Política Global de Privacidad de MetLife

Modificado y Actualizado: *Marzo 2017*

MetLife

Índice

INTRODUCCIÓN: PRINCIPIOS GLOBALES DE PRIVACIDAD DE METLIFE

Los principios globales de privacidad de MetLife ("los Principios") establecen el marco de esta Política y son valores diseñados para inspirar a los empleados de MetLife en todo el mundo con el objetivo de lograr que actúen de manera consistente, ética y con el debido cuidado al trabajar con la información personal. Se alienta a los empleados de MetLife para que sigan estos Principios que se basan en requisitos legales y reglamentarios aplicables, o según se considere apropiado.

Principio 1: limitar la recopilación y el uso de información personal
Recopilar información personal de una manera ética y justa con el consentimiento individual cuando esto sea factible. Enfocarse únicamente en recopilar la información que es necesaria para realizar negocios, desarrollar y proporcionar productos o servicios, y cumplir con las disposiciones reglamentarias. ***Consulte* la Sección II: aviso, consentimiento y control.**

Principio 2: brindar transparencia en la recopilación y uso de información personal
Sea franco y transparente acerca de las políticas y procedimientos relacionados con la información personal. Proporcione notificaciones claras, concisas y de fácil lectura con el fin de informar a las personas, de manera razonable, acerca del propósito por el cual se recopila, utiliza, comparte y conserva la información personal. ***Consulte* la Sección II: aviso, consentimiento y control.**

Principio 3: proporcionar opciones sobre la información personal
Informar a las personas acerca de las opciones con las que cuentan para administrar su información personal y brindar oportunidades para que las personas tengan la opción de inclusión voluntaria, exclusión voluntaria o de registrarse en relación con la cláusula de no captación de clientes. ***Consulte* la Sección II: aviso, consentimiento y control.**

Principio 4: proporcionar acceso a la información personal y otros derechos de los dueños de la información
Proporcionar a los individuos la capacidad de ejercer los derechos como dueños de la información incluyendo la capacidad de acceder, revisar, corregir y/o borrar información personal. Permitir que los titulares de la información se comuniquen con la Compañía para tratar quejas y litigios relacionados con la privacidad y tomar medidas para garantizar que la información personal que resulte ser inexacta o incompleta se rectifique sin demora. ***Consulte* la Sección II: aviso, consentimiento y control.**

Principio 5: limitar la retención de información personal
Conservar la información personal únicamente durante el tiempo que sea necesario para cumplir con los objetivos comerciales o según lo requiera la ley o las normas reglamentarias. Se deberá eliminar la información personal de manera adecuada y segura después del uso que se le ha designado. ***Consulte* la Sección III: protección de la información.**

Principio 6: mantener salvaguardas de seguridad
Proteger la seguridad, confidencialidad e integridad de la información personal con medidas administrativas, técnicas y físicas de seguridad que sean apropiadas y que eviten pérdidas, accesos no autorizados o usos indebidos de la información personal. ***Consulte* la Sección III: protección de la información.**

Principio 7: limitar la información personal que se comparte con terceros
Compartir la información personal con terceros sólo cuando sea necesario divulgarla, únicamente para fines comerciales o cuando sea requerido por la ley o las normas reglamentarias. ***Consulte*** **la Sección IV: procesamiento de datos para terceros.**

Principio 8: mantener la responsabilidad
Continuar siendo responsable de supervisar y exigir el cumplimiento de esta Política y de las leyes y regulaciones de privacidad aplicables, así como proporcionar capacitación sobre privacidad con el fin de integrar una sólida cultura de concientización sobre la privacidad en toda la Compañía. ***Consulte*** **la Sección I: perspectiva general y la Sección VIII: capacitación.**

I. PERSPECTIVA GENERAL

A. DECLARACIÓN DE POLÍTICAS

Los clientes, **empleados**[1] y socios comerciales de todo el mundo proporcionan a **MetLife información personal** día tras día. Confían en MetLife (de aquí en adelante, "MetLife" o "la Compañía") para proteger y limitar el uso de esa información y para respetar su privacidad. MetLife tiene el compromiso de cumplir con estas expectativas al ser un administrador de confianza de la información personal que se proporciona a la Compañía. Existe un vínculo fundamental entre la protección de datos personales y la confianza del cliente. La pérdida de confianza del cliente causada por el uso indebido de la información personal o filtración de los datos personales puede dañar la reputación global de fiabilidad que posee MetLife y puede tener un impacto negativo en los ingresos. Dicho de manera sencilla, el tener buenas prácticas de privacidad no sólo es lo correcto, sino que también es bueno para los negocios.

La Política Global de Privacidad de MetLife ("Política") establece los principios a nivel de toda la empresa y los estándares mínimos globales diseñados para mitigar los riesgos de privacidad. En virtud de esta Política, se requiere que cada **operación** desarrolle y mantenga controles relacionados con la **recopilación**, uso y protección de la información personal con el fin de cumplir con esta Política y con cualquier ley o regulación local de privacidad que sea aplicable. Muchos países en los que MetLife lleva a cabo negocios han promulgado leyes y/o regulaciones sobre privacidad. Las operaciones de MetLife que **procesan** información personal inicialmente recopilada en otro país, pueden también estar obligadas a cumplir con las leyes y regulaciones del país en donde se recopiló dicha información. Asimismo, MetLife tiene muchos acuerdos contractuales que pueden imponer obligaciones a la Compañía para proteger ciertos grupos de datos, incluyendo la información personal. El incumplimiento de los requisitos legales aplicables puede dañar la reputación de MetLife y exponer a la Compañía a obligaciones legales y regulatorias, incluyendo multas y litigios.

Atención

Las excepciones a esta Política sólo pueden ser otorgadas por escrito por parte de la **Oficina de Privacidad Corporativa de MetLife.**

Esta Política no pretende responder a todas las preguntas relacionadas con la privacidad. Cualquier pregunta concerniente a esta Política debe dirigirse a la Oficina de Privacidad Corporativa de MetLife en askprivacy@metlife.com.

[1] Los términos que aparecen en negrita se definen en la **Sección X** de esta Política. Los términos definidos sólo aparecerán en negrita cuando se utilicen por primera vez.

¿QUÉ ES LA INFORMACIÓN PERSONAL?

Las leyes y regulaciones de privacidad de los países de todo el mundo tienen varias definiciones para información personal[2]. En la mayoría de los países y en virtud de esta Política, la información personal se define como aquella información que se conserva en formato electrónico o soporte físico y que sirve para identificar o por medio del cual se puede identificar[3] a una persona directa o indirectamente. Los ejemplos pueden incluir, pero no se limitan a:

- Identificación general e información de contacto (por ejemplo: nombre, dirección de correo electrónico, números de teléfono y dirección);
- Números de identificación emitidos por organismos o entidades gubernamentales (por ejemplo: número de identificación nacional y número de pasaporte);
- Información financiera y detalles de la cuenta (por ejemplo: números de tarjetas de crédito u otros números de tarjetas que se utilizan para realizar pagos y números de cuentas bancarias);
- **Información personal confidencial** (por ejemplo: información médica o relacionada con la salud, origen racial o étnico y opiniones políticas);
- Identificadores técnicos (por ejemplo: ID de usuario o nombre de usuario y contraseña, número de identificación del dispositivo y geolocalización); e
- Identificadores biométricos (por ejemplo: geometría facial, huella digital, escaneo de retina e información genética).

Todos los empleados de MetLife deben respetar la confidencialidad y manejar la información personal de conformidad con esta Política. Para los fines de esta Política, el término **información personal de MetLife** se utilizará para referirse a la información personal de los clientes de MetLife (incluyendo los grupos participantes), clientes potenciales, empleados, contratistas independientes, solicitantes de empleo, socios comerciales y otros **terceros**.

B. LEY APLICABLE

MetLife y sus empleados están sujetos a las leyes de privacidad de las jurisdicciones en las cuales la Compañía lleva a cabo negocios y deben cumplir con las mismas. Si las leyes o regulaciones de privacidad en un país en donde MetLife opera, establecen estándares que son más altos que los establecidos en virtud de esta Política o que están en conflicto con éstos, los empleados de ese país deberán seguir el estándar más estricto. Los empleados que busquen aclarar la coherencia de esta Política con cualquier ley o regulación de privacidad que sea aplicable deberán comunicarse con la Oficina de Privacidad Corporativa de MetLife (askprivacy@metlife.com), con el departamento de **Cumplimiento Local** y/o con el Departamento Legal.

Atención

Esta Política no es aplicable a la supervisión en el lugar de trabajo ni a la vigilancia electrónica de las actividades de los empleados de MetLife (por ejemplo: supervisión del uso del correo electrónico o del internet). Por favor, comuníquese con el departamento Legal y/o con el departamento de Relaciones Laborales si tiene preguntas sobre las leyes aplicables, regulaciones y políticas de la Compañía relacionadas con la privacidad en el lugar de trabajo.

[2] Para las definiciones de información personal específicas de cada país, consulte las políticas y procedimientos aplicables en cada país.

[3] A medida que madura la granularidad del análisis de datos también aumenta la posibilidad de identificar a individuos a partir de los datos relacionados con éstos, sin utilizar identificadores específicos.

C. ¿A QUIÉN SE APLICA ESTA POLÍTICA?

Esta Política se aplica a todas las compañías, sucursales, filiales, empresas conjuntas e inversiones de capital privado de MetLife en las que MetLife tiene el control de la administración. Cuando MetLife no tiene el control de la administración, la Compañía deberá realizar esfuerzos de buena fe para lograr que se adopten, implementen y apliquen las políticas de privacidad adecuadas, en la medida de lo posible.

Esta Política se aplica a todos los empleados, funcionarios, directores (conjuntamente llamados "empleados") y contratistas independientes que actúan en nombre de MetLife en cualquier parte del mundo. El incumplimiento puede resultar en el deterioro de la confianza del cliente, daño a la reputación de la Compañía, investigaciones regulatorias y sanciones (incluyendo multas), litigios y sanciones penales. En consecuencia, los empleados que no cumplan con esta Política y/o con las leyes y regulaciones de privacidad aplicables pueden enfrentar acciones disciplinarias que podrían extenderse incluso al cese de la relación laboral.

Atención

La privacidad es responsabilidad de todos, no sólo ocasionalmente, sino todos los días. Mantener la seguridad, confidencialidad e integridad de la información personal de MetLife no es meramente una sugerencia, sino un requisito de esta Política.

D. ADMINISTRACIÓN DE RIESGOS DE PRIVACIDAD

1. ¿Cómo se administran los riesgos y controles de privacidad?

