Actualización de la Política Global de Privacidad de MetLife con aspectos regulatorios locales

Uruguay

Este documento forma parte de Política Global de Privacidad de MetLife emitida por la Oficina Corporativa de Privacidad) de MetLife. La presente información sobre Consideraciones locales ha sido revisada y autorizada por la Oficina Corporativa de Privacidad

A lo largo de este documento se definen los criterios aplicables en Uruguay con base en su regulación local y que se consideran **adicionales a la Política Global.**

INTRODUCCIÓN

El prestigio como así también la información creada, procesada y utilizada por MetLife y sus empresas vinculadas, es uno de nuestros activos más valiosos. Considerando la naturaleza competitiva de nuestras Compañías y el significativo valor de los recursos que manejamos, será nuestra obligación proteger estos activos en concordancia con los riesgos del negocio.

Comprometer nuestro prestigio y los activos de información puede impactar severamente sobre nuestros Clientes y Empleados, constituir una violación a las leyes y regulaciones vigentes, y afectar negativamente la reputación, la imagen y los resultados económicos de nuestras Compañías y de la Corporación.

El presente documento establece los tipos de información que requieren protección dentro de la Compañía, y el tratamiento que se le debe prestar a la misma.

La presente política tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.

I. PERSPECTIVA GENERAL

1. Ley aplicable

El marco regulatorio que rige al país en materia de privacidad de la información, comprende:

- ✓ La Ley 18.831 de Protección de Datos Personales y Acción de Habeas Data.
- ✓ Decreto Reglamentario 414/009.
- ✓ Decreto 308/14 - Actualizacion del Decreto Reglamentario 414/009
- ✓ Disposiciones de la Unidad Reguladora y de Control de Datos Personales (URCDP).

2. Responsable

La figura del Data Privicy Officer no es requerida por la regulación local. La ley solo requiere que sea designado un responsable de las bases de datos registradas. A tal efecto, se encuentra designado el Local Pricacy Champion como responsable de las bases de datos registradas.

Su responsabilidad abarca el cumplimiento de los aspectos regulatorios, garantizar el derecho de acceso y la seguridad de las bases de datos registradas.

La registración de la base de datos le dará carácter legal a su administración y utilización.

1. Definiciones

- ✓ **Datos personales:** Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

- ✓ **Datos sensibles**: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

- ✓ **Archivo, registro**, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

- ✓ **Tratamiento de datos:** Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

- ✓ **Responsable de archivo, registro, base o banco de datos**: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

- ✓ **Datos informatizados:** Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

- ✓ **Titular de los datos:** Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

- ✓ **Usuario de datos:** Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

- ✓ **Disociación de datos:** Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

2. Principíos Generales

1. Legalidad.

La formación de bases de datos será lícitacuando se encuentren debidamente inscriptas

2. Veracidad.

- Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

- La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.

- Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquéllas que motivaron su obtención.

- Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.

- Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud.

3. Registración de bases de datos

Consiste en la inscripción de las Bases de Datos que contienen datos de personas físicas y jurídicas, independientemente de que el soporte de almacenamiento sea informatizado o en papel.

El trámite se realiza únicamente a través de la web de la Unidad Reguladora de Datos Personales (datospersonales.gub.uy)

Acceso en Línea https://www.datospersonales.gub.uy/SRCiudadanoWeb

Los responsables de las bases de datos deberán mantener actualizados los datos inscriptos en el Registro de Base de Datos Personales, comunicando trimestralmente las actualizaciones

1. Finalidad.

- Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

- Los datos objeto de tratamiento no podrán serutilizados para finalidades distintas o incompatibles con aquellas quemotivaron su obtención.

2. Previo consentimiento informado.

- El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse.

3. Seguridad de los datos.

- El responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

- Los datos deberán ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

4. Reserva.

- Aquellas personas físicas o jurídicas que obtuvieren legítimamente información proveniente de una base de datos que les brinde tratamiento, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros.

5. Responsabilidad.

El responsable de la base de datos esresponsable de la violación de las disposiciones de la presente ley.

II. AVISO, CONSENTIMIENTO Y CONTROL

1. Información al cliente

Aspectos regularorios

Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa, precisa e inequívoca:

a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios.

b) La existencia de la base de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable.

c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles.

d) Las consecuencias de proporcionar los datos y de la negativa a hacerlo o su inexactitud.

e) La posibilidad del titular de ejercer los derechos de acceso, rectificación y supresión de los datos.

El consentimiento no es requerido, cuando:

f) Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación.

g) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

h) Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma.

i) Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.

j) Se realice por personas físicas para su uso exclusivo personal, individual o doméstico.

Procedimiento

a) Clientes

En todos aquellos casos en que MetLife colecte datos personales de sus Clientes, se le debe notificar de sus derechos sobre sus datos según los establece el Decreto Reglamentario 414/009 y Articulo 9 de la ley 18.331. Esto incluye los que se requieren:

a) a través de las solicitudes de pólizas por las características propias de la contratación del seguro
b) en las Solicitudes de denuncias de siniestros o de rescates
c) en las Solicitudes de actualización de datos del Cliente o de los Beneficiarios
d) con fines de captación de datos con objetivos comerciales por cualquier medio, internet o campañas de marketing en eventos o en la vía pública.
e) A través de la opción de actualización de datos personales existente en el sitio Web de MetLife.

El responsable del área de **Marketing** deberá asegurar la inclusión en la documentación o medios mencionados en los puntos que anteceden, de la siguiente notificación al Cliente:

a) Formularios de Beneficios con datos sensibles.
CONSENTIMIENTO PARA COMUNICACIÓN DE DATOS PERSONALES SENSIBLES: *Por medio del presente, autorizo al médico firmante a que comunique mi información de carácter personal sensible contenida en este formulario a MetLife Seguros S.A., para que ésta la incorpore en la correspondiente base de datos con la finalidad de evaluar la procedencia del pago del beneficio bajo el seguro contratado.*

b) Resto de los formularios donde se colectan datos del cliente.
DATOS PERSONALES - CONSENTIMIENTO**:** *MetLife Seguros S.A. ("MetLife") recaba y trata sus Datos Personales con el único fin de administrar su seguro, así también como para el envío de información y ofertas sobre los productos de MetLife. Al suscribir este documento, (i) presto mi consentimiento previo, libre, expreso e informado para el referido tratamiento de los Datos Personales que proporciono a MetLife; (ii) autorizo a MetLife a transferir internacionalmente los Datos Personales a sus afiliadas; y (iii) autorizo a cualquier médico o profesional de la salud, hospital, clínica, compañía de seguros u otra institución o persona que tenga conocimiento, información, registros y/o datos sensibles vinculados a la salud o actividades, sea presente o pasada, para que pueda dar o entregar cualquier antecedente, información o examen solicitados por MetLife, así también como para que para que ésta la incorpore en la correspondiente base de datos con la finalidad de realizar cualquier gestión específica que sea requerida a los efectos del seguro solicitado. A su vez autorizo MetLife para que solicite, reciba y retire copia de tales antecedentes, exámenes o informes de las personas o instituciones mencionadas. Una fotocopia de esta autorización será tan válida como el original. Tomo conocimiento y autorizo a que tanto los empleados de MetLife como sus terceros proveedores que requieran acceso a mis datos personales para las finalidades antes mencionadas. El responsable de la base de datos es MetLife Seguros S.A., domiciliada en Yaguarón 1407, piso 4, of. 401, Montevideo. Usted podrá ejercer sus derechos legales de acceso, rectificación, actualización, inclusión o supresión de sus Datos Personales, mediante una comunicación escrita a nuestras oficinas. Dicho derecho podrá ser ejercido en forma gratuita a intervalos de seis meses, salvo que se hubiere suscitado nuevamente un interés legítimo de acuerdo con el ordenamiento jurídico*.

Corresponde a la **Dirección de Legales** y a la **Gerencia de Ethics & Compliance** asegurar la inclusión de la presente notificación al Cliente, dentro del proceso de aprobación de Material de Venta.

b) Empleados

Respecto de los empleados de MetLife y la administración de sus datos personales, así como su transferencia al exterior dentro del proceso de gestión de recursos humanos, al momento del ingreso dentro del proceso de reclutamiento se les informan sus derechos sobre sus datos personales a través del formulario “Data Consent Form” - ANEXO II

2. Consentimiento

Aspectos regulatorios

El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el punto anterios “CONSENTIMIENTO..”

No será necesario el previo consentimiento cuando:

A) Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación.

B) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

C) Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma.

D) Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.

E) Se realice por personas físicas para su uso exclusivo personal, individual o doméstico.

Procedimiento

a) Clientes

El concentimiento del cliente sobre el uso de los datos personales es obtenido al momento de suscripción de la solicitud del seguro o cuando los datos con colectados a través del sitio Web de MetLife. (ver punto II.1)

Cuando los datos personales son utilizados con fines de venta a través de campañas realizadas por medios electrónicos, todos los envíos deben contener al pie del mismo:

- Que el correo ha sido remitido a través del Sistema Masterbase

- La opción habilitada para que el receptor pueda modificar o anular la suscripción.

