Política Corporativa

Protección de Datos Personales (Gestión Datos)

DOCUMENTO PÚBLICO
VERSIÓN 7.0

Área: Legal.

Departamento: Ética y Cumplimiento.

Subdepartamento: Oficina de Privacidad

Macroproceso: Ética y Cumplimiento

Proceso: Gestión de Privacidad

Fecha de publicación: 25/07/2025

NEW YORK LIFE SEGUROS MONTERREY

Contenido

1. Objetivo

Establecer los requerimientos y lineamientos mínimos necesarios para que todos los colaboradores traten y protejan los Datos de los que Seguros Monterrey New York Life (SMNYL) es Responsable, de forma adecuada y se garantice el cumplimiento con lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y mejores prácticas aplicables.

2. Alcance

Este documento es obligatorio y aplica a todo el personal que realice Tratamiento de Datos de SMNYL.

3. Área responsable

La **Oficina de Privacidad de la Dirección de Ética y Cumplimiento** es responsable de la elaboración, revisión, modificación y derogación de este documento.

4. Entrada en vigor

La entrada en vigor del presente documento será a partir del 05 de agosto de 2025.

5. Frecuencia de la revisión

Este documento debe ser revisado y, en caso necesario, actualizado a más tardar el 25 de julio de todos los años subsecuentes a su entrada en vigor.

Cualquier modificación extemporánea podrá solicitarse previo a la fecha de revisión bajo los lineamientos establecidos en el procedimiento corporativo: **"Creación, modificación y derogación de documentos controlados".**

6. Especificaciones

10.1 Principios y Deberes

Con apego a la regulación y de acuerdo con las necesidades del negocio, SMNYL cuenta con los lineamientos necesarios para gestionar la obtención, acceso, uso, divulgación, almacenamiento, bloqueo, y eliminación de Información, en conjunto Tratamiento de los Datos.

La regulación en materia de Protección de Datos Personales establece que todo Tratamiento de Datos debe llevarse con apego a los siguientes principios:

- **Licitud:** Para cumplir con este principio, el Tratamiento de los Datos debe ser conforme a lo establecido en el presente documento.

  Además de ello, todos los colaboradores deben apegarse a la normativa que en lo particular regule la(s) actividad(es) en la que se tratan los Datos involucrados en sus actividades diarias, por ejemplo: Código Fiscal, Código de Comercio, Ley de Instituciones de Seguros y de Fianzas (LISF), Circular Única de Seguros y de Fianzas (CUSF), e identificar si dicha normativa incluye disposiciones que se vinculen, de manera directa o indirecta, con la protección o el Tratamiento de Datos para poder actuar conforme a lo que establece la presente política.

  La obtención de Información debe ser lícita y en apego a lo establecido en esta política, los documentos relacionados y la regulación aplicable a sus actividades.

- **Consentimiento:** SMNYL únicamente puede tratar Datos con el consentimiento de los Titulares, el cual debe obtenerse previo a que el Titular comparta sus Datos con SMNYL a través de cualquier medio.

- **Finalidad:** Los Datos solo podrán ser tratados de acuerdo con las finalidades establecidas en el Aviso de Privacidad.

  Es responsabilidad de todos los colaboradores asegurarse que la(s) finalidad(es) con la(s) que están tratando los Datos para cumplir con sus tareas, están incluidas en el Aviso de Privacidad. En caso de dudas sobre si la(s) finalidad(es) por las que se tratan Datos están o no previstas en el Aviso de Privacidad, es necesario contactar a la Oficina de Privacidad de la Dirección de Ética y Cumplimiento para verificarlo.

- **Información:** Se debe dar a conocer al Titular la Información relativa a la existencia y características principales del Tratamiento al que se someterán sus Datos a través del Aviso de Privacidad.

  El Aviso de Privacidad debe darse a conocer a todos los proveedores (Encargados y Terceros que tengan una relación con SMNYL).

- **Proporcionalidad:** Tratar los menos Datos posibles, y sólo aquéllos que resulten necesarios, adecuados y relevantes con relación a las finalidades previstas en el Aviso de Privacidad.

  Por ejemplo: Si por algún proceso de la Compañía se requiere nombre y fecha de nacimiento de una base de Datos que usualmente contiene otros Datos adicionales, únicamente se deberán tratar el nombre y fecha para el proceso en particular, sin utilizar los otros Datos.

- **Calidad:** Este principio implica que todos los colaboradores que tratan Datos se aseguren de que son correctos y actualizados.

Este principio también va de la mano con la obligación de eliminar los Datos que ya no son indispensables y conservarla solo por el tiempo que es necesario. Si hay dudas sobre este punto debe consultarse la Política M17.P04.S00.004.A Mantenimiento y Retención de Registros.

- **Lealtad:** Debemos respetar la confianza que nuestros clientes y la de los otros Titulares que han depositado en SMNYL, respetando la expectativa razonable de privacidad y no usando medios engañosos o fraudulentos para recabar y/o tratar los datos, por ejemplo: Si se está trabajando en una aplicación con clientes, en esta únicamente se pedirán los Datos necesarios para prestar el servicio y no se pondrán algoritmos o funciones que recaben Datos sin que el cliente tenga conocimiento.

- **Responsabilidad:** No se podrá llevar a cabo Tratamiento para finalidades distintas que no resulten compatibles con aquéllas para las que hubiese recabado de origen los Datos. Y se deberá velar por el cumplimiento de los demás principios, establecer medidas de seguridad adecuadas y demostrar que se cumple con lo establecido en esta política durante el Tratamiento de los Datos.

  Además de actuar con apego a los principios antes mencionados, SMNYL y los colaboradores tienen la obligación de seguir el principio "necesidad de conocer" (need to know) al accesar o permitir el acceso a otros, esto significa que solo aquellas personas con una necesidad legitima de negocio deben tener acceso a Datos Personales, si un colaborador es dueño de cualquier Activo de Información que tenga Datos Personales es su responsabilidad velar porque se cumpla este principio.

10.2 Aviso de Privacidad

Publicación

El Aviso de Privacidad Integral de SMNYL debe estar publicado en todas las oficinas, módulos hospitalarios y todas las instalaciones en donde se recaben Datos.

De igual forma todos los Sitios Electrónicos públicos (aplicaciones, sistemas, portales, plataformas, perfiles de redes sociales y/o páginas públicas) deben dirigir a los Titulares al Portal Público, en donde podrán consultar el Aviso de Privacidad Integral, con la finalidad de que este a disposición de todos los Titulares.

Asimismo, durante los mensajes iniciales en el Call Center debe incluirse la referencia al Aviso de Privacidad, indicando que puede ser consultado en el portal público de SMNYL.

Responsables de la publicación

a) Aviso de Privacidad impreso

El área de Operaciones es responsable de garantizar la publicación del Aviso de Privacidad en las oficinas regionales y módulos hospitalarios.

El área de Seguridad Corporativa de la dirección de Recursos Humanos es responsable de la publicación del Aviso de Privacidad en las oficinas divisionales y de agencia.

Las áreas antes mencionadas deben proveer a la Oficina de Privacidad de la Dirección de Ética y Cumplimiento el layout de Listado de Instalaciones en donde este publicado el Aviso de Privacidad, así como, sus correspondientes actualizaciones en cuanto se abran o cierre alguna instalación. La Oficina de Privacidad de la Dirección de Ética y Cumplimiento es responsable de notificar a las áreas de Operaciones y Seguridad Corporativa de cualquier actualización en el Aviso de Privacidad.

b) Aviso de Privacidad digital

En caso de Sitios Electrónicos públicos es responsabilidad del propietario de dicha herramienta garantizar que se incluya la liga al Aviso de Privacidad en el portal público, así como, notificar a la Oficina de Privacidad de la Dirección de Ética y Cumplimiento utilizando el layout Listado de Sitios Electrónicos. La Oficina de Privacidad de la Dirección de Ética y Cumplimiento es propietaria y la única facultada para solicitar ajustes en la sección del Aviso de Privacidad en el portal público y la Intranet.

La Oficina de Privacidad de la Dirección de Ética y Cumplimiento cada dos años solicitará a los responsables la verificación del Listado de Instalaciones y Listado de Sitios Electrónicos para corroborar que se encuentre actualizado. Asimismo, la Oficina de Privacidad de la Dirección de Ética y Cumplimiento será quien los resguarde.

Actualización de Aviso de Privacidad

En caso de que algún colaborador identifique la necesidad de añadir algo al Aviso de Privacidad, como una finalidad de acuerdo con las actividades que lleva un área, debe comunicarlo a la Oficina de Privacidad de la Dirección de Ética y Cumplimiento para que se valore la situación y en su caso, se realice la modificación.

Si el Aviso de Privacidad sufre alguna modificación, la Oficina de Privacidad de la Dirección de Ética y Cumplimiento solicitará al área a cargo, apoyo para que el Aviso de Privacidad se actualice en las páginas, aplicaciones y/o portales de SMNYL. En el supuesto de que las modificaciones sean en el apartado de Finalidades, el Aviso de Privacidad debe darse a conocer no solo a los Titulares de los cuales se recabe Datos a partir de la modificación, incluso se podría requerir dar a conocer a aquellos Titulares de quién se recolectaron Datos antes de la modificación del Aviso de Privacidad si se pretenden utilizar sus Datos para las nuevas finalidades, así como contar con el consentimiento correspondiente. En caso de que se determine que sea necesario dar a conocer el Aviso de Privacidad en su momento se determinará el mecanismo de la publicación.

La Oficina de Privacidad de la Dirección de Ética y Cumplimiento lleva una bitácora con registro de las modificaciones al Avisos de Privacidad, fechas de últimas publicaciones y evidencia de estas a partir de la creación del Inventario.

Entrega

El Aviso de Privacidad debe ponerse a disposición de todos los Titulares de Datos en los diferentes escenarios en los que se recaben Datos, sin importar el medio o sistema por el cual se ha entablado contacto: Correo, teléfono, portal, etc. De igual forma, debe informarse que pueden encontrar la versión actualizada en la página https://www.mnyl.com.mx/aviso-de-privacidad.aspx

El propietario del Sitio Electrónico público que pueda recabar o tratar Datos, debe incluir un apartado para la aceptación del Aviso de Privacidad de SMNYL, que debe canalizarse directamente al apartado electrónico en la página de SMNYL https://www.mnyl.com.mx/aviso-de-privacidad.aspx y no al documento descargable. Es responsabilidad del propietario de la plataforma, asegurar que la plataforma tiene la capacidad de generar un listado de usuarios que aceptaron el Aviso de Privacidad de SMNYL.