La administración de riesgos de privacidad es responsabilidad de todos en MetLife. Cada línea de negocio y función global de la primera línea sirven como la primera línea de defensa en el manejo de los riesgos de privacidad cotidianos. Los riesgos de privacidad también se rigen por las funciones de supervisión de MetLife, incluyendo Cumplimiento, riesgo informático y seguridad, así como seguridad corporativa global, mismas que actúan como la segunda línea de defensa y Auditoría Interna que actúa como la tercera línea de defensa. Las funciones y responsabilidades en el contexto de la administración de riesgos de privacidad son las siguientes:

Administración (Líneas de Negocio/Funciones Globales de la Primera Línea, Oficiales Regionales de Privacidad y Campeones de Privacidad)

Responsabilidad primaria y rendición de cuentas

- ✓ Regula el entorno de control de riesgos
- ✓ Identifica, mide y mitiga el riesgo

Cumplimiento

Supervisión y Asesoría

- ✓ Asesora a las áreas funcionales y de negocio
- ✓ Realiza evaluaciones de riesgos de privacidad

- ✓ Realiza seguimientos y pruebas independientes
- ✓ Comparte los resultados del seguimiento/pruebas con la primera línea de defensa

Auditoría interna

Aseguramiento independiente

- ✓ Valida la fuerza de control
- ✓ Proporciona una evaluación objetiva

Las funciones y responsabilidades específicas para cada línea de defensa y función se describen con mayor detalle a lo largo de esta Política.

2. Funciones de la primera línea de defensa en riesgos de privacidad

La administración en las líneas de negocio y en las funciones globales de la primera línea es responsable de implementar los procesos y controles en las operaciones de MetLife diseñados para disuadir, detectar y prevenir riesgos potenciales de riesgos de privacidad. Para los fines de esta Política, el término **Dirección de negocios** se utilizará para referirse de manera colectiva a la administración en las líneas de negocio y en las funciones globales de la primera línea.

Oficiales Regionales de Privacidad

Con el fin de facilitar el cumplimiento de esta Política, cada operación comercial regional de MetLife[4] deberá nombrar a un empleado del equipo de Dirección de negocios de la operación para que desempeñe la función de Oficial Regional de Privacidad con la aprobación del Director de Privacidad. Cada Oficial Regional de Privacidad debe: (i) estar familiarizado con esta Política, así como con las políticas/ procedimientos desarrollados para los países de su región con el fin de apoyar al departamento de Cumplimiento con el mantenimiento y supervisión del programa de cumplimiento de privacidad; (ii) estar familiarizado con las leyes y regulaciones de privacidad vigentes en toda la región; (iii) coordinarse con los Campeones de Privacidad dentro de su región para garantizar que la implementación de políticas, procedimientos y controles internos sean consistentes con esta Política y con los requisitos regulatorios locales; (iv) coordinarse con la Oficina de Privacidad Corporativa de MetLife y con los Especialistas Regionales de Privacidad con el fin de formular estrategias empresariales y/o regionales relacionadas con el programa de cumplimiento de privacidad (incluyendo estrategias para el mejoramiento de programas y mitigación de riesgos); (v) participar en las reuniones del Consejo de administración/asesoramiento de privacidad de la Oficina de Privacidad Corporativa de MetLife; (vi) garantizar que cualquier cuestión regional planteada por las revisiones realizadas por el departamento de Cumplimiento o auditorías relacionadas con el cumplimiento de la privacidad sean manejadas adecuadamente; (vii) comunicarse con la Dirección de negocio regional y los empleados, según sea necesario, con respecto a avances/tendencias legales y regulatorias importantes en toda la región en riesgos de privacidad; (viii) garantizar que la finalización de la capacitación de los empleados por parte del departamento de Cumplimiento en toda la región cumpla con los requisitos de MetLife; y (ix) cuando sea factible, generar conciencia sobre el riesgo potencial de privacidad que surge de nuevos productos comerciales, iniciativas y proyectos en toda la región.

Campeones de Privacidad

En colaboración con el Oficial Regional de Privacidad correspondiente, cada operación de MetLife nombrará a un empleado del equipo de Dirección de negocio de la operación para que desempeñe la función de Campeón en Privacidad con la aprobación del Director de Privacidad. Cada Campeón en

[4] De acuerdo con esta Política, las operaciones comerciales regionales de MetLife son América-Estados Unidos, América-Latinoamérica, Europa, Medio Oriente y África (“EMEA”) y Asia.

Privacidad debe tener antigüedad suficiente dentro de la operación para poder plantear problemas directamente ante la cúpula directiva y los órganos de gobierno internos. Cada Campeón en Privacidad debe: (i) estar familiarizado con esta Política, así como con las políticas/procedimientos desarrollados para su país con el fin de apoyar al departamento de Cumplimiento con el mantenimiento y la supervisión del programa de cumplimiento de privacidad; (ii) estar familiarizado con las leyes y regulaciones de privacidad aplicables a su país; (iii) estar familiarizado con la forma en que su operación recopila, utiliza, almacena, transfiere o procesa la información personal, y cualquier riesgo de privacidad que se derive de ello; (iv) garantizar que la implementación de políticas, procedimientos y controles internos sean consistentes con esta Política y con los requisitos regulatorios locales; (v) garantizar que todos los empleados dentro de la operación conocen y siguen los procedimientos para identificar y reportar **incidentes de datos personales**; (vi) participar en las reuniones del Consejo de administración/asesoramiento de privacidad de la Oficina de Privacidad Corporativa de MetLife; (vii) garantizar que cualquier cuestión planteada por las revisiones realizadas por el departamento del Cumplimiento o auditorías relacionadas con el cumplimiento de la privacidad sean manejadas adecuadamente y presentadas a la Dirección de negocio local, a la Oficial Regional de Privacidad y al departamento de Cumplimiento; (viii) comunicarse con la Dirección de negocio local y los empleados, según sea necesario, con respecto a avances/tendencias legales y regulatorias importantes de privacidad; (ix) garantizar que la finalización de la capacitación de los empleados por parte del departamento de Cumplimiento en toda la región cumpla con los requisitos de MetLife y trabajar con el departamento de Cumplimiento para coordinar la capacitación periódica dirigida a los empleados; y (x) generar conciencia sobre el riesgo potencial en riesgos de privacidad que surge de nuevos productos comerciales, iniciativas y proyectos a fin de establecer controles internos apropiados.

Oficial de Protección de Datos

Se puede requerir que las operaciones de MetLife nombren a un Oficial responsable de la protección de datos de conformidad con la ley o regulación de privacidad aplicable, misma que establecerá las responsabilidades relativas a este rol. Cuando se requiera a un Oficial responsable de la protección de datos, la Dirección de negocio local deberá garantizar que se designe a un individuo calificado y que sus responsabilidades se comuniquen, cumplan y documenten adecuadamente según sea necesario.

3. Delegación de la supervisión del cumplimiento

Cumplimiento Local

El departamento de Cumplimiento Local, incluyendo la administración de Cumplimiento, es responsable de supervisar que la administración de controles se ha implementado para mitigar riesgos relativos a la privacidad en cada operación de MetLife a través del Programa de Administración de Riesgos de Cumplimiento (“CRMP”, por sus siglas en inglés). El departamento de Cumplimiento Local también es responsable de garantizar que: (i) los empleados estén familiarizados con las leyes de privacidad aplicables; (ii) la operación mantiene un programa sólido relativo al cumplimiento de riesgos de privacidad; (iii) se proporciona capacitación continua a la cúpula directiva, al personal operativo clave y a otros empleados en función del riesgo; (iv) los empleados se mantienen actualizados sobre cualquier cambio en el programa de cumplimiento de privacidad y/o requisitos regulatorios aplicables; y (v) las evaluaciones de riesgos se realizan de acuerdo con la Política Global de la Administración de Riesgos de Cumplimiento de MetLife.

Especialistas Regionales de Privacidad

Los Especialistas Regionales de Privacidad apoyan la supervisión por parte del departamento de Cumplimiento Local en lo referente a los programas de cumplimiento de privacidad dentro de su región para garantizar que las operaciones de MetLife cumplen con esta Política y con las leyes y regulaciones de privacidad de datos correspondientes. El Especialista Regional de Privacidad debe: (i) establecer una

estrategia de cumplimiento en privacidad para la región que apoya; (ii) consultar con el departamento Legal para analizar las leyes y regulaciones que se aplican en toda la región y asesorar a la Dirección de negocio sobre asuntos de privacidad dentro de su región; (iii) involucrarse, en coordinación con el departamento de Relaciones Gubernamentales, con las partes interesadas externas a nivel regional (incluyendo organismos reguladores y grupos de la industria) para anticiparse a las nuevas leyes/regulaciones que puedan afectar a MetLife e influir en las mismas; (iv) apoyar campañas de capacitación sobre privacidad a nivel local, regional y corporativo, incluyendo la impartición de capacitación a empleados nacionales y regionales; (v) supervisar el resultado de las actividades de seguimiento y pruebas del departamento de Cumplimiento Local para garantizar el cumplimiento de las leyes y regulaciones nacionales y regionales, así como de esta Política; (vi) revisar las evaluaciones de riesgos nacionales y regionales para confirmar que la exposición al riesgo de privacidad se mide y documenta con exactitud y de acuerdo con la Política Global de la Administración de Riesgos de Cumplimiento de MetLife; (vii) garantizar que los Agentes Regionales de Privacidad, los Campeones de Privacidad y la Dirección de negocio comprenden los riesgos de privacidad existentes y/o emergentes en toda la región y que se mitiguen eficazmente mediante la implementación de controles reforzados, cuando proceda; (viii) apoyar al departamento de Cumplimiento Local, según corresponda, para responder e informar sobre las filtraciones de datos cuando así lo requiera la ley o la regulación local; (ix) apoyar a la Oficina de Privacidad Corporativa de MetLife con la revisión y aprobación de políticas de privacidad específicas de cada país para asegurar la alineación con la ley local y con los requisitos regulatorios, así como con esta Política; y x) prestar apoyo a proyectos/iniciativas de privacidad a nivel local, regional y global, trabajando con las principales partes interesadas de toda la región (por ejemplo: Riesgo Informático y Seguridad, Departamento Legal y Administración de Datos Empresariales) para garantizar la coordinación de actividades y la implementación de productos que acaten las normas.