- La opción de “opt-out” y no contuinuar a recibiendo comunicaciones.

b) Empleados

El consentimiento del empleado sobre la utilización de sus datos personales es obtenido a través del formulario “Data Consent Form” que debe ser firmado por el empleado al momento de su ingreso a MetLife como parte del proceso de reclutamiento. (Ver Anexo II)

El consentimiento del empleado otorgado a través de su firma habilita a MetLife a la utilización de sus datos dentro de la gestión de Recursos Humanos, ya sea para transferirlos al exterior como para compartirlo con terceros.

3. Derecho de acceso

Aspectos regularorios

- Todo titular de datos personales que previamente acredite su identificación con el documento de identidad o poder respectivo, tendrá derecho a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas. Este derecho de acceso sólo podrá ser ejercido en forma gratuita a intervalos de seis meses, salvo que se hubiere suscitado nuevamente un interés legítimo de acuerdo con el ordenamiento jurídico.

- Cuando se trate de datos de personas fallecidas, el ejercicio del derecho al cual refiere este artículo, corresponderá a cualesquiera de sus sucesores universales, cuyo carácter se acreditará debidamente.

- La información debe ser proporcionada dentro de los cinco días hábiles de haber sido solicitada. Vencido el plazo sin que el pedido sea satisfecho o si fuera denegado por razones no justificadas de acuerdo con esta ley, quedará habilitada la acción de habeas data.

- La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen.

- La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aún cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aUn cuando se vinculen con el interesado.

- La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.

Procedimiento

El pedido de derecho de acceso a sus datos personales o la rectificación o anulación de los mismos debe ser requerido a través de las líneas telefónicas de Atención al Cliente o del link de contacto dentro del sitio Web deMetLife.

Ingresado el pedido por parte del cliente / tercero, el área de Atención al Cliente registra el evento dentro de la base de administración y gestión de llamadas entrantes con el código **"Privacy – Gestión de Datos Personales"**

La gestión es diligenciada y el cliente contactado dentro de los 5 días hábiles de ingresada.

Si el pedido es recibido por escrito en las oficinas de Atención al Cliente de MetLife se sigue el mismo

III. PROTECCION DE LA INFORMACIÓN

Aspectos regularorios

- El responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

- Los datos deberán ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

- Queda prohibido registrar datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad.

Política de Escritorios Limpios

Se encuentra publicada y a disposición de todos los empleados la Política de Resguardo de Información en Escritorios (https://app.mymetlife.com/sites/CST4001/normas/SitePages/Home.aspx) cuyo objeto es e stablecer la política de resguardo de reportes que contengan información personal, confidencial o restringida, con el fin de reducir los riesgos de acceso no autorizado, daño o pérdida de información para la compañía.

- La clasificación de la información administrada por cada sector, será responsabilidad de los **Responsables de cada área de negocio** según las características y naturaleza de la misma.

- Todos los Empleados de la Compañía deben asegurarse que la oficina a la que pertenecen, quede en condiciones ordenadas al finalizar la jornada de trabajo. Todos los escritorios, muebles, y cualquier otra superficie debe quedar libre de materiales con información clasificada con niveles de seguridad CRÍTICO y MEDIO, independientemente del medio en el cual se encuentre almacenada.

- Los **Responsables de cada área** deberán asegurar la existencia de medios aptos para el resguardo y almacenamiento de la información de nivel CRÍTICA y MEDIO de personal (gabinetes cerrados, cajas ignífugas, salas de archivo). En caso que se decidiera, se podrá etiquetar la documentación a nivel de carpetas, expedientes o legajos siempre y cuando estos medios se manejen como un todo y sus partes componentes no sean removidas por separado.

- La criticidad de la información sujeta a protección es definida dentro de la Política de Protección de Datos Personales publicada en la Intranet y está relacionada con su calificación regulatoria en Información Sensible o Pública.

- Todo contrato con Proveedores externos deberá incluir una cláusula de confidencialidad y otra relacionada con la destrucción de la información luego de su procesamiento / uso.

Otras Políticas relacionadas con el manejo de datos personales.

- En referencia a la información almacenada digitalmente, las políticas de seguridad de **IT** más relevantes (https://app.mymetlife.com/sites/CST4001/normas/Lists/Chart/GrupoNormas.aspx) son:

  a) **Administración de RiesgosSeguridad Física**

  b) **Monitoreo de la Seguridad y Respuesta**

  c) **Continuidad del Negocio**

  d) **Administración de Incidentes de IT**

  e) **Privacidad**

  La lista completa de políticas de seguridad de IT pueden ser consultadas en el link arriba mencionado o en ARCHER a través del siguiente link: IT Security Policies and Standards

- En referencia a la gestión de datos e información personal, en la intranet corporativa pueden ser ubicadas las siguientes políticas:

  a) Manejo del Ciclo de Vida de la Información (ILM - https://my.metlife.com/en/us/tools/ILM)

  b) Política de Gestión de Datos Corporativos (DGP - https://team.amer.mymetlife.com/Teams/bdcsm/SitePages/Enterprise_Data_Governance_Portal.aspx)

Destrucción de Información y documentación

El proceso de destrucción de la información de la Compañía es tan importante como la correcta clasificación de la misma. Desde el momento en que todos los esfuerzos son canalizados a proteger nuestra información de accesos o divulgaciones no autorizados, en el mismo sentido debemos prestar la máxima atención para establecer mecanismos que nos permitan destruir la información de manera segura, previniendo posibles accesos no deseados. Para ello será necesario tener en consideración los siguientes tópicos:

:

a) Información en Papel / Carpetas / Legajos / Expedientes

- Toda la información deberá ser destruida al final de su ciclo de vida, contemplando los plazos legales de la misma y cumpliendo con los lineamientos del "Record Information Management" (RIM) disponible en la base de Normas y Procedimientos. (https://app.mymetlife.com/sites/CST4001/normas/SitePages/Home.aspx) Cualquier consulta asociada al ciclo de vida por tipo de documento deberá ser canalizada a través de la Dirección de Legales.

  Adicionalmente, se puede consultar en la intranet de MetLife la polítical global sobre retención de documentación (ILM – Informatio Lifecycle Management) en : https://my.metlife.com/en/us/tools/ILM (versión vigente en Inglés)

- Los reportes y/o documentos clasificados con niveles de seguridad Medios o Críticos que vayan a ser destruidos, no deben ser dejados por ningún motivo sobre el piso,

escritorios, pasillos, escaleras, ni en dispositivos de basura. Todos estos materiales deberán ser destruidos inmediatamente o depositados en los contenedores de destrucción de información provistos por la Compañía (sistema Shred-it). En caso de no existir este servicio (como por ejemplo en las Agencias) se procederá, bajo la supervisión del responsable del área o de la Agencia, a la destrucción manual de dicha documentación de tal manera que no sea posible volver a reconstruir la documentación ya destruida.

- En caso de no poder realizar la destrucción de la información de manera inmediata, todo reporte o documento pendiente de destrucción deberá ser protegido hasta el momento de efectivizar la misma. Dicho proceso deberá realizarse tan pronto como sea posible.
- Si bien la responsabilidad final por el correcto cumplimiento de estos procedimientos es de los Responsables de cada área, todos los Empleados de la Compañía y personal contratado son responsables por la información que la Compañía administra.

Transferencia de Datos fuera de la red de MetLife (a terceros habilitados por contrato)

La transferencia de datos personales (no críticos) se realiza por medios seguros de protección de la información tales como; “Safe File Transfer Protocol” (SFTP) a través de usuarios habilitados por el área de Seguridad de IT y según requerimiento remitido al Help Desk previamente autorizado. (Por ej: información remitida por Sponsors).

Los arhivos remitidos por mail fuera de la red de MetLife a terceros deben sere al menos encriptados, no calificados como críticos (Procedimiento “política de privacidad y resguardo de la información” publicado en Intranet) y la clave remitida por mail separado.

No se pueden remitir datos fuera de MetLife que no cuenten con estas medidas de protección.

Importante: La regulación local no establece la obligación de proteger la información remitidas por medios electrónicos con herramientas tecnológicas como “Envío seguro”

Cuando se requiera el envío de información peronal a través del correo electrónico dirigida a una dirección externa a MetLife, los empleados deberán tipear en el “Asunto” del mail alguna de las siguientes opciones:

- {Seguro}
- {Mensaje seguro de MetLife}
- {Encriptado}

O asegurar que la documentación adjunta o información contenida en el mail es encriptada antes de ser trasmitida.

IV. PROCESAMIENTO DE DATOS PARA TERCEROS

Aspectos regularorios

✓ Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.

- ✓ Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.

Procedimiento

A) Aspectos legales

El proceso de emisión y renovación de contratos se encuentra centralizado en el área Legal de Argentina. Corresponde al área legal, en función de esta adenda y del procedimientos de contratación vigente, incluir en los contratos las cláusulas e indeminidades correspondientes a efectos del cumplimiento regulatorio y de las cláusulas sugeridas en la Políticga Global de Privacidad disponible en la base de Normas y Procedimientos. (https://app.mymetlife.com/sites/CST4001/normas/SitePages/Home.aspx

La versión aprobada del "Compromiso de Confidencialidad de la Información – 2017" se encunetra transcirpto como ANEXO III de la presente Adenda.