Para el caso de Titulares en su calidad de prospectos o clientes de pólizas de seguro es responsabilidad del intermediario poner a disposición el Aviso de Privacidad de SMNYL y el suyo si aplica, a efecto de recabar constancia de dicha entrega, los distintos formatos utilizados para recabar Datos de Titulares deben contener una leyenda de Protección de Datos Personales que haga referencia a que el Aviso de Privacidad de SMNYL se puso a disposición del Titular, que éste declara conocerlo y sabe en dónde

consultar su actualización. La leyenda aplicable es proporcionada por la Oficina de Privacidad de la Dirección de Ética y Cumplimiento y no puede ser modificada o alterada por alguien más.

Aviso de Privacidad en correos electrónicos

Es responsabilidad de cada usuario que por sus funciones envíe o intercambie correos electrónicos directamente o por medio de aplicativos con cualquier Titular de Datos de incluir al pie del correo debajo de la firma institucional la leyenda de Aviso de Privacidad correspondiente que puedes localizar en documentos relacionados de esta política como Cláusulas y Leyendas.

Tipos de Avisos

La regulación prevé diferentes tipos de Aviso de Privacidad y SMNYL ha adoptado dos de ellas:

- **Aviso de Privacidad Integral:** Cumple con todos los elementos que señala la ley, mismos que de forma enunciativa más no limitativa son: Identidad y domicilio de SMNYL como responsable, Datos a recabar de los Titulares, finalidades de Tratamiento, mecanismos para que el Titular pueda manifestar su negativa para finalidades secundarias o accesorias, transferencias de Datos, medios para ejercer Derechos ARCO, medios para revocar consentimiento para el Tratamiento o limitar el uso o divulgación de sus Datos y comunicación de actualizaciones en el Aviso de Privacidad.

  El Aviso de Privacidad que SMNYL pone a disposición de los Titulares en oficinas, módulos hospitalarios, aplicación y página de internet, es Integral, ya que cuenta con todos los elementos mencionados anteriormente.

- **Aviso de Privacidad Corto:** Este tipo de Aviso es empleado cuando el espacio utilizado para la obtención de los Datos sea mínimo y limitado, de forma tal que la Información personal recabada o el espacio para la difusión o reproducción del Aviso de Privacidad también lo sean.

El Dueño de la Información/Proceso que recolecta los Datos es responsable de la publicación del Aviso de Privacidad que corresponda, previa confirmación del tipo de Aviso que debe utilizar con la Oficina de Privacidad de la Dirección de Ética y Cumplimiento.

Finalidades Primarias y Secundarias

El Aviso de Privacidad de SMNYL establece dos tipos de finalidades:

- **Finalidades Primarias:** Aquellas que dan origen y son necesarias para llevar a cabo y mantener la relación jurídica entre el Responsable y el Titular. Las que no cumplan con esta condición son las secundarias o accesorias.

- **Finalidades Secundarias:** No son indispensables para prestar el servicio contratado, pero en algunos casos permiten ofrecer o mejorar un servicio. Un ejemplo de finalidades secundarias es el utilizarlas con fines mercadotécnicos, de publicidad o promoción.

Previo a utilizar los Datos con fines mercadotécnicos, debe cumplirse con lo estipulado en el Instructivo Corporativo M17.P04.S01.035.D Gestión de Disposiciones en Materia de Registros ante CONDUSEF (REUS).

De requerir llevar a cabo alguna actividad que no entren en las finalidades plasmadas en el Aviso de Privacidad de SMNYL debe solicitarse a la Oficina de Privacidad de la Dirección de Ética y Cumplimiento un Aviso y/o Consentimiento con las finalidades requeridas y la justificación de llevarlo a cabo, por ejemplo, capturar un testimonial en video de un Cliente.

10.3 Clasificación de los Datos

La Compañía cuenta con un Estándar de Clasificación de la Información que considera cuatro categorías; Pública, Interna, Confidencial y Secreta; los Datos Personales usualmente entran en la categoría de Información Confidencial. A su vez la LFPDPPP clasifica los Datos en los siguientes grupos:

1. **Datos Personales:** Cualquier información concerniente a una persona física identificada o identificable. De manera enunciativa, más no limitativa se pueden mencionar:

- **Datos de identificación**: Nombre completo, estado civil, firma autógrafa y electrónica, fotografía, Registro Federal de Contribuyentes (RFC), Clave Única de Registro Poblacional (CURP), lugar y fecha de nacimiento, edad.
- **De contacto:** Dirección, número de teléfono, correo electrónico, número de teléfono celular.
- **Datos laborales:** Ocupación, nombre de la empresa o dependencia, puesto, área o departamento, domicilio, número de teléfono y correo electrónico, actividades extracurriculares, referencias laborales y referencias personales.
- **Datos de características físicas**: Género, color de cabello, señas particulares, estatura, peso, complexión, discapacidades.
- **Datos académicos:** Trayectoria educativa, escolaridad, títulos obtenidos, cédula profesional, certificados y reconocimientos.
- **Datos biométricos**: Huellas dactilares, retina, iris, patrones faciales, voz, firma, geometría de la mano, tipo de sangre.

2. **Datos Personales Sensibles**: Aquellos Datos que afecten a la esfera más íntima de su Titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, más no limitativa se pueden mencionar:

- **Raciales o étnicos:** Hábitos, costumbres, indumentaria, forma de vida, idioma, color de piel, raza.
- **Estado de salud:** Estado de salud, historial clínico, alergias, enfermedades, discapacidades, Información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis.
- **Información genética:** ADN, Información celular.
- **Afiliación sindical:** Si pertenece a algún sindicato, nombre del sindicato.
- **Vida sexual:** Preferencia sexual, hábitos sexuales.
- **Datos migratorios:** Nacionalidad, lugar de nacimiento, lugar de residencia, número de pasaporte, número de visa, estatus en el país (residente, turista, ciudadano.).
- **Procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales.**
- **Geolocalización.**

- **Creencias:** Religiosa, filosófica, moral y/o políticas.

3. **Datos Financieros y Patrimoniales**: De manera enunciativa, más no limitativa se pueden mencionar:

Información relacionada con títulos de propiedad y/o posesión sobre bienes muebles e inmuebles, historial crediticio, detalle sobre ingresos y egresos, Datos de identificación de cuentas bancarias pólizas de seguros contratadas, fondos de ahorro para el retiro, fianzas contratadas, Información fiscal, cualquier tipo de garantía otorgada, y servicios contratados, saldos bancarios, estados y/o número de cuenta, cuentas de inversión, buró de crédito, afores, sueldos y salarios, número de tarjeta bancaria de crédito y/o débito.

Además de las categorías estipuladas por la Ley, en la Compañía utilizamos una categoría adicional: **Datos Críticos**, utilizada para identificar y proteger algunos Datos, que no necesariamente por sí solos pudieran encuadrarse en la definición de Datos Personales, no obstante, por su naturaleza podrían ser aprovechados para ser comercializados de manera indebida, vendidos en volumen, intercambiados por un bien o servicio, por ser asociados a un grupo particular, por ejemplo, clientes o colaboradores, los **Datos Críticos** son: número telefónico y correo electrónico de clientes, número telefónico y correo electrónico personales de colaboradores, domicilios completos, cuenta CLABE, números de tarjetas de crédito o cuentas de redes sociales de clientes y colaboradores.

10.4 Consentimiento

El Consentimiento es un mecanismo para recabar la aceptación del Titular para el Tratamiento de los Datos. SMNYL no puede tratar los Datos sin el consentimiento previo de su Titular y este debe ir siempre ligado a las finalidades concretas para las cuales fueron recabados y que se establecen en el Aviso de Privacidad.

Tipos de Consentimientos

- **Tácito:** Es utilizado para cualquier Dato Personal, a excepción de los Datos Patrimoniales y Financieros y los Datos Personales Sensibles. El Consentimiento tácito se obtiene si el Titular no se niega a que sus Datos Personales sean tratados, después de haberle dado a conocer el Aviso de Privacidad.

- **Expreso:** Utilizado para cualquier tipo de Dato, con excepción de los Datos Personales Sensibles. Este tipo de Consentimiento debe expresarse de las siguientes maneras: Verbal, por escrito, por medios electrónicos, ópticos, signos inequívocos o cualquier otra tecnología.

- **Expreso y por escrito:** Se requiere para Tratamiento de Datos Personales Sensibles, se deberá otorgar por escrito, mediante firma autógrafa, huella dactilar, firma electrónica del Titular o cualquier otro mecanismo autorizado que permita identificarlo plenamente, el cual podrá ser físico o electrónico.

De quién se requiere el Consentimiento y cómo se recaba

SMNYL requiere el Consentimiento de todos los Titulares de los Datos que recabe y trate.

a) Colaboradores y candidatos:
Durante el proceso de reclutamiento, el área de Recursos Humanos es responsable de obtener el consentimiento del Titular, que contempla los siguientes elementos:

- El Titular declara conocer el Aviso de Privacidad de SMNYL.
- Otorga o niega su Consentimiento para que SMNYL trate sus Datos para finalidades secundarias que establece el Aviso de Privacidad.
- Acepta o niega la Transferencia de Datos conforme a lo que establece el Aviso de Privacidad de SMNYL.

En caso de que un colaborador o candidato no acepte las finalidades y/o transferencias del Aviso de Privacidad el responsable de Recursos Humanos debe notificar de inmediato a la Oficina de Privacidad de la Dirección de Ética y Cumplimiento.

b) Clientes y prospectos:
Como ya se mencionó en el apartado del Aviso de Privacidad, los formatos utilizados para recolectar la Información de los Clientes incluyen las leyendas referidas en los documentos Clausulas y Leyendas en las cuales además de la referencia del Aviso de Privacidad se incluye lenguaje relacionado al consentimiento, por lo que con la firma del documento se entiende que el clientes o prospecto otorga su consentimiento expreso y por escrito.

Para la línea de Negocio Individual se ha desarrollado un mecanismo para la recolección del Consentimiento para Finalidades Secundarias, las cuales se registran en el sistema de Tecnisys para mantener actualizada la base de aquellos Titulares que se hayan opuesto a estas.

