MUFG Bank Ltd., Oficina de Representación en Colombia

Nombre del Documento	*Estándar para el Tratamiento de Datos Personales*		
Applicabilidad	MUFG CUSO		☐ MUTB NY
		MUAH	☐ MUSA ☐ MFS(USA) ☐ Intrepid ☐ Others
		MUFG Bank	☐ MUFG Bank U.S.
	MUFG Bank non-U.S.		☐ MUFG Bank Canada
			☐ MUFG Bank Chile
			☒ MUFG Bank Colombia
			☐ MUFG Bank Peru
	Other MUFG Entities		☐ MUFG Securities Canada
Dueño del Documento y Organización	Andrea Munizaga, Oficial de Cumplimiento – Cumplimiento		
Tipo de Documento	Estándar		
Aprobado Por	Head de la Oficina de Representación en Colombia		
Fecha de Aprobación	18/12/2025		
Fecha de Vigencia	18/12/2025		
Frecuencia de Revisión	Cada 2 años		
Fecha de Última Revisión	10/12/2025		
Fecha de Próxima Revisión	10/12/2027		
Fecha de Retiro	N/A		
Clasificación de Información	Uso General		
Política/Estándar Relacionado	MUFG Americas Data Privacy and Information Handling Policy		
Reemplaza a	N/A		
Reemplazado Por	N/A		
Version #	2.0		
Información de Contacto	Para escalaciones y consultas relacionadas con este Estándar, por favor contactar a la dueña del Manual (amunzagacorvacho@cl.mufg.jp).		
Notes	N/A		

Control del Documento

Cualquier cambio a este documento debe estar reflejado en la tabla debajo.

Tabla 1: Historia de Modificaciones

Versión	Autor	Fecha	Descripción
Versión 1.0	Juan Camilo Gómez	Noviembre 2019	Establecido
Versión 1.1	Andrea Munizaga	Agosto 2021	Revisado. Se controló con los abogados locales, no se realizaron cambios.
Versión 1.3	Andrea Munizaga	Junio 2022	Revisado. Se actualiza el formato del documento en general y agrega las secciones 'Control del Documento', 'Procedimiento para el tratamiento de los Consentimientos firmados por los Empleados' y 'Procedimiento para Incidentes de Privacidad'.
Versión 1.4	Andrea Munizaga	12/13/2023	Revisión periódica.
Versión 1.5	Andrea Munizaga	19/08/2025	Revisión periódica. Actualización de portada y formato del documento.
Versión 2.0	Andrea Munizaga	10/12/2025	Revisión periódica. Ajuste de plazos de respuesta para solicitudes de titulares conforme a la Ley 1581 de 2012 y Decreto 1377 de 2013. Actualización general del documento.

Mapa de Contenido

1. Introducción

El presente documento contiene los estándares para el tratamiento de Datos Personales (los "Estándares") de la Oficina de Representación en Colombia de MUFG Bank, Ltd. ("MUFG") con la finalidad de garantizar el derecho fundamental a la protección de los datos personales, de acuerdo con las normas aplicables en Colombia.

MUFG considera como un principio fundamental la confidencialidad y la protección de datos personales de toda la información que recolecte, procese y almacene de sus clientes, clientes potenciales, empleados, exempleados, contratistas, proveedores o individuos que vayan a trabajar con la compañía.

Las reglas contenidas en el siguiente estándar aplican al tratamiento de cualquier información personal sobre la cual MUFG tenga posesión y control, incluidas en sus archivos físicos o virtuales, o guardadas en bases de datos u otros sistemas administrados a través de esta oficina.

Todos los empleados de la Empresa deben leer, entender y respetar estos estándares en el cumplimiento de sus funciones. Los Estándares son de obligatorio cumplimiento por parte de todos los empleados, contratistas y terceros que obren en nombre de MUFG. El incumplimiento de las disposiciones contenidas podrá llevar a sanciones laborales o de responsabilidad civil contractual según sea el caso.