Oficina de Privacidad Corporativa de MetLife (MCPO -MetLife Corporate Privacy Office)

La Oficina de Privacidad Corporativa de MetLife cuenta con la supervisión global del programa de cumplimiento de privacidad de MetLife. La Oficina de Privacidad Corporativa de MetLife es responsable de: (i) redactar y actualizar las políticas y procedimientos globales de cumplimiento por escrito; (ii) supervisar la implementación y el cumplimiento continuo de esta Política; (iii) al menos una vez al año, realizar una evaluación independiente del riesgo de privacidad para cada operación de MetLife con el fin de evaluar el riesgo de privacidad y la efectividad del entorno de control de privacidad; (iv) elaborar informes para la cúpula directiva; (v) asesorar a la Dirección de negocio sobre riesgos de privacidad en colaboración con los Especialistas Regionales de Privacidad y el departamento de Cumplimiento Local; (vi) capacitar a la cúpula directiva, personal operativo clave y otros empleados de acuerdo con esta Política y con el programa global de cumplimiento de privacidad; (vii) revisar y evaluar las relaciones con terceros que son consideradas como de alto riesgo para la privacidad; (viii) desarrollar estrategias de cumplimiento en línea con las leyes de privacidad aplicables para mitigar la exposición de la Compañía al riesgo de privacidad; (ix) realizar pruebas sustantivas y capacitación presencial durante las visitas personales a los países; (x) asistir a Auditoría Interna en sus revisiones al programa de cumplimiento de privacidad; (xi) mantenerse actualizado en lo relacionado con el conocimiento de las tendencias de la industria, los cambios legales/ regulatorios que presentan un impacto global y las prácticas actuales de aplicación; (xii) apoyar a los Especialistas Regionales de Privacidad en la ejecución de estrategias regionales de privacidad, según corresponda; y (xiii) apoyar la respuesta a solicitudes de información relacionadas con asuntos de privacidad.

Director de Privacidad

El Director de Privacidad es el encargado de la Oficina de Privacidad Corporativa de MetLife. El Director de Privacidad y su(s) designado(s) es/son responsable(s) de: (i) supervisar el diseño y la implementación del cumplimiento continuo con esta Política a través de MetLife; (ii) revisar periódicamente y, en caso necesario, actualizar los procedimientos establecidos en esta Política; (iii) coordinarse con el liderazgo interfuncional, incluyendo Riesgo Informático y Seguridad y el Director de Tecnologías de la Información, Administración de Datos Empresariales y el Director responsable de la información, Seguridad Corporativa Global, Administración de la Información, Relaciones Gubernamentales, Tecnologías de la Información ("IT") y el departamento Legal, para establecer estrategias de riesgos de privacidad, así como para identificar intersecciones de programas, dependencias y mejoras; (iv) facilitar la colaboración con la primera línea de defensa al encabezar el Consejo de administración/asesoramiento de privacidad y guiando al negocio para establecer "la pauta adecuada a seguir" de MetLife con el propósito de cumplir con esta Política y con las leyes/regulaciones aplicables; (v) realizar y documentar periódicamente una evaluación de toda la empresa concerniente a la exposición potencial de MetLife a los riesgos de privacidad; (vi) en conjunto con el departamento Legal, establecer comunicación con los empleados sobre avances y tendencias legales y regulatorias importantes que se encuentren relacionadas con la privacidad; (vii) coordinar la concienciación, capacitación y orientación continua dirigida a los empleados sobre esta Política y las leyes y regulaciones de privacidad; (viii) mantenerse informado sobre las tendencias de la industria, los cambios legales y regulatorios y las actividades de aplicación actuales; (ix) involucrarse con las partes interesadas externas (incluyendo organismos reguladores y grupos de la industria), en colaboración con el departamento de Relaciones Gubernamentales, con el fin de anticiparse a las nuevas leyes/regulaciones que puedan afectar a MetLife e influir en las mismas; (x) coordinarse con Auditoría Interna para realizar pruebas y revisar periódicamente el cumplimiento con esta Política, con cualquier política/procedimiento que complementen esta Política y con las leyes y regulaciones aplicables; xi) coordinar la revisión, investigación, evaluación y presentación de informes sobre las violaciones a las leyes de privacidad y/o Política de Privacidad; y (xii) cuando corresponda, responder a las solicitudes de información y comunicarse con las autoridades reguladoras/agencias gubernamentales sobre cuestiones de cumplimiento, aplicación y privacidad.

Director de Cumplimiento

El Director de Cumplimiento de MetLife o su designado proporcionará un informe anual al Comité de Administración y Responsabilidad Social Corporativa de la Junta Directiva de MetLife sobre cualquier riesgo significativo de privacidad y problemas que pudieran haber sido identificados durante el año anterior en las operaciones globales de MetLife, así como los planes de mitigación para estos riesgos y problemas.

4. Requisitos para la supervisión del cumplimiento

Evaluación de riesgos

MetLife realizará evaluaciones de riesgos de forma continua para medir el riesgo interno y externo en posibles violaciones a las leyes y regulaciones de privacidad y a esta Política. Las evaluaciones de riesgos tomarán en cuenta, como mínimo, el riesgo geográfico con base en el desarrollo y severidad del entorno regulador aplicable, las amenazas de seguridad de información (incluyendo la ciberseguridad), el tamaño del negocio, las prácticas de administración de datos, el uso de terceros para procesar información personal de MetLife, uso y recopilación de información personal confidencial, prácticas de mercadeo y si los datos se transfieren o se accede a los mismos a través de las fronteras entre países.

Cumplimiento Local realizará evaluaciones de riesgos de privacidad de acuerdo con la Política Global de la Administración de Riesgos de Cumplimiento de MetLife. Cada trimestre, la Oficina de Privacidad

Corporativa de MetLife validará la solidez de las evaluaciones de riesgos del departamento de Cumplimiento Local y notificará al departamento de Cumplimiento Local sobre cualquier desacuerdo con la evaluación de riesgo local. Asimismo, al menos una vez al año, la Oficina de Privacidad Corporativa de MetLife llevará a cabo evaluaciones independientes de riesgos de privacidad para cada operación de MetLife. Al realizar las evaluaciones de riesgo, la Oficina de Privacidad Corporativa de MetLife considerará el riesgo inherente, la eficacia del entorno de control y los resultados de cualquier prueba realizada por Cumplimiento o Auditoría Interna como componentes clave de la evaluación.

Métricas, seguimiento y pruebas

El departamento de Cumplimiento Local llevará a cabo la supervisión, seguimiento y pruebas continuas de conformidad con la Política Global de la Administración de Riesgos de Cumplimiento de MetLife. Dichas actividades de supervisión son el fundamento de las evaluaciones de riesgo antes descritas y se deben mantener en el sistema de administración de riesgos adecuado.

El departamento de Cumplimiento Local, con el apoyo de la Dirección de negocio, también está obligado a presentar un Informe Trimestral de Métricas al equipo Central de Cumplimiento International ("International Compliance Central team"). El departamento de Cumplimiento Local y la Oficina de Privacidad Corporativa de MetLife analizarán las métricas de privacidad relevantes, según lo define la Oficina de Privacidad Corporativa de MetLife, con el fin de: (i) identificar posibles debilidades en los controles; (ii) identificar las tendencias y riesgos emergentes; (iii) realizar una evaluación general de los riesgos de cada operación; y (iv) desarrollar estrategias para las acciones correctivas en colaboración con la Dirección de negocio.

Implementación de políticas y procedimientos locales

Como un suplemento a esta Política, cada operación de MetLife en el país debe desarrollar e implementar una política de privacidad local que defina los requisitos para cumplir con las leyes y regulaciones de privacidad aplicables. Todos los suplementos que se añadan por país deben ser revisados y aprobados por la Oficina de Privacidad Corporativa de MetLife para asegurar la coherencia con esta Política.

Atención

La Oficina de Privacidad Corporativa de MetLife debe aprobar cualquier suplemento que se añada a esta Política a nivel local.

5. Riesgo informático y seguridad

Bajo el liderazgo del Director de Tecnologías de la Información de MetLife, la función de riesgo informático y seguridad de MetLife es responsable, en parte, de la implementación y supervisión de políticas y estándares de seguridad en las tecnologías de la información diseñados para proteger los datos (incluyendo la información personal) del **acceso**, uso, alteración o destrucción no autorizados, mismos que se encuentran contenidos en los sistemas, aplicaciones y bases de datos de MetLife. El Director de Seguridad de la Información, o una persona designada, se reunirá periódicamente con el Director de Privacidad para revisar la efectividad de los controles de seguridad administrativa y técnica de los datos de MetLife en toda la empresa, de acuerdo con las evaluaciones realizadas por la Dirección de Seguridad de Tecnología de la Información, y cualquier riesgo que pudiera derivarse de la información personal de MetLife.

6. Seguridad corporativa global

La función de seguridad corporativa global de MetLife es responsable, en parte, de la implementación y supervisión de políticas y estándares de seguridad del sitio diseñados para proteger los datos de MetLife (incluyendo la información personal) del acceso, uso, alteración o destrucción no autorizados. El encargado de la función de seguridad corporativa global de MetLife, o una persona designada, se reunirá periódicamente con el Director de Privacidad para revisar la efectividad de los controles de seguridad de datos físicos de MetLife en toda la empresa, de acuerdo con las evaluaciones realizadas por la función de seguridad corporativa global de MetLife, y cualquier riesgo que pudiera derivarse de la información personal de MetLife.

7. Auditoría Interna

Auditoría Interna realizará auditorías de forma periódica y con base en el riesgo a fin de evaluar la implementación de esta Política y el cumplimiento de las leyes/regulaciones de privacidad aplicables. Estas auditorías incluirán una evaluación de la eficacia y calidad de los procedimientos de MetLife, documentación, controles internos, procedimientos de capacitación, pruebas de cumplimiento y cualquier acción correctiva que se haya tomado como respuesta a auditorías y evaluaciones previas por parte de las entidades reguladoras. Como mínimo, se deberá proporcionar un informe escrito que resuma los resultados de la auditoría y cualquier acción correctiva sugerida al Director de Privacidad, al Especialista Regional de Privacidad correspondiente y al Oficial Regional de Privacidad, a los Oficiales de Cumplimiento Local apropiados, al Oficial responsable de la protección de datos (cuando proceda), al Departamento Legal y a la dirección empresarial apropiada correspondiente a la operación revisada.

E. REQUISITOS DEL MANTENIMIENTO DE REGISTROS

Todos los empleados de MetLife deberán cumplir con la Política de Administración del Ciclo de Vida de la Información ("Information Lifecycle Management Policy") de MetLife con respecto a la creación, administración, retención, preservación y disposición de la información de MetLife. Cada operación de MetLife debe contar con políticas, procedimientos y controles internos establecidos para cumplir con los requisitos de mantenimiento de registros establecidos por las leyes y regulaciones de privacidad aplicables. Los registros que se conserven deben incluir, como mínimo, los relacionados con las **evaluaciones de impacto en la privacidad**, **avisos de privacidad**, **consentimientos**, quejas de privacidad, relaciones con terceros (incluyendo toda la diligencia debida realizada a terceros), **transferencias transfronterizas de datos** (incluyendo cualquier acuerdo para la transferencia de datos u otro mecanismo de transferencia válido) y cualquier notificación al cliente o regulatoria que esté relacionada con alguna filtración de datos. Todos estos registros y documentación de respaldo deben mantenerse de manera auditable y accesible por un periodo de cinco (5) años como mínimo, a menos que la ley local o la política de retención de registros de la operación específica de MetLife determine un periodo de tiempo diferente.