Es indispensable que antes de contactar a algún Titular de Datos, se corrobore si ha negado su Consentimiento para ser contactado por finalidades distintas a Finalidades Primarias establecidas en el Aviso de Privacidad. Para más Información revisar el apartado de Fines Mercadotécnicos o Publicitarios de esta Política.

c) Proveedores y promotores:
De acuerdo con lo establecido en el artículo 5 del Reglamento de la Ley, las disposiciones del dicho reglamento no serán aplicables a la relativa a personas morales y personas físicas en su calidad de comerciantes y profesionistas.

d) Agentes:

Debe solicitarse el consentimiento a los Agentes de seguros, así como poner a su disposición el Aviso de Privacidad de Seguros Monterrey New York Life, lo anterior con la finalidad de garantizar la protección a todos sus Datos Personales Sensibles y demás Datos Personales que, atendiendo a la expectativa razonable de privacidad, La Compañía considere que deben ser protegidos por las implicaciones que pueden tener para los Titulares, la exposición de estos.

Adicionalmente, de conformidad con el Artículo 5 del Reglamento de la Ley, al tratarse de Datos Personales como nombre, imagen en eventos, datos de contacto, indicadores de producción de los Agentes, en su calidad de comerciantes, de acuerdo con el Código de Comercio, las disposiciones referentes a la protección de Datos Personales no serán aplicables a estos datos, no obstante, dicha excepción, todos los colaboradores responsables de esta, deberán procurar que no exista pérdida, destrucción no autorizada, robo, extravío, copia no autorizada, uso, acceso, tratamiento no autorizado, daño, alteración o modificación no autorizada sobre esta información.

e) Otros:
En los casos en que se proporcionen Datos Personales de terceros, como es el caso de los beneficiarios y cualquier otro que se identifique, debe recabarse la aceptación de la figura quien lo está dando sobre informar a los terceros que ha otorgado sus Datos Personales, las finalidades para las cuales los proporcionó y la confirmación de conocer como consultar el Aviso de Privacidad de SMNYL.

10.5. Derechos ARCO

Son los derechos que otorga la Ley a todos los Titulares para que accedan, rectifiquen, cancelen o se opongan al Tratamiento de sus Datos.

Quienes los pueden Solicitar

La Ley confiere a todos los Titulares de Datos la facultad de ejercer sus derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).

Cómo se atienden

SMNYL como Responsable del Tratamiento de Datos, cuenta con el Procedimiento M17.P04.S01.004. B Atención de Derechos ARCO (sistema ARCO) para la recepción y atención de estos derechos, así como solicitudes de negativa o limitación de Tratamiento que se reciban por parte de los diferentes Titulares de Datos.

Limitación del uso y/o divulgación de Datos

Los Titulares pueden negarse o limitar el Tratamiento de sus Datos de acuerdo como lo establece el Aviso de Privacidad, en cuyo caso el procedimiento para atenderlo está estipulado en el Procedimiento Atención de Derechos ARCO (sistema ARCO).

10.5.1 Solicitud de Información

En ocasiones los Titulares solicitan a la Compañía Información relacionada con su póliza y/o documentación previamente entregada, no se deberá interpretar que el Titular está ejerciendo el Derecho de Acceso o cualquier otro Derecho ARCO si el Titular no es expreso en solicitarlo, en ninguna circunstancia debe sugerirse los Derechos ARCO como opción para allegarse de Información.

Toda solicitud de Información debe ser atendida de acuerdo con la Política M05.P05.S00.005.A Centro de Contacto del área de Operaciones.

10.6 Atención de Quejas de Datos Personales

En caso de que SMNYL reciba una Queja relacionada al Tratamiento de Datos, esta queja debe ser registrada conforme a lo establecido en el instructivo M05.P05.S01.035.D Atención de Quejas del área de Operaciones, en el cual se prevé lo siguiente:

- Verificar que la identidad del quejoso coincida con la del Titular de los Datos que señala han recibido un Tratamiento inadecuado o bien, que se trata del tutor o representante que, de ser el caso, debe acreditar su facultad con documento legal, por ejemplo: poder notarial.

- En caso de que el Ejecutivo de Servicio tenga dudas sobre cómo responder la queja sobre Tratamiento de Datos, podrá consultar a la Oficina de Privacidad de la Dirección de Ética y Cumplimiento.
- Solamente se podrá utilizar la categoría de queja "Datos Personales" en aquellos casos donde la persona exprese claramente una inconformidad relacionada con el Tratamiento de sus Datos.

Nota: En caso de que el cliente no esté realizando una queja y se trate de una duda sobre el Tratamiento de sus Datos, se solicitará al cliente que envíe su duda vía correo electrónico a d_arco@mnyl.com.mx.

10.7 Fines Mercadotécnicos o Publicitarios (publicidad, promoción y de acuerdo con lo definido por CONDUSEF en REUS)

Línea de negocio de Individual

Para la línea de negocio de Individual se ha homologado en distintos formatos la leyenda relativa a la protección de Datos Personales, en dicha leyenda se encuentra implícito el consentimiento de los Titulares para Fines mercadotécnicos o publicitarios, dicha elección se encontrará predeterminada de forma afirmativa en el sistema correspondiente y únicamente se realizará el cambio a negativa en los casos en que el Titular así lo manifieste expresamente, esta preferencia debe ser verificada previo a cualquier actividad de Publicidad, Promoción y Telemarketing, de igual forma, el Aviso de Privacidad indica el proceso para que un cliente pueda indicar o renovar sus preferencias para Fines mercadotécnicos o publicitarios a través del formato de "Preferencias de Publicidad".

Similar al REUS, SMNYL lleva registro de los clientes que expresaron su deseo de no recibir Publicidad, Promoción y Telemarketing, la cual tiene una vigencia de dos años contados a partir de la fecha en que se indicó la negativa de acuerdo con los siguientes tiempos: si la solicitud fue recibida entre el día primero y el día quince del mes, ésta surtirá efectos el día uno del mes inmediato siguiente y si la solicitud fue recibida entre el día dieciséis y el día último del mes, surtirá efectos el día dieciséis del mes inmediato siguiente, en caso de que el día de inicio de vigencia sea un día inhábil comenzara el día hábil inmediato siguiente.

Línea de Negocio de Grupo y Colectivo

Para la línea de Grupo y Colectivo por decisión de negocio no se podrán utilizar los datos para Fines mercadotécnicos o publicitarios.

En caso de cualquier otro Titular de Datos debe consultarse a la Oficina de Privacidad de la Dirección de Ética y Cumplimiento antes de hacer cualquier actividad de Fines mercadotécnicos o publicitarios.

Previo a realizar cualquier actividad de Publicidad, Promoción y Telemarketing debe cumplirse con lo estipulado en el Instructivo Corporativo M17.P04.S01.035.D Gestión de Disposiciones en Materia de Registros ante CONDUSEF (REUS).

10.7.1 Disposiciones en Materia de Registros ante CONDUSEF

De conformidad con las Disposiciones en Materia de Registros ante CONDUSEF, la Compañía debe rendir reportes de manera mensual y quincenal referentes a:

- Datos de personas que no hayan aceptado que los mismos sean utilizados para Fines Publicitarios o Mercadotécnicos.
- Datos de terceros contratados para realizar actividades Publicitarias o Mercadotécnicas.

- Datos de personas a quienes se les realizará Publicidad o Mercadotecnia de forma personalizada.

Las actividades contempladas en dichas Disposiciones se encontrarán a cargo de la Oficina de Privacidad de la Dirección de Ética y Cumplimiento, para este fin se ha desarrollado el Instructivo Corporativo M17.P04.S01.035.D Gestión de Disposiciones en Materia de Registros ante CONDUSEF (REUS).

10.8 Ciclo de Vida de los Datos Personales

Creación u obtención

Representa el primer paso en el ciclo de vida de los Datos, debe garantizarse cualquier nuevo proceso o cambio a los existentes, que impliquen la obtención de Datos sea con apego a todos los Principios que establece la Ley y previamente determinar que:

- La finalidad por la que están siendo requeridos se encuentra incluida en el Aviso de Privacidad.
- Determinar el tipo de Consentimiento que se requiere del Titular y la forma en que se obtendrá.
- Poner a disposición del Titular el Aviso de Privacidad correspondiente.

Uso

Una vez que SMNYL obtiene los Datos indispensables y mínimos para cumplir con las finalidades de tratamiento, debe dar un uso adecuado y tratarlos conforme a lo que establece el Aviso de Privacidad.

Es importante que para el uso de los Datos se contemple:

- **Documentación:** Todos aquellos procesos de negocio que impliquen el Tratamiento de Datos deben estar documentados en una política, procedimiento, instructivo, manual o cualquier otro documento indicado por el área de Políticas y Procedimientos de la Dirección Ejecutiva de Riesgos, Control Interno y Seguridad de la Información, la documentación apropiada se hace señalando los Activos de Información que contengan los Datos en el documento, salvo contadas excepciones que el Dueño de la Información/Proceso debe verificar con la Oficina de Privacidad de la Dirección de Ética y Cumplimiento podrá haber tratamiento de Datos que no esté formalmente documentado, no obstante debe cumplirse con todos los requisitos estipulados en la presente política.

  Es responsabilidad del Dueño de la Información/Proceso asegurarse de que esto suceda, ya que no podrá llevarse a cabo ningún Tratamiento si no está documentado.

- **Trazabilidad de los Datos:** Los Dueños de la Información/Procesos que utilicen Datos Personales deberán tener la capacidad de seguir el rastro de estos, desde su punto de origen hasta el destino final dentro de su proceso, teniendo claro todo el tránsito que tengan los Datos, ya sea en Activos de Información o sistema/aplicativos.

- **Clasificación y Etiquetado de Información:** Una medida de seguridad durante el Tratamiento de los Datos es el etiquetado de la Información, ya que, desde que un documento nace puede ser etiquetado y clasificado, permitiendo su rastreo durante el Tratamiento e impide que haya accesos no autorizados. Para más Información consultar los estándares de Seguridad de la Información.