B) Aspectos de evaluación de seguridad del tercero.

Dentro de la Política Global de Privacidad deben seguirse los siguientes pasos:

Para evaluar el riesgo de privacidad de terceros, se debe llevar a cabo el Proceso de Tres Pasos. Por cada nueva contratación de un tercero y por cada contrato existente que se renueve, los empleados de la línea de negocios o área funcional que busquen contratar al tercero deberán realizar el análisis de tres pasos en virtud de la Política Global de Privacidad, antes de celebrar o renovar el contrato.

a) Realizar una pre-evaluación de riesgo
   i. Para terceros que requieren el cuestionario de Evaluación de Riesgos de Productos-Servicios y de Proveedores (PSRA) en virtud de la Política Global de Compras y Procedimientos, los empleados deberán asegurarse que todas las preguntas de la pre-evaluación de riesgo sean contestadas al completar el PSRA.
   ii. Para contratos que no requieran el cuestionario de Evaluación de Riesgos de Productos-Servicios y de Proveedores (PSRA), o que no están incluidos en los procesos de Compras Globales, los empleados deberán documentar su pre-evaluación de riesgos utilizando el Check-list de Riesgos de Privacidad para Terceros, (Apéndice A de la Política Global de Privacidad). Anexo 1; Seccion 2 (para una documentación eficiente y mejor control, el Apendice A de la Política Global de Privacidad ha sido agregado al Check List Anticorrupción como sección 2 para que ambas evaluaciones sean realizadas(por la línea de negocios) al momento de presentación del acuerdo al área legal. **(ANEXO I de la presente adenda)**

b) Realizar la debida diligencia a través de la Evaluación de Riesgos de Seguridad TI para terceros (Proceso MORE)
   i. Para las contrataciones realizadas sin la intervención del área de Compras (definidas como no procurables en la Política de Compras), el área de negocios debe requerir la evaluación MORE del proveedor dirigiendo un email al área de Riesgos de Tecnología de la Información la siguiente dirección ARS_MOREs@metlife.com.

c) Trabajar con el área Legal para asegurar que disposiciones de privacidad sean incorporadas en los contratos con terceros.

El procesamiento de datos de terceros establecido en la Política Global de Privacidad de MetLife debe ser respetado por todos los colaboradores.

V. TRANSFERENCIAS TRANSFRONTERIZAS DE DATOS

Aspectos regularorios

a) Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.

b) La prohibición no regirá en los siguientes supuestos:

- ✓ Colaboración judicial internacional;
- ✓ Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica aplicando procedimientos de disociasión de la información.
- ✓ Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;
- ✓ Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Oriental del Uruguaysea parte;
- ✓ Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

Procedimiento

La transferencia de datos fuera del país para su tratamiento dentro de los procesos de gestión del negocio o por aspectos regulatorios (por ejemplo: cruce con listas antiterroristas, administración de recursos humanos), deberá estar respaldada por la firma de un acuerdo escrito donde queden resguardados los datos personales suministrados, el fin para el que van a ser utilizados y el cumplimiento de las regulaciones locales referidas a la materia.

Corresponde al área legal, dentro del proceso de evalución del acuerdo, evaluar la necesitad de la firma de un acuerdo de transferencia de datos a terceros conocido como (DTA – Data Transfer Agreement) siguiendo el modelo aprobado y validado por el regulador.

Corresponde al área legal, asegurar que los mecanismos de transferencia son adecuados y cumplen con los requisitos y restricciones locales y corporativas.
Todos los empleados están obligados a recurrir al área legal ante la necesidad de transferencia de datos fuera de las fronteras del país. El área legal evaluará la necesidad de firmar un acuerdo de transferencia (DTA) según el modelo homologado por el regulador.

La firma y guarda de los acuerdos mencionados es responsabilidad de la **Dirección de Legales**, siendo supervisado el cumplimiento por la **Gerencia de Ethics & Compliance**.

En todos aquellos casos mencionados y en cumplimiento del punto 2.1 del presente procedimiento, se incluirá la notificación mencionada más abajo donde el Cliente otorga su consentimiento para uso de datos personales y su transferencia al exterior.

CONSENTIMIENTO PARA USO DE DATOS PERSONALES: *MetLife Seguros S.A. ("MetLife") recaba y trata sus Datos Personales con el único fin de administrar su seguro. MetLife podrá transferir internacionalmente sus Datos Personales a sus afiliadas, con la finalidad de que procesen los datos por cuenta y orden de MetLife. En todos los casos MetLife adoptará las medidas contractuales para proteger la integridad y seguridad de los datos, y evitar su alteración, pérdida, acceso y/o tratamiento no autorizado por terceros. El responsable de la base de datos es MetLife Seguros S.A., domiciliada en Yaguarón 1407, piso 4, of. 401, Montevideo. Usted podrá ejercer sus derechos legales de acceso, rectificación, actualización, inclusión o supresión de sus Datos Personales, mediante una comunicación escrita a nuestras oficinas. Dicho derecho podrá ser ejercido en forma gratuita a intervalos de seis meses, salvo que se hubiere suscitado nuevamente un interés legítimo de acuerdo con el ordenamiento jurídico. Por el presente presto mi consentimiento previo, libre, expreso e informado para el referido tratamiento y transferencia de los Datos Personales que proporciono a MetLife en esta solicitud y en el futuro con las finalidades descriptas.*

VI. ADMINISTRACIÓN DE INCIDENTES DE DATOS PERSONALES

Aspectos regularorios

Los incidentes o la fuga de datos personales no se encuentra explícitamente definida en la regulación local. El responsable de la base de datos debe adoptar las medidas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado

Procedimiento Interno.

Un Incidente de Datos Personales ocurre cuando información personal ha sido o existe la posibilidad que sea trasmitida o puesta a disponición de alguien que no debería tener acceso a la misma.

El procedimiento de identificación del incidente y los pasos a seguir se encuentran descriptios en el procedimiento **"Manejo del Incidente de Datos Personales"** a efectos de responder apropiadamente. (https://app.mymetlife.com/sites/CST4001/normas/SitePages/Home.aspx) publicado dentro de a carpeta de PRIVACIDAD.

Alcance.

El procedimiento alcanza a todos los empleados de MetLife quienes son responsables de reportar (según lo definido en el mismo) todos los "incidentes de datos personales" sonbre los que tomen conocimiento. Es muy importante que todos los potenciales IDP sean reportados, independientemente de la cantidad de individuos afectados, incluso cuando la regulación local no lo exija, de forma oportuna para disminuir los riesgos de los individuos afectados y de MetLife.

Según se describe en el procedimiento se deben seguir los siguientes pasos:

Paso 1
Reportarlo al responsable local de Etica y Cumplimiento

Paso 2
Identificar los datos personales sujetos al incidente e investigar las causas y el alcance

Paso 3

A partir de la investigación, definir si se trata de un incidente de fuga de datos o solo un incidente que involucra o puede involucrar datos personales pero no su conocimiento a terceros.

Paso 4
Evaluar con la Dirección Legal el incidente y si el mismo debe ser reportado a terceros.

Paso 5
Notificarlo al "MetLife Corporate Privacy Office" si se cumplen con los supuestos definidos en el procedimiento publicado.

Paso 6
Mantener toda la documentación y datos referidos a la investigación realizad según se establece en la Política Incidentes de Datos Personales según se describe a continuación.

Paso 7
Registrar el casos en la bitácora "Registro de incidentes de seguridad" adjunta al procedimiento vigente.

Al respecto, la Disposición 10/2006 (Ver Punto I del presente) define y requiere un responsable de la seguridad de las bases de datos autorizadas, en nuestro caso el Gerente de Riesgos de Tecnología de la Información. Para todos los niveles de seguridad (Bajo, Medio, Crítico) definidos en el Manual de Seguridad de MetLife, debe llevarse un registro de "Incidentes de Seguridad"

Dando soporte al "Responsable de Seguridad" designado, dentro del registro de Incidentes de Datos Personales llevado por Ethics & Compliance, se indentifican aquellos referidos a incidentes de seguridad, siguiendo el proceso de notificación, gestión y respuesta definido dentro de la Política de Incidentes de Datos Personales.

El área de Ethics & Compliance será responsable de mantener el mencionado "Registro de incidentes de seguridad" a efectos de ser reportado a la Oficina Corporativa de Privacidad o a la Dirección Nacional de Protección de Datos Personales (el regulador) si es requerido.

El área legal como parte del "paso 4" evaluará la necesidad de reportar el incidente al regulador (DNPDP)

Documentación del proceso de investigación

El proceso de investigación del incidente o de la fuga de datos personales será conducido dentro del protocolo de investigación seguido por Etica y Cumplimiento, identificando según los estándadares de Auditoría Intera:

- ✓ Origen del incidente
- ✓ Universo y personal afectado pudiendo ser caratulado como fraude de ser necesario y dando intervención a Recusrsos Humanos.
- ✓ Impacto
- ✓ Posibles consecuencias legales
- ✓ Conclusión y definición de los planes de acción necesarios.
- ✓ Identificar si corresponde a un Incidente de Seguridad (Disposición 10/2006)

VII. EVALUACIÓN DEL IMPACTO

La normativa local no exige evaluación del impacto de los nuevos proyectos sobre las reglas de privacidad en el manejo de información personal o sensible.