Atención

El periodo de tiempo de retención aplicable y los registros específicos que requieran ser conservados pueden variar según el país en el que MetLife recopiló inicialmente la información personal. Por ejemplo, una operación de MetLife ubicada en el país A que procesa la información personal del cliente inicialmente recolectada en el país B puede estar obligada a cumplir con los requisitos de retención de registros del país B, además de los del país A.

II. AVISO, CONSENTIMIENTO Y CONTROL

Para mantener la reputación de MetLife y garantizar la confianza continua de los clientes, empleados y socios comerciales, MetLife otorga ciertos derechos de privacidad a los individuos (incluyendo el aviso, consentimiento y control), según lo requiera la ley, en relación con las actividades de procesamiento de la información de la Compañía. Muchas jurisdicciones requieren que MetLife proporcione cierta información a las personas cuando se recopila su información personal. Este aviso de información, que usualmente toma la forma de un aviso de privacidad en línea o escrito, brinda a los individuos una explicación de qué información personal se recopila, por qué se recopila, cómo se utilizará y protegerá y con quién podría compartirse. Los avisos de privacidad pueden ser considerados como el compromiso por parte de la Compañía de manejar la información personal de conformidad con los términos del aviso.

El consentimiento a menudo se refiere a la opción de **inclusión voluntaria** o **exclusión voluntaria** que tiene un individuo en relación con el uso de la información personal por parte de la Compañía y generalmente se obtiene a través de una "casilla de verificación" o firma con el fin de confirmar que el individuo entiende y acepta el procesamiento de su información personal. En algunas ocasiones, puede requerirse el consentimiento expreso por escrito del individuo con base en la actividad de procesamiento de la información. Podría requerirse que MetLife obtenga el consentimiento de clientes individuales, empleados y socios comerciales antes de: (i) recopilar, usar o procesar su información personal de ciertas maneras, incluyendo la información personal confidencial o compartir la información personal del individuo con cualquier tercero; (ii) transferir la información personal del individuo fuera del país de residencia de dicho individuo (***Consulte* la Sección V: transferencias transfronterizas de datos)**; (iii) utilizar la información personal para comercializar los bienes o servicios de MetLife, ya sea directa o indirectamente; y (iv) utilizar o colocar ***web cookies*** en la computadora u otros dispositivos electrónicos de algún individuo. Según lo requiera la ley, MetLife también otorga a los individuos el derecho de controlar su información personal, lo cual incluye, por ejemplo, el derecho de acceder, modificar, borrar, restringir, transmitir u oponerse a ciertos usos de su información.

Ejemplos

Consentimiento de inclusión voluntaria: la persona indica de forma afirmativa en la casilla de verificación que desea que su información se comparta con otra organización.

Consentimiento de exclusión voluntaria: se requiere que la persona haga clic en el enlace "cancelar la suscripción" en la parte inferior del correo electrónico publicitario con el fin de dejar de recibir correos similares en el futuro.

El hecho de no otorgar y/o respetar de forma adecuada los derechos individuales de privacidad puede no sólo impactar negativamente en la reputación de MetLife, sino también puede resultar en la insatisfacción del cliente, auditorías regulatorias y/o multas/sanciones. En términos más específicos, en muchas jurisdicciones, MetLife puede ser considerado responsable por:

- no explicar a las personas de manera clara y concisa cómo se recopila, utiliza o comparte la información personal;
- no actualizar a las personas cuando la Compañía cambia su aviso de privacidad;
- recopilar o utilizar datos sin el consentimiento de las personas;
- utilizar datos para propósitos diferentes a los establecidos en el aviso de privacidad de la Compañía; o
- responder de manera inapropiada o inoportuna a la solicitud de alguna persona para acceder, modificar o borrar información personal.

Por estas razones, cada operación de MetLife debe tener procedimientos establecidos que obliguen, tal y como lo requieren las leyes y regulaciones locales aplicables, a las líneas de negocio a:

- Proporcionar a los individuos un aviso de privacidad antes o durante la recopilación de información personal y en cualquier otro momento según lo prescrito por la ley aplicable, y actualizar los avisos de privacidad pertinentes en caso de que el negocio modifique la manera en que se utiliza, comparte o procesa la información personal. El departamento Legal debe redactar, revisar y aprobar el idioma de cualquier aviso de privacidad antes de su uso.
- Obtener el consentimiento por parte de los individuos, de la manera y forma en que la ley local lo requiera, antes de procesar la información personal o utilizar la información personal de alguna manera que sea inconsistente con cualquier aviso de privacidad previamente proporcionado y/o con la comercialización de los bienes o servicios de MetLife.
- Dejar de procesar la información personal de un individuo dentro del tiempo requerido por la ley local aplicable si el individuo revoca su consentimiento o se opone al procesamiento.
- Proporcionar a los individuos acceso a su información personal para su revisión y actualización, lo que puede incluir mantener una forma fácil y segura para que las personas se contacten con MetLife, obtener copias de sus registros y enviar solicitudes para modificar, actualizar o borrar su información personal. Todas las solicitudes individuales deben atenderse dentro del plazo requerido por la ley local aplicable.

Asimismo, cada operación de MetLife debe tener procedimientos que requieran que el departamento de Recursos Humanos, si la ley o regulación aplicable lo solicita, proporcione un aviso de privacidad y/u obtenga los consentimientos requeridos por parte de los solicitantes de empleo y empleados durante el proceso de contratación y/o en cualquier otro momento posterior.

RESUMEN DE LAS FUNCIONES Y RESPONSABILIDADES CLAVE: AVISO, CONSENTIMIENTO Y CONTROL

Funciones	Responsabilidades
Todos los empleados	Recopilar, utilizar y procesar información personal únicamente de manera que sea consistente con los propósitos establecidos en el aviso de privacidad.
Operaciones comerciales	Según lo requiera la ley, proporcionar el aviso adecuado a los clientes y recopilar los consentimientos de dichos clientes (incluyendo el uso de sitios web y aplicaciones móviles que se presentan públicamente) con el fin de recabar, utilizar y procesar la información personal y mantener los consentimientos de manera auditable. Proporcionar a los individuos avisos de privacidad actualizados y obtener consentimientos actualizados o adicionales, según lo requiera la ley y la regulación aplicables. Según lo requiera la ley, atender de manera oportuna las solicitudes individuales de acceso a la información personal, lo que puede incluir proporcionar a los individuos acceso y poder para modificar o eliminar su información personal. Respetar el derecho del individuo a oponerse al procesamiento o a revocar el consentimiento para el uso de su información personal, en la medida que lo requiera la ley.

Venta Directa /Telemercadeo	Respetar el derecho del individuo a rechazar o revocar su consentimiento para el uso de su información personal con fines de comercialización, cuando sea requerido por la ley.
Recursos Humanos	Según lo requiera la ley, proporcionar el aviso adecuado a los solicitantes de empleo y empleados y recopilar los consentimientos de dichos solicitantes de empleo y empleados con el fin de recabar, utilizar y procesar la información personal y mantener los consentimientos de manera auditable.
Departamento Legal	Elaborar, revisar y aprobar el contenido de los avisos de privacidad y consentimientos, según lo determine la ley/regulación aplicable, mismos que utilizará el negocio.

III. PROTECCIÓN DE LA INFORMACIÓN

La seguridad de la información es un componente esencial del cumplimiento de privacidad. Si bien la seguridad de la información se relaciona con la protección de la información más allá de la información personal, la implementación de salvaguardas de seguridad de la información es fundamental para proteger la información personal recopilada, almacenada y procesada por la Compañía de accesos no autorizados, usos, divulgación, destrucción u otras amenazas de seguridad, ya sea de naturaleza interna o externa. El incumplimiento en el establecimiento de medidas de seguridad de la información para proteger la información personal puede conducir a investigaciones regulatorias, multas/sanciones, litigios, daños a la reputación y el deterioro de la confianza del cliente en la Compañía.

AMENAZAS DE SEGURIDAD INTERNA

Muchos empleados y terceros que prestan servicios a MetLife tienen acceso regular a los datos de la Compañía, lo que da lugar al riesgo de que la información personal pueda vulnerarse de manera accidental, negligente o incluso de manera maliciosa.

Las amenazas internas maliciosas suponen la intención de hacer daño y la decisión de actuar inapropiadamente. Ejemplos comunes incluyen la filtración intencional de información patentada/ personal o el uso de los derechos de acceso para beneficio personal.

Las amenazas internas por negligencia no suponen la intención de hacer daño, pero requieren una decisión consciente para actuar inapropiadamente. Estos actos pueden estar bien intencionados, como el uso de servicios o dispositivos no autorizados para ahorrar tiempo, aumentar la productividad o habilitar el trabajo móvil. El comportamiento a menudo se acompaña con el conocimiento de que la acción viola la política aplicable.

Las amenazas internas accidentales no requieren algún motivo para hacer daño o una decisión consciente de actuar inapropiadamente. Las personas con información privilegiada pueden poner en riesgo los datos de una organización con muy poco esfuerzo con acciones como adjuntar el archivo equivocado a un correo electrónico enviado, compartir demasiada información en las redes sociales, hacer clic en un enlace o archivo adjunto que contenga algún código malicioso, perder una computadora portátil o unidad USB o por algún otro acto que implique errores humanos.

AMENAZAS DE SEGURIDAD EXTERNA

Los ataques más severos a la seguridad de la información suelen provenir de actores de amenazas externas calificados y sofisticados que son capaces de encontrar vulnerabilidades en la red o de manipular socialmente a las personas con información privilegiada para romper las defensas de la red externa. Los actores de amenazas externas pueden asumir muchas formas, incluyendo: organizaciones criminales como los hackers que operan esencialmente como un negocio; hackers patrocinados por el estado, quienes eligen sus objetivos con posibles consecuencias geopolíticas; "hacktivistas" que eligen a sus objetivos porque estos realizan actividades que se consideran moralmente o políticamente confidenciales; o los "lone wolf" hackers (lobos solitarios) que normalmente intentan lavar grandes cantidades de dinero o comerciar con propiedad intelectual robada.

SALVAGUARDAS DE LA INFORMACIÓN

Para protegerse contra el riesgo de que la información personal de MetLife pueda verse comprometida por amenazas internas y externas de seguridad, la Compañía se apoya en protecciones de la información que pueden clasificarse de la siguiente manera: **medidas administrativas de seguridad, medidas físicas de seguridad y medidas técnicas de seguridad**.

Ejemplos

Medidas administrativas de seguridad: políticas y estándares de seguridad en las tecnologías de la información, procedimientos de respuesta a incidentes y capacitación.

Medidas físicas de seguridad: cerraduras de puertas, cámaras de seguridad y credenciales de identificación de empleados.