- **Desarrollo o mejoras tecnológica que implique el Tratamiento de Datos:** Toda iniciativa, ya sea mejora o nuevo proyecto de sistemas, aplicativos, portales o cualquier otra herramienta tecnológica que implique Tratamiento de Datos, debe cumplir con el llenado del documento relacionado Checklist Proyectos con Datos Personales y es responsabilidad del Owner de la iniciativa,

así como del Scrum Master encargado del proyecto garantizar que dicho análisis sea realizado y obtener el Vo.Bo. de la Oficina de Privacidad de la Dirección de Ética y Cumplimiento, el análisis deberá desarrollar que Datos usarán, su finalidad o finalidades, si tendrá conexión con otro sistema o aplicativo, quiénes tendrán acceso, si el servicio lo prestará un proveedor debe asegurarse de que se cumplan las medidas mínimas necesarias para su protección, por cuánto tiempo se conservan los Datos, y actividades de depuración según la Política M17.P04.S00.004.A Mantenimiento y Retención de Registros.

- **Ambientes de desarrollo y/o pruebas:** De manera general no se deben utilizarse Datos reales o productivos en ambientes de desarrollo y/o pruebas, lo anterior en cumplimiento a los estándares de Seguridad de la Información, para conocer con mayor detalle la forma apropiada de Ofuscado de los Datos consultar las políticas, procedimientos e instructivos de la Dirección de Tecnología de la Información. En caso de por alguna razón no sea factible desarrollar o probar sin los Datos reales o productivos debe documentarse una autorización especial a las Políticas de Seguridad de la Información, obteniendo el Vo.Bo. del Oficial de Privacidad.

- **Habilitación de Herramientas Corporativas:** Previo a habilitar cualquier Herramienta Corporativa que permita el Tratamiento de Datos, el área de Tecnología de la Información debe analizar y entender los alcances, atributos y usos de la misma, de manera que los riesgos a la protección de Datos sean identificados, así como las capacidades de depuración, conservación, etiquetado, por mencionar algunas, sean entendidas y configuradas de acuerdo con lo estipulado en esta política, la política de Mantenimiento y Retención de Registros y los estándares de Seguridad de la Información aplicables.

- **Herramientas No Corporativas para la explotación o análisis de Datos:** Previo a utilizar Herramientas No Corporativas para la explotación o análisis, creación de contenido o cualquier otro propósito que implique el uso de Datos (por ejemplo herramientas de inteligencia artificial) debe evaluarse si no existe una Herramienta Corporativa que cumpla con dicha necesidad, en su defecto, previo a utilizar la Herramienta No Corporativa se debe consultar y seguir las recomendaciones de las áreas de Tecnología de la Información, Seguridad de la Información y la Oficina de Privacidad de la Dirección de Ética y Cumplimiento.

Divulgación

Solo los Dueños de la Información/Proceso tienen la facultad de divulgar o autorizar Datos a terceros a través de los mecanismos y procesos autorizados y apropiados, tales como:

1. Para aprobar el acceso a sistemas, aplicativos, portales o cualquier otra herramienta tecnológica que implique el Tratamiento de Datos, así como;

2. La Extracción de Información de los Sistemas Automatizados de Tratamiento de Información (SATI), se recomienda que el tratamiento de los Datos se realice dentro de los SATIs que la Compañía ha desarrollado o implementado para ello, pues se consideran un entorno seguro y monitoreado, sin embargo, se reconoce que existen necesidades de negocio y/o regulatorias, que demandan la extracción de Información de dichos SATIs.

Tanto para la aprobación de acceso a sistemas, aplicativos, portales o cualquier otra herramienta que implique el Tratamiento de Datos, así como para extracción de Datos fuera de los SATIs deben atenderse los siguientes lineamientos:

- No debe contener Datos que no se justifiquen por el propósito especifico de negocio que se solicitó la Información, siguiendo el Criterio de Minimización.

- No debe aprobarse ningún reporte si la Información pretende ser compartida con algún tercero, colaborador, proveedor o cualquier otra persona que no tenga necesidad de conocerla, principio Need To Know establecido en el Código de Conducta de SMNYL.

Adicionalmente, solo para la Extracción de Información de los SATIs se aplican los siguientes lineamientos:

- La Información debe atender solo un propósito específico de negocio, esto significa que una base de datos utilizada para cumplir con el requerimiento "A" no debe ser reciclada o reutilizada para otro propósito diferente de la inicial, requerimiento "B".
- El dueño del proceso que origina la necesidad de extraer la Información se convertirá en el Dueño de la Información/Proceso y con ello, adquirirá las responsabilidades de dicha función.
- Si por necesidades de negocio o regulatorias la Información debe salir de la infraestructura de la Compañía deben seguirse todos los lineamientos y recomendaciones estipulados en la presente política y los de Seguridad de la Información, que sean aplicables, principalmente al decidir el mecanismo más seguro para compartir la Información, para mejor referencia consultar el instructivo M21.P02.S01.002.D Estándar de Clasificación de la Información.
- Por regla general, la Información extraída de los sistemas de tratamiento debe ser eliminada inmediatamente después de que haya cumplido el propósito de negocio por el cual se extrajo del SATI, en caso de que el resguardo sea exigido por alguna regulación o política, este debe ser controlado, seguro y documentado en políticas y/o procedimientos del área responsable.
- Todo tratamiento de Información con Datos fuera de los SATIs que sea recurrente, debe estar documentado en las políticas, procedimientos, instructivos, manuales o cualquier otro documento indicado por el área de Políticas y Procedimientos de la Dirección Ejecutiva de Riesgos, Control Interno y Seguridad de la Información, donde se aprecie el ciclo de tratamiento desde la obtención de la Información, su aprovechamiento, propósito, método y ruta de resguardo, así como el proceso de destrucción.
- Todos los dueños de procesos que requieran el tratamiento de Información con Datos fuera de los SATIs, deben evaluar continuamente su forma de operación para determinar si existen nuevas formas de procesamiento de la Información, de manera que no se requiera extraer de los SATIs.
- Los Especialistas de Soporte y Mantenimiento de aplicaciones u otras áreas, que, por sus funciones y responsabilidades formalizadas, sólo participen como intermediario entre el SATI y el dueño del proceso, que requieren la Información con Datos, no deben resguardar la Información una vez que haya sido entregada al Dueño de la Información/Proceso.
- Todos los usuarios que gestionen extracciones de Información de los SATIs, a través de la Mesa de Ayuda (911), deben seguir lo estipulado en el instructivo: M17.P04.S01.005.D Extracción de Información de los Sistemas Automatizados de Tratamiento de Información.

Mecanismo o herramientas apropiadas para compartir Datos: En todo momento se deben utilizar herramientas corporativas provistas por SMNYL para compartir Datos tanto de forma interna (colaboradores), como con externos (proveedores o terceros).

Al momento de decidir la mejor herramienta para compartir los Datos se deben tomar en consideración la frecuencia en que se compartirá la Información y el volumen de esta, usualmente servirá el Correo Electrónico Corporativo o la aplicación en turno que la compañía haya definido para

colaborar, por ejemplo; SFTP, (Internos o externos) o File Shares (Internos), a continuación, algunas sugerencias de uso:

Frecuencia	Volumen	Ejemplo	Herramienta recomendada
Por única ocasión	Datos de un solo titular	Respuesta de un trámite a un cliente	Correo Electrónico Corporativo
Por única ocasión	Base de datos con 2000 nombres y domicilios	proveedor que hará envío de reconocimientos a colaboradores	Correo Electrónico Corporativo
Varias ocasiones en un tiempo determinado	Archivos con alrededor de 10 mil registros con Información fiscal	proveedor que está desarrollando la nueva versión de timbrado de facturas	SFTP
Varias ocasiones en un tiempo determinado	Bases de datos con todas las pólizas emitidas y pagadas en 2020	Proceso de Auditoría Interna	File Shares o SFTP
Diaria	Todo el vigor de clientes de Grupo y Colectivo, así como de individual.	proveedor de asistencias para que consulte el estatus de las pólizas y pueda prestar los servicios aplicables	Solución a la medida, revisada por Tecnologías de la Información, Seguridad de la Información y la Oficina de Privacidad de la Dirección de Ética y Cumplimiento de la Dirección de Ética y Cumplimiento.

Como en el caso del último ejemplo, habrá escenarios que requieran una solución a la medida de forma que el Correo Electrónico Corporativo o SFTP no sean idóneos para compartir la Información, para dichas necesidades específicas, es responsabilidad del Dueño de la Información/Proceso buscar la asesoría y/o aprobación según corresponda de las áreas de Tecnología de la Información, Seguridad de la Información y la Oficina de Privacidad de la Dirección de Ética y Cumplimiento.

Adicionalmente se deben considerar las medidas estipuladas en los estándares aplicables de Seguridad de la Información, como lo es el cifrado adicional de correo electrónico o la protección de archivos con contraseña, según corresponda.

Queda estrictamente prohibido compartir Datos por mecanismos de comunicación no autorizados por SMNYL, por ejemplo: WhatsApp o cuentas de correo electrónico personales (Hotmail, Yahoo, Gmail, por mencionar algunos).

Almacenamiento

Queda estrictamente prohibido almacenar Datos en un Repositorio Corporativo Personal, es responsabilidad del Dueño de la Información/Proceso habilitar y señalar el Repositorio Corporativo de Proceso apto para el almacenamiento de Datos. Para más Información consultar el instructivo M21.P02.S01.006.D Estándar de Repositorio de Información de Seguridad de la Información.

En ningún caso deben almacenarse Datos en repositorios físicos o electrónicos que no tengan una medida de control de acceso como pueden ser llaves, candados, usuarios y contraseñas o cualquier otro mecanismo aprobado por SMNYL que impida el acceso libre a cualquier persona no autorizada para Tratar los Datos.

En ningún caso se podrán utilizar dispositivos móviles, unidades de almacenamiento extraíble o servicios de almacenamiento públicos o privados no autorizados por SMNYL

Bloqueo

Aquellos Datos asociados a un Activo de Información que hayan cumplido la finalidad para la cual fueron recabados deben entrar en una etapa de Bloqueo, durante dicho periodo, los Datos no podrán ser objeto de Tratamiento; usualmente las finalidades se cumplen cuando el contrato celebrado con el Titular llega a su fin, por ejemplo, en el caso de una póliza de seguros, cuando esta se cancela o indemniza, para el caso de Colaboradores, cuando su contrato se termina o rescinde; en ambos ejemplos se puede decir que no hay más obligaciones que cumplir para con el Titular, a partir de ese momento los Datos deben entrar en su etapa de Bloqueo, de forma que no estén disponibles para consulta, modificación, uso, explotación, divulgación, copia o cualquier otro Tratamiento sin la previa aprobación del Oficial de Privacidad. Una vez terminado el plazo estipulado en el Esquema de Retención de Registros deben ser eliminados definitivamente.