2. Disposiciones Generales

2.1. Legislación aplicable

Este Estándar incorpora los mandatos contenidos en los artículos 15 y 20 de la Constitución Política de Colombia, la Ley 1581 de 2012, el Decreto 1377 de 2013 y el Decreto 1074 de 2015.

2.2. Ámbito de aplicación

Este Estándar es de aplicación al Tratamiento de los Datos Personales de los cuales MUFG sea responsable, o quien éste designe, sea Responsable o Encargado en los términos de la ley.

2.3. Definiciones

a) Autorización. Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de los Datos Personales.

b) Base de Datos Personales. Conjunto organizado de los Datos Personales que son objeto de Tratamiento por parte de MUFG, o quien ésta designe, en su condición de Responsable y/o Encargada de los Datos Personales.

c) Dato Personal. Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

d) Dato Público. Es el dato calificado como tal según la ley o la Constitución Política de Colombia, tales como estado civil, profesión y aquellos que puedan obtenerse sin reserva alguna. Por su naturaleza, los Datos Públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

e) Datos Sensibles. Son los que pueden afectar la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

f) Encargado del Tratamiento o Encargado. Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de Datos Personales por cuenta del Responsable del Tratamiento.

g) Responsable del Tratamiento o Responsable. Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la Base de Datos y/o el Tratamiento de los Datos Personales.

h) SIC. Es la Superintendencia de Industria y Comercio, autoridad administrativa en materia de protección de Datos Personales en Colombia.

i) Titular. Persona natural cuyos Datos Personales son objeto de Tratamiento.

j) Transferencia. Envío de Datos Personales de parte del Responsable y/o Encargado a un tercero que se encuentra fuera o dentro del país y que a su vez será tratado como el Responsable del Tratamiento.

k) Transmisión. Tratamiento de Datos Personales que hace el Encargado por cuenta del Responsable, y que implica una comunicación o envío de los Datos Personales dentro o fuera del territorio colombiano.

l) Tratamiento. Cualquier operación o conjunto de operaciones que recae sobre los Datos Personales, tales como la recolección, almacenamiento, uso, circulación o supresión de los Datos Personales.

2.4. Principios

Los siguientes principios constituyen el marco general de cumplimiento de las disposiciones consagradas en los presentes Estándares:

a) Principio de finalidad. El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al Titular.

b) Principio de libertad. El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los Datos Personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

c) Principio de veracidad o calidad. La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

d) Principio de transparencia. En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de Datos Personales que le conciernan.

e) Principio de acceso y circulación restringida. El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los Datos Personales y de la ley aplicable.

f) Principio de seguridad. La información sujeta a Tratamiento por el Responsable o Encargado se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

g) Principio de confidencialidad. Todas las personas que intervengan en el Tratamiento de Datos Personales que no tengan la naturaleza de públicos, están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas por la ley y en los términos de la misma.

h) Protección de Datos Sensibles. MUFG, y/o a quien éste designe como Responsable o Encargado del Tratamiento, recolectarán y tratarán los Datos Sensibles previa autorización expresa e informada de su Titular, o de su tutor o representante legal según sea el caso.

2.5. Base de Datos

Los estándares y procedimientos sobre las que MUFG sea Responsable, son objeto de inscripción en el Registro Nacional de Bases de Datos de conformidad con lo dispuesto en el artículo 25 de la Ley 1581 de 2012, el Decreto 886 de 2014 y las demás normas que lo reglamenten, modifiquen o compilen.

3. Derechos de los Titulares

Los Titulares de los Datos Personales contenidos en las Bases de Datos Personales de MUFG tienen los derechos consagrados en el artículo 8 de la Ley 1581 de 2012 referentes a acceso, actualización, rectificación, cancelación, revocatoria del consentimiento, y presentación de quejas y reclamos y a solicitar prueba de la autorización otorgada a MUFG, salvo cuando la ley no lo requiera y previa solicitud, ser informado sobre el uso que MUFG o quienes por cuenta de este realicen el tratamiento le han dado a sus Datos Personales. Estos derechos no limitan aquellos que se encuentran consagrados en la Constitución Política de Colombia y en la ley.