VIII. CAPACITACIÓN

La Oficina de Privacidad Corporativa de MetLife es responsable de desarrollar y brindar capacitación sobre esta Política a los empleados de MetLife. Se requiere un curso de capacitación en línea sobre privacidad para todos los empleados de MetLife, al menos cada dos años. Los nuevos empleados deberán completar un curso de capacitación en línea sobre privacidad dentro de los treinta (30) días posteriores a la contratación. La Oficina de Privacidad Corporativa de MetLife proporcionará de manera periódica materiales de capacitación adicionales que pueden ser utilizados a discreción de la operación local para brindar capacitación sobre esta Política. Cualquier desviación significativa o alteración al contenido de cualquier material de capacitación sobre esta Política deberá ser aprobada por la Oficina de Privacidad Corporativa de MetLife.

El departamento de Cumplimiento Local, en colaboración con la Dirección de negocio, deberá proporcionar capacitación específica a los empleados cuyos deberes y responsabilidades laborales presentan un mayor riesgo de privacidad (por ejemplo, los empleados que frecuentemente manejan información personal de MetLife). Si bien la frecuencia y el enfoque de la capacitación especializada se establecerán según lo determine el departamento de Cumplimiento Local, la capacitación especializada deberá abocarse a las leyes y regulaciones aplicables, así como a las políticas y procedimientos locales aplicables. El departamento de Cumplimiento Local deberá mantener registros de todas las actividades de capacitación que se han realizado a nivel local, incluyendo el tema o categoría de capacitación, el público objetivo y el porcentaje del público objetivo realmente capacitado. La Dirección de negocio es responsable de garantizar que los empleados cumplan con todos los requisitos de capacitación

Funciones	Responsabilidades
Todos los empleados	Completar todas las actividades obligatorias de capacitación de privacidad.
Operaciones comerciales y funciones globales	Asegurarse de que todos los empleados completen las actividades de capacitación requeridas en privacidad. En colaboración con el departamento de Cumplimiento, identificar las necesidades de capacitación y brindar la capacitación en privacidad a los empleados seleccionados.
Cumplimiento Local	Obtener la aprobación de la Oficina de Privacidad Corporativa de MetLife con respecto a cualquier desviación/modificación significativa a fin de planificar materiales de capacitación de acuerdo con esta Política. En colaboración con la Dirección de negocio, identificar las necesidades de capacitación y brindar la capacitación de privacidad a los empleados seleccionados. Mantener un registro de todas las capacitaciones realizadas a nivel local.

IX. FUSIONES Y ADQUISICIONES

En caso de existir alguna adquisición o venta de negocios, el departamento Legal en conjunto con Cumplimiento local y el Gerente de Privacidad definirán el alcance de la debida diligencia en materia de privacidad.

ANEXO I

Políticas de Anticorrupción y Privacidad

Riesgos Anticorrupción y Privacidad

Lineamientos para la contratación de terceros

Instrucciones: Para cada **nuevo contrato** con terceros o para cualquier contrato con terceros que deba **ser renovado**, este **CHECK LIST** debe ser usado para la evaluación del Riesgo asociado con el tercero por **Anti-Corrupción (Sección 1) y de Privacidad (Sección 2**).

Ambas secciones deben ser completadas en su totalidad, firmadas y fechadas por el responsable del área contratante.

Sección 1: Anti - Corrupción

Perspectiva general

Los Terceros, incluyendo empresas conjuntas u otros socios comerciales, intermediarios, agentes, corredores o consultores que actúen en representación o en nombre de MetLife, tienen estrictamente prohibido participar en Sobornos u otras actividades corruptas. Cualquier Tercero que actúe indebidamente en nombre de MetLife podría exponer a la Compañía y a sus Asociados a responsabilidad penal. Por lo tanto, esta política establece requisitos y procedimientos especiales para evaluar y mitigar el riesgo potencial que el Tercero representa para MetLife.

El siguiente proceso que consta de cuatro pasos deberá ser completado y enviado al departamento correspondiente para su revisión y aprobación definitiva antes de la celebración de cualquier acuerdo nuevo o su renovación. Este proceso no se aplica a las declaraciones individuales de trabajo u órdenes de compra incluidas en los acuerdos marco que se sometieron a este proceso y que contienen los términos apropiados en contra de la corrupción. Este proceso tampoco se aplica a los contratos de seguros de MetLife celebrados directamente con los clientes.

Cualquier desviación de los requisitos establecidos en estos lineamientos deberá ser revisada y aprobada por la Unidad Global de Lucha en contra de la Corrupción. Se deberá consultar a la Unidad Global de Lucha en contra de la Corrupción si existe alguna duda en cuanto a la aplicación de estos lineamientos con respecto a algún acuerdo, contrato u orden de compra.

Este proceso de contratación, incluyendo los resultados de la diligencia debida, deberá documentarse y conservarse de manera imparcial y precisa durante al menos (7) siete años a partir de la terminación de la relación contractual con el Tercero.

PASO 1: IDENTIFICAR LA JUSTIFICACIÓN DEL NEGOCIO PARA LA CONTRATACIÓN

Por cada contrato o acuerdo nuevo u orden de compra nueva o renovación de los mismos, explique la justificación que tiene el negocio para celebrar esta Contratación y la capacidad que tiene el Tercero para satisfacer la necesidad de la empresa.

¿Existe alguna justificación comercial legítima para celebrar esta relación contractual? En caso afirmativo, indique los detalles a continuación. En caso negativo, no continúe con esta contratación.

¿El Tercero tiene la experiencia necesaria para satisfacer la necesidad de la empresa? En caso afirmativo, indique los detalles a continuación. En caso negativo, no continúe con esta contratación.

PASO 2: EVALUAR EL RIESGO DE LA CONTRATACIÓN

A cada Contratación propuesta se le debe asignar una categoría de riesgo de Soborno (alto, moderado o bajo) como se clasifica a continuación. En caso de duda sobre el nivel de riesgo asociado a un contrato propuesto, consulte con la Unidad Global de Lucha en contra de la Corrupción para recibir orientación.

Con base en la tabla de evaluación de riesgos que se encuentra en las páginas siguientes, ¿cuál es el nivel de riesgo para esta Contratación? *Marque la casilla aplicable.*

□ Bajo □ Moderado □ Alto

Atención: todos los acuerdos u órdenes de compra de alto riesgo deberán ser reportados a la Unidad Global de Lucha en contra de la Corrupción para una revisión y aprobación exhaustivas antes de contratar al Tercero. El departamento de Cumplimiento Local, con la colaboración de la línea de negocio o área funcional que pretenda contratar al Tercero, deberán completar la hoja de trabajo para el reporte de la contratación de alto riesgo de la lucha en contra del Soborno y la Corrupción (“ABC”) que se encuentra en el **Apéndice E** con base en la información de la diligencia debida que proporcionó la línea de negocio o área funcional y deberán enviar el formulario a la Unidad Global de Lucha en contra de la Corrupción.

Evaluación del Riesgo	Puntaje IPC* ≤ 45	Puntaje IPC* > 45
Alto	**Se han detectado una o más de las señales de advertencia de corrupción que se encuentran en el Apéndice C.** **O** **El acuerdo corresponde a uno de los siguientes tipos que se presentan a continuación:** 1. Acuerdo de empresas conjuntas 2. Contrato relacionado con la adquisición de licencias o registros 3. Acuerdo con funcionarios del gobierno, miembros de su familia o entidades del gobierno 4. Acuerdo relativo a la distribución o venta de productos o servicios de MetLife a entidades del gobierno o entidades no gubernamentales 5. Contrato con Terceros que son intermediarios y que interactuarán con la entidad del gobierno o entidad no gubernamental en nombre de MetLife 6. Cualquier acuerdo con corredores nuevos o existentes por servicios distintos a los servicios de ventas **7.** Contratos de pagos relacionados con un grupo de clientes por servicios (incluyendo el acceso a las instalaciones del cliente para fines de ventas) **Todas las contrataciones de alto riesgo requieren la aprobación previa de la Unidad Global de Lucha en contra de la Corrupción.**	**Se han detectado una o más de las señales de advertencia de corrupción que se encuentran en el Apéndice C.** **O** **El acuerdo corresponde a uno de los siguientes tipos que se presentan a continuación:** 1. Acuerdo de empresas conjuntas 2. Contrato relacionado con la adquisición de licencias o registros 3. Acuerdo con funcionarios del gobierno, miembros de su familia o entidades del gobierno 4. Acuerdo relativo a la distribución o venta de productos o servicios de MetLife a entidades del gobierno 5. Contrato con Terceros que son intermediarios y que interactuarán con la entidad del gobierno en nombre de MetLife 6. Cualquier acuerdo con corredores nuevos o existentes por servicios distintos a los servicios de ventas **Todas las contrataciones de alto riesgo requieren la aprobación previa de la Unidad Global de Lucha en contra de la Corrupción.**
Moderado	**El acuerdo es del siguiente tipo:** 1. Acuerdo para el desarrollo del negocio de MetLife (planificación de estrategias, consultorías o estudios de mercado)	**El acuerdo corresponde a uno de los siguientes tipos que se presentan a continuación:** 1. Acuerdo para el desarrollo del negocio de MetLife (planificación de estrategias, consultorías o estudios de mercado) 2. Acuerdo relativo a la distribución o venta de productos o servicios de MetLife a entidades no gubernamentales 3. Contrato con Terceros que interactuarán con la entidad no gubernamental en nombre de MetLife 4. Contratos de pagos relacionados con un grupo de clientes por servicios (incluyendo el acceso a las instalaciones del cliente para fines de ventas)
Bajo	**El acuerdo corresponde a uno de los siguientes tipos que se presentan a continuación:** 1. Acuerdo relativo a la distribución o venta de productos o servicios de MetLife a individuos por compensación estándar con base en las tarifas del mercado local 2. Contrato relacionado con compras a un proveedor privado sin conexiones gubernamentales conocidas y con el que MetLife ha tenido una relación de 3 años, como mínimo.	

