

## Anexo Colombia - Política Global de Privacidad

---

### Sección I. Visión General

De acuerdo con lo establecido en la Ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013, Este documento forma parte de la Política Global de Privacidad de MetLife emitida por la Oficina Corporativa de Privacidad de MetLife (MCPO por sus siglas en inglés – MetLife Corporate Privacy Office). La presente información sobre Consideraciones locales ha sido revisada y autorizada por la MCPO. A lo largo de este documento se definen los criterios aplicables sólo a Colombia con base en su regulación local. Por eso adopta las siguientes consideraciones locales de tratamiento de datos personales de obligatoria aplicación en todas las actividades que involucre, total o parcialmente, la recolección, el almacenamiento, el uso, la circulación y transferencia de esa información, comprometida con el respeto y garantía de los derechos de sus clientes, empleados y terceros en general.

**Definiciones:** para efectos de esta adenda a la Política Global y en concordancia con las Leyes Colombianas, se presentan las siguientes definiciones específicas:

**Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

**Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.

**Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

**Encargado del Tratamiento:** 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.

**Responsable del Tratamiento:** 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.

**Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento.

**Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

**Aviso de privacidad:** Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

**Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio ya su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

**Datos sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquello 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.

**Transferencia:** La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

**Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

**Incidente de Datos Personales:** Los incidentes se refieren cualquier evento en los sistemas de información o bases de datos manuales o sistematizadas que atenten contra la seguridad de los datos

personales en ellos almacenados, adicional, un incidente de datos personales ocurre cuando la información personal ha sido o puede haber sido divulgada a alguna persona u obtenida por alguna persona que no debería tener acceso a dicha información. En otras palabras, un incidente de datos personales es una posible filtración de datos causada por la pérdida, mal uso, extravío o acceso no autorizado a la información personal de un individuo.

### **Oficial del Protección de Datos**

La Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio en ejercicio de sus funciones publicó la Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability) el 28 de mayo de 2015, en concordancia con el artículo 26 y 27 del Decreto 1377 de 2013. Directriz que acoge los planteamientos formulados por la Organización para la Cooperación y el Desarrollo Económico (OCDE) y en específico a lo relativo al Programa Integral de Protección de Datos Personales.

Como prevé el Artículo 23 del Decreto 1377 de 2013, todo responsable y Encargado debe designar a una persona o área que “asuma la función de Protección de datos personales y que de trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a se refiere la Ley 1581 de 2012”.

La función del Oficial de Protección de Datos o del Área encargada de protección de datos en la compañía es la de velar por la implementación efectiva de las políticas y procedimientos adoptados por esta para cumplir con las normas, así como la implementación de buenas prácticas de gestión de datos personales.

Dentro de sus actividades se encuentra entre otras las siguientes:

- Coordinar la definición e implementación de los controles del Programa Integral de Gestión de Datos Personales
- Servir de enlace y coordinador con la demás área de la organización para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales
- Impulsar una cultura de protección de datos dentro de la organización
- Mantener un inventario de las bases de datos personales en poder de la organización y clasificarla según su tipo.
- Registrar las bases de datos de la organización en el Registro Nacional de Base de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la SIC
- Obtener las declaraciones de conformidad de la SIC cuando sea requerido
- Revisar los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con encargados no residentes en Colombia
- Analizar las responsabilidades de cada cargo de la organización, para diseñar un programa de entrenamiento en protección de datos personales específico para cada uno de ellos
- Realizar un entrenamiento general en protección de datos personales para todos los empleados de la compañía
- Realizar el entrenamiento necesario a los nuevos empleados, que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización
- Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización (talento Humano, Seguridad, Call centers y gestión de proveedores)
- Medir la participación, y calificar el desempeño, en los entrenamientos de protección de datos
- Requerir que dentro de los análisis de desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre protección de datos personales
- Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de sus políticas de tratamiento de la información personal



- Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la superintendencia de industria y comercio
- Realizar el seguimiento al Programa de Gestión de Datos Personales
- Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales.

