obtener información completa y detallada de sus clientes y/o potenciales clientes a través de un proceso conocido como “Conozca a Su Cliente” o “Debida Diligencia.”

3.3.1 Tipo de Información Requerida y/o Recolectada. La siguiente información es requerida:

3.3.1.1 Para personas naturales:

Datos Personales (no son los únicos datos): nombre, fecha de nacimiento, documento de identificación personal (documento nacional de identificación o pasaporte), estado civil, domicilio (con documento que lo sustente), lugar de trabajo, profesión o trabajo, residencia fiscal, procedencia de los fondos y/o del portafolio, referencias bancarias, comerciales y/o personales, número de identificación tributaria. Para clientes que invertirán en instrumentos financieros es obligatorio, adicional a los datos personales: información sobre experiencia y/o conocimiento previo sobre inversiones: perfil financiero, perfil del inversionista.

3.3.1.2 Para personas jurídicas (no son los únicos datos):

Data y documentos de incorporación de la institución: identidad de accionistas finales, directores, dignatarios, apoderados, firmantes autorizados, fiduciarios, fideicomitentes y/o beneficiarios finales y su domicilio, actividades de la institución, fuentes de ingresos.

3.3.1.3 Otras fuentes para recolectar información:

Para cumplir con la obligación de obtener información de sus clientes MMG Bank recolecta y almacena la información de sus clientes utilizando los canales electrónicos de MMG Bank (por ejemplo: página web, banca en línea, uso de medios de pago). Adicionalmente, se podrá recolectar información de terceros públicos y/o privados, extranjeros y locales, como el Registro Público de Panamá, La Asociación Panameña de Crédito (APC), el Tribunal Electoral, Data Jurídica Listas de Organizaciones Gubernamentales como las Naciones Unidas, la Oficina de Control de Activos Extranjeros, Worldcheck, entre otros.

3.3.1.4 Tratamiento y protección de la información obtenida bajo la obligación de Debida Diligencia.

Los lineamientos y regulaciones actualizadas imponen a las instituciones financieras la obligación de mantener la confidencialidad y no divulgar la información de sus clientes relacionado a sus operaciones, salvo en casos específicos:

a. Cuando la información ha sido solicitada por una autoridad competente de acuerdo con la ley aplicable.

b. Cuando, por iniciativa propia del banco, la información deberá ser divulgada para cumplimiento con los lineamientos legales y regulatorios relacionados a la prevención del lavado de dinero, financiamiento del terrorismo, financiamiento de armas de destrucción masiva y relacionados a cualquier otro crimen indicado por las autoridades competentes.

c. Cuando sea requerido por una autoridad local o extranjera bajo provisión de algún acuerdo, tratado o acuerdo de intercambio de información fiscal, o para evitar la doble tributación suscrita por la República de Panamá, o si debe ser reportado por provisión de la Ley de Cumplimiento Tributario de Cuentas Extranjeras o “FATCA” de los Estados Unidos, o por provisión del Estándar Común de Reporte o CRS fomentado por el Foro Global de la OCDE sobre Transparencia e Intercambio de Información para propósitos fiscales.

d. Cuando debe ser utilizado para cualquier proceso legal entre el cliente y MMG Bank.

e. Por cualquier razón o motivo autorizado por los lineamientos y regulaciones adoptadas por las autoridades competentes.

3.3.1.5 Plazo para obtener la información obtenida para cumplir la obligación de Debida Diligencia.

De acuerdo con los lineamientos legales aplicables, los registros y documentación que soporta las operaciones comerciales realizadas por la institución financiera deberán ser almacenadas hasta que la prescripción de cada acción que pueda resultar de dichas operaciones. Los plazos de prescripción son de 1 a 10 años. El tiempo de prescripción aplicable dependerá del tipo de operación comercial realizada.

Una vez vencido este plazo, la ley de Protección de Datos Personales de Panamá establece un período de 7 años, dentro del cual, a solicitud de parte interesada y/o por iniciativa del MMG Bank deberá eliminar dicha información de forma segura.

3.4 TRATAMIENTO DE DATOS PERSONALES CONFIDENCIALES Y SENSIBLES.

Se permite el almacenamiento o transferencia de datos personales originados o almacenados dentro de la República de Panamá que sean confidenciales, sensibles o restringidos, que reciban un tratamiento transfronterizo, siempre y cuando el responsable del almacenamiento de esos datos o el custodio de estos cumpla con los estándares de protección de datos personales exigidos por la Ley de PDP, o pueda demostrar que cumple con los estándares y normas de protección de datos personales iguales o superiores a los exigidos por dicha Ley.