Aquellos Datos que no necesariamente estén asociados a un Activo de Información deben ser eliminados en cuanto hayan cumplido su finalidad, sin necesidad de entrar en una etapa de Bloqueo, por ejemplo: base de datos que sirvió para una investigación de una queja la cual ya fue concluida y en caso de ser necesaria la misma Información podría generarse a raíz del Activo de Información origen.

Es responsabilidad del Dueño de la Información/Proceso garantizar que los Datos a su cargo, se encuentran considerados en los proyectos de depuración automatizada gestionados por la Oficina de Privacidad de la Dirección de Ética y Cumplimiento, en caso contrario, desarrollar acciones para que aquellos Datos que lo ameriten entren en etapa de Bloqueo.

Depuración (Supresión/Cancelación)

SMNYL cuenta con una política y Programa de Mantenimiento y Retención De Registros (MRR), la cual establece los requerimientos y lineamientos mínimos necesarios para la gestión del ciclo de vida (creación u obtención, uso, divulgación, almacenamiento, bloqueo y depuración) de todos los Registros y No Registros de la Compañía, para poder cumplir con las necesidades de negocio, facilitar el acceso a la Información y garantizar el cumplimiento en cuanto a conservación y eliminación estipulados en las de las leyes y normativas correspondientes. Asimismo, proporcionar prácticas consistentes de administración de Registros en toda la Compañía.

Los Registros deben administrarse, conservarse y eliminarse adecuadamente conforme al Esquema de Retención de Registros. Deben almacenarse o respaldarse en repositorios oficiales de la Compañía para cumplir con los requisitos de retención, recuperación y respaldo, conforme a lo establecido en el instructivo M21.P02.S01.006.D Estándar de Repositorios de Información del área de Seguridad de la Información.

Por lo tanto, la política y Programa de MRR establecen los lineamientos para que la Compañía:

- Preserve todos los Registros y No Registros necesarios y requeridos y

- Elimine todos los Registros y No Registros innecesarios y obsoletos.

Para la ejecución del Programa de MRR y la eliminación de Registros y no Registros de manera correcta debes llevar a cabo lo establecido en la Política M17.P04.S00.004.A Mantenimiento y Retención de Registros y en el procedimiento M17.P04.S01.024.B Ejercicio de Depuración de Información.

Dentro del Programa de MRR de SMNYL se estipulan las formas y periodos de retención en que los Activos de Información, incluidos aquellos que contienen Datos, deben ser conservados y llegado el plazo, depurados.

SMNYL busca automatizar la depuración de los Activos de Información con Datos, es responsabilidad del Dueño de la Información/Proceso garantizar que los Activos de Información con Datos estén considerados en el proyecto de depuración automatizada y en caso contrario, desarrollar acciones para que aquellos Datos que lo ameriten sean depurados (suprimidos o cancelados) cumpliendo con los procesos apropiados para eliminar los Datos dependiendo del medio en el que se encuentren, para mayor Información consultar la Guía para el borrado seguro de Información digital del área de Seguridad de la Información.

10.8.1. Envío de Información fuera de la infraestructura tecnológica de la Compañía

Si un colaborador por sus funciones y puesto requiere enviar Información que contenga Datos fuera de la Compañía, por ejemplo: Con agentes, promotores, autoridades o proveedores (Encargados), debe seguir los Estándares de Seguridad de la Información, el Procedimiento para Compartir Información con externos del área de TI, los requisitos estipulados en el instructivo M17.P04.S01.005.D Extracción de Información de los Sistemas Automatizados de Tratamiento de Información y verificar que cumple con al menos los siguientes elementos:

- Que existe una finalidad real y sustentada para ello.
- La actividad que realiza está prevista en alguna política, procedimiento, manual o instructivo que especifique el Tratamiento de los Datos (qué Datos usa, su finalidad, si se comparte, a quién, medio por el cual se hace, lugar de almacenamiento, tiempo de conservación, etc.).
- Con el fin de evitar fuga de Información se debe verificar destinatario(s), contenido y designación (por ejemplo, en el correo electrónico, CC o con copia, CCO o con copia oculta).
- Revisar que la Información o documentación enviada es únicamente la solicitada.
- Los mensajes y la Información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo de sus labores.
- En ninguna circunstancia, salvo excepciones documentadas aprobadas por la Oficina de Privacidad de la Dirección de Ética y Cumplimiento, puede enviarse Información de la Compañía no publica a cuentas de correo propias (@gmail, @hotmail, @yahoo, etc.).
- Si el correo o cualquier otro mecanismo donde se intentó enviar los Datos fue bloqueado o se presenta alguna dificultad con él, debe levantarse un reporte a Servicios 911 o en el aplicativo Service Now https://smnyl.service-now.com/sp, seleccionado las siguientes opciones: Hacer una solicitud-> Compartir Información con Externos.

Si la Oficina de Privacidad de la Dirección de Ética y Cumplimiento identifica que la información adjunta en el reporte es inconsistente o incompleta, rechazará el requerimiento, en caso contrario, procede a aprobarlo.

Adicional a los puntos anteriores, deben considerarse los siguientes requisitos según la persona con quién se compartan los Datos:

Clientes

La comunicación de Datos con clientes únicamente puede hacerse por parte de las áreas facultadas para ello y utilizando los canales oficiales para dicho fin. Es importante que dichas áreas cuenten con los medios de autenticación necesarios para validar la personalidad del solicitante, independientemente de si se comunicaron de forma presencial o por otra vía, como correo electrónico o teléfono.

El colaborador del área facultada debe cerciorarse de que se trata del Titular de los Datos o bien, su Representante legal, el cual deberá acompañar cualquier solicitud de Datos con su identificación e instrumento legal que avale su facultad de representación, por ejemplo: un Poder para pleitos y cobranzas, actos de administración, dominio, carta poder firmada por dos testigos, etc. o en su caso un poder especial para el trámite en específico.

Para entregar cualquier documento, se debe tener certeza de que sea la persona correcta para recibir cualquier Información y/o documentación que te solicite. Debe acreditar su personalidad en caso de ser representante legal y acompañarlo de su identificación oficial.

Agentes o Promotores

En el caso en que un promotor o asesor, requiera documentación o Información de un cliente, debe adjuntar el escrito del Cliente, el cual debe contener el detalle de la Información o documentación requerida, el medio por el cual el Cliente desea recibir dicha Información o documentación para que se envíe a ese medio, o en su defecto, establecer que se le ha facultado al agente o promotor para tal acción y recepción de la Información, debe entregarse el escrito del Titular con su firma, así como adjuntar copia de su identificación oficial.

Autoridad

Ante requerimiento de autoridades que impliquen la solicitud de entregar Datos Personales debe atenderse todo lo estipulado en esta política, destacando el seguir en todo momento el Criterio de Minimización.

Si se trata de un requerimiento del INAI, la Oficina de Privacidad de la Dirección de Ética y Cumplimiento es la única facultada para atender y dar respuesta a dicho requerimiento, por lo que, en caso de que se identifique que el requerimiento viene de esta autoridad, debe ser canalizado inmediatamente, no obstante, el resto de las áreas tienen la obligación de proveer y cooperar con la Oficina de Privacidad de la Dirección de Ética y Cumplimiento para la atención del requerimiento.

10.9 Figuras que desempeña SMNYL en el Tratamiento de Datos Personales

10.9.1 Relación con proveedores (Encargados)

Toda área de SMNYL que trabaje con un proveedor en calidad de Encargado del Tratamiento de Datos de cualquier Titular (cliente, colaborador, etc.); tiene la obligación de verificar que dicho Encargado cumple con los elementos que se señalan a continuación.

Antes de iniciar la relación

Las áreas de SMNYL que están por iniciar una relación con algún proveedor (Encargado) que tratará Datos, además de apegarse a los procedimientos relativos a la selección y contratación, deben contemplar y seguir con lo siguiente, según aplique:

- Asegurarse que el proveedor (Encargado) y el Tratamiento que dará a los Datos cumpla con lo establecido en esta Política.
- Hay que confirmar que el contrato u orden de compra contenga una cláusula de Protección de Datos Personales que señale como Encargados a los proveedores de SMNYL, siendo este último el único *Responsable del Tratamiento de los Datos de los Titulares.

  *A menos que en conjunto que con la Oficina de Privacidad se determine lo contrario.

- Asegurarse de que el proveedor (Encargado) tenga acceso sólo a la Información estrictamente indispensable para el servicio que se le ha contratado.
- Corroborar que el proveedor (Encargado) cuente con un Programa de Protección de Datos.
- El proveedor (Encargado) debe contar con mecanismo para identificar y atender, así como, notificar Vulneraciones de Datos a SMNYL.
- Si el proveedor (Encargado) emplea medios electrónicos como plataformas o sistemas para el Tratamiento de los Datos, el Dueño de la Información/Proceso debe cerciorarse de que esta herramienta electrónica es segura. Para este punto podrán apoyarse con las áreas de Tecnología de Información y Seguridad de la Información de SMNYL.
- En los casos en los que el proveedor (Encargado) entable comunicación directa con los clientes de SMNYL, se debe generar un Script de comunicación creado por el Dueño de la Información/Proceso y validado con la Oficina de Privacidad de la Dirección de Ética y Cumplimiento.
- Se faculte a SMNYL para llevar a cabo auditorías para verificar cumplimiento con la regulación, incluyendo la facultad de solicitar Información precisa respecto de dónde, cuándo y quién ha almacenado o procesado los Datos (dentro de los recursos propios del proveedor (Encargado) o de la cadena de subcontrataciones).

Durante la Relación

- El proveedor no puede poner a disposición de los Titulares un Aviso de Privacidad distinto al de SMNYL.
- En caso de que el proveedor tenga acceso a Datos, El Dueño de la Información/Proceso debe asegurarse de que el proveedor (Encargado) imparta capacitación a sus colaboradores para el adecuado Tratamiento de los Datos y en apego a lo establecido por SMNYL.