Estas funciones se encuentran implementadas en la compañía en la Vicepresidencia de Operaciones dentro de la Subgerencia de ramos masivos y colectivos

### **Conservación de los registros**

El Estatuto Orgánico del Sistema Financiero indica el mantenimiento de los registros o los tiempos de retención y conservación de los documentos producidos por MetLife Colombia, para el caso de los datos personales MetLife Colombia solo recolectará, almacenará, usará o circulará los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el Tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información del EOSF, Artículo 96. Una vez cumplida la o las finalidades del Tratamiento y sin perjuicio de normas legales que dispongan lo contrario, MetLife Colombia o el Encargado por MetLife Colombia deberán proceder a la supresión de los datos personales en su posesión. No obstante lo anterior, los datos personales deberán ser conservados cuando así se requiera para el cumplimiento de una obligación legal o contractual.

### **Responsable del Tratamiento de la Información**

Nombre o razón social: Metlife Colombia Seguros de Vida S.A.

Domicilio o dirección: Carrera 7 No. 99-53 Piso 17

Correo electrónico: [servicio.cliente@metlife.com.co](mailto:servicio.cliente@metlife.com.co)

Teléfono: 3 58 12 58 - 6 38 82 40 (Bogotá, Colombia)

Página web: [www.metlife.com.co](http://www.metlife.com.co)

Lo anterior en cumplimiento al Decreto 1377 del 2013, por el cual se reglamenta la Ley 1581 de 2012.

### **Comité de Protección de Datos Personales**

La compañía cuenta con un Comité de Protección de Datos Personales que se ejecuta teniendo en cuenta el reglamento creado para tal fin con las siguientes funciones:

- Velar por el cumplimiento a lo establecido en la Ley 1581 de 2012 y en sus decretos reglamentarios.
- Evaluar los resultados de las investigaciones cuando así se requiera de los incidencias de seguridad que se presenten en la Compañía y que se relacionen con datos personales.
- Revisar y monitorear el cumplimiento de las políticas en materia de protección de datos que apliquen a la Compañía.
- Sugerir ajustes, recomendaciones o comentarios a la normatividad relacionada con protección y tratamiento de datos personales.

### **Sección II. Aviso, consentimiento y control**

**Aviso de privacidad.** Según la regulación local, en los casos en los que no sea posible poner a disposición del Titular las políticas de Tratamiento de la Información, MetLife deberá informar por medio de un Aviso de Privacidad al Titular sobre la existencia de tales políticas y la forma de acceder a las mismas, de manera oportuna y en todo caso a más tardar al momento de la recolección de los datos personales. *Contenido mínimo del Aviso de Privacidad.* El Aviso de Privacidad, como mínimo, deberá contener la siguiente información:



1. Nombre o razón social y datos de contacto del Responsable del Tratamiento.
2. El Tratamiento al cual serán sometidos los datos y la finalidad del mismo.
3. Los derechos que le asisten al Titular.
4. Los mecanismos dispuestos por el Responsable para que el Titular conozca la política de Tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el Aviso de Privacidad correspondiente. En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información.

No obstante lo anterior, cuando se recolecten datos personales sensibles, el Aviso de Privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos.

*Medios de difusión del aviso de privacidad y de las políticas de Tratamiento de la información.* Para la difusión del Aviso de Privacidad y de la política de Tratamiento de la información, MetLife Colombia podrá valerse de documentos, formatos electrónicos, medios verbales o cualquier otra tecnología, siempre y cuando garantice y cumpla con el deber de informar al Titular, cuando se cambie la finalidad para la cual fueron recolectados los datos, se debe informar al titular sobre la nueva finalidad para la cual se realizara el nuevo tratamiento. No hay una frecuencia determinada por la ley para proporcionar el aviso de privacidad. Igualmente, no hay mención expresa por la ley para suministrar un aviso de privacidad actualizado a las personas.

**Consentimiento.** MetLife Colombia como Responsable del Tratamiento adopta procedimientos adecuados para solicitar, a más tardar en el momento de la recolección de los datos de los clientes, empleados y proveedores, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento.