MMG Bank sólo solicitará datos sensibles de sus clientes cuando sean estrictamente necesarios para el cumplimento de las responsabilidades contractuales o por requerimiento expreso de una normativa legal. Los datos sensibles recogidos serán especialmente protegidos y el acceso a los mismos será restringido sólo a aquellas personas que lo requieran en virtud de su responsabilidad laboral.

En consecuencia, MMG Bank tendrá especial cuidado y precaución en la gestión y protección de todo dato sensible de un cliente al que MMG Bank pueda o deba tener acceso en virtud de la relación

comercial con el titular de los derechos ARCOP. Adicionalmente, MMG Bank declara que no condicionará el uso de cualquier servicio o producto al acceso a datos personales de carácter sensible.

4. PROTECCIÓN DE DATOS PERSONALES

4.1 DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES.

Los titulares de los Datos Personales son las personas naturales cuyos Datos Personales sean objeto de algún tratamiento por parte de MMG Bank.

En virtud de lo establecido por la normatividad vigente en materia de protección de datos, a los titulares de los Datos Personales se les reconocen los llamados derechos ARCOP, los cuales los pueden ejercer en cualquier momento:

1. Derecho de Acceso: Permite al titular obtener sus Datos Personales que se encuentren almacenados o sujetos a tratamiento en bases de datos de instituciones públicas o privadas, además de conocer el origen y la finalidad para los cuales han sido recabados.

2. Derecho de Rectificación: Permite al titular solicitar la corrección de sus Datos Personales que sean incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes.

3. Derecho de Cancelación: Permite al titular solicitar la eliminación de sus Datos Personales incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes.

4. Derecho de Oposición: Permite al titular, por motivos fundados y legítimos relacionados con una situación en particular, negarse a proporcionar sus Datos Personales o a que sean objeto de determinado tratamiento, así como a revocar su consentimiento.
5. Derecho de Portabilidad: derecho a obtener una copia de los Datos Personales de manera estructurada, en un formato genérico y de uso común, que permita ser operado por distintos sistemas y/o transmitirlos a otro responsable, cuando:
   a. El titular haya entregado sus datos directamente al responsable.
   b. Sea un volumen relevante de datos, tratados de forma automatizada.
   c. El titular haya dado su consentimiento para el tratamiento o se requiera para la ejecución o el cumplimiento de un contrato.

Con base a los derechos ARCOP antes mencionados, MMG Bank declara que el propietario de los Datos Personales tiene derecho a:

1. Conocer y acceder, de forma gratuita, a los Datos Personales que MMG Bank tiene almacenados y/o sobre los cuales esté haciendo el algún tipo de tratamiento. Cuando el titular solicite que la información le sea suministrada en un soporte físico (papel, usb, disco compacto, etc.) deberá asumir el costo de esta solicitud.
2. Solicitar, en cualquier momento, que sus datos sean actualizados o rectificados cuando los datos se encuentran incompletos, incorrectos, inexactos, fragmentados,
3. Ser informado por MMG Bank, de uso que le ha dado a sus Datos Personales.
4. Oponerse a algún tratamiento que no haya sido autorizado o hay sido expresamente prohibido.
5. Revocar, sin necesidad de justificación, la autorización de tratamiento y/o solicitar la supresión del dato cuando no se respeten los parámetros de autorización de tratamiento expresamente indicados, los derechos ARCOP, ni las regulaciones sobre la materia.
6. Solicitar y verificar en cualquier momento el formulario de autorización expresa entregado a MMG Bank para el tratamiento de los Datos Personales.
7. Incoar ante la Superintendencia de Bancos de Panamá o la Superintendencia del Mercado de Valores de Panamá, procesos administrativos por infracciones a lo dispuesto en la Ley 81 de 2019 y las demás normas que la modifiquen, adicionen o complementen, previo trámite de consulta o requerimiento ante MMG Bank.

4.2 PROCEDIMIENTOS PARA CONSULTAS Y EJERCICIO DE LOS DERECHOS ARCOP POR PARTE DE LOS TITULARES DE LOS DATOS PERSONALES.

Para iniciar el proceso de ejercicio de los Derechos ARCOP, el/la titular de los Datos Personales debe acceder los formularios de solicitud para cada derecho que se encuentran disponibles en www.mmgbank.com/pdp, a fin de que MMG Bank le indique qué Datos Personales tiene almacenados y/o para que sus Datos Personales sean actualizados, corregidos, rectificados o suprimidos, porque ya no existe una relación comercial con MMG Bank y ha vencido el plazo establecido por ley para que los Datos Personales sean mantenidos en posesión de MMG Bank, o en caso de que los datos hayan sido obtenidos y/o tratados sin autorización expresas o en caso de incumplimiento con relación a la

autorización expresa del propietario o por incumplimiento de la regulación vigente sobre tratamiento y protección de Datos Personales o en las políticas y/o procesos establecidos en la PO-PDP de MMG Bank.