* El **IPC** es el Índice de Percepción de la Corrupción establecido por Transparencia Internacional (“CPI”, por sus siglas en inglés) (http://cpi.transparency.org)

MATRIZ DE RIESGOS PARA CONTRATOS DE INVERSIÓN

Evaluación del Riesgo	
Alto	**Se han detectado una o más de las señales de advertencia de corrupción que se encuentran en el Apéndice C.** **O** **El acuerdo corresponde a uno de los siguientes tipos que se presentan a continuación:** 1. Acuerdos de desarrollo inmobiliario/gestión de proyectos para propiedades fuera de Estados Unidos 2. Acuerdos de desarrollo inmobiliario/empresas conjuntas para propiedades fuera de Estados Unidos 3. Acuerdos con asesores profesionales para proporcionar análisis financiero y otros servicios de inversiones relacionados que estén vinculados con inversiones extranjeras en las que estén involucrados funcionarios del gobierno o empresas patrocinadas por el gobierno 4. Acuerdos con agentes de colocación de terceros para la solicitud de clientes fuera de Estados Unidos para servicios de gestión de inversiones **Todas las contrataciones de alto riesgo requieren la aprobación previa de la Unidad Global de Lucha en contra de la Corrupción.**
Moderado	**El acuerdo corresponde a uno de los siguientes tipos que se presentan a continuación:** 1. Acuerdos de desarrollo inmobiliario/gestión de proyectos para propiedades estadounidenses 2. Acuerdos de desarrollo inmobiliario/empresas conjuntas para propiedades estadounidenses 3. Acuerdos con asesores profesionales para proporcionar análisis financiero y otros servicios de inversiones relacionados que estén vinculados con inversiones extranjeras en las que no estén involucrados funcionarios del gobierno o empresas patrocinadas por el gobierno 4. Acuerdos con agentes de colocación de terceros para la solicitud de clientes estadounidenses para servicios de gestión de inversiones
Bajo	**El acuerdo corresponde a uno de los siguientes tipos que se presentan a continuación:** 1. Acuerdos para que los terceros administren los activos de MetLife 2. Acuerdos concernientes a la gestión o arrendamiento de propiedades de MetLife 3. Acuerdos con asesores profesionales para proporcionar análisis financiero y otros servicios de inversiones relacionados que estén vinculados con inversiones estadounidenses 4. Acuerdos de servicios de corretaje

PASO 3: REALIZAR LA DILIGENCIA DEBIDA EN EL TERCERO

Después de que MetLife haya definido el objetivo comercial de la relación y haya determinado el nivel de riesgo que el Tercero representa, iniciará el proceso principal de diligencia debida. El proceso de diligencia debida para los Terceros clasificados como de riesgo bajo, moderado o alto se define en las siguientes tablas.

Una vez que se haya llevado a cabo el reporte, la Unidad Global de Lucha en contra de la Corrupción determinará los pasos para llevar a cabo la diligencia debida reforzada para las Contrataciones de alto riesgo que podrían incluir que el Tercero complete un cuestionario. La Unidad Global de Lucha en contra de la Corrupción también podría requerir que el Tercero revise y complete la declaración de políticas contra la corrupción para terceros y formulario de certificación (**Apéndice J**).

La línea de negocio o área funcional que pretende contratar al Tercero deberá mantener registros detallados y documentar cada paso de la investigación de diligencia debida. Toda la información obtenida acerca del Tercero y todos los esfuerzos para obtener dicha información, deberán registrarse en un archivo de diligencia debida.

El registro de diligencia debida deberá incluir análisis sobre las razones por las que el Tercero atrajo la atención de MetLife, una evaluación de su preparación y reputación y las razones por las que fue seleccionado. Si otros candidatos se consideraron, pero al final se rechazaron, el archivo de diligencia debida deberá reflejar los motivos del rechazo. El registro de diligencia debida también deberá incluir toda la documentación relacionada con la evaluación de riesgos y procesos de diligencia debida y la evaluación de las banderas rojas (señales de alarma).

La línea de negocio o área funcional deberá conservar el archivo de diligencia debida durante el tiempo que dure la relación con el Tercero y por lo menos siete (7) años adicionales a partir de entonces o de conformidad con la legislación local, optando por el periodo más largo.

Contratación de Terceros que representen riesgo bajo

Los Asociados deberán llevar a cabo la diligencia debida estándar cuando se trate de una Contratación de Terceros que representen riesgo bajo. La diligencia debida estándar requiere búsquedas básicas en internet, bases de datos y en medios de comunicación. Los resultados de la ejecución de la diligencia debida pueden evidenciar una elevación del riesgo (por ejemplo: la re-categorización de bajo a alto riesgo si se identifican noticias negativas o banderas rojas de corrupción).

Contratación de Terceros que representen riesgo moderado a alto

Los Asociados deberán llevar a cabo la diligencia debida reforzada cuando se trate de una Contratación de Terceros que representen riesgo moderado a alto. Los resultados de la ejecución de la diligencia debida pueden evidenciar una elevación del riesgo (por ejemplo, la re-categorización de moderado a alto riesgo si se identifican noticias negativas o banderas rojas de corrupción). Los Terceros que representen un riesgo moderado o alto requieren, como mínimo, que se lleve a cabo la siguiente diligencia debida reforzada:

□	Obtener una lista de referencias, el currículum e historial de empleo del Tercero (o de los funcionarios principales si se trata de una corporación), así como el plan de trabajo propuesto, la descripción de la estrategia de ventas o alguna propuesta similar que describa detalladamente los servicios específicos que el Tercero proporcionará. Este paso no se aplica a corporaciones multinacionales o que cotizan en la bolsa de valores.
□	Ponerse en contacto con el mayor número de referencias y empleadores anteriores o clientes del Tercero, en cuanto sea razonablemente posible, y documentar sus comentarios.
□	Revisar las fuentes públicas de información (incluyendo los informes de prensa que se han publicado), realizar búsquedas en internet y, si es posible, consultar con otras personas de la jurisdicción sobre el Tercero, así como con sus directivos y miembros de alto nivel para asegurarse de que el Tercero tenga experiencia en el área, que esté bien informado, que posee el grado apropiado de honestidad, integridad y cualquier otro requisito esencial que justifique la contratación contemplada.
□	Evaluar la razonabilidad de la compensación que se proporcionará al Tercero de acuerdo con las funciones que este desempeñará, así como el valor justo del mercado de los servicios en el mercado en el que se realizarán las transacciones.
□	Verificar las identidades de cada uno de los altos directivos, directores, miembros de la junta directiva y accionistas del Tercero, así como cualquier otro individuo que actuará como contacto primario en virtud del acuerdo propuesto.
□	Solicitar una lista de cualquiera de los familiares de los altos directivos del Tercero (o de cualquier otro individuo que actuará como contacto primario o proveedor de servicios de MetLife en virtud del acuerdo) que son o que han sido empleados en alguna área del gobierno que tiene la capacidad para influir en el contenido del acuerdo.
□	En el caso de ciertas Contrataciones de alto riesgo, se podría considerar la contratación de los servicios de una empresa privada de investigación para llevar a cabo un examen completo de los antecedentes y/o llamar a la dependencia del país correspondiente en el Departamento de Estado de E.U.A., a la mesa de trabajo en el Departamento de Comercio de E.U.A. o al agregado comercial de la Embajada de E.U.A. en el país o países en los que el Tercero propuesto o sus directivos hacen negocios; asimismo, pregunte al oficial encargado si tiene conocimiento de alguna conducta indebida por parte del Tercero propuesto. Documente la respuesta o la carencia de ella.
□	Llevar a cabo una revisión interna de la diligencia debida para asegurarse de que ninguna de las señales de advertencia de corrupción estén presentes, según se establece en el **Apéndice C** de esta política.
□	En algunos casos, cuando se trate de Contrataciones de alto riesgo, la Unidad Global de Lucha en contra de la Corrupción también podría requerir que el Tercero y la línea de negocio completen los cuestionarios de diligencia debida (**Apéndices F** y **G**).