*Tratamiento de datos personales sensibles.* (Requisitos de consentimiento para usar información personal para comercializar productos) Cuando dicho Tratamiento sea posible conforme a lo establecido en el artículo 6 de la Ley 1581 de 2012, deberán cumplirse las siguientes obligaciones:

1. Informar al Titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.
2. Informar al Titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.

Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles.

*Modo de obtener la Autorización o Consentimiento.* Para efectos de dar cumplimiento a lo dispuesto en las normas locales, MetLife como responsable de datos personales establece mecanismos para obtener la autorización de los Titulares o de quien se encuentre legitimado de conformidad con lo establecido en el artículo 20 del Decreto 1377 del 2013, que garanticen su consulta. Los mecanismos podrán ser a través de medios técnicos que faciliten al Titular su manifestación automatizada. Se entenderá que; la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del Titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca.

## **Datos Sensibles**

Los datos personales suministrados a MetLife Colombia Seguros de Vida S.A por Clientes, Empleados, Proveedores, Intermediarios y Procesos de Selección de Personal, tienen derecho a optar por no responder información sensible solicitada en cualquiera de las etapas de recolección, o que tengan que ver con datos sobre su origen racial o étnico, la pertenencia a sindicatos, organizaciones sociales o de derechos humanos, convicciones políticas, religiosas, de la vida sexual, biométricos o datos de salud.

### **Revocatoria de la autorización y/o supresión del dato**

Los Clientes, Empleado o Proveedores podrán en todo momento solicitar al MetLife Colombia como Responsable o Encargado, la supresión de sus datos personales y/o revocar la autorización otorgada para el Tratamiento de los mismos, mediante la presentación de un reclamo, de acuerdo con lo establecido en el procedimiento para la realización de PQR establecido por la compañía.

En todo caso, la solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular, Cliente, Empleado o Proveedor tenga un deber legal o contractual de permanecer en la base de datos.

### **Procedimiento para que los titulares puedan ejercer sus derechos**

A continuación se detallan los procedimientos para que los titulares de los datos puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información o revocar la autorización.

Los derechos de los Titulares, podrán ejercerse por las siguientes personas legitimadas de conformidad con el artículo 20 del decreto 1377 de 2013:

- a) Por el Titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición MetLife.
- b) Por sus causahabientes, quienes deberán acreditar tal calidad.
- c) Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
- d) Por estipulación a favor de otro o para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Todas las consultas y reclamos se canalizarán a través de los medios habilitados por el MetLife, quien a Todos los reclamos se canalizarán a través de del Área de Servicio al Cliente en la Carrera 7 No. 99-53 Piso 1 - local 1 o por correo electrónico [servicio.cliente@MetLife.com.co](mailto:servicio.cliente@MetLife.com.co), quien lo enviará a la persona de MetLife que sea competente para dar respuesta. Si la persona competente es un tercero, se le dará traslado en un término máximo de dos (2) días hábiles, y se le informará de la situación al interesado.

El reclamo debe presentarse mediante solicitud dirigida a MetLife, y debe contener la siguiente información:

- a) Nombre e identificación del titular del dato o la persona legitimada.
- b) Descripción precisa y completa de los hechos que dan lugar al reclamo.
- c) Dirección física o electrónica para remitir la respuesta e informar sobre el estado del trámite.
- d) Documentos y demás pruebas pertinentes que quiera hacer valer.

Si el reclamo del titular resulta incompleto, se requerirá al interesado dentro de los cinco (5) días hábiles siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

Si el reclamo está completo, se incluirá en la base de datos o sistema de información una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Esta deberá mantenerse hasta que el reclamo sea decidido.

El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término,



se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

MetLife dispone de un sistema de información para llevar el registro de todas las actuaciones efectuadas respecto de cada reclamo en el cual se anotará, entre otras, lo siguiente:

- a) Fecha de recibo del reclamo.
- b) Nombre y dirección del titular o de quien realice el reclamo.
- c) Descripción de los hechos que dan lugar al reclamo.
- d) Documentos que el titular anexa para que se tengan en cuenta en el reclamo (opcional).
- e) Nombre de la persona de MetLife encargada de dar respuesta al reclamo.
- f) Fecha de envío de la respuesta al titular del dato.