4.2.1 FORMULARIOS DERECHOS ARCOP

Existe un formulario específico para que el titular pueda ejercer cada uno de los derechos ARCOP y en cada formulario se indica de forma clara y sencilla la información requerida y la documentación que debe ser aportada (en caso de ser necesario) para que el titular de los Datos Personales pueda ejercer sus derechos. En todo caso, la información mínima para el ejercicio de los derechos ARCOP es la siguiente:

1. Nombre completo y número de identificación del titular de los datos, o de la persona legalmente autorizada a representarle.
2. Selección y/o descripción detallada de los hechos que motivan la solicitud.
3. Datos de contacto del titular como domicilio, teléfono de contacto y correo-e.
4. Descripción del procedimiento que desea realizar.
5. Indicar los documentos que se aportan con la solicitud (sólo en caso de ser necesario).

Cuando se haya completado y firmado el formulario, el titular de los Datos Personales debe enviar el formulario y los adjuntos a pdp@mmgbank.com.

4.2.2 REGISTRO DE SOLICITUDES

Una vez recibida la solicitud del Titular de los Datos Personales, se procesará la solicitud y se le asignará un número del Registro de Solicitudes. Este número deberá ser utilizado por el titular de los Datos Personales para solicitar información sobre el estatus de su solicitud. MMG Bank tendrá un plazo de dos (2) días hábiles para acusar recibo de la solicitud, ingresarla al registro de solicitudes e indicar el número de la solicitud al titular de los Datos Personales.

En el mismo correo electrónico en que se indica el número asignado a la solicitud, se indicará al solicitante si es necesario corregir la solicitud y/o aclarar algún punto de la misma y/o adjuntar algún documento. El titular de los Datos Personales tendrá un plazo de diez (10) días hábiles, contados a partir del día siguiente del envío del correo electrónico, para cumplir con lo solicitado. Al vencimiento del término antes indicado, si no se ha recibido respuesta alguna o si se insiste en el incumplimiento de los

requisitos, se levantará un informe de situación y se anotará en el Registro de Solicitudes que el titular de los datos ha desistido de su solicitud.

4.2.3 TRÁMITE DE SOLICITUDES

Al día hábil siguiente del envío de la respuesta con el número de la solicitud empieza a correr el plazo de ocho (8) días hábiles, plazo dentro del cual se debe dar respuesta y solución a la solicitud. Si la solicitud implica la modificación, eliminación y/o suspensión de tratamiento de los datos personales, se notificará a unidad administrativa o la persona encargada de ejecutar la solución propuesta. Una vez recibida esta notificación, quien sea responsable de ejecutar la solución propuesta tendrá un plazo máximo de cinco (5) días hábiles contados a partir del día siguiente a la recepción, para atenderla y ejecutarla.

En caso de que MMG Bank no pueda realizar las acciones solicitadas dentro del plazo establecido, podrá pedir, por una sola vez, una prórroga por un plazo no mayor de cinco (5) días hábiles, para cumplir las instrucciones establecidas en la solicitud presentada por el titular de los Datos Personales. Al momento de acogerse al derecho aquí establecido MMG Bank deberá enviar una comunicación al titular de los Datos Personales indicando los motivos por los cuales no ha sido posible atender su solicitud antes del vencimiento del plazo máximo para ejecutar la solución.

4.3 PROCESO PARA REVOCACIÓN DE AUTORIZACIONES DE TRATAMIENTO DE DATOS PERSONALES.

El titular de los Datos Personales podrá, en cualquier momento, revocar su autorización para cualquier tratamiento de sus Datos Personales por parte de MMG Bank. Para tal fin, deberá completar el formulario de Revocación de Autorización de Tratamiento que se encuentra disponible en www.mmgbank.com/pdp y enviarlo a través de correo-e, debidamente firmado a pdp@mmgbank.com.

El procedimiento para el trámite indicado para la revocación de autorización de tratamiento es el mismo establecido para el ejercicio de los derechos ARCOP, incluyendo el registro de la solicitud y los plazos.

4.4 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES.