PASO 4: INCLUIR LAS CLÁUSULAS NECESARIAS EN CONTRA DE LA CORRUPCIÓN

Contratación de Terceros que representen riesgo moderado a alto

Las Contrataciones de riesgo moderado o alto deberán incluir la siguiente disposición en el acuerdo, contrato u orden de compra. Cualquier omisión o modificación a esta disposición requerirá la aprobación previa de la Unidad Global de Lucha en contra de la Corrupción. Siempre que sea posible, la disposición deberá incluir una referencia específica a la Ley de E.U.A. sobre Prácticas en contra de la Corrupción en el Extranjero ("FCPA") y a la Ley contra el Soborno del Reino Unido.

- Cumplimiento de las leyes en contra de la corrupción. El [Tercero], sus funcionarios, directores y empleados y cualquier persona por cuyos actos u omisiones puedan ser responsables indirectamente o cualquier persona que actúe en nombre de alguno de ellos, no ofrecerá ni realizará ningún pago ni ofrecerá ni proporcionará ningún objeto de valor a ninguna persona cuando esto infrinja cualquier ley aplicable en contra del soborno en relación con este Acuerdo o que de alguna manera se relacione con este Acuerdo o que afecte al mismo. El [Tercero] reconoce que las leyes internacionales en contra de la corrupción, incluyendo la Ley de E.U.A. sobre Prácticas en contra de la Corrupción en el Extranjero ("FCPA") y la Ley contra el Soborno del Reino Unido, prohíben cualquier ofrecimiento, pago o recepción de dinero de manera directa o indirecta o de cualquier objeto de valor de parte de/para cualquier persona (incluyendo, pero no limitado a cualquier Funcionario del Gobierno, organización internacional, partido político o candidato a un cargo político) con el fin de obtener, retener o dirigir negocios, asegurar alguna ventaja indebida en la conducción del negocio o inducir al ejercicio indebido de cualquier función pública o de negocio. El [Tercero] declara y garantiza que, en el desempeño de sus obligaciones en virtud de este Acuerdo, o de otro modo, en relación con este Acuerdo, no ha ofrecido o realizado ningún pago prohibido y está de acuerdo en que no ofrecerá o realizará ningún pago prohibido.

Contratación de Terceros que representen riesgo alto

Las contrataciones de riesgo alto también deberán incluir las siguientes disposiciones **obligatorias** en el acuerdo, contrato u orden de compra. Estas disposiciones son altamente recomendadas para Contrataciones de riesgo moderado. Cualquier omisión o modificación a estas disposiciones requerirá la aprobación previa de la Unidad Global de Lucha en contra de la Corrupción. Siempre que sea posible, la disposición deberá incluir una referencia específica a la Ley de E.U.A. sobre Prácticas en contra de la Corrupción en el Extranjero ("FCPA") y a la Ley contra el Soborno del Reino Unido.

- Terminación/Suspensión. MetLife no estará obligado en virtud del presente Acuerdo, a realizar alguna acción o dejar de tomar cualquier acción que considere que, de buena fe, pueda provocar la violación de cualquier ley aplicable. MetLife tendrá derecho a dar por terminado este Acuerdo o a suspender los pagos en virtud del presente Acuerdo en cualquier momento antes de la fecha de terminación, si MetLife considera, de buena fe y con base en información fidedigna, que la violación de la Ley de E.U.A. sobre Prácticas en contra de la Corrupción en el Extranjero ("FCPA"), de la Ley contra el Soborno del Reino Unido o de cualquier otra ley, norma o reglamento aplicable en contra de la corrupción se ha producido o es relativamente probable que ocurra por parte de o en nombre del [Tercero] o es atribuible al [Tercero]. En el caso de la terminación o suspensión en virtud de esta sección, MetLife no tendrá ninguna obligación de realizar ningún pago en virtud del presente Acuerdo, excepto por los servicios legales ya realizados y sólo si el pago por dichos servicios no viola ninguna ley. En caso de incumplimiento del presente Acuerdo, este será nulo desde el principio sin necesidad de ningún aviso de cancelación por escrito. Cualquier reclamación de pago por parte del [Tercero] en relación con cualquier transacción quedará rescindida y cancelada automáticamente.

.

- Cesión. El [Tercero] no cesará, total o parcialmente, ningún derecho, deber u obligación en virtud de este Acuerdo (incluyendo los pagos que se deban o que venzan en el futuro) a cualquier tercero, incluyendo cualquier subcontratista, sin la previa y expresa autorización por escrito de MetLife. La cesión estará supeditada a la realización de la diligencia debida en el tercero/subcontratista. A menos que MetLife acuerde lo contrario por escrito, los directores, funcionarios o empleados del [Tercero] llevarán a cabo todos los servicios prestados en virtud del presente Acuerdo.

- Divulgación. Cualquiera de las partes podrá, en cualquier momento y por cualquier motivo, revelar la existencia y los términos de este Acuerdo a cualquier persona si dicha parte determina que tiene una necesidad legítima de esta información, incluyendo cualquier gobierno u organismo gubernamental.

- Derechos de auditoría. Todos los servicios que el [Tercero] proporcione en virtud del presente Acuerdo, todas las facturas y solicitudes de reembolso de gastos presentadas a MetLife por el [Tercero], así como todos los pagos efectuados o beneficios otorgados a terceros por el [Tercero] en el transcurso de la ejecución de los servicios del [Tercero], en virtud del presente Acuerdo, están sujetos a auditoría por MetLife, a su total discreción, o por un tercero contratado por MetLife. El [Tercero] deberá cooperar plenamente en cualquier auditoría que pueda llevarse a cabo. Tras la notificación de alguna auditoría prevista, el [Tercero] deberá, dentro de un plazo de [ ] días, poner a disposición de MetLife o de un tercero contratado por MetLife todas las facturas, recibos de respaldo y comprobantes, así como los registros de entrada originales para todos los cargos facturados a MetLife y, a petición de MetLife, todas las personas bajo el control del [Tercero] que realicen los servicios o que incurran en los gastos o que de otro modo tengan conocimiento de estos servicios o gastos deberán estar disponibles para ser entrevistadas. El [Tercero] deberá conservar libros y registros que describan con precisión y detalle todos los servicios y los gastos para los que el [Tercero] solicita el reembolso por parte de MetLife.

Asimismo, se **recomienda encarecidamente** que las contrataciones de Alto riesgo incluyan las siguientes disposiciones. Siempre que sea posible, la disposición deberá incluir una referencia específica a la Ley de E.U.A. sobre Prácticas en contra de la Corrupción en el Extranjero ("FCPA") y a la Ley contra el Soborno del Reino Unido.

- Certificaciones de cumplimiento de las medidas en contra de la corrupción. El [Tercero] se compromete a proporcionar las certificaciones de su cumplimiento con la sección [X][1] antes de cualquier pago en virtud de este Acuerdo y/o cada 12 meses, a discreción de MetLife.

- Cumplimiento con la política de MetLife en contra de la corrupción. El [Tercero] ha revisado la política global en contra de la corrupción de MetLife y las cláusulas para cumplir con dicha política.

- Indemnización. El [Tercero] indemnizará a MetLife por y en contra de todas las pérdidas, responsabilidades, daños, deficiencias, juicios, evaluaciones, multas, pagos, costos y gastos (incluyendo, pero no limitado a los gastos legales) que sufra MetLife o en los que incurra derivado de o en relación con cualquier violación a la Ley de E.U.A. sobre Prácticas en contra de la Corrupción en el Extranjero ("FCPA"), a la Ley contra el Soborno del Reino Unido o a cualquier otra ley o norma aplicable en contra de la corrupción en que incurra el [Tercero], sus Subsidiarias y Filiales, así como cualquier director, funcionario, agente, empleado u otra persona asociada con el [Tercero] o que actúe en nombre del [Tercero] o de cualquiera de sus Subsidiarias y Filiales.

- Pagos. El [Tercero] reconoce y acepta que MetLife no realizará pagos al [Tercero] en efectivo o con instrumentos al portador o en una cuenta que se encuentre en un país distinto de aquel en que se prestan los servicios y que no se harán pagos, directa o indirectamente, a través de cualquier fideicomiso, Entidad intermediaria u otro intermediario. El [Tercero] también acepta que los pagos serán coherentes con las tasas de mercado y en moneda de curso legal en el país en el que el [Tercero] reside o en donde se realizan los servicios.

[1] Haga referencia a la disposición de "cumplimiento con las leyes en contra del soborno".

- Afiliaciones del Gobierno. El [Tercero] declara y garantiza que ninguno de sus empleados, agentes, accionistas, ni ninguno de sus parientes cercanos (i) son Funcionarios del Gobierno o (ii) tienen negocios personales u otras conexiones, relaciones o asociaciones con cualquier Funcionario del Gobierno. El [Tercero] acuerda informar a MetLife en caso de que esta declaración deje de ser correcta en cualquier momento durante la vigencia de este Acuerdo.