El ejercicio de estos derechos será gratuito e ilimitado por parte del Titular del Dato Personal, sin perjuicio de las disposiciones legales que regulen el ejercicio de los mismos. El ejercicio de estos derechos constituye una potestad personalísima y será ejercido por el Titular de manera exclusiva, salvo las excepciones consagradas en la ley.

3.1. Mecanismos para otorgar la Autorización

La Autorización del Titular se recolectará mediante documento físico, electrónico o en cualquier otro formato que permita garantizar su posterior consulta. La Autorización la otorgará el Titular a MUFG, o a quien éste designe, y garantiza que se ha puesto en conocimiento del Titular tanto los Estándares como los derechos que le asisten en torno al Tratamiento al que son objeto los Datos Personales que suministra.

3.2. Prueba de la Autorización

MUFG y/o a quien éste designe, adoptará las medidas que sean necesarias para mantener registros de cuándo y cómo obtuvo Autorización por parte de los Titulares para el Tratamiento de los mismo.

4. Obligaciones de MUFG

4.1. Obligaciones del Responsable del Tratamiento

MUFG, en su calidad de Responsable del Tratamiento de los Datos Personales que reposen en las Bases de Datos Personales, cumplirá con las obligaciones consagradas en el artículo 17 de la Ley 1581 de 2012, con miras a garantizar los derechos de los Titulares, garantizar la conservación de la información recolectada, actualizarla cuando sea necesario, tramitar las consultas y reclamos que se le formulen y cumplir los requerimientos y solicitudes de la SIC.

4.2. Obligaciones del Encargado del Tratamiento

MUFG, y/o a quien éste designe, en su calidad de Encargado del Tratamiento de los Datos Personales que reposen en las Bases de Datos Personales, cumplirá con las obligaciones consagradas en el artículo 17 de la Ley 1581 de 2012 para garantizar el cumplimiento de la ley y garantizar los derechos de los Titulares.

4.3. Transmisión de Datos Personales

Para la Transmisión de los Datos Personales de los Titulares, así como como para cualquier Transmisión que MUFG realice para el cumplimiento de las finalidades del Tratamiento o para delegar el Tratamiento en un tercero que se convierta en Encargado, MUFG tomará todas las medidas que sean necesarias para garantizar el cumplimiento de las presentes Estándares, así como para garantizará al Titular el ejercicio de sus derechos. Para estos efectos, MUFG establecerá cláusulas contractuales o celebrar un contrato de Transmisión de Datos Personales en el que, entre otros, se pacte lo siguiente:

a) Los alcances y finalidades del Tratamiento;

b) Las actividades que el Encargado realizará en nombre de MUFG;

c) Las obligaciones que debe cumplir el Encargado respecto del Titular del dato y MUFG;

d) El deber del Encargado de tratar los datos de acuerdo con la(s) finalidad(es) autorizada(s) para el mismo y observando los principios establecidos en la Ley colombiana y la presente Política;

e) La obligación del Encargado de proteger adecuadamente los Datos Personales y las bases de datos, así como de guardar confidencialidad respecto del tratamiento de los datos transmitidos;

f) Una descripción de las medidas de seguridad concretas que van a ser adoptadas tanto por MUFG como por el Encargado de los datos en su lugar de destino.

MUFG no solicitará la autorización del Titular cuando la Transmisión nacional y/o internacional de Datos Personales se encuentre amparada en alguna de las excepciones previstas en la Ley; y sus Decretos Reglamentarios.

4.4. Transferencia de Datos Personales

En el evento en que MUFG transfiera temporal o definitivamente los Datos Personales a un tercero, dentro o fuera del país incluyendo las jurisdicciones que no brindan niveles adecuados para el tratamiento de Datos Personales caso en el cual dicho tercero se convertirá en el Responsable del Tratamiento de los Datos Personales, tomará las medidas necesarias para preservar los derechos de los Titulares durante la Transferencia. Para estos efectos, MUFG establecerá cláusulas contractuales o celebrar un contrato de Transferencia de Datos Personales en el que, entre otros, se pacte lo siguiente:

a) Los alcances y finalidades del Tratamiento;

b) Las actividades que el Responsable realizará;

c) Las obligaciones que debe cumplir el Responsable;

d) El deber del Responsable de tratar los datos de acuerdo con la(s) finalidad(es) autorizada(s) para el mismo y observando los principios establecidos en la Ley colombiana y la presente Política;

e) La obligación del Responsable de proteger adecuadamente los Datos Personales y las bases de datos, así como de guardar confidencialidad respecto del tratamiento de los datos transferidos;

f) Una descripción de las medidas de seguridad concretas que van a ser adoptadas tanto por la MUFG como por el Responsable de los datos en su lugar de destino.