Medidas técnicas de seguridad: firewalls, software antivirus, cifrado de datos y registros de acceso.

A. MEDIDAS ADMINISTRATIVAS DE SEGURIDAD

Las medidas administrativas de seguridad incluyen políticas, procedimientos y controles de seguridad que MetLife adopta con el fin de garantizar que los empleados comprendan su obligación de administrar y proteger la información personal. Además de los requisitos establecidos a continuación, los empleados de MetLife deberán cumplir con todos los demás aspectos de esta Política al manejar información personal.

- **Requisitos de administración y clasificación de datos:** los empleados deben administrar la información personal de acuerdo con la Política de Administración de Datos Empresariales ("Enterprise Data Governance Policy") de MetLife, así como clasificar la información personal de conformidad con las políticas y estándares de seguridad en las tecnologías de la información ("IT Security Policies and Standards") de MetLife y la ley aplicable para garantizar que el nivel de seguridad apropiado se implementa con el fin de proteger la información.
- **Requisitos de "escritorio limpio":** los empleados no deben dejar la información personal de MetLife desatendida en las oficinas, salas de conferencias o en cualquier otro espacio público/espacio sin las debidas medidas de seguridad. Como práctica general, cualquier archivo, documento o registro que contenga información personal debe ser almacenado en armarios o escritorios cerrados cuando no esté en uso y, en todos los casos, deberá quedar asegurado al final del día hábil.
- **Requisitos de eliminación de la información personal:** cuando la información personal ya no sea necesaria para cumplir un objetivo comercial y su retención ya no sea requerida por ley o regulación, dicha información deberá ser eliminada de acuerdo con la Política de Administración del Ciclo de Vida

Atención

Consulte la Política de Administración del Ciclo de Vida de la Información de MetLife o envíe un correo electrónico a la Oficina del Programa de Administración del Ciclo de Vida de la Información (RIMPO@metlife.com) para obtener más información sobre los requisitos de retención

de la Información de MetLife, así como con las políticas y estándares de seguridad en las tecnologías de la información y retenciones legales.

- **Requisitos de "envío seguro":** al enviar información personal por correo electrónico a una dirección de correo electrónico que no sea de MetLife, los empleados deberán escribir "[Seguro]" en la línea de asunto del correo electrónico o, si está disponible, hacer clic en el ícono "enviar seguro" del correo electrónico para garantizar que la información se cifrará cuando se transmita. Consulte las políticas y estándares de seguridad en las tecnologías de la información de MetLife para obtener información adicional sobre los requisitos de envío seguro de MetLife.
- **Requisitos para las herramientas de colaboración:** con excepción de la información básica de un empleado (por ejemplo: nombre, cargo, dirección del lugar de trabajo, número de teléfono), los empleados no pueden almacenar, compartir, subir o publicar información personal de los empleados o clientes en ningún sitio o herramienta de colaboración utilizada por MetLife (por ejemplo: SharePoint, Box, MyMetLife, Yammer, WebEx, Microsoft Lync). Los empleados deberán notificar a la Oficina de Privacidad Corporativa de MetLife (askprivacy@metlife.com) si cualquier información personal es descubierta en un foro público o herramienta de colaboración. Consulte los Lineamientos de Colaboración de MetLife ("MetLife's Collaboration Guidelines") para obtener información adicional.

B. MEDIDAS FÍSICAS DE SEGURIDAD

Las medidas físicas de seguridad son las políticas, procedimientos y controles de seguridad establecidos por la función de seguridad corporativa global de MetLife para proteger a los empleados, edificios, oficinas, activos, equipos, tecnología e información (incluyendo la información personal) pertenecientes a la Compañía de los riesgos naturales y ambientales y de la intrusión no autorizada. Todos los empleados de MetLife deberán cumplir con las políticas, procedimientos y estándares de la función de seguridad corporativa global de MetLife. La función de seguridad corporativa global de MetLife se reunirá periódicamente con la Oficina de Privacidad Corporativa de MetLife para revisar la efectividad de los controles de seguridad de datos físicos de MetLife en toda la empresa, de acuerdo con las evaluaciones realizadas por la función de seguridad corporativa global de MetLife, y cualquier riesgo que pudiera derivarse de la información personal de MetLife.

C. MEDIDAS TÉCNICAS DE SEGURIDAD

Las medidas técnicas de seguridad son las políticas, procedimientos y controles de seguridad establecidos por el Director de Seguridad de la Información de MetLife y la función de riesgo informático y seguridad de MetLife para proteger la información de MetLife que es almacenada por medios electrónicos, usos, accesos o destrucción no autorizados, incluyendo la información personal almacenada en los sistemas, aplicaciones y bases de datos de MetLife. Todos los empleados de MetLife deberán cumplir con las políticas y estándares de seguridad en las tecnologías de la información de MetLife. La Dirección de Seguridad de Tecnología de la Información se reunirá periódicamente con la Oficina de Privacidad Corporativa de MetLife para revisar la efectividad de los controles de seguridad de datos técnicos de MetLife en toda la empresa, de acuerdo con las evaluaciones realizadas por

Ejemplos de medidas técnicas de seguridad

Las medidas técnicas de seguridad fundamentales para proteger la información personal incluyen:

Controles de prevención de pérdida de datos: ayudan a evitar que los empleados envíen información confidencial o crítica fuera de la red corporativa.

Controles de administración de acceso: proporcionan, recertifican y supervisan el acceso de los usuarios a las aplicaciones e infraestructura, lo cual garantiza que los derechos de acceso se aprueben y se alineen con las responsabilidades laborales.

Controles de administración de vulnerabilidades: detectan, evalúan y corrigen las deficiencias de los servidores, redes y puntos terminales que pueden ser explotados por los actores de la amenaza.

la Dirección de Seguridad de Tecnología de la Información, y cualquier riesgo que pudiera derivarse de la información personal de los clientes y empleados de MetLife.

RESUMEN DE LAS FUNCIONES Y RESPONSABILIDADES CLAVE: PROTECCIÓN DE LA INFORMACIÓN

Funciones	Responsabilidades
Todos los empleados	Cumplir con las políticas y procedimientos de seguridad relacionadas con tecnología de la información, seguridad corporativa global, administración de datos empresariales y administración del ciclo de vida de la información, así como las pautas de colaboración de MetLife en lo referente a las herramientas de colaboración. Cumplir con los requisitos de "escritorio limpio" y destrucción de información de MetLife. Enviar correos electrónicos externos que contengan información personal de manera segura utilizando las funciones de "envío seguro" de MetLife.
Operaciones comerciales y funciones globales	Apoyar el cumplimiento de las políticas y estándares por parte de los empleados para proteger la información personal. Asociarse con el departamento de Cumplimiento, el departamento Legal, riesgo informático y seguridad y tecnologías de la información para garantizar que los procesos nuevos (o cambios a los procesos) relacionados con la tecnología, productos y procesos comerciales cumplan con los requisitos legales de privacidad aplicables.
Riesgo informático y seguridad y seguridad corporativa global	Garantizar que las protecciones de la información apropiadas se encuentren establecidas para proteger la información personal y cumplir con las políticas y estándares de cada función. Informar periódicamente a la Oficina de Privacidad Corporativa de MetLife sobre la efectividad de las protecciones de la información y sobre cualquier riesgo que pudiera derivarse de la información personal.

IV. PROCESAMIENTO DE DATOS PARA TERCEROS

MetLife cuenta con un gran número de terceros (incluyendo proveedores de servicios, vendedores, intermediarios, agentes, corredores, consultores, distribuidores y socios de empresas conjuntas) para llevar a cabo negocios a nivel mundial. En muchos casos, con base en la naturaleza de los bienes o servicios proporcionados a MetLife, puede requerirse que el tercero obtenga o acceda a la información

personal de los empleados o clientes de la Compañía. Cuando la información personal sale del entorno de MetLife o un tercero accede a ella, la Compañía tiene menos control sobre cómo se maneja o protege dicha información, lo que aumenta el riesgo de una posible filtración de datos.

De conformidad con las leyes y regulaciones de privacidad de muchos países en los que MetLife opera, la Compañía puede ser considerada responsable si un tercero a quien se confía la información personal de MetLife causa, de manera voluntaria o accidental, que la información se pierda, sea mal utilizada, se acceda a ella de modo inapropiado o que sea puesta en peligro. Por lo tanto, esta Política establece el siguiente proceso para evaluar y mitigar el riesgo potencial que plantea a la Compañía cada tercero que maneja información personal de MetLife.

EL PROCESO DE TRES PASOS

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[5].

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”.

Atención

El cuestionario de Evaluación de Riesgos de Productos-Servicios y de Proveedores (“PSRA”) de Adquisiciones Globales incluye las preguntas 1 y 2 mencionadas anteriormente. Para terceros que requieren el cuestionario de Evaluación de Riesgos de Productos-Servicios y de Proveedores en virtud de la Política Global de Adquisiciones (“Global Procurement Policy”) y Procedimientos (“Procedures”), los empleados deberán asegurarse de que estas preguntas preliminares de evaluación del riesgo sean contestadas al completar dicho cuestionario.

Para terceros que no requieren el cuestionario de Evaluación de Riesgos de Productos-Servicios y de Proveedores o que no estén incluidos en los procesos de Adquisiciones Globales, los empleados deberán documentar su evaluación preliminar de riesgos empleando el **Apéndice A** o cualquier formulario, sistema o proceso sustituto diseñado para cumplir con este requisito, mismo que deberá ser aprobado por la Oficina de Privacidad Corporativa de MetLife.

[5] Este proceso no se aplica a los contratos de seguro de MetLife que se celebran directamente con los clientes (por ejemplo, una póliza de seguro de grupo emitida a un cliente del grupo).

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[6] 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.

Atención

Una vez que se determine que el tercero manejará, procesará o tendrá acceso a información personal de MetLife, la línea de negocio o área funcional pertinente deberá trabajar con la Dirección de Seguridad de Tecnología de la Información en ARS_MOREs@metlife.com para llevar a cabo la diligencia debida en la seguridad de la información y en el programa de privacidad y controles del tercero.

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.

[6] Para facilitar la diligencia debida en el tercero de conformidad con esta Política, la Dirección de Seguridad de Tecnología de la Información aplicará su proceso de evaluación de proveedores (anteriormente, proceso de Evaluación Global de Riesgos o MÁS de MetLife), el cual ha sido diseñado para incluir una revisión de la seguridad de la información y protecciones de privacidad del tercero.

- **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 uno al tres mencionados anteriormente, la línea de negocio o área funcional responsable deberá obtener las firmas apropiadas como se especifica en el **Apéndice A**.