Este sistema dispondrá de mecanismos automáticos de alerta que informen sobre los plazos para responder lo más pronto posible o, en todo caso, dentro de los términos establecidos en esta política y en los amparados en el Régimen General de Protección de Datos.

*Persona o Área Responsable para la atención de Peticiones, Quejas y Reclamos.* MetLife cuenta con un área de Servicio al Cliente la cual asumirá la función de recepción y trámite a las Peticiones, Quejas y Reclamos que realicen los titulares en materia de protección de datos personales y escalará las solicitudes de los titulares al Data Privacy Local o quien asuma la función de protección de datos Personales al interior de la compañía, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012, el decreto 1377 de 2013 y la presente política.

La Persona o Área responsable de la Protección de Datos Personales puede ser contactada a través de los siguientes medios:

Email: [Data.privacy@metlife.com.co](mailto:Data.privacy@metlife.com.co)

Teléfono: 3 58 12 58 – 6 38 82 40 (Bogotá, Colombia)

Página web: [www.metlife.com.co](http://www.metlife.com.co)

### **Uso de Cookies**

El acceso a la Web en internet puede implicar el uso de cookies, aunque la página de internet de MetLife Colombia Seguros de Vida S.A puede funcionar sin su uso. Las cookies son archivos pequeños que almacenan información en el navegador de cada usuario de modo que el servidor pueda reconocer cierta información que solamente el servidor pueda leer. Las cookies duraran un tiempo limitado. Ninguna cookie permite revelar el teléfono, correo electrónico u otros detalles de identificación personal, más si la dirección de IP de su computadora. Las cookies no pueden extraer ninguna información de su PC u obtener información personal sobre el mismo. Aunque las cookies en MetLife Colombia Seguros de Vida S.A, nos ayudan a optimizar los procesos de reserva, los clientes o usuarios que accedan a la página web de la compañía que no deseen recibir las cookies o que no quieran que se informe de su visita, pueden configurar su navegador a tal efecto. Todos los navegadores de Internet tienen opciones disponibles en su configuración que permiten bloquear o permitir las cookies de sitios web concretos.

### **Sección III. Protección de información**



MetLife Colombia cuenta con las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, para ello cuenta con Políticas de IT robustas, así como la Política de Escritorio Limpio y envío Seguro de Información.

#### **Sección IV. Procesadores de datos de terceros**

Por cada nueva contratación de un tercero y por cada contrato existente que se renueve, los empleados en la línea de negocio o área funcional que busquen contratar al tercero deberán realizar un análisis de tres pasos antes de celebrar o renovar el contrato

##### *Paso uno: realizar una evaluación preliminar del riesgo*

Los empleados en la línea de negocio o área funcional que buscan contratar a un tercero o renovar alguna relación existente con un tercero deberán determinar si la contratación presenta algún riesgo de privacidad, el cual surge cuando el tercero maneja, procesa o accede a información personal del cliente o empleado de MetLife. Para hacer esta determinación, el empleado deberá responder a las siguientes preguntas:

1. ¿El tercero o subcontratista del tercero recopilará, accederá, compartirá, utilizará, visualizará o almacenará la información personal de los empleados, clientes existentes o clientes potenciales de MetLife?
2. ¿El tercero o subcontratista del tercero realizará actividades de comercialización en nombre de MetLife utilizando la información personal de empleados, clientes existentes o clientes potenciales de MetLife?

Si la respuesta a cualquiera o ambas preguntas es “Sí”, entonces el empleado deberá seguir los pasos dos y tres para evaluar y mitigar el riesgo de privacidad de manera más exhaustiva. En virtud de esta Política, los empleados no están obligados a completar los pasos dos y tres si la respuesta a ambas preguntas es “No”.