MMG Bank, en su calidad de responsable de los Datos Personales y de la IIP que gestiona en virtud de la actividad comercial que desarrolla y con la finalidad de responder a los titulares de eso datos

personales dentro de los plazos y en las formas establecidas en la regulación vigente en materia de PDP ha designado a un Oficial de Protección de Datos Personales.

4.4.1 OFICIAL DE PDP

Oficial de PDP	HIRAM HARRIS
Correo-e:	pdp@mmgbank.com
Oficina:	MMG Tower, Piso 22, Ave. Paseo del Mar, Costa del Este, Ciudad Panamá, República de Panamá.

4.4.2 FUNCIONES DEL OFICIAL DE PDP.

El Oficial de PDP tiene las siguientes funciones:

1. Liderar la creación, implementación y promoción de un sistema que permita gestionar los riesgos del tratamiento de Datos Personales.
2. Promover una cultura de protección de datos dentro de la organización.
3. Coordinar la gestión de datos personales en todas las áreas administrativas de MMG Bank para garantizar el cumplimiento normativo y la ejecución de las Políticas de Protección de Datos Personales manera transversal en la organización.
4. Verificar, auditar y mantener un inventario actualizado de las Bases de Datos de MMG Bank para realizar los reportes y/o registros requeridos por parte del Regulador.
5. Desarrollar y supervisar un programa de capacitación y concienciación constante en materia de Protección de Datos Personales dentro de la organización.
6. Analizar y diagnosticar las responsabilidades de los roles, cargos y perfiles de acceso a plataformas y otras herramientas tecnológicas dentro de MMG Bank.
7. Garantizar que, dentro del proceso de análisis de desempeño de los empleados, se incluya la capacitación sobre la protección de Datos Personales.
8. Participar en el proceso de capacitación de nuevos colaboradores, en especial de aquellos que por la naturaleza de responsabilidades tengan acceso a las Bases de Datos y/o deban tener acceso constante a Datos Personales, a fin de trasmitirles los conocimientos necesarios y la responsabilidad derivada de la normativa de PDP.
9. Coordinar y dar seguimiento a la implementación de planes de auditoría interna, para verificar el cumplimiento normativo y de la PD-PDP dentro de la organización.

10. Servir de enlace entre MMG Bank y el regulador de PDP y asistir a todos los representantes de regulador durante los procesos de auditoría y/o requerimientos de evidencias de cumplimiento.
11. Servir de intermediario entre MMG Bank y los propietarios de los Datos Personales que gestiona MMG Bank y asistirles en el ejercicio de los derechos ARCOP, garantizando las respuestas de MMG Bank en los tiempos establecidos en la normativa vigente y en la PO-PDP.

5. GESTIÓN DE DATOS OBTENIDOS DE VIDEOVIGILANCIA Y CONTROLES DE ACCESO.

MMG Bank informa a sus colaboradores y visitantes de la existencia de un sistema de videovigilancia y controles de acceso, a través de anuncios visibles de sus instalaciones.

El sistema de videovigilancia está compuesto por una red de cámaras fijas, instaladas en sitios estratégicos en el interior de instalaciones y áreas de acceso, para garantizar la seguridad física de los colaboradores y de los activos del banco. La gestión de los datos personales/imágenes obtenidas como consecuencia de los controles de acceso y del sistema de videovigilancia ha sido organizada en cumplimiento de los derechos de tratamiento de datos personales para los empleados y de las personas que visitan las instalaciones de MMG Bank.

La información así obtenida sólo se utilizará con fines de seguridad de los empleados, personas naturales, bienes y activos que en ella se contengan. Dicha información podrá ser utilizada como prueba en cualquier momento que sea requerida, ante cualquier autoridad, institución oficial u organización privada que lo solicite. Esta información será conservada por un plazo máximo de doce (12) meses contados a partir de la fecha en que la imagen fue capturada o que los datos personales hayan sido recolectados al momento de controlar el acceso.

Los archivos obtenidos a través del sistema de videovigilancia se almacenan en un sistema con elevados estándares de confidencialidad, privacidad, seguridad y controles efectivos de acceso y a dicho material solo tiene acceso el personal del área seguridad. El titular de los datos personales podrá solicitar acceso a sus propios datos cumpliendo los procedimientos establecidos para el ejercicio de los Derechos ARCOP.

5.1 SISTEMA DE VIDEO VIGILANCIA (CCTV)

MMG Bank cuenta con un sistema de cámaras de circuito cerrado (CCTV), en lugares estratégicos, con el objetivo de grabar la actividad y eventos relevantes para garantizar la seguridad de los colaboradores, visitantes y de los equipos del banco.