DILIGENCIA DEBIDA CONTINUA

La línea de negocio o área funcional responsable deberá trabajar con la Dirección de Seguridad de Tecnología de la Información como parte del proceso de reevaluación de proveedores de la Dirección de Seguridad de Tecnología de la Información con el fin de llevar a cabo la diligencia debida en terceros que procesan la información personal de los clientes o empleados de MetLife. La frecuencia de las reevaluaciones de terceros se basará en el riesgo de acuerdo con lo determinado por la Dirección de Seguridad de Tecnología de la Información, en colaboración con la Oficina de Privacidad Corporativa de MetLife. Al igual que con la diligencia debida inicial en virtud de esta Política, la reevaluación se enfocará en las prácticas de protección de datos por parte de terceros, protección de seguridad de la información, programa de cumplimiento de privacidad y uso de los datos de MetLife para garantizar que la información personal de MetLife permanezca protegida de manera adecuada. Si después de realizar una reevaluación 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.

RESUMEN DE LAS FUNCIONES Y RESPONSABILIDADES CLAVE: PROCESAMIENTO DE DATOS PARA TERCEROS

Funciones	Responsabilidades
Todos los empleados	Compartir información personal de MetLife sólo con terceros aprobados, sólo para fines comerciales legítimos y sólo cuando sea necesario.
Operaciones comerciales y funciones globales	Para todos los terceros que procesarán la información personal de MetLife se deberá trabajar con: (i) la Dirección de Seguridad de Tecnología de la Información para llevar a cabo la diligencia debida en las protecciones de seguridad de la información de terceros y las prácticas de protección de datos; y (ii) con el departamento Legal a fin de incluir disposiciones apropiadas en

	en protección de datos en el acuerdo con terceros y establecer un mecanismo apropiado de transferencias transfronterizas de datos, cuando sea necesario.
Riesgo informático y seguridad	Para todos los terceros que procesarán la información personal de MetLife, se deberá llevar a cabo la diligencia debida inicial y continua de las protecciones de seguridad de la información de terceros y las prácticas de protección de datos conforme al proceso de evaluación del proveedor por parte de la Dirección de Seguridad de Tecnología de la Información. Después de llevar a cabo la diligencia debida o de volver a evaluar a un tercero, se deberá reportar a terceros considerados como de alto riesgo al departamento de Cumplimiento para que se determinen los siguientes pasos.
Departmento Legal	Para todos los terceros que procesarán la información personal de MetLife, se deberán incluir las disposiciones apropiadas de protección de datos en el acuerdo con terceros y establecer un mecanismo apropiado de transferencias transfronterizas de datos, cuando sea necesario.

V. TRANSFERENCIAS TRANSFRONTERIZAS DE DATOS

Al realizar negocios, trabajar en proyectos de la Compañía o implementar nuevos procesos o sistemas, alguna operación de MetLife podría requerir la transferencia de información personal a otras entidades de MetLife o a terceros que se encuentren fuera del país de la operación de MetLife. Muchos de los países en donde opera MetLife cuentan con leyes o regulaciones que restringen la transferencia de información personal fuera del país sin un **mecanismo de transferencia de datos** válido. Aunque los mecanismos permisibles de transferencia de datos están definidos por la ley o regulación aplicable, los ejemplos incluyen:

Atención

Cualquier operación de MetLife que procese información personal recopilada en otro país debe garantizar que la información se procesa de acuerdo con las leyes y regulaciones del país en donde originalmente se recopiló la información.

- acuerdo para la transferencia de datos con la parte que tendrá acceso u obtendrá la información personal;
- notificación a la autoridad y/o aprobación por parte de la autoridad local encargada de la protección de datos de un país; o
- notificación al individuo y/o consentimiento por parte del individuo cuyos datos deben ser transferidos.

Las transferencias transfronterizas de datos sin un mecanismo de transferencia de datos válido requeridas por la ley local puede resultar en investigaciones regulatorias, multas/sanciones y daño a la reputación de la Compañía. Por lo tanto, los empleados de MetLife deberán trabajar con el departamento Legal para establecer un mecanismo válido de transferencia de datos (según lo requerido por la ley o regulación aplicable) antes de transferir, directa o indirectamente a través de terceros, información personal de MetLife a cualquier entidad de MetLife o a terceros ubicados en un país que no sea el país en donde originalmente se recopiló la información. Los empleados de la línea de negocio o área funcional responsable de la transferencia de datos deberán mantener el mecanismo de transferencia de datos adecuado de manera auditable.

Ejemplos

Una transferencia transfronteriza de datos se define como la transmisión de información personal de un país a otro. En algunas jurisdicciones, esto no requiere la transferencia física de datos a otro país, sino simplemente la capacidad de acceder a los datos de otro país. Ejemplos de transferencias transfronterizas de datos incluyen, pero no se limitan a:

- Cajas de envío que contengan registros físicos de la información personal de MetLife del país A al país B.
- Transferencia de archivos electrónicos que contengan información personal de MetLife desde un centro de proceso de datos en el país A a un centro de proceso de datos en el país B.
- Enviar por correo electrónico una hoja de cálculo de Excel que contenga información personal de MetLife del país A al país B.
- Visualización desde el país A de un sitio de SharePoint o WebEx alojado en el país B que contiene información personal de MetLife.
- Subir información personal de MetLife desde el país A a una plataforma en la nube con un servidor en el país B.
- Proporcionar información personal de MetLife del país A a un proveedor de servicios externos también ubicado en el país A, pero que almacenará la información personal en el centro de proceso de datos del tercero ubicado en el país B.

RESUMEN DE LAS FUNCIONES Y RESPONSABILIDADES CLAVE: TRANSFERENCIAS TRANSFRONTERIZAS DE DATOS

Funciones	Responsabilidades
Operaciones comerciales y funciones globales	Antes de transferir información personal de MetLife a través de las fronteras entre países, se deberá trabajar con el departamento Legal para asegurarse de que existe un mecanismo de transferencia de datos válido (según lo requiera la ley) y mantener los mecanismos de transferencia de datos necesarios de manera auditable.
Departmento Legal	Trabajar con la operación comercial o área funcional apropiada para garantizar que los mecanismos de transferencia de datos requeridos estén en su sitio antes de realizar la transferencia de información personal de MetLife a través de las fronteras del país.

VI. ADMINISTRACIÓN DE INCIDENTES DE DATOS PERSONALES

¿QUÉ ES UN INCIDENTE DE DATOS PERSONALES?

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. Los ejemplos incluyen, pero no se limitan a los siguientes casos:

- Un informe que contenía números de identificación nacional fue enviado por correo electrónico al cliente del grupo equivocado.
- Una póliza de seguro de auto que contenía el nombre de una persona y el número de licencia de conducir fue enviada por correo al asegurado equivocado.
- Un empleado de MetLife publicó los nombres de clientes y números de cuenta en un sitio público sin seguridad.
- Un empleado de MetLife encuentra los formularios de solicitud de póliza ya completados en un contenedor de basura fuera de la oficina.
- Alguien pierde o roba una computadora portátil de MetLife (encriptada o no encriptada), pero se recupera más tarde.
- El procesamiento de datos se realiza utilizando la información personal de los clientes de MetLife, aunque el uso de información personal para este propósito no se especifica en el aviso de privacidad.
- Un tercero que está probando un nuevo sistema de MetLife no oculta o elimina la información personal del cliente de entornos que no sean de producción.

PROCEDIMIENTOS DE ADMINISTRACIÓN DE INCIDENTES DE DATOS PERSONALES

Los incidentes de datos personales pueden dar lugar a identificar un robo, fraude, pérdida financiera, daño físico o daño emocional/a la reputación para el individuo cuya información personal podría haber sido filtrada. Los incidentes de datos personales también pueden conducir a la insatisfacción de los clientes, prensa negativa y multas/sanciones regulatorias para MetLife, así como el riesgo de pérdidas considerables de la marca y datos de la Compañía, dos de los activos más valiosos de ésta. Estas consecuencias adversas pueden ser más significativas cuando los incidentes de datos personales no se reportan de manera oportuna o no se administran correctamente.

Todas las operaciones de MetLife deben documentar y mantener procedimientos de administración de incidentes de datos personales para informar sobre la identificación, reporte y prevención de incidentes con datos personales, incluso si no es requerido por la ley o regulación aplicable con el fin de minimizar el daño potencial que puede resultar de incidentes de datos personales. Los procedimientos de administración de incidentes de datos personales de cada operación deberán incluir, como mínimo, los siguientes pasos requeridos.

Paso uno: reportar al departamento de Cumplimiento Local los incidentes de datos personales

Todos los empleados de MetLife son responsables de identificar incidentes con datos personales. Los empleados que identifiquen, o incluso sospechen, la existencia de un incidente de datos personales deberán reportarlo inmediatamente al departamento de Cumplimiento Local. Excepto por lo señalado en esta Política, no es necesario que los empleados consideren si un incidente de datos personales cumple con los requisitos de una filtración de datos en virtud de la ley o regulación aplicable.

Atención

Las leyes o regulaciones aplicables pueden requerir la notificación reglamentaria y/o individual de las trasgresiones confirmadas dentro de un cierto plazo de tiempo. Por lo tanto, es fundamental que los empleados que sepan o sospechen de algún incidente de datos personales lo reporten de inmediato al departamento de Cumplimiento Local.

Cuando un incidente de datos personales no se reporta inmediatamente al departamento de Cumplimiento Local, ni reporta en absoluto, MetLife no puede responder o solucionar correctamente el incidente, lo cual puede resultar en el incumplimiento de los requisitos legales aplicables. El hecho de no reportar un incidente de datos personales, de acuerdo con esta Política, puede resultar en acciones disciplinarias que podrían extenderse incluso al cese de la relación laboral.

Paso dos: investigar el incidente de datos personales

La Dirección de negocio deberá trabajar con el empleado(s) que reporte(n) algún incidente de datos personales para identificar los elementos de información personal involucrados en el incidente, determinar la causa de origen y el alcance del incidente (incluyendo, cuando corresponda, la participación de proveedores externos), confirmar que el incidente se ha contenido debidamente y, de ser posible, identificar a las personas afectadas por dicho incidente. La Dirección de Seguridad de Tecnología de la Información seguridad y/o seguridad corporativa global deberán apoyar la investigación de incidentes de datos personales que se cree que son resultado del fallo de las protecciones de seguridad de la información y/o que pueden involucrar sistemas informáticos.

Paso tres: determinar si se ha producido una filtración de datos

El departamento de Legal debe determinar si el incidente de datos personales se puede clasificar como una filtración de datos de conformidad con la ley o regulación aplicable. 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.

Paso cuatro: notificar a los organismos reguladores aplicables y a las personas afectadas, según sea necesario

La ley o regulación aplicable podría requerir la notificación a organismos reguladores específicos y/o a las personas afectadas sobre las filtraciones de datos que hayan sido confirmadas. Adicionalmente, los contratos con clientes o empleados pueden requerir que MetLife notifique a los clientes de un grupo o individuos no sólo sobre las filtraciones de datos que hayan sido confirmadas, sino también sobre los incidentes de datos personales que afectan al cliente/empleado.