- Informes Periódicos. El [Tercero] acuerda proporcionar informes detallados por escrito a MetLife sobre los servicios prestados en virtud del presente Acuerdo, de acuerdo con lo solicitado por MetLife periódicamente.

.
-

CoComentarios:

Terceros que representan riesgo bajo: (1) el jefe de la línea de negocio/área funcional que busque establecer relaciones comerciales con el Tercero deberá revisar estos lineamientos y firmar la siguiente declaración o (2) el departamento de Cumplimiento Local puede revisar mensualmente todos los acuerdos de riesgo bajo y órdenes de compra para asegurar el cumplimiento con las evaluaciones del nivel de riesgo del Tercero.

Terceros que representan riesgo moderado: el jefe de la línea de negocio/área funcional que busque establecer relaciones comerciales con el Tercero deberá revisar estos lineamientos y firmar la siguiente declaración.

Terceros que representan riesgo alto: el jefe de la línea de negocio/área funcional que busque establecer relaciones comerciales con el Tercero deberá revisar estos lineamientos, obtener la aprobación de la Unidad Global de Lucha en contra de la Corrupción y firmar la siguiente declaración.

Sección 2: Privacidad

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.

Pregunta 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?	□ Sí □ No
Pregunta 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?	□ Sí □ No
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	
(a) Contactar a la función de riesgo informático y seguridad en ARS_MOREs@metlife.com para realizar la diligencia debida en las protecciones de seguridad de la información de terceros y las prácticas de protección de datos.	□ *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) 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.	□ *Marque esta casilla para confirmar que el departamento Legal colaborará para incluir disposiciones sobre privacidad y protección de datos en el acuerdo.*
(c) ¿De qué país/países se generará la información personal?	
(d) ¿En qué país/países se visualizará, almacenará, procesará o accederá a la información personal? ***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.*	
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.*

CERTIFICACIÓN

Certifico que;

Con respecto a la Política Anticorrupción*; (i) realicé la evaluación de riesgos del tercero, (ii) lleve a cabo la diligencia debida mediante la recopilación y revisión de información relevante sobre el tercero, incluyendo estructura y titularidad, competencia y experiencia y estructura de compensaciones y comisiones,(iii) investigué exhaustivamente cualquier posible laguna o señal de alarma (banderas rojas) en la información recopilada*

(Anexo C de la Política) *y (iv) en caso necesario, incorporé las disposiciones en contra de la corrupción en el acuerdo, contrato u orden de compra*

Con respecto a la Política de Privacidad*, 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

ANEXO II

FORMULARIO DE CONSENTIMIENTO DE PROTECCIÓN DE DATOS DEL EMPLEADO

Estimado Empleado:

Durante el transcurso de su empleo con MetLife (en adelante "Compañía"), la compañía reúne, usa, archiva, transfiere o procesa (en adelante "Proceso") cierta información personalmente identificable sobre Ud. (en adelante "Datos Personales"). Estos Datos Personales incluyen: (1) información personal y familiar; como nombre, información de contacto (incluso domicilio particular, números de teléfono, etc.) fecha y lugar de nacimiento; seguro social u otras identificaciones, sexo, nacionalidad, idioma de comunicación, educación y otros antecedentes, estado civil; (2) información relacionada con su trabajo, como estado de su empleo, horas laborales, sueldo, información sobre compensación y gastos laborales, información sobre beneficios, otros términos de su empleo, desempeño laboral e información relacionada con evaluaciones, detalles de cualquier acción disciplinaria o investigación hecha por la compañía, detalles de pago de sueldo, información sobre salud y seguridad relacionadas con su rol laboral; (3) información proporcionada por Ud. sobre su familia u otras personas a cargo; y (4) información proporcionada por Ud. relacionada con sus deberes como empleado.

Propósitos

La compañía procesa datos personales con el objeto de: (1) cumplir con las obligaciones legales y regulatorias de la compañía, tales como las relacionadas con permisos de trabajo (si fuera necesario); pago de la nómina, ingresos, impuestos extranjeros y otros impuestos; cumplir con las obligaciones de salud y seguridad; proporcionar un ambiente de trabajo libre de discriminaciones ilícitas y cumplir con otra legislación de protección de empleo, y cumplir con requisitos inmigratorios; (2) mejorar y mantener una administración efectiva de los empleados y, en todo caso, cumplir con sus obligaciones contractuales, inclusive con la administración de personal, asignando el trabajo y los beneficios de los empleados, como por ejemplo sueldos, bonos, pensiones, beneficios de salud y derecho a licencias; (3) facilitar el rastreo de gastos y presupuesto; (4) rastrear asignaciones y determinar calificaciones para asignaciones específicas; (5) facilitar las revisiones de desempeño del empleado y las relacionadas con sueldos; (6) permitir a la compañía planear y monitorear requisitos de capacitación; (7) monitorear el cumplimiento de las políticas y códigos de práctica de la compañía; (8) mantener y mejorar los sistemas de seguridad; (9) mantener uno o más listados internos de empleados, incluyendo información sobre nombre, puesto/título y ubicación, información del contacto en el trabajo y líneas de reporte; (10) cumplir con los requisitos de informes gerenciales; y (11) ejercer los derechos de la compañía y cumplir con sus derechos como empleado según las leyes y reglamentaciones locales.

Acceso y Revisión

De cuando en cuando, la compañía puede pedirle revisar y actualizar sus Datos Personales. Usted puede acceder y actualizar sus Datos Personales más frecuentemente si lo desea y, en algunos casos, usted puede tener derecho a acceder a dichos datos según las leyes y reglamentaciones de aplicación. La Compañía le proporcionará una explicación escrita si, de acuerdo con las leyes y reglamentaciones de aplicación, este pedido se le negara.

Transferencia

Como la Compañía es parte de un grupo más grande de empresas que operan internacionalmente, puede transferir Datos Personales por los propósitos descriptos anteriormente a sus propias operaciones, o a otras subsidiaria o compañías afiliadas, ubicadas en Estados Unidos, Europa, Asia y otras jurisdicciones, donde las leyes y reglamentaciones de protección de datos pueden diferir de las de su jurisdicción. Además, la Compañía puede también transferir los Datos Personales a: (1) autoridades legales y regulatorias (inclusive de servicios de seguros y financieros, impositivos y de empleo); (2) asesores impositivos, auditores y otros asesores profesionales externos; y (3) terceros que proveen productos o servicios a la compañía, tales como proveedores de sistemas IT, médicos clínicos y compañías privadas de salud. Los empleados de la compañía y de las compañías subsidiarias o afiliadas así como terceros autorizados, pueden acceder a los Datos Personales del listado interno de empleados. Los Datos Personales también pueden revelarse o transferirse para responder a imposiciones legales o cuando lo requieran las leyes, reglamentaciones u órdenes de la corte, como lo relacionado con una reestructuración corporativa, venta o asignación de activos, fusión, despojo, u otros cambios de control o estado financiero

de la compañía o sus compañías subsidiarias o afiliadas. Éstos pueden estar ubicados en Estados Unidos, Europa, Asia y otras jurisdicciones, donde las leyes y reglamentaciones de protección de datos pueden diferir de las de su jurisdicción.

Seguridad

La compañía toma medidas razonables de seguridad técnica y organizacional para proteger los Datos Personales contra pérdida, mal uso, y acceso no autorizado, divulgación, alteración y destrucción. Sus Datos Personales se guardarán en lugares físicos seguros y/o servidores seguros ubicados en Argentina, Uruguay, Estados Unidos y/o cualquier otra jurisdicción donde sus Datos Personales puedan transferirse.

Información sobre Personas a Cargo

Si usted proporciona a la Compañía Datos Personales sobre miembros de su familia y/u otras personas a cargo, como por ejemplo, información sobre salud y otros beneficios que ellos puedan obtener debido a su empleo, es su responsabilidad obtener el consentimiento explícito de estos individuos (siempre que sean legalmente competentes para dar su consentimiento) para que la Compañía procese (incluyendo transferencia) los Datos Personales según lo establece este documento. Al firmar este Formulario de Consentimiento, usted confirma que ha obtenido ese consentimiento y, con respecto a cualquier individuo que no sea legalmente competente para dar su consentimiento, el consentimiento suyo en su nombre (y usted confirma que tiene autoridad para hacerlo).

Información del Contacto

Si, en algún momento, usted desea revocar su consentimiento, pedir acceso, copias, o enmendar sus Datos Personales, o formular alguna pregunta relacionada con este Formulario de Consentimiento o las políticas y prácticas de la Compañía, usted debe notificar a la Compañía poniéndose en contacto con su representante local de Recursos Humanos. Usted puede encontrar el nombre e información de contacto de su representante local de recursos humanos en la Intranet RH (http://mww.metlife.com.ar/rrhh/) en la Sección Institucional -> Organigrama.