- Asegurarse de que el proveedor que tiene comunicación directa con los clientes de SMNYL, utilice el Script de comunicación.
- Enfatizar con el Encargado que, en caso de recibir solicitudes de Derechos ARCO respecto a Información de SMMYL, debe canalizar al Titular de los Datos que haya ejercido sus Derechos, con SMNYL de acuerdo con el Aviso de Privacidad de la Compañía.
- El Dueño de la Información/Proceso que entable relación con un proveedor (Encargado), debe corroborar que el flujo de los Datos por parte del proveedor empate con el procedimiento establecido por el área de SMNYL. Este flujo debe establecer medidas de seguridad pertinentes para el cuidado de los Datos, la justificación del tratamiento, segregación de perfiles para acceder a los Datos, supresión/cancelación o devolución de Información una vez cumplida la finalidad o el periodo de conservación establecido.

Subcontrataciones

- Toda subcontratación de servicios por parte de un proveedor (Encargado) que implique el Tratamiento de Datos debe ser autorizada por la Oficina de Privacidad de la Dirección de Ética y Cumplimiento. Es por ello por lo que, el Dueño de la Información/Proceso involucrado en la relación con el proveedor (Encargado) que pretenda subcontratar, debe informarlo a la Oficina de Privacidad de la Dirección de Ética y Cumplimiento previo a cualquier subcontratación.
- Cuando las cláusulas contractuales o los instrumentos jurídicos mediante los cuales se haya formalizado la relación entre el Responsable y el proveedor (Encargado), y prevean que este último pueda llevar a cabo a su vez las subcontrataciones de servicios, la autorización se gestionará a través de lo estipulado en éstos.
- En caso de subcontratación, se debe contar en el contrato entre el proveedor (Encargado) y el subcontratado con una cláusula de Protección de Datos Personales.
- La persona física o moral subcontratada debe asumir las mismas obligaciones que se establezcan para el proveedor (Encargado) en la Ley, el Reglamento y demás disposiciones aplicables legales, así como lo señalado en la presente política.
- La obligación de acreditar que la subcontratación se realizó con autorización de la Compañía corresponderá al proveedor (Encargado).

Terminada la Relación

- Establecer un control o medio por el cual el Dueño de la Información/Proceso, tenga la certeza de que el proveedor (Encargado) ha eliminado o devuelto toda la Información al terminar la relación contractual entre el proveedor y SMNYL o a solicitud de este último.

10.9.2 Excepciones a SMNYL como Responsable.

Usualmente SMNYL actuará como Responsable de conformidad con la LFPDPPP en el tratamiento de los Datos Personales de clientes, colaboradores, agentes y cualquier otro Titular, no obstante, se reconoce que podría haber casos extraordinarios en los que SMNYL puede actuar en calidad de Encargado, en caso de que exista duda sobre la calidad que Seguros Monterrey New York Life ostenta en una relación se tendrá que solicitar el apoyo de la Oficina de Privacidad para determinar dicha calidad, así como para proporcionar la cláusula en

materia de protección de Datos Personales que corresponda, según la relación de la que se trate, para ser incluida en el contrato que ampare dicha relación.

10.9.3 Transferencias de Datos Personales.

Previo a hacer una transferencia de datos a otro Responsable, se deberá determinar si dicha transferencia requiere el consentimiento del Titular así como garantizar el cumplimiento de las obligaciones de SMNYL como Responsable que transfiere los datos.

En todos los casos en que se realice una transferencia, esta deberá quedar estipulada con los requisitos que requiere la LFPDPPP a nivel contractual con el Responsable al que se transfieran los datos.

10.10 Jurisdicción

Por regla general todo tratamiento de Datos se hará conforme a lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, por lo que en cualquier relación comercial que se entable debe hacer referencia a la regulación y jurisdicción mexicana, cualquier otro escenario debe verificarse con el área Jurídica y la Oficina de Privacidad de la Dirección de Ética y Cumplimiento.

10.11 Computo en la Nube

Para el Tratamiento de Datos en servicios, aplicaciones e infraestructura en el Cómputo en la Nube, el área que requerirá el servicio del proveedor, además de verificar el cumplimiento con los puntos anteriores de la sección relación con proveedores (Encargados), debe asegurarse de que estos:

- Cuenten con un programa de protección de Datos afines a los principios y deberes aplicables que establece la Ley, su reglamento y la presente política.
- Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la Información sobre la que presta el servicio.
- Informe sobre la(s) ubicación(es) geográfica(s) de sus centros de Datos y la regulación aplicable en cada caso. Esto con la finalidad de poder evaluar si existe un riesgo derivado de la jurisdicción aplicable al tratamiento de los Datos.
- Evidenciar si cuenta con alguna certificación o auditoría por parte de un tercero que valide su cumplimiento con estándares como lo son: estándares internacionales como ISO/IEC 27002, ISO/IEC 27017 Y/O ISO/27001.
- Cuente con mecanismos, al menos, para:

✓ Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta.

✓ Permitir a la Compañía limitar el tipo de Tratamiento de los Datos sobre los que se presta el servicio.

✓ Establecer y mantener medidas de seguridad adecuadas para la protección de los Datos sobre los que se preste el servicio.

✓ Garantizar la supresión de los Datos una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos.

- ✓ Impedir el acceso a los Datos a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al Responsable.

- ✓ Informar el nivel de control que maneja en sus recursos, por ejemplo, si es Iaas, Paas o Saas (para este punto en particular, se requerirá apoyo del área de Tecnología de la Información para validar funcionamiento y seguridad).

- ✓ Identificar si el proveedor (Encargado) cuenta con portabilidad abierta o cerrada, es decir, si al terminar la relación cuenta con la infraestructura para devolver la Información y/o migrarla a otro entorno.

Adicional a lo anterior, se recomienda al Dueño de la Información/Proceso responsable de la relación con el proveedor (Encargado):

- Buscar antecedentes del proveedor.
- Llevar un registro de la Información que vive en el centro de datos, fechas de entrega, responsables, etc.
- Acercarse al área de Tecnología de la Información para confirmar los alcances tecnológicos y que puedan emitir una conclusión sobre la seguridad del servicio.

10.12 Capacitación

Con el fin de asegurar el cumplimiento de esta Política y de la Ley, se llevan a cabo las siguientes acciones:

- Al inicio de la relación laboral cada colaborador debe presentar la Capacitación en Línea de "Protección de Datos Personales".

- Todos los colaboradores pueden recibir capacitación periódica ya sea en línea o presencial por parte del área de Ética y Cumplimiento de conformidad con los calendarios que se establezcan en coordinación con el área de Recursos Humanos.

- La Oficina de Privacidad de la Dirección de Ética y Cumplimiento puede impartir capacitaciones específicas a aquellas áreas que por sus funciones así lo considere o requieran.

- La Oficina de Privacidad de la Dirección de Ética y Cumplimiento podrá impartir capacitaciones, certificaciones y recertificaciones específicas, por ejemplo, a Dueños de la Información/Procesos, Enlaces de Seguridad o cualquier otro rol/área específica que requiera reforzar o conocer temas relacionados con Protección de Datos Personales.

- Los entrenamientos asignados para la protección de Datos Personales son obligatorios.

Todo lo relacionado a las capacitaciones normativas para la protección de Datos Personales se puede consultar en el Procedimiento M11.P04.S01.002.B Seguimiento a capacitación normativa.

10.13 Consultoría

Los Dueños de la Información/Procesos son los responsables de cuidar la Información que contiene Datos, tomar decisiones adecuadas para ello y en ocasiones otorgar vistos buenos respecto a solicitudes y consultas, sin embargo, la Oficina de Privacidad de la Dirección de Ética y Cumplimiento puede intervenir en algunas actividades como:

- Análisis de Documentos relacionados a Protección de Datos a petición de proveedores (Encargados) o clientes.

En ocasiones, clientes o proveedores (Encargados) solicitan que SMNYL firme o acepte documentos que confirmen que la Compañía cuenta con las medidas de seguridad y protección de Datos adecuadas, como primera respuesta, el Dueño de la Información/Proceso o persona que está gestionando la comunicación, debe entregar el Brochure de Ética y Cumplimiento, en el cual se señalan los programas normativos de la Compañía y sus principales características para el cumplimiento con la regulación aplicable. En el escenario de que el Brochure no sea suficiente y el tercero insista en la firma o aceptación de los documentos, estos deben ser inicialmente verificados por el Dueño de la Información/Proceso para determinar que lo estipulado en los mismos es operable/aceptable por SMNYL y solo en caso positivo, debe remitir los documentos a la Oficina de Privacidad de la Dirección de Ética y Cumplimiento para que se puedan emitir recomendaciones y comentarios pertinentes.

10.14 Inventario de Activos de Información

El Inventario de Activos de Información es una herramienta de SMNYL que forma parte del Programa de Mantenimiento y Retención de Registros para identificar la Información que tiene valor en la Compañía y, en consecuencia, permita tratarla, protegerla, resguardarla, almacenarla y eliminarla de manera apropiada de acuerdo con las mejores prácticas y regulaciones aplicables, ya que es el activo más importante de la Compañía y ayuda a la toma de diferentes decisiones.

El Inventario de Activos de Información permite identificar aquellos Activos con Datos, el detalle de los Datos, el volumen de Titulares de quienes se tienen Datos, los medios por los cuales se acceden a los Datos, así como, cuantos usuarios tienen acceso a los mismo. Identificar donde se encuentran los Activos de Información más riesgosos y es el principal insumo para realizar el Análisis de Riesgo de Datos, en su caso, poder emitir recomendaciones para su debido tratamiento y protección.

La Oficina de Privacidad de la Dirección de Ética y Cumplimiento puede realizar monitoreos de los Activos de Información para garantizar el debido tratamiento, así como corroborar la Información reportada por el Dueño de la Información/Proceso.

Es responsabilidad de cada Dueño de la Información/Proceso el uso y custodia de los Activos de Información que por el desempeño de sus actividades en SMNYL genera, del mismo modo debe registrar y actualizar el Inventario de Activos de Información con aquellos que emanan de los procesos a su cargo.

Para conocer más sobre el Inventario de Activos de Información consultar la política M21.P02.S00.008.A Estándar de Inventario de Activos de Información y la Política M17.P04.S00.004.A Mantenimiento y Retención de Registros.