Con la finalidad de cumplir con lo estipulado en los Acuerdos 1-2007 y 1-2012 de la SBP, las grabaciones del sistema de CCTV se conservarán durante tres (3) meses para las áreas del banco y (12) meses para ATM. Se realiza una revisión mensual por el Departamento de Seguridad, para validar que efectivamente el sistema este grabando con eficiencia, dejando constancia en una bitácora. Los enfoques de las cámaras son ser aprobadas por el Oficial de Seguridad.

5.2 SISTEMA DE CONTROL DE ACCESO

El banco cuenta con un sistema de control de acceso, para proteger de los colaboradores, visitantes y de los activos del banco. Es responsabilidad del Departamento de Seguridad mantener el sistema de Control de Acceso en óptimas condiciones para su debido funcionamiento y deberá asegurarse, mediante una revisión mensual, que únicamente las personas autorizadas por los Vicepresidentes de cada área tengan acceso al banco.

6. ELIMINACIÓN SEGURA DE DATOS PERSONALES.

En cumplimiento de la normativa de PDP y de los estándares de seguridad reconocidos por la industria, tan pronto desaparece el interés legítimo para el tratamiento los Datos Personales, la IIP, y de los documentos que incluyan datos personales. En consecuencia, los Datos, la IIP y los documentos que incluyan Datos Personales deben ser eliminados de acuerdo con un procedimiento que garantice la protección y confidencialidad de esa información hasta el momento de su destrucción, la imposibilidad de recuperación y cuando sea necesario, de los soportes.

Los documentos electrónicos que se van a destruir deben estar protegidos para evitar accesos externos no autorizados hasta el momento de su destrucción definitiva. Durante el proceso de descarte los Datos Personales son extraídos de las Bases de Datos y de los repositorios utilizados por las plataformas y aplicaciones operativas de MMG Bank y almacenados en repositorios protegidos mientras se ejecuta el protocolo de eliminación segura.

La información almacenada en formato físico nunca permanece al descubierto en el exterior de los edificios, ni amontonarse en lugares de paso, ni en lugares abiertos dentro de las instalaciones. Para este formato existe un protocolo de descarte con medidas de seguridad adecuadas que garantizan su protección hasta el momento de su eliminación definitiva.

En el caso de documentos que contengan información personal, Una vez expirada la obligación legal de conservación, todo documento que contenga Datos Personales e IIP deberá iniciar un proceso de descarte/eliminación que inicia con la restricción y/o limitación de acceso.

Salvo autorización expresa de los titulares de los Datos Personales, la Ley 81 de 2019, establece un plazo de siete (7) años, para que el responsable de datos personales los elimine.

7. LIMITACIÓN DE RESPONSABILIDAD POR USO DE REDES SOCIALES.

Las redes sociales constituyen plataformas complementarias de divulgación de la información (comunicación) y garantizan elevados niveles de acceso e interconexión con los medios digitales de los usuarios y no se encuentran bajo la responsabilidad de MMG Bank.

Como regla general MMG Bank no utiliza estos mecanismos de comunicación como medio de promoción de productos y servicios, pero en caso de llegar a utilizarlos, cualquier información que los usuarios proporcionan a través de estas plataformas no constituye ni forma parte de los Datos Personales sujetos a la protección de MMG Bank, siendo de total responsabilidad de la persona que proporciona la información y de las empresas que gestionan estas plataformas.

En caso de que MMG Bank utilice las redes sociales como medio de comunicación, solicitará la autorización expresa de todas las personas cuyas imágenes sean utilizadas por MMG Bank en sus comunicaciones.

8. VIGENCIA DE LA PO-PDP.

La PO-PDP de MMG Bank entró en vigor de la fecha de su publicación y sustituye y deja sin efecto cualquier otra disposición organizacional que le sea contrarias o que haya sido emitida con anterioridad.

Toda información no contemplada en la presente política será tratada de la forma como lo establece la Ley 81 de 2019 y su reglamentación.

La actualización de la PO-PDP dependerá de las instrucciones y lineamientos que adopte MMG Bank, así como de las normativas emitidas por el regulador de PDP para la actividad bancaria y del mercado de valores, a saber, la Superintendencia de Bancos de Panamá y la Superintendencia del Mercado de Valores de Panamá, y en su defecto por el regulador nacional en materia de PDP, la Autoridad Nacional de Transparencia y de Acceso a la Información (ANTAI).