##### *Paso dos: realizar la diligencia debida inicial*

Para garantizar que el tercero cuente con medidas de seguridad adecuadas para proteger la información personal de MetLife, la línea de negocio o área funcional responsable deberá trabajar con la Dirección de Seguridad de Tecnología de la Información para realizar la diligencia debida sobre las prácticas de

Protección de datos de terceros, protecciones de seguridad de la información, programa de cumplimiento de privacidad y el uso previsto de los datos de MetLife, incluyendo el riesgo en cualquier transferencia de datos en proceso. Si después de realizar la diligencia debida se determina, con base en parámetros definidos por la Oficina de Privacidad Corporativa de MetLife, que el tercero presenta un posible riesgo sin mitigar para la información personal de MetLife, entonces la Dirección de Seguridad de Tecnología de la Información deberá reportar el asunto al departamento de Cumplimiento para que se determinen los siguientes pasos a seguir en coordinación con la línea de negocio/área funcional pertinente, con la Dirección de Seguridad de Tecnología de la Información y con otras partes interesadas que sean pertinentes.

##### *Paso tres: incluir las disposiciones sobre privacidad y protección de datos en el acuerdo*

Para garantizar la responsabilidad del tercero y la seguridad de los datos personales de MetLife, los empleados de la línea de negocio o área funcional responsable deberán trabajar con el departamento Legal para incorporar las disposiciones de protección de datos (según lo requerido por la ley o regulación aplicable) en el acuerdo escrito, el contrato u orden de compra. El departamento Legal deberá incluir, como mínimo, disposiciones que aborden las siguientes obligaciones por parte del tercero:

- Disposición de cumplimiento regulatorio: el tercero reconoce que comprende y acepta cumplir con todas las leyes y regulaciones de privacidad y seguridad de datos que sean aplicables al procesar información personal de MetLife.
- Disposición de especificación del propósito: la información personal de MetLife sólo puede ser utilizada para los fines especificados en el acuerdo que el tercero celebra con MetLife y para ningún otro propósito.
- Disposición de seguridad de la información: la información personal de MetLife debe estar protegida por controles de seguridad específicos (por ejemplo: cifrado de datos en tránsito, seguridad de la red y controles de acceso).
- Disposición de confidencialidad: la información personal de MetLife debe estar protegida por una disposición de confidencialidad que restrinja la divulgación de la información a otras partes.
- Disposición de retención de datos: toda la información personal de MetLife, ya sea en formato electrónico o soporte físico, deberá ser devuelta o destruida por el tercero en el momento en que las actividades de procesamiento finalicen y deberá estar sujeto a la ley o regulación aplicable.
- Disposición de notificación de filtración de datos: el tercero debe gestionar incidentes que podrían conducir a una filtración de datos y notificar sin demora a MetLife sobre cualquier posible filtración de datos que involucre a la información personal de MetLife y se deberá realizar dentro del plazo de tiempo establecido.
- Disposición sobre subcontratistas: todos los subcontratistas que pudieran procesar información personal de MetLife deben estar sujetos a los mismos términos de privacidad y seguridad especificados en el acuerdo entre terceros y, cuando corresponda, MetLife deberá aprobarlos por escrito.
- Disposición sobre derecho a auditoría: MetLife debe disponer del derecho de auditar las medidas de seguridad y el uso de la información personal de MetLife del tercero con el fin de garantizar el cumplimiento del acuerdo y de la ley/regulación aplicable.
- Disposición de indemnización y reparto de responsabilidades: MetLife debe ser indemnizado por cualquier pérdida, reclamación o responsabilidad en que se haya incurrido a causa del incumplimiento por parte del tercero de proteger la información personal de los clientes o empleados de MetLife.

Al completar los pasos, la línea de negocio o área funcional responsable deberá obtener las firmas apropiadas como se especifica en el Apéndice A.

Por favor valide el Apéndice A de este documento (Checklist de riesgos de privacidad para terceros).