El departamento Legal deberá determinar si las autoridades encargadas de hacer cumplir la ley deben ser notificadas sobre el incidente o filtracion. El departamento Legal también debe determinar los requisitos de notificación de MetLife según lo definido por la ley, regulación o contrato aplicable. En particular:

- Cuando se requiera una notificación regulatoria de algún incumplimiento relacionado con los datos, el departamento Legal y el departamento de Cumplimiento Local deberán notificar a los organismos reguladores apropiados dentro del plazo de tiempo y en los términos que establezca la ley o regulación aplicable.
- Cuando se requiera enviar alguna notificación al grupo afectado o a clientes individuales, la línea de negocio apropiada, en coordinación con el departamento Legal y Cumplimiento Local, deberá notificar a los clientes dentro del plazo de tiempo y en los términos que establezca la ley, regulación o contrato aplicable.

- Cuando se requiera enviar alguna notificación a los empleados afectados, el departamento de Recursos Humanos, en coordinación con el departamento Legal y Cumplimiento Local, deberá notificar a los empleados dentro del plazo de tiempo y en los términos que establezca la ley o regulación aplicable.

Paso cinco: notificar a la Oficina de Privacidad Corporativa de MetLife sobre los incidentes de datos personales significativos

El departamento de Cumplimiento Local deberá notificar a la Oficina de Privacidad Corporativa de MetLife (askprivacy@metlife.com) y al Especialista Regional de Privacidad adecuado sobre cualquier incidente significativo relacionado con datos personales, los cuales son incidentes de datos personales que: (i) afectan a más de 100 personas o registros; (ii) son causados por personas internas o externas malintencionadas (por ejemplo: un hacker); o (iii) se determinan como significativos de acuerdo con las leyes o regulaciones de privacidad aplicables, y/o el riesgo de daño sustancial a la Compañía o a clientes/ empleados individuales. La información personal en cuestión debe ser excluida al reportar incidentes con datos personales significativos a la Oficina de Privacidad Corporativa de MetLife y al Especialista Regional de Privacidad.

Paso seis: mantener la documentación relativa al incidente de datos personales

La línea de negocio y/o área funcional pertinente debe mantener registros (por ejemplo: correos electrónicos, correspondencia escrita, minutas y cartas de notificación) relacionados con la administración de todos los incidentes de datos personales de acuerdo con los requisitos de mantenimiento de registros de esta Política. ***Consulte* la Sección I.E: requisitos de mantenimiento de registros**. Los registros que deberán conservarse en virtud de esta Política incluyen documentación relacionada con: (i) la causa de origen del incidente de datos personales, incluyendo esfuerzos de contención; (ii) la descripción de los elementos de información personal involucrados en el incidente de datos personales; (iii) análisis de la necesidad de notificación regulatoria o individual y, en caso afirmativo, la carta/correspondencia de notificación pertinente; y (iv) medidas correctivas adoptadas para evitar que se produzcan nuevos incidentes con datos personales.

RESUMEN DE LAS FUNCIONES Y RESPONSABILIDADES CLAVE: ADMINISTRACIÓN DE INCIDENTES DE DATOS PERSONALES[7]

Funciones	Responsabilidades
Todos los empleados	Identificar y comunicar al departamento de Cumplimiento Local sobre todos los incidentes con datos personales de los que se tenga conocimiento o se sospeche. Mantener registros relacionados con la administración de todos los incidentes de datos personales de conformidad con esta Política.

[7] También se puede encontrar un resumen del flujo de trabajo de los requisitos de administración de incidentes de datos personales en el **Apéndice B** de esta Política.

Operaciones comerciales y funciones globales	Mantener y comunicar procedimientos para administrar y reportar incidentes de datos personales. Con el apoyo de la Dirección de Seguridad de Tecnología de la Información y/o seguridad corporativa global (cuando corresponda), determinar y solucionar la causa de origen de los incidentes con datos personales que han sido reportados, confirmar que los incidentes con datos personales han sido contenidos e identificar a los individuos afectados por cualquier incidente. En coordinación con el departamento Legal y Cumplimiento Local, notificar a los clientes individuales/grupales sobre incidentes con datos personales o filtraciones de datos, según lo requiera la ley, regulación o contrato aplicable.
Recursos Humanos	En coordinación con el departamento Legal y Cumplimiento Local, notificar a los empleados sobre incidentes con datos personales o filtraciones de datos, según lo requiera la ley o regulación aplicable.
Departmento Legal	Analizar los incidentes con datos personales para determinar si dichos incidentes se clasifican como filtración de datos de conformidad con la ley/ regulación aplicable y determinar los requisitos de notificación aplicables. Trabajar con el departamento de Cumplimiento Local para notificar a los organismos reguladores sobre las filtraciones de datos, según lo requiera la ley. Trabajar con la línea de negocio y/o área funcional pertinente con el fin de notificar a los clientes o empleados sobre incidentes con datos personales o filtraciones de datos, según lo requiera la ley, regulación o contrato aplicable.
Riesgo informático y seguridad y seguridad corporativa global	Trabajar con el área operativa/funcional pertinente a fin de investigar, contener y solucionar incidentes con datos personales.
Cumplimiento Local	Trabajar con el departamento Legal a fin de notificar a los organismos reguladores sobre las filtraciones de datos, según lo requiera la ley. Asesorar a la línea de negocio y/o área funcional pertinente a cerca de la notificación a los clientes o empleados sobre incidentes con datos personales

	o filtraciones de datos, según lo requiera la ley, regulación o contrato aplicable. Notificar a la Oficina de Privacidad Corporativa de MetLife sobre los incidentes con datos personales significativos, según se define en esta Política.

VII. EVALUACIONES DE IMPACTO EN LA PRIVACIDAD

A medida que MetLife se globaliza cada vez más y las tecnologías continúan evolucionando, es vital que la Compañía encuentre maneras de integrar la privacidad en la fase de diseño de **proyectos**. Las evaluaciones de impacto en la privacidad se han convertido en un componente esencial de los programas de cumplimiento de privacidad ya que ayudan en el enfoque de **privacidad por diseño**. Un proceso eficaz de evaluación de impacto en la privacidad permitirá que MetLife identifique y resuelva las posibles deficiencias de privacidad en la etapa inicial de un proyecto, reduciendo el riesgo de costos asociados y el daño a la reputación.

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.

La Oficina de Privacidad Corporativa de MetLife identificará las áreas en toda la Compañía que pudieran beneficiarse del proceso de evaluación de impacto en la privacidad (por ejemplo: análisis de datos de MetLife o equipos de desarrollo de aplicaciones móviles), independientemente de si la ley lo requiere o no. Una vez que se ha identificado, la Oficina de Privacidad Corporativa de MetLife trabajará con la línea de negocio y/o área funcional pertinente para implementar el proceso de evaluación de impacto en la privacidad, según lo aprobado por la Oficina de Privacidad Corporativa de MetLife.

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.

RESUMEN DE LAS FUNCIONES Y RESPONSABILIDADES CLAVE: 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

Al igual que otras empresas, MetLife puede adquirir compañías o vender unidades de negocio para innovar y mantener el ritmo en la economía actual. Sin embargo, al hacerlo, MetLife debe cumplir con sus promesas de privacidad y las promesas de privacidad hechas por cualquier compañía recién adquirida. En otras palabras, la compra de una compañía por otra compañía no anula las promesas de privacidad hechas a los individuos cuando se recopiló su información personal por primera vez. De acuerdo con las leyes de privacidad, las compañías generalmente tienen dos opciones cuando se produce una adquisición: (i) manejar la información personal como se prometió a los individuos cuando ésta fue recolectada por primera vez, o (ii) modificar sustancialmente la forma en que se recopila, utiliza o comparte la información personal, en algunos casos con el permiso de los individuos a quienes se hizo una promesa desde un principio.

Las fusiones y adquisiciones presentan inquietudes especiales en virtud de las leyes internacionales de privacidad. Una compañía adquirente que no realice una revisión de diligencia debida efectiva y exhaustiva en un objetivo de fusión o adquisición propuesto corre el riesgo de tener que rendir cuentas a las autoridades a causa de violaciones de privacidad que la compañía adquirida haya cometido en el pasado o en el presente. La Oficina de Privacidad Corporativa de MetLife estará involucrada desde la fase inicial en cualquier actividad de fusiones y adquisiciones. El departamento de Cumplimiento Local solicitará al equipo de fusiones y adquisiciones pertinente que involucren a la Oficina de Privacidad Corporativa de MetLife en cualquier actividad de fusiones y adquisiciones significativas y probables (relacionadas con el país y el nivel de riesgo de privacidad según lo determinado por el departamento de Cumplimiento) que a su vez incluirá a la Oficina de Privacidad Corporativa de MetLife en el equipo, según corresponda. Desarrollo Corporativo, Fusiones y Adquisiciones, la Oficina de Privacidad Corporativa de MetLife, Cumplimiento Local y el Departamento Legal definirán conjuntamente el alcance de la diligencia debida en privacidad.

El equipo de fusiones y adquisiciones pertinente deberá notificar inmediatamente a la Oficina de Privacidad Corporativa de MetLife si, como parte del proceso de diligencia debida, descubren cualquier violación a la privacidad que ocurrió previamente y/o cualquier control de privacidad inadecuado de negocios o entidades recién adquiridos que se han fusionado con MetLife.

A. DILIGENCIA DEBIDA

Los esfuerzos de diligencia debida de una empresa fusionante o adquirente, antes de la celebración de un acuerdo de fusión o de adquisición y en cualquier periodo de diligencia debida adicional antes del cierre de una transacción, deberán estructurarse razonablemente para saber si existe la posibilidad de que la empresa o división que será absorbida ha violado las leyes o regulaciones de privacidad aplicables. En circunstancias en las que MetLife tenga oportunidades limitadas para realizar la diligencia debida de manera rigurosa antes del cierre, MetLife tendrá que considerar si se puede proceder con la transacción dado el riesgo elevado y, si es así, deberá estar preparado para llevar a cabo un examen exhaustivo de las operaciones del objetivo inmediatamente después del cierre para detectar y corregir cualquier posible violación en privacidad y conductas de riesgo.

Las medidas de diligencia debida que deberán ser consideradas con especial atención incluyen, pero no se limitan a:

- Evaluaciones del perfil de riesgo de los países en los que la empresa que será absorbida o cualquiera de sus subsidiarias hacen negocios.
- Análisis del perfil de riesgo de la industria o actividad empresarial involucrada (por ejemplo: ¿la industria o actividad involucra datos estrictamente regulados y/o confidenciales?).