MUFG no solicitará la autorización del Titular cuando la Transferencia nacional y/o internacional de Datos Personales se encuentre amparada en alguna de las excepciones previstas en la Ley; y sus Decretos Reglamentarios.

4.5. Tratamiento de Datos Sensibles

Los Datos Personales que sean de naturaleza sensible serán tratados conforme al objeto social de MUFG, garantizándose la especial protección que sobre estos recae, el cual será aplicado a cualquier Tratamiento al que estos sean sometidos. El Tratamiento de Datos Sensibles respetará las disposiciones legales contenidas en los artículos 6 y 7 de la Ley 1581 de 2012, y siempre que se traten Datos Sensibles, se le informara al titular que su tratamiento es enteramente facultativo.

4.6. Confidencialidad

MUFG protegerá la privacidad de la información. Puede suceder que en virtud de órdenes judiciales, o de regulaciones legales, se deba revelar información a las autoridades que así lo requieran, caso en el cual se informará al titular de manera previa a la remisión de información.

5. Procedimientos establecidos para garantizar el ejercicio de los derechos de los titulares

Conforme a lo indicado en el numeral 4, literal f), del presente Estándar, MUFG cuenta con un procedimiento destinado a atender las solicitudes presentadas por los titulares de información personal para el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición. A continuación, se describe cómo es que dicho procedimiento se encuentra regulado:

5.1. Procedimiento de solicitud

La dirección electrónica designada por MUFG para el ejercicio de los derechos por parte del titular es replegal@co.mufg.jp. Asimismo, y en caso el titular desee ponerse en contacto con MUFG, podrá hacerlo por escrito a la siguiente dirección: Carrera 7 No. 71-21 Oficina 507 de la ciudad de Bogotá D.C. o llamando al +57 601 325 9000.

5.2 Información requerida en la solicitud

Para efectos de completar su solicitud, el titular deberá incluir la siguiente información: (i) nombres y apellidos, (ii) petición concreta que da lugar a la solicitud, (iii) domicilio o dirección, que puede ser física o electrónica, (iv) fecha y firma del titular, (v) documentos que sustenten la petición, de ser el caso.

5.3. Recepción de solicitud

Todas las solicitudes serán recibidas por MUFG. A partir de ello, y por un plazo máximo de 5 días contado desde el día siguiente a la recepción de la solicitud, MUFG iniciará un procedimiento interno a fin de determinar si la solicitud cumple con los requisitos detallados en el apartado anterior. Las observaciones identificadas serán puestas en conocimiento del titular y deberán subsanarse en un período no mayor a 5 días desde la notificación de las mismas. En caso contrario la solicitud será declarada inadmisible, procediendo a su notificación y correspondiente archivo.

5.4. Procedimiento para responder las solicitudes

El ejercicio de los derechos del titular será efectuado a través del siguiente procedimiento:

a. Envío de solicitud al correo electrónico replegal@co.mufg.jp . Recepción inmediata.
b. Evaluación de la solicitud por parte de MUFG.
c. Admisión a trámite de la solicitud.
d. MUFG efectuará una respuesta a la solicitud del Titular en observancia de los siguientes plazos:
   - Para el ejercicio de su derecho de información, se emitirá una respuesta en un plazo máximo de 10 días contados a partir del día siguiente a la recepción de la solicitud.
   - Para el ejercicio de su derecho de acceso, se emitirá una respuesta en un plazo máximo de 10 días contados a partir del día siguiente a la recepción de la solicitud.
   - Para el ejercicio de los derechos de rectificación, cancelación u oposición, se emitirá una respuesta en un plazo máximo de 15 días, contados a partir del día siguiente a la recepción de la solicitud.