## **Sección V. Transferencias Transfronterizas de Datos**

Para la transmisión y transferencia de datos personales, se aplicarán las siguientes reglas de acuerdo a la regulación local:

1. Las transferencias internacionales de datos personales deberán observar lo previsto en el artículo 26 de la Ley 1581 de 2012.
2. Las transmisiones internacionales de datos personales que se efectúen entre un Responsable y un Encargado para permitir que el Encargado realice el Tratamiento por cuenta del Responsable, no requerirán ser informadas al Titular ni contar con su consentimiento cuando exista un contrato. El contrato que suscriba el Responsable con los Encargados para el Tratamiento de datos personales bajo su control y responsabilidad señalará los alcances del Tratamiento, las actividades que el Encargado realizará por cuenta del Responsable para el Tratamiento de los datos personales y las obligaciones del Encargado para con el Titular y el Responsable. Mediante dicho contrato el Encargado se comprometerá a dar aplicación a las obligaciones del Responsable bajo la política de Tratamiento de la información fijada por éste y a realizar el Tratamiento de datos de acuerdo con la finalidad que





los Titulares hayan autorizado y con las leyes aplicables. Además de las obligaciones que impongan las normas aplicables dentro del citado contrato, deberán incluirse las siguientes obligaciones en cabeza del respectivo Encargado:

1. Dar Tratamiento, a nombre del Responsable, a los datos personales conforme a los principios que los tutelan.
2. Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
3. Guardar confidencialidad respecto del Tratamiento de los datos personales.

## **Sección VI. Gestión de Incidentes de Datos Personales**

Cualquier área de la compañía que trate, manipule o modifique Datos Personales de los clientes, proveedores o empleados, según sea el caso, deberá incluir en sus Procedimientos un plan para reportar, gestionar, analizar y prevenir las violaciones de seguridad de datos y que cumpla con los requerimientos legales, regulatorios, de la Compañía y comerciales. Dicho plan deberá atender por lo menos, y conforme se explicará en la presente sección, lo siguiente:

- El reporte de incidentes debe realizarse al Oficial de Cumplimiento por los medios de comunicación que tengan establecidos para este propósito. Es importante resaltar que se debe reportar cualquier incidente de datos personales sin importar el tamaño.
- Identificación de Incidentes de datos personales.
- Plan de Acción de contención y recuperación de la información que fue objeto de violación;
- Medidas preventivas para evitar incidentes de violación de la seguridad de datos.

Posterior al descubrimiento de cualquier acceso no autorizado potencial, pérdida, revelación o desviación de Información Personal que comprometa la seguridad, confidencialidad o integridad de dicha Información Personal, sesionara el Comité de Protección de Datos Personales, compuesto por el Líder de Riesgo operativo, Oficial de Cumplimiento, área Legal, Oficial de Seguridad de la Información y Oficial de Datos Personales, que permitirá el monitorear el progreso de la investigación y trabajar con la Dirección de Privacidad de MetLife para asegurarse de que la Compañía cumpla con todas las leyes y regulaciones que apliquen que requieran de un aviso a los reguladores e individuos, adicionando lo siguiente:

- Respuesta que incluyan los requerimientos adecuados de informado y notificación en lo relacionado con los reguladores, individuos afectados y clientes del grupo, conforme aplique, en concordancia con el grupo de trabajo de incidentes de datos personales
- Evaluación fáctica de las causas que ocasionaron la violación, datos comprometidos y riesgo en curso; y
- Análisis legal y evaluación del impacto de la violación de los sistemas.
- Plan de acción para las posibles irregularidades presentadas en los procesos y procedimientos de las áreas.

Los incidentes de violación de la seguridad de datos deberán informarse a la Dirección de Privacidad de MetLife (i) en los casos en que, como resultado del incidente de violación de la seguridad de datos, una ley o Política Global de regulación aplicable requiera aviso a los clientes, individuos y/o entes reguladores y (ii) en ausencia de un requerimiento de aviso, en donde el incidente de violación de seguridad se considere material en conformidad con los parámetros provistos al Directivo de Privacidad Regional y al Experto Local de Privacidad ocasionalmente por parte de la Dirección de Privacidad de MetLife

Además, el departamento de Legal debe determinar si el incidente de datos personales se puede clasificar como una filtración de datos de conformidad con la regulación aplicable,



deberá informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares. Los reportes deberán hacerse a los 15 días hábiles siguientes que el área Legal determine que el incidente debe reportarse. Este reporte lo hará un Representante Legal de la compañía.

La cuestión de determinar si un incidente de datos personales se puede clasificar como una filtración de datos es una determinación legal basada en una serie de factores, incluyendo la ley aplicable, los hechos y las circunstancias del incidente de datos personales, la confidencialidad de la información personal involucrada y el posible daño resultante hacia los individuos afectados.