- Análisis de la dependencia que tiene el objetivo con terceros para llevar a cabo negocios y el grado en que dichos terceros requieren acceso a información personal.
- Revisiones de la experiencia previa de la empresa objetivo en lo referente a filtraciones de datos, si los hubiere, y cualquier demanda legal y/o investigaciones regulatorias.
- Revisiones de las políticas escritas, procedimientos, controles y materiales de capacitación escritos de la empresa objetivo relacionados con la seguridad y privacidad de la información, incluyendo la recopilación, uso y protección de la información personal.
- Revisiones de los informes de auditoría interna y de investigación interna a cargo de auditoría interna, seguridad corporativa o departamentos legales de la empresa objetivo, así como cualquier otro documento relacionado que el asesor legal externo de la empresa objetivo haya revisado.
- Entrevistas al personal de cumplimiento de alto nivel de la empresa objetivo o a proveedores para evaluar el programa de cumplimiento en privacidad de la empresa objetivo o de los proveedores e identificar cualquier problema de privacidad o de cumplimiento que pueda no ser evidente.
- Revisiones de los registros, informes y análisis preparados por los auditores de la empresa objetivo o del proveedor, si esto es factible.

B. DECLARACIONES Y GARANTÍAS

Al considerar una fusión o adquisición potencial, MetLife deberá buscar declaraciones y garantías apropiadas por parte del objetivo de la fusión o del proveedor que ofrezcan la confianza y seguridad de que la empresa objetivo o el proveedor no estén violando, ni hayan violado las leyes internacionales en privacidad, o, alternativamente, que hayan declarado de manera concluyente todas y cada una de estas violaciones. Si el objetivo de la fusión o proveedor no están dispuestos a proporcionar tal declaración, entonces se deberán establecer las razones con detalle, evaluarlas y, si es posible, investigarlas. Consulte con el departamento Legal o con un asesor legal externo sobre las disposiciones contractuales específicas que deben incluirse en cada transacción.

El que el objetivo de la fusión o el proveedor proporcionen una declaración de los activos en una adquisición en la que se niegue tener conocimiento de violaciones de privacidad, ya sean presentes o pasadas, es, sin duda, insuficiente para proteger a MetLife del riesgo de responsabilidades heredadas.

Atención

En el momento en que MetLife esté vendiendo alguna operación comercial (de manera total o parcial), la información personal del empleado o del cliente de MetLife no deberá proporcionarse a ningún comprador potencial antes de completar la venta sin la aprobación previa de la Oficina de Privacidad Corporativa de MetLife y del Departamento Legal.

X. DEFINICIONES

1. **Acceso** se refiere a la capacidad o los medios necesarios para leer, visualizar o utilizar cualquier recurso del sistema.

2. **Medidas administrativas de seguridad** incluyen políticas, procedimientos y controles de seguridad que MetLife adopta para garantizar que los empleados manejen y protejan adecuadamente la información personal.

3. **Dirección de negocio** se refiere colectivamente a la administración en las líneas de negocio y funciones globales de la primera línea.

4. **Recopilar o recopilación** significa obtener cualquier información personal de un individuo por cualquier medio, ya sea directo o indirecto.

5. **Compañía** incluye todas las compañías, sucursales, subsidiarias, empresas conjuntas e inversiones de capital privado de MetLife, en las MetLife tiene control administrativo.

6. **Consentimiento** se refiere al acuerdo por parte de un individuo para que la Compañía recopile, utilice, procese, retenga y divulgue la información personal para un propósito específico.

7. **Transferencia transfronteriza de datos** se refiere a la transmisión de información personal de un país a otro. En algunas jurisdicciones, esto no se limita a la transferencia física de datos a otro país, sino que también puede incluir la posibilidad de acceder a los datos de otro país.

8. **Mecanismos de transferencia de datos** se utilizan para transferir datos de manera legal fuera de las jurisdicciones en las que las leyes o regulaciones restringen la ubicación geográfica de los datos. Los mecanismos válidos de transferencia de datos están definidos por la ley o regulación aplicable y pueden incluir un acuerdo para la transferencia de datos con la parte que tendrá acceso a la información personal, notificación a la autoridad y/o aprobación por parte de la autoridad local encargada de la protección de datos de un país o consentimiento por parte del individuo cuyos datos deben ser transferidos.

9. **Empleados** incluye a todos los empleados, funcionarios y directores de MetLife en todo el mundo. No incluye a los miembros independientes de la junta directiva, tales como los miembros de la Junta de Fideicomisarios de los Fondos de MetLife que están cubiertos por el código de conducta y ética empresarial del Director.

10. **Contratación** se refiere a cualquier tipo de acuerdo, contrato, orden de compra o factura.

11. **Cifrado** se refiere al proceso en el que se cambia el texto sin formato a una forma ininteligible que requiere un mecanismo de descifrado (por ejemplo: una clave secreta o contraseña) para descifrar y acceder a la información. El cifrado se utiliza como medio para lograr la seguridad de los datos.

12. **Cumplimiento Local** se refiere a la función de Cumplimiento de cada operación en el país en el cual MetLife opera. Esto incluye a los equipos de Cumplimiento que apoyan las operaciones de MetLife que no pertenecen a Estados Unidos (incluyendo la administración regional y subregional), al equipo de Inversiones de Cumplimiento que apoya a la función de inversiones

globales y al equipo de Cumplimiento de Estados Unidos que apoya a las líneas de negocio de Estados Unidos.

13. **MetLife** incluye todas las compañías, sucursales, subsidiarias, empresas conjuntas e inversiones de capital privado de MetLife, en las que MetLife tiene control de la administración.

14. **Oficina de Privacidad Corporativa de MetLife** de Ética y Cumplimiento Corporativo tiene la supervisión central del programa global de cumplimiento en privacidad de MetLife.

15. **Información personal de MetLife**[8] incluye cualquier información que MetLife recopile u obtenga y que identifique o pueda identificar a un individuo, incluyendo a los clientes de MetLife (y a los grupos participantes), clientes potenciales, empleados, contratistas independientes, solicitantes de empleo, socios comerciales y otros terceros. El uso que MetLife le da a este término no pretende implicar la propiedad de la información personal.

16. **Operaciones** se refiere al negocio de MetLife en cada país en el cual MetLife opera. En ciertos países, incluyendo Estados Unidos, las líneas de negocio separadas y/o entidades reguladas por separado se pueden considerar como operaciones.

17. **Inclusión voluntaria** se refiere a un mecanismo de consentimiento en el que un individuo debe afirmar activamente que la información se puede divulgar de una manera específica o compartir con un tercero. La inclusión voluntaria es similar a obtener el consentimiento expreso por parte del individuo para utilizar la información de una manera específica.

18. **Exclusión voluntaria** se refiere a un mecanismo de consentimiento en el cual la información puede ser revelada de una manera específica o compartida con un tercero en ausencia de cualquier acción por parte de un individuo. La exclusión voluntaria es semejante a obtener el consentimiento implícito por parte del individuo para utilizar la información de una manera específica.

19. **Información personal**[9] se refiere a la información que se mantiene en formato electrónico o soporte físico y que sirve para identificar o por medio de la cual se puede identificar a una persona directa o indirectamente. Para obtener información adicional, ***consulte*** **la Sección I: perspectiva general**.

20. **Incidentes con datos personales** ocurren 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.

21. **Medidas físicas de seguridad** se refiere a políticas, procedimientos y controles de seguridad física (por ejemplo: cerraduras y códigos de acceso a edificios) para proteger los sistemas de información electrónicos de la Compañía y los edificios y equipos relacionados con los riesgos naturales y ambientales, así como la intrusión no autorizada.

[8] En Estados Unidos, la información personal de MetLife generalmente no incluye los términos y condiciones laborales de los empleados de MetLife (por ejemplo: información sobre compensaciones y beneficios). Consulte con el departamento Legal para obtener información adicional.

[9] Consulte el pie de página número 8.

22. **Privacidad por diseño** se refiere al concepto en el que cada nueva tecnología, sistema, servicio o proceso que utiliza información personal toma en cuenta la protección de dicha información durante la fase de diseño para garantizar que los controles de privacidad apropiados están integrados desde el inicio y durante el ciclo de vida del proyecto.

23. **Evaluaciones de impacto en la privacidad** se refiere a los procesos de evaluación que utilizan listas de control o herramientas diseñadas para identificar y evaluar los riesgos de privacidad a lo largo del ciclo de vida de desarrollo de un programa, sistema, producto u otro proyecto.

24. **Aviso de privacidad**, también conocido como aviso de información o declaración de privacidad, se refiere a la declaración que se hace a un individuo y que describe la manera en que la Compañía recopila, utiliza, conserva y divulga información personal.

25. **Procesamiento** de información personal se define en términos generales con el fin de incluir cualquier operación que se realiza en relación con la información personal; por ejemplo: visualizar, recopilar, almacenar, alterar, recuperar, utilizar, transferir, revelar, diseminar, bloquear, borrar o destruir.

26. **Proyectos** se refiere a cualquier sistema, servicio, tecnología, aplicación, acción administrativa, producto o iniciativa, cuando se utiliza en el contexto de evaluaciones de impacto en la privacidad.

27. **Información personal confidencial** se refiere a un subconjunto de información personal definido por la ley local que puede requerir restricciones adicionales de privacidad y seguridad para salvaguardar su recopilación, utilización y divulgación. Ejemplos de información personal confidencial, como se define en la legislación local, pueden incluir origen racial o étnico, información sobre la salud individual o médica, opiniones políticas y creencias religiosas o filosóficas.

28. **Medidas técnicas de seguridad** se refiere a las políticas, procedimientos y controles técnicos de seguridad (por ejemplo: sistemas de autenticación para acceder a datos o herramientas de cifrado) con el fin de proteger la información de la Compañía que es almacenada por medios electrónicos de pérdidas, usos, accesos o destrucción no autorizados.

29. **Terceros** se refiere a cualquier individuo (no empleado por MetLife) o entidad que la Compañía haya contratado (formal o informalmente) para representar a MetLife o actuar en nombre de MetLife o proporcionar productos o servicios a MetLife. Los terceros incluyen, pero no se limitan a los siguientes: proveedores de servicios, vendedores socios de empresas conjuntas, agentes, corredores, intermediarios, contratistas/subcontratistas y distribuidores.

30. **Web cookies**, cuando se utilizan en relación con computadoras u otros dispositivos electrónicos, se refieren a la información que un sitio web envía a la computadora/dispositivo de un usuario mientras el usuario visualiza el sitio web. Las cookies se pueden utilizar para registrar información sobre un usuario individual, como nombres, direcciones y contraseñas ingresadas en el sitio web o la actividad del individuo en el mismo.

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.

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.*

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 – Flujo de trabajo de respuesta a incidentes de datos personales ("IDP")