- En caso la información proporcionada en la solicitud sea insuficiente o errónea de forma que no permita su atención, el titular de la Base de Datos Personales podrá requerir dentro de los 5 días calendario siguientes a la recepción de la solicitud, documentación adicional al Titular de los Datos Personales.
- Si en un plazo no mayor a dos (2) meses de recibido el requerimiento por parte de MUFG, de lo contrario se entenderá que ha desistido del reclamo.

Los plazos establecidos en el presente documento se deberán considerar como “hábiles”, salvo que se indique lo contrario.

5.5. Quejas ante la SIC

El Titular, sus causahabientes o apoderados, deberán agotar el trámite de consulta ante MUFG o quien éste designe, con anterioridad a la presentación de cualquier queja ante la SIC.

5.6. Reporte de información negativa

MUFG podrá efectuar el reporte de información negativa sobre incumplimiento de obligaciones de los Titulares que hayan dado su Autorización para tal efecto, pero en cualquier caso requerirá comunicarlo previamente al Titular.

6. Finalidad y Vigencia de los Datos Personales

6.1. Finalidad del Tratamiento de Datos Personales

MUFG podrá utilizar los Datos Personales que recolecte, incluidos los Datos Personales y los Datos Sensibles (incluidos aquellos recopilados como consecuencia del uso los Recursos Tecnológicos, según se define más adelante), para las finalidades previstas en la correspondiente autorización o consentimiento obtenido de los Titulares.

En especial, MUFG podrá utilizar los Datos Personales que recolecte, según la naturaleza o calidad del Titular con: (i) propósitos comerciales para clientes y proveedores, tales como la realización de procesos de conocimiento de beneficiarios finales de clientes y proveedores y el cumplimiento con políticas de vinculación de clientes y proveedores, y (ii) propósitos laborales para trabajadores, tales como la verificación del cumplimiento de los estándares de la empresa y el reglamento de trabajo; comerciales, como consecuencia de convenios, o beneficios en favor del Titular, entre otros; contractuales, con ocasión de relaciones existentes entre MUFG y terceros o MUFG y el Titular; seguridad, la protección de los recursos tecnológicos de MUFG que sean utilizados durante la relación laboral, llevar a cabo análisis de seguridad en el Centro de Operaciones de Seguridad Global (“GSOC”) de MUFG, adelantar procesos e investigaciones disciplinarias o forenses por el incumplimiento de los deberes de los trabajadores y administradores, investigar el posible uso indebido de la información comercial confidencial de MUFG y revisar la configuración de seguridad de los equipos; y financieros, como también para adelantar las actividades inherentes a su objeto social. Dichos Datos Personales pueden haber sido o pueden ser obtenidos de usted, ya sea personalmente; directamente por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología que haya sido utilizada como mecanismo de recopilación por parte de MUFG (incluyendo mediante el uso de herramientas tecnológicas, ya sea hardware o software, tendientes a identificar y prevenir ataques a los recursos tecnológicos de MUFG). Dichos datos también pueden proceder de terceros y otras fuentes permitidas por la ley, como las sociedades y operadores de información crediticia. Los datos también pueden ser procesados, almacenados, transmitidos o accedidos por proveedores de servicios externos de MUFG, incluyendo aquellos que actúen como encargados del Tratamiento de los Datos Personales.

6.2. Uso de Recursos Tecnológicos

Uso de Recursos Tecnológicos. Los equipos y otras redes, sistemas y software de computadores y redes y equipos de telecomunicaciones, incluidos los sistemas de administración o bases de datos locales e internacionales, y plataformas y sistemas de recursos humanos utilizados por las sociedades y entidades del Grupo MUFG, del que forma parte MUFG (“Recursos Tecnológicos”) son de propiedad o están arrendados o licenciados para su uso legítimamente por MUFG y/o sus afiliadas. Los Recursos Tecnológicos pueden ser utilizados por usuarios autorizados ("Usuarios Autorizados") solo en cumplimiento de la ley aplicable y los estándares de MUFG y están destinados a ser utilizados exclusivamente con fines profesionales. MUFG es el propietario de toda la información y datos que se almacenen en los Recursos Tecnológicos y cualquier Activo de la Información. Los trabajadores de MUFG se obligan a no hacer uso de los Recursos Tecnológicos ni de cualquier Activo de la Información para fines personales y deberán abstenerse de almacenar en los mismos información y Datos Personales de los usuarios.