10.15 Sistema de Gestión de Datos

Análisis de Riesgos
La Oficina de Privacidad de la Dirección de Ética y Cumplimiento debe realizar y actualizar al menos cada dos años un Análisis de Riesgos Datos, a la fecha de creación se usa como base la metodología BAA publicada por el INAI en su portal público. Tomando como base el Inventario de Activos de Información de SMNYL para poder determinar el riesgo inherente por tipo de dato, las medidas de seguridad implementadas y el análisis de brechas.

El análisis consistente en la evaluación cuantitativa y cualitativa de tres factores:

- Beneficio: Deriva en el nivel de riesgo por tipo de Dato, este se determina por el riesgo inherente del Dato en combinación con el volumen de Titulares de estos.
- Accesibilidad: Determina el nivel de riesgo por tipo de acceso, es decir, el número de accesos potenciales a los Datos.
- Anonimidad: Determina el nivel de riesgo por tipo de entorno desde el que se tiene acceso a los Datos. Considera qué tan posible es que el atacante potencial provoque consecuencias, por ejemplo, si accede en un entorno físico, desde una red interna e internet.

Matriz de Riesgos
La Oficina de Privacidad de la Dirección de Ética y Cumplimiento en conjunto con Monitoreos y Testeos de la Dirección de Ética y Cumplimiento, actualizan de forma recurrente la Matriz de Riesgos de Privacidad, la cual contempla los controles con los que se cuentan para la Protección De Datos.

Identificación de Brechas
Como resultado del Análisis de Riesgo es posible que se identifiquen brechas o áreas de oportunidad dentro del proceso, desde la base del análisis que es el Inventario de Activos de Información, su creación, registro y actualización, hasta determinar si las medidas de seguridad con las que se cuentan no son suficientes o es necesario implementar una nueva.

Derivado de lo anterior, la Oficina de Privacidad de la Dirección de Ética y Cumplimiento trabajará en coordinación con las áreas de Tecnología de la Información y Seguridad de la Información para crear e implementar uno o varios planes de acción que subsanen esas brechas.

10.16 Medidas para la Protección de Datos Personales

- **Ofuscado de Datos:** SMNYL cuenta con procesos de ofuscado en sus diferentes aplicativos para asegurar la protección de los Datos en los ambientes de prueba y desarrollo.

  El área de Tecnología de la Información trabaja con reglas para Ofuscar los Datos para estos aplicativos, basándose en una categorización de Datos y diccionarios que consisten en colección de Datos como nombres, direcciones, etc. ficticios que sustituyen los valores reales.

  Para más información, consultar documentación del área de Transformación.

- **PCI:** Es una herramienta que censura los datos de tarjeta bancaria, sustituyéndolos con un Token, con la finalidad de no almacenar datos de tarjeta dentro de los equipos locales de los usuarios y proteger los Datos de los Titulares.

- **Data Loss Prevention (DLP):** Herramienta que previene la fuga de Información que funciona a partir de políticas establecidas por la Compañía. Esta herramienta se encuentra administrada por el equipo de Tecnología de la Información, quienes periódicamente revisan los eventos que se identifiquen por alertas que lanza la misma herramienta.

  La Oficina de Privacidad de la Dirección de Ética y Cumplimiento es dueña de algunas de las reglas que rigen esta herramienta y son responsables de verificar que las reglas estén vigentes, solicitar la actualización o bien, modificarlas con la finalidad de proteger los Datos.

Para la actualización y carga de las políticas en la herramienta DLP, la Oficina de Privacidad de la Dirección de Ética y Cumplimiento debe trabajar en coordinación con el equipo de Tecnología de la Información, quienes son los encargados de la administración de la herramienta.

Previo a modificar o crear una regla para el DLP, se deben considerar diversos factores, por ejemplo: Si existe alguna nueva regulación, surgen nuevas líneas de negocio, nuevos productos o cambios o resultados de análisis de riesgos de Datos.

El equipo de TI procederá a la carga de políticas en la herramienta conforme a lo establecido en su documentación interna.

La evidencia de la creación o modificación de las reglas de DLP relacionadas a Datos, pueden solicitarse al equipo de TI y resguardarse en la carpeta de privacidad en servidores por un periodo de acuerdo con lo establecido en la política M17.P04.S00.004.A Mantenimiento y Retención de Registros.

10.17 Incidentes y Vulneraciones de Datos

Todo incidente relativo a Datos Personales debe ser notificado a la Oficina de Privacidad de la Dirección de Ética y Cumplimiento de manera inmediata al correo electrónico compliance_comunica@mnyl.com.mx, tomando en cuenta la siguiente Información:

- Datos comprometidos.
- Nivel de Riesgo por tipo de Dato.
- Titular de los Datos vulnerados.
- Tipo de incidente/naturaleza:

✓ Uso o Tratamiento indebido de Información.
✓ Divulgación no autorizada de Información y/o documentación.
✓ Acceso o intento de acceso no autorizado de Datos.
✓ Pérdida o destrucción o daño no autorizado de Datos.
✓ Envío de Datos no autorizado.
✓ Robo o copia o extravío o pérdida o alteración de Datos.

- De ser el caso, se deberá dar recomendaciones al Titular respecto a medidas que pueda adoptar para proteger sus intereses.
- Propuesta de acciones correctivas.

Una vez identificada la Vulneración por parte de las áreas involucradas con apoyo de la Oficina de Privacidad de la Dirección de Ética y Cumplimiento deben realizar el análisis de las causas del incidente para establecer las medidas correctivas para reducir los efectos de la Vulneración, así como establecer medidas a largo plazo para evitar futuros incidentes.

NOTA: Si la vulneración fue identificada y/o reportada por algún otro medio, mecanismo, grupo de trabajo en el que participe algún miembro de la Oficina de Privacidad, este podrá atenderla sin necesidad de reportarla a través de compliance_comunica@mnyl.com.mx, no obstante, el Dueño de la Información/Proceso si será responsable de proveer la Información antes listada a solicitud de la Oficina de Privacidad.

10.18 Proyectos o Mejoras con Tratamiento de Datos Personales

Toda iniciativa, ya sea mejora o nuevo proyecto de sistemas, aplicativos, portales o cualquier otra herramienta tecnológica que implique Tratamiento de Datos, debe cumplir con el llenado del documento relacionado Checklist Proyectos con Datos Personales y es responsabilidad del Owner de la iniciativa, que previo a cualquier desarrollo se haya completado el Checklist, así como del Scrum Master encargado del proyecto garantizar que dicho análisis sea realizado y obtener el Vo.Bo. de la Oficina de Privacidad de la Dirección de Ética y Cumplimiento.

10.19 Monitoreo y Testeo

La dirección de Ética y Cumplimiento realiza los monitoreos que considera necesarios con el fin de validar el cumplimiento de lo establecido en la presente política.

Dichos monitoreos se hacen conforme a lo establecido en el programa de Monitoreo y Testeo de Ética y Cumplimiento.

10.20 Programa de Enlaces de Seguridad

SMNYL cuenta con un Programa de Enlaces de Seguridad, que está integrado por colaboradores con un perfil definido para cumplir con diversas tareas, mismas que son evaluadas según su desempeño. Los Enlaces de Seguridad reciben capacitación enfocada y sensibilización en general sobre la importancia de su rol como intermediario entre su dirección, la Oficina de Privacidad de la Dirección de Ética y Cumplimiento y Seguridad de la Información.

10.21 Dueños de la Información/Procesos

Para SMNYL, la administración de la Información es un tema relevante por varias razones, más allá de que su tratamiento y protección estén regulados, adoptar prácticas que nos permitan administrarla y explotarla de la mejor manera trae beneficios para clientes, colaboradores y asesores.
En SMNYL existen los programas de Protección de Datos Personales, Mantenimiento y Retención de Registros, Seguridad de la Información y Gobierno de Datos orientados a proveerte de dichas prácticas y, con ello, establecer un modelo de gestión para la administración de la Información en el que el Dueño de la Información/Procesos, es el control clave para la implementación y éxito de dichos programas.

Por lo cual en SMNYL existe la Certificación del Taller de Administración de Información para los Dueños de la Información/Procesos que fue creada con la finalidad de compilar en una guía las prácticas de administración de la Información, contenidas en las políticas y procedimientos de los programas antes mencionados y que deben seguir para cumplir con sus responsabilidades como Dueño de la Información/Procesos. Cuidar los Datos como un activo de la empresa y generar una cultura del Dato, da como resultado que SMNYL pueda ser una compañía Data-Driven, es decir, que esté impulsada por los Datos, además de proteger apropiadamente la Información y cumplir con las obligaciones que como Responsables de Datos tiene SMNYL.

10.22 Prohibiciones

- Dejar cualquier documento que contenga Datos sobre la mesa de trabajo, sin importar si el colaborador se encuentra en casa, oficina o cualquier lugar de trabajo.

- "Reciclar" o reutilizar hojas o documentos que contengan Datos (por ejemplo: identificaciones, estados de cuenta, comprobantes de domicilio, Información de la póliza del individuo, contratos, etc.)
- "Reciclar" o reutilizar las bases de Datos creadas para alguna campaña. Cada campaña o esfuerzo diseñado para contactar a clientes con el Fines mercadotécnicos y publicitarios debe ser realizada con bases de datos actualizadas y que hayan pasado por el proceso para validar que los Titulares no se encuentren en algún listado de exclusión (consultar el procedimiento de solicitud y entrega de Información cuantitativa del área de Mercadotecnia y Experiencia del Cliente). Lo anterior tiene por objeto no contactar a los clientes que hayan ejercido su Derecho Oposición y/o estén inscritos en la lista REUS.
- Tratar y recabar Datos de manera ilícita.
- Actuar con dolo, mala fe o negligencia respecto del Tratamiento de los Datos del Titular.
- Vulnerar de forma dolosa o de mala fe, la expectativa razonable de privacidad del Titular.
- Compartir Datos a terceros sin asegurarse de que se cuentan con las facultades y autorizaciones correspondientes (señaladas arriba).
- Notificar al Titular finalidades distintas a las señaladas en el Aviso de Privacidad.
- Obtener Datos a través de medios engañosos o fraudulentos.
- Crear bases de Datos que contengan Datos Personales sensibles, sin que se justifique su creación para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue la Compañía.
- Llevar a cabo Tratamiento destino a las finalidades que no resulten compatibles o análogas con aquéllas para las que hubiese recabado de origen los Datos y que hayan sido previstas en el Aviso de Privacidad.
- Entregar, enviar, compartir, modificar, imprimir cualquier Información que contenga Datos a persona ajena, al Titular de los Datos sin que exista un proceso de validación, así como la justificación de dicha entrega.
- Tratar y compartir Datos por medio o canales de comunicación no oficiales de la Compañía, por ejemplo: Redes Sociales.