### **Sección VII. Evaluaciones de Impacto de la Privacidad**

Actualmente la ley local no requiere ninguna evaluación de impacto sobre la privacidad, pero cuando la ley local lo requiera, las operaciones de MetLife deberán tener procesos implementados para llevar a cabo evaluaciones de impacto en la privacidad en cualquier proyecto que procese, recopile, utilice, comparta o almacene información personal a nivel local. Si el proyecto contiene la información personal de individuos provenientes de un país fuera del lugar de negocios de la operación, entonces la línea de negocio o área funcional responsable del proyecto deberá ponerse en contacto con el departamento de Cumplimiento o con el departamento Legal para obtener orientación.

Por favor remítase al Apéndice B (Fases iniciales de una evaluación de Impacto en protección de datos personales)

### **Sección VIII. Capacitacion**

Se requiere que todos los Colaboradores recién ingresados, reciban capacitación para seguir los programas de privacidad y seguridad de la información de MetLife, así como una capacitación anual a todo el personal en temas de Protección de Datos Personales. Para el desarrollo de los cursos de capacitación adecuados la Dirección de Privacidad de MetLife colaborará con Enseñanza y Desarrollo MetLife, así como con las unidades comerciales y operaciones a nivel país diseñaran la capacitación general en protección de datos personales.

### **Sección IX. Derechos que asisten como Titulares del Dato**

#### **Derechos de los Titulares de los datos**

Las personas obligadas a cumplir estas políticas deben respetar y garantizar los siguientes derechos de los titulares de los datos:

- a) Conocer, actualizar y rectificar los datos personales. Para el efecto es necesario establecer previamente la identificación de la persona para evitar que terceros no autorizado accedan a los datos del titular del dato.
- b) Obtener copia de la autorización.
- c) Informar sobre el uso que MetLife ha dado a los datos personales del titular.
- d) Dar trámite a las consultas y reclamos siguiendo las pautas establecidas en la ley y en la presente política.
- e) Acceder a la solicitud de revocatoria de la autorización y/o supresión del dato personal cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento por parte de MetLife se ha incurrido en conductas contrarias a la ley 1581 de 2012 o a la Constitución.



El Titular también podrá revocar la autorización y solicitar la supresión del dato, cuando no exista un deber legal o contractual que le imponga el deber de permanecer en la base de datos o archivo del Responsable o Encargado.

La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el titular tenga un deber legal o contractual de permanecer en la base de datos del Responsable o Encargado.

- f) Acceder en forma gratuita a sus datos personales. La información solicitada por el titular podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos o Archivo de MetLife.

Los derechos de los Titulares, podrán ejercerse por las siguientes personas:

- a) Por el Titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición MetLife
- b) Por sus causahabientes, quienes deberán acreditar tal calidad.
- c) Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento. Por estipulación a favor de otro o para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

#### **Datos Sensibles**

Los datos personales suministrados a MetLife Colombia Seguros de Vida S.A por Clientes, Empleados, Proveedores, Intermediarios y Procesos de Selección de Personal, tienen derecho a optar por no responder información sensible solicitada en cualquiera de las etapas de recolección, o que tengan que ver con datos sobre su origen racial o étnico, la pertenencia a sindicatos, organizaciones sociales o de derechos humanos, convicciones políticas, religiosas, de la vida sexual, biométricos o datos de salud.

**Apéndice A: Lista de control sobre riesgos de privacidad para terceros (Privacy Check list)**

MetLife ha asumido el compromiso de proteger la seguridad, la confidencialidad y la integridad de la información personal de sus clientes y empleados, así como cumplir con las leyes de privacidad y protección de datos de cada país en el que la Compañía realiza negocios. MetLife puede ser considerado responsable de los actos de un tercero si la información personal de los clientes o empleados de MetLife se ve comprometida mientras realiza servicios para MetLife o en nombre de MetLife. Con el objetivo de mitigar el riesgo de realizar negocios con terceros que procesan información personal de clientes o empleados de MetLife, la línea de negocio o área funcional pertinente deberá completar la siguiente lista de control para cada nueva contratación de un tercero y por cada contrato existente que se renueve. Una vez que ésta se complete, el encargado de la línea de negocio o área funcional pertinente deberá certificar la exactitud de las respuestas de la lista de control y las acciones tomadas.