Los Usuarios Autorizados tendrán una expectativa limitada de privacidad en el uso de estos Recursos Tecnológicos y en cualquier información, datos o archivos, que puedan incluir información personal, creada, obtenida, procesada, transmitida o almacenada o comunicada a través de los Recursos Tecnológicos (colectivamente, “Activos de la Información”), independientemente de (1) el propósito del uso, (2) el contenido de los Activos de la Información, (3) cualquier permiso de acceso (como la configuración de seguridad), (4) si los Activos de la Información se han eliminado o cifrado, o (5) cualquier otro factor. Los Usuarios Autorizados no deben utilizar los Recursos Tecnológicos respecto de información o material que deseen mantener en privado. Sujeto a las leyes o procesos legales aplicables, y el estándar de protección de datos aplicable, MUFG, y sus proveedores de servicios, pueden monitorear en cualquier momento el uso o la ubicación de cualquier Recurso Tecnológico, al igual que acceder, ver, inspeccionar, analizar, copiar, transferir y transmitir (incluyendo a las jurisdicciones que no ofrecen niveles adecuados de protección en cumplimiento de las obligaciones bajo las leyes aplicables), registrar, modificar, almacenar en caché, almacenar, eliminar, descifrar o procesar cualquier Activo de la Información, con el fin de manejar solicitudes de escalamiento, llevar a cabo análisis de seguridad en el GSOC de MUFG, revisar la idoneidad de la configuración de seguridad del dispositivo, investigando el posible uso indebido de la información o los sistemas de MUFG y verificando el cumplimiento de los Usuarios Autorizados con las políticas de MUFG y la ley aplicable. Los Usuarios Autorizados deben tener en cuenta que MUFG se reserva el derecho, y las agencias gubernamentales u otros terceros pueden obtener, acceder, inspeccionar, bloquear, borrar, modificar, eliminar, confiscar, revocar, congelar o retener los en cualquier tiempo, y sin necesidad de notificación previa, los Recursos Tecnológicos y cualquier Activo de la Información, sujeto a los requisitos de la ley aplicable o proceso legal.

El uso de los Recursos Tecnológicos está sujeto a las políticas de seguridad de la información de MUFG y otros documentos relacionados, disponibles en https://bridge.mufgamericasbridge.com/community/hr-gateway/hr-policies.

6.3. Vigencia

Los presentes Estándares rigen a partir de la fecha de su expedición. El periodo de vigencia de las bases de datos se regirá por las disposiciones que rigen la materia conforme a los principios de finalidad y temporalidad de la información.

Realice un análisis de seguridad en el GSOC de MUFG, investigue el posible uso indebido de la información comercial confidencial o de propiedad de MUFG y revise la suficiencia de la configuración de seguridad del dispositivo.

7. Procedimiento para el tratamiento de los Consentimientos firmados por los Empleados

7.1. Nuevos Empleados

Una vez el correo electrónico del empleado es creado, recibirá un mail de Workday indicándole que tiene una tarea pendiente en su bandeja de entrada.

El nuevo integrante de MUFG podrá dar su consentimiento a través de la plataforma.

7.2. Empleados Existentes

A partir de fines de 2019 se ha solicitado a los empleados de forma voluntaria la firma del Consentimiento de Datos Personales. La solicitud es realizada por el/ la Gerente de Recursos Humanos.

El nuevo integrante de MUFG podrá dar su consentimiento a través de Workday.

7.3. Reporte semanal

El/La Gerente de Recursos Humanos recibe semanalmente vía correo electrónico un reporte de todos los empleados de las Oficinas de Representación de Andes (Colombia y Perú) indicando cuáles son los individuos que han firmado el Consentimiento de Privacidad y quiénes están todavía pendientes.