Reconocimiento y Consentimiento

Por favor, note que usted no está obligado a firmar este Formulario de Consentimiento como una condición para su empleo. Sin embargo, de no hacerlo, esto podría interferir en su posibilidad, entre otras cosas, de determinar su elegibilidad para obtener beneficios

Mi firma al pie de este documento, implica mi reconocimiento de que he leído y entendido la información precedente, y en este acto ofrezco mi consentimiento explícito, dado libremente, y sin ambigüedades, para:

- **Procesar mis Datos Personales según se describe anteriormente; y**
- **Transferir mis Datos Personales (incluyendo datos de salud o cualquier otro dato confidencial) según lo descripto anteriormente, inclusive a aquellas jurisdicciones donde las leyes y reglamentaciones de protección de datos puedan diferir de las de mi jurisdicción.**

Desde el momento que he proporcionado (o voy a proporcionar) Datos Personales a la Compañía sobre mi familia y/u otras personas a cargo, también confirmo con mi firma al pie que he obtenido su consentimiento para procesar (e incluso transferir) esos Datos Personales de acuerdo con este Formulario de Consentimiento y, con respecto a cualquier individuo que no sea legalmente competente para dar su consentimiento, yo consiento en su nombre (y confirmo que tengo autoridad para ello).

_____	_____	_____
Firma del empleado	**Nombre del empleado**	**Fecha**

ANEXO III

Fecha: XX de XXXX de XXXX

MetLife Seguros S.A.
Presente

De nuestra consideración:

Hacemos referencia a la relación comercial con vuestras empresas y/o con cualquier otra sociedad afiliada del Grupo MetLife, ya sea actual y/o que se forme en el futuro, ya sea local o extranjera (denominadas indistintamente "MetLife" o las "Empresas").

Con motivo de la prestación de los Servicios hemos accedido y accederemos a cierta información de exclusiva propiedad de las Empresas, que pese a no estar en ocasiones calificada como tal, es secreta y confidencial. A los fines de esta carta se considerará información confidencial (en adelante, la "Información Confidencial") a toda información y datos, incluyendo pero no limitado a propiedad intelectual, secretos comerciales, información de/sobre los dependientes de las Empresas, información técnica, información sobre remuneración al personal, información sobre clientes y/o posibles clientes, datos personales, información en desarrollo, información operativa, información societaria, información contable, información impositiva, información de ventas, información de mercados, información de costos, información de procesos investigaciones, desarrollos, productos, servicios, conocimientos técnicos, pasados, presentes y futuros, información de *know how* y de negocios, técnicas de programación de computación, y cualquier sistema de registro de información que contenga o divulgue dichas informaciones o técnicas con relación al o que sea entregado en virtud y/o con motivo de los Servicios, que haya sido o sea suministrada ya sea en forma verbal, escrita o magnética.

Reconocemos que las Empresas han realizado inversiones para el desarrollo de la Información Confidencial y que ella posee valor estratégico y competitivo, por lo que nos hacemos responsables de mantener secreta la Información Confidencial aun luego de finalizada la relación comercial que nos une, utilizándola solamente para desarrollar las tareas para las cuales fuimos contratados. En este sentido, realizaremos un tratamiento adecuado a la información acorde a su criticidad, y tomaremos todas las medidas necesarias a tal fin, haciéndonos responsables por la actuación de nuestros empleados y de toda aquella persona que, aunque no esté en relación de dependencia, realice tareas o actividades encomendadas en nuestro nombre, e incluso cuando aquellos dejen de ser empleados o dejen de estar de cualquier forma vinculados con nuestra compañía. Asumimos el compromiso de administrar y acceder a la Información Confidencial en ambientes controlados, resguardando la misma en entornos encriptados, y otorgando permisos apropiados únicamente a los usuarios que requieren acceso a dicha información. Cualquier transmisión de información confidencial será realizada por medios seguros de conformidad con los estándares vigentes al momento de la transmisión.

Siempre que administremos y/o recolectemos datos personales en nuestros sistemas, o siempre que nuestros sistemas se conecten a los sistemas de las Empresas, entonces, periódicamente (pero al menos una vez por año), realizaremos una prueba de vulnerabilidad automatizada y manual realizada por un tercero acreditado (incluso prueba de penetración basada en las mejores prácticas reconocidas de la industria) en todos nuestros

sistemas, redes, software y dispositivos utilizados para acceder a dicha información. A este respecto, anualmente brindaremos evidencia de la realización de las pruebas a MetLife.

En supuestos de recopilar Información Confidencial directamente de personas, proporcionaremos un aviso de privacidad claro y evidente a dichas personas. El aviso describirá con exactitud la manera en que accedemos y protegemos dicha información y que cumplimos con las normas y estándares aplicables a dicha recolección.

En la medida en que accedamos o procesemos información de tarjetas de pago, incluidos números de cuenta principal (*primary account numbers* o "PAN") de conformidad con los Estándares de Seguridad de Datos del sector de tarjetas de pago (Payment Card Industry Data Security Standards o "PCI DSS") para la prestación de los Servicios, asegurará la certificación o conformidad actuales y demostrables con los PCI DSS, según lo documente un Informe de conformidad o un texto similar de un auditor externo independiente, y mantendremos el estado de conformidad siempre que accedamos o procesemos PAN en relación con los Servicios prestados a MetLife.

Asimismo, sólo divulgaremos la Información Confidencial sólo nuestros directores, empresas afiliadas, empleados y/o profesionales que tengan la necesidad de conocer la Información Confidencial en conexión con los Servicios, quienes serán informados de la naturaleza confidencial de la información.

Asumimos las obligaciones de contar con Políticas de Seguridad apropiadas, con un Plan de Contingencia Anual que garantice la seguridad de la información y la continuidad de los servicios que oportunamente se presten a MetLife, así también como la obligación de notificar a las Empresas de cualquier fuga de Información Confidencial dentro de los 3 (tres) días corridos de ocurrida la misma, y nos comprometemos en cooperar con las Empresas respecto de cualquier requerimiento y/o plan de acción en relación a dicha fuga.

Del mismo modo, y para el caso de que así nos lo soliciten, asumimos el compromiso de informar a las Empresas la identidad de cada persona a quién le será entregada la Información Confidencial, y a entregar a la brevedad y al solo requerimiento de las Empresas todo aquel documento o material que contenga la Información Confidencial y/o datos y/o parte de ellos, juntamente con todas las copias que hubieran hecho, y en caso de que así se solicite a destruir aquellos apuntes, anotaciones o cualquier otro material conteniendo o reflejando de alguna manera la Información Confidencial que se hubiera accedido. Al término de la relación comercial que nos une con las Empresas, procederemos a la devolución de toda información que se encuentre amparada por la Ley 25.326 de Protección de Datos Personales, y a entregar a las Empresas, en el plazo de 10 (diez) días hábiles, una certificación notarial de la destrucción de todo registro que contenga datos personales que hubieren sido obtenidos en virtud de nuestra relación con las Empresas.

Nos obligamos a dar cumplimiento a la Ley 25.326 de Protección de Datos Personales así como a sus normas complementarias y reglamentarias, manteniendo indemne a las Empresas como consecuencia de cualquier incumplimiento a dicha normativa en el que incurramos. Dicha indemnidad será aplicable tanto a acciones judiciales como a procesos administrativos, e incluirá las costas y honorarios de los abogados que las Empresas contraten para defenderse en dichas acciones.

Adicionalmente les confirmamos que entendemos que la Información Confidencial se encuentra protegida por la legislación local (Ley 24.766) e internacional y que la divulgación de la misma constituye delito penal en los términos del artículo 156 del Código Penal o en los términos del artículo 159 del mismo Código. En caso de incumplimiento con el presente compromiso de confidencialidad, vuestra parte podrá reclamar judicialmente la totalidad de los daños y perjuicios ocasionados. La responsabilidad por los daños ocasionados será integra y de ningún modo podrá estar alcanzada por limitación alguna, ya sea en cuanto a montos o en cuanto al tipo de daños alcanzados por la misma.

Declaramos que la obligación de confidencialidad establecida en la presente se mantendrá vigente aun en supuesto en el que la relación comercial con las Empresas termine por cualquier motivo, y cederá únicamente en caso que exista requerimiento fehaciente de alguna autoridad pública, administrativa y/o judicial que así lo exija. Sin perjuicio de ello, una vez finalice la relación comercial con MetLife, procederemos a la destrucción segura de la Información Confidencial, obligándonos a aportar a MetLife evidencia de ello en un plazo de 5 (cinco) días hábiles de realizada la destrucción.

La presente declaración constituye el completo entendimiento respecto de las materias contenidas en la presente y deja sin efecto a todos y cada uno de los acuerdos, representaciones y entendimientos entre las partes sobre las materias contenidas en la presente, sean éstos previos o contemporáneos al presente.

Sin otro particular, les saludamos muy atentamente,

Firma: _____

Por: _____

Aclaración: _____

Cargo: _____

Domicilio: _____

[NOTA: IMPRIMIR EN HOJA MEMBRETE Y DOBLE FAZ, ELIMINANDO DE FORMA PREVIA ESTA NOTA]