<b>Pregunta 1:</b> ¿El tercero o subcontratista del tercero recopilará, accederá, compartirá, utilizará, visualizará o almacenará la información personal de los empleados, clientes existentes o clientes potenciales de MetLife?	<input type="checkbox"/> Sí <input type="checkbox"/> No
<b>Pregunta 2:</b> ¿El tercero o subcontratista del tercero realizará actividades de comercialización en nombre de MetLife utilizando la información personal de empleados, clientes existentes o clientes potenciales de MetLife?	<input type="checkbox"/> Sí <input type="checkbox"/> No
<b>Si la respuesta a las preguntas 1 y/o 2 es “Sí”, <u>deberá</u> completar los incisos (a), (b), (c) y (d) a continuación</b>	
<b>(a)</b> Contactar a la función de riesgo informático y seguridad en <a href="mailto:ARS_MOREs@metlife.com">ARS_MOREs@metlife.com</a> para realizar la diligencia debida en las protecciones de seguridad de la información de terceros y las prácticas de protección de datos.	<input type="checkbox"/> Marque esta casilla para confirmar que la Dirección de Seguridad de Tecnología de la Información colaborará para llevar a cabo la diligencia debida en terceros.
<b>(b)</b> Trabajar con el departamento Legal para incluir disposiciones sobre privacidad y protección de datos en el acuerdo, contrato u orden de compra de un tercero.	<input type="checkbox"/> Marque esta casilla para confirmar que el departamento Legal colaborará para incluir disposiciones sobre privacidad y protección de datos en el acuerdo.
<b>(c)</b> ¿De qué país/países se generará la información personal?	
<b>(d)</b> ¿En qué país/países se visualizará, almacenará, procesará o accederá a la información personal?  <i>Nota: el procesamiento de la información personal se define en términos generales para incluir cualquier operación que se realiza en relación con la información, tal como visualizar, recopilar, almacenar, alterar, recuperar, utilizar, transferir, revelar, diseminar, bloquear, borrar o destruir.</i>	

**Si los países identificados en las respuestas (c) y (d) son diferentes, entonces usted deberá trabajar con el departamento Legal para determinar si se requiere algún acuerdo para la transferencia de datos u otro mecanismo de transferencia en virtud de la ley o regulación aplicable.**

*Nota: puede haber limitaciones contractuales sobre dónde se pueden almacenar los datos o acceder a éstos en ausencia de restricciones legales. Usted deberá trabajar con la línea de negocio que mantiene la relación comercial con los datos a fin de abordar cualquier limitación contractual que pueda aplicarse.*

*Marque esta casilla para confirmar que el departamento Legal colaborará para evaluar los requisitos legales de la transferencia transfronteriza de datos.*

*Certifico que, según mi leal saber y entender, las respuestas proporcionadas en esta lista de control son precisas y completas, y que antes de realizar la contratación del tercero he completado todas las acciones que se requieren de conformidad con la Política Global de Privacidad, incluyendo, siempre que sea necesario: (i) colaborar con la Dirección de Seguridad de Tecnología de la Información para completar la diligencia debida en el tercero; y (ii) colaborar con el departamento legal para incluir disposiciones adecuadas de privacidad y protección de datos en el acuerdo, así como para garantizar que el mecanismo apropiado de transferencias transfronterizas de datos esté establecido de acuerdo con lo exigido por la legislación local aplicable.*

\_\_\_\_\_  
**Nombre de la persona que completa este formulario**

\_\_\_\_\_  
**Firma**

\_\_\_\_\_  
**Fecha**

\_\_\_\_\_  
**Nombre del jefe de la línea de negocio/área funcional**

\_\_\_\_\_  
**Firma**

\_\_\_\_\_  
**Fecha**



**Apéndice B: Fases iniciales de una evaluación de Impacto en protección de datos personales.**