8. Procedimiento para Incidentes de Privacidad

Los empleados deben informar de inmediato los incidentes de privacidad que causen o de los que tengan conocimiento.

8.1. Conceptos

- Material Non-Public Information (MNPI)

  MNPI (también conocida como Información Privilegiada) se define como información que:

  - no es conocido por el público, pero si lo fuera probablemente afectaría el precio de mercado de los instrumentos financieros a los que se refiere la información

  - un inversionista razonable consideraría material, o probablemente se usaría como parte de su juicio al mantener, vender o comprar esos instrumentos financieros, según corresponda.

  MNPI, como un subconjunto de información confidencial de la empresa, está sujeta a controles más estrictos y específicos que permiten a la Compañía cumplir con requisitos regulatorios específicos. MNPI también está sujeto al principio de necesidad de saber. Consulte la Política de información no pública/barrera de información para obtener más información.

- Información Interna

  Toda otra Información no pública de MUFG que no sea Información Confidencial de Empleados/Clientes/Terceros o Confidencial de la Empresa, p. políticas, memorandos internos y correspondencia.

- Incidente de privacidad

  Cualquier evento que impacte o potencialmente impacte la confidencialidad de la Información Confidencial de Empleados/Clientes/Terceros y la Información Confidencial de la Empresa. Un incidente de privacidad puede incluir el posible acceso no autorizado, adquisición, divulgación, pérdida, robo o uso indebido de información confidencial de empleados/clientes/terceros e información confidencial de la empresa. Se debe investigar un incidente de privacidad para determinar las acciones de mitigación adecuadas y si se requiere una notificación externa. Una empresa o función puede optar por proporcionar una notificación voluntaria a una parte externa, que se clasificaría como un incidente de privacidad.

- Violación de la privacidad

  Un incidente de privacidad que cumpla con ciertos umbrales legales y reglamentarios puede constituir una violación de la privacidad. Junto con otros requisitos aplicables, tales Violaciones de privacidad pueden implicar una obligación legal o contractual de notificar a cualquier parte externa, incluidos clientes, consumidores, clientes comerciales, reguladores, agencias u otras personas.

8.2 Reporte Interno

Los empleados deben:

- Reportar incidentes de privacidad inmediatamente. Las leyes de notificación de violación de datos incluyen obligaciones de notificar a las personas y reguladores afectados dentro de ciertos plazos.
- Completar el formulario de Informe de violación de datos. El formulario se encuentra en la página de inicio de Bridge.
- Comuníquese con IRT_CCG@unionbank.com para informar un incidente de privacidad si no tiene acceso a Bridge.
- Responder con prontitud a las solicitudes del IRT de privacidad y apoyar las investigaciones.

8.3 Detección de un Incidente de Privacidad

Un incidente de privacidad se puede detectar de varias formas. Los ejemplos de incidentes de privacidad notificables pueden incluir, entre otros,

- Destinatarios o archivos adjuntos incorrectos en el correo electrónico
- Empleados que envían o transfieren información de MUFG a una cuenta de correo electrónico personal o a un sitio, plataforma o dispositivo externo para compartir archivos no aprobado (excluyendo la información personal de un Empleado)
- Equipos o documentos perdidos o robados
- Ataques cibernéticos que afectan la confidencialidad de la información
- Uso indebido o acceso no autorizado de información identificada a través de la supervisión de actividades o controles departamentales
- Notificación de un proveedor de servicios externo u otro Tercero
- Reclamos de clientes (p. ej., recepción de un estado de cuenta no relacionado)
- Eliminación inadecuada de activos/equipos de TI (p. ej., en el contenedor de basura de la oficina)

Para mayor información referirse al documento ‘Americas Privacy Incident Response Policy’.

9. Información de contacto

Las preguntas o comentarios sobre este Estándar deben enviarse al Oficial de Cumplimiento.

1. Nombre: Andrea Munizaga Corvacho
2. Correo electrónico: amunizagacorvacho@cl.mufg.jp