10.23 Autorizaciones especiales

Cualquier situación que requiera una autorización especial por no cumplir o cumplir parcialmente lo estipulado en esta política tendrá que ser revisada con la Oficina de Privacidad de la Dirección de Ética y Cumplimiento, será requisito indispensable que el departamento solicitante de la autorización especial tenga documentado en políticas, procedimientos, manuales, instructivos corporativos, etcétera, la información relacionada a su proceso que justifique la necesidad de dicha autorización especial.

7. Responsabilidades

No.	Responsable	Responsabilidades
1	Dueño de la Información/Proceso	• Documentar el Tratamiento de los Datos. • Adoptar medidas de seguridad tanto físicas como electrónicas para el resguardo y transmisión de los Datos Personales de forma que se evite la alteración, pérdida o acceso no autorizado. • Identificar e informar las obligaciones de las personas que están involucradas en el tratamiento de Datos Personales, para que comprendan la relevancia de la protección de los Datos.

		• Verificar que las solicitudes de extracción de Información cumplan con todos los requisitos establecidos en el procedimiento para Extracción Información de SATIs. • Mantener y actualizar el control de acceso a los Datos Personales, es decir, que únicamente los usuarios que por sus funciones tienen una razón legítima para acceder a los Datos Personales, tengan acceso a ellos. • Revisar que los Datos contenidos en las bases de datos sean pertinentes, correctos y actualizados, exactos y completos para los fines para los cuales fueron recabados de acuerdo con el programa y política de MRR. • Establecer un procedimiento de destrucción de Información tanto física como electrónica que contenga Datos y que su relación contractual o la finalidad para la que fueron recabados haya concluido. • Asegurarse que el proveedor (Encargado) y el Tratamiento que dará a los Datos cumpla con lo establecido en la Política de Protección de Datos Personales. • Si se tiene una relación con un proveedor (Encargado) debe de llevar a cabo todas las acciones que se señalan en la política antes, durante y posterior a la relación con este. • Validar que los contratos con Encargados cuenten con cláusula de Protección de Datos y se haya definido que la jurisdicción ante cualquier controversia no será otra diferente a la mexicana. • Asegurarse de que los Datos a recabar, finalidades y transferencias, según sea el caso, se encuentren cubiertos por los términos del Aviso de Privacidad. • Identificar el flujo y ciclo de vida de los Datos. • Proteger del uso inapropiado, daño, pérdida, divulgación indebida o venta de los Datos.
2	Enlaces de Seguridad	• Ser el vínculo entre la dirección a la que pertenecen, Seguridad de la Información y la Oficina de Privacidad de la Dirección de Ética y Cumplimiento. • Recibir capacitación enfocada a sus tareas.
3	Oficina de Privacidad de la Dirección de Ética y Cumplimiento	• Asegurarse de que el Aviso de Privacidad esta actualizado y publicado en todas las oficinas. • Hacer modificaciones necesarias al Aviso de Privacidad. • Llevar a cabo Análisis de Riesgo tomando como base la metodología del INAI. • Trabajar en la actualización de la Matriz de Riesgos de privacidad. • Identifiquen brechas o áreas de oportunidad en materia de Protección de Datos. • Hacer recomendaciones para el debido Tratamiento y protección de los Datos. • Recibir las solicitudes de Derechos ARCO y asegurarse de que se atiendan en tiempo y forma.

		• Atender requerimientos de la Autoridad en materia de Protección de Datos (INAI), así como acompañar y emitir recomendaciones si se trata de otra autoridad, pero están involucrados Datos. • Analizar y de ser el caso, aprobar los reportes de Service Now para compartir Información que contenga Datos Personales con externos. • Emitir las recomendaciones y pasos a seguir en caso de que exista una Vulneración o bien, se presuma que pueda existir. • Difundir y comunicar la política y/o prácticas de protección de Datos Personales implementadas al interior de la organización, así como capacitar a todo el personal sobre las mismas. • Fomentar una cultura de protección de Datos Personales orientada a elevar el nivel de concienciación del personal y terceros involucrados, como Encargados, en el tratamiento de Datos Personales. • Identificar e implementar mejores prácticas relacionadas con la protección de Datos Personales. • Gestionar el cumplimiento del ciclo de vida de los Activos de Información y supervisar el ejercicio de depuración de cada una de las direcciones.
4	Seguridad de la Información	• Definir los repositorios oficiales para el resguardo de Información. • Establecer la herramienta o medio seguro para compartir Información fuera de la infraestructura de SMNYL. • Colaborar con la Oficina de Privacidad de la Dirección de Ética y Cumplimiento en la creación, definición o implementación de medidas de seguridad que deba implementar el área de TI para proteger los Datos. • Establecer lineamientos para el uso de cómputo en la nube siempre en consideración a la protección, privacidad y seguridad de los Datos.
5	Colaboradores	• Actuar con apego a lo establecido en la Presente política y a la regulación en la materia. • En caso de recabar Datos Personales y/o sensibles: Debe poner a disposición el Aviso de Privacidad al Titular de manera inmediata. • Cuando los Datos Personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, deberá proveer los mecanismos para que el titular conozca el texto completo del Aviso de Privacidad • Conocer la normativa que en lo particular regule la(s) actividad(es) en la que se tratan Datos e identificar si dicha normativa incluye disposiciones que se vinculen, de manera directa o indirecta, con la protección o el Tratamiento de Datos.

	• Tratar los Datos con previo consentimiento de los Titulares. • Tratar los menos Datos posibles, y sólo aquéllos que resulten necesarios, adecuados y relevantes con relación a las finalidades previstas en el Aviso de Privacidad. • Si su función es contactar al Titular con motivos publicitarios o de promoción, cerciorarse de que el Titular no se encuentra en algún listado de exclusión (Oposición, REUS, etc.) • Asegurarse de que los Datos que traten son correctos, actualizados y de depurar aquellos que ya no son necesarios o han cumplido con su periodo de conservación de acuerdo con lo que se establece en la Política de Mantenimiento y Retención de Registros. • Guardar confidencialidad de los Datos. • Conocer el Aviso de Privacidad y Tratar los Datos con apego a éste. • Conocer la clasificación de los Datos. • No encaminar al Titular a que ejerza sus derechos ARCO, esta debe de expresar su deseo. • Documentar en política, procedimiento, manual o instructivo Tratamiento que dan a los Datos por sus funciones, indicando qué datos usa, cómo los obtiene, su finalidad, lugar de almacenamiento y tiempo de resguardo. • Si por sus funciones requiere se le proporcionen Datos, debe de allegarse de ellos a través de los medios oficiales. • Si tiene acceso a varios Datos, únicamente debe de utilizar aquellos que son necesarios para cumplir con las finalidades y no puede compartir a otros sin justificación alguna, de acuerdo con lo que se establece este documento. • Si un colaborador se encuentra trabajando en una mejora, creación de un sistema, aplicación o portal que contiene Datos, debe de realizar un análisis enfocado a Protección de Datos, en cumplimiento con la presente política. • Asegurarse de que en las pruebas que se lleven a cabo en sistemas, se utilicen Datos disociados y no reales. • Resguardar la Información con Datos en los repositorios oficiales y validados por la compañía, comprometiéndose a no resguardar Información en su equipo o correo electrónico. • Conocer y cumplir con lo que establece la Política y Programa de Mantenimiento y Retención de Registros. • Asegurarse de que los destinatarios en un correo que contenga Datos son los indicados y que todos tienen la facultad de conocer esos Datos. • Realizar los cursos de Protección de Datos Personales que se asignen en tiempo y forma, además de asistir a las capacitaciones que lleguen a ser presenciales. • Reportar cualquier incidente de datos de manera inmediata a la Oficina de Privacidad de la Dirección de Ética y Cumplimiento. • No dejar Información con Datos expuesta en su área de trabajo, no reciclar o reutilizar hojas que contengan Datos, no reutilizar bases de Datos, no actuar con dolo o mala fe, así

		como conocer y aplicar las prohibiciones señaladas en este documento.
6	Tecnología de la Información	• Cargar, probar y verificar eficiencia de las políticas de protección de Datos que señalan las reglas con las cuales funciona la herramienta para evitar fuga de Información. • Asegurarse de que las herramientas de la Compañía para proteger Datos funcionen adecuadamente. • Apoyar a validar que herramientas, sistemas o plataformas utilizados por terceros y que traten Datos sean seguras.
7	Monitoreos y Testeos	• Realizar Monitoreos y Testeos de acuerdo con su programa. • Actualizar Matriz de Riegos de acuerdo con los monitoreos y testeos que realice.
8	Legal	• Apoyar en la creación de cláusulas de Protección de Datos Personales e incluirlas en los contratos. • Emitir recomendaciones para cumplir con la regulación y evitar faltas normativas.
9	Atención a Clientes	• Contar con procedimientos que regulen el Tratamiento de Datos en sus actividades. • Contar con medios para autenticar la personalidad de los Titulares de datos y verificar su facultad para recibir los Datos. Eso independientemente de si se comunicaron de forma presencial o por otra vía, como correo electrónico o vía telefónica. • Entregar información al Titular de sus Datos según aplique y evitar encaminar al Titular a que ejerza sus derechos ARCO, esta debe de expresar su deseo.
10	Encargado	• Tratar únicamente los Datos conforme a las instrucciones de la Compañía. • Abstenerse de tratar los Datos para finalidades distintas a las instruidas por la Compañía. • Implementar las medidas de seguridad conforme a la Ley, el Reglamento y las demás disposiciones aplicables, así como aquellas establecidas y requeridas por la Compañía. • Guardar confidencialidad respecto de los Datos Tratados. • Suprimir los Datos objeto de Tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones de este, siempre y cuando no exista una previsión legal que exija la conservación de los Datos. • Cooperar con SMNYL para que se implementen medidas que garanticen la correcta devolución o supresión de los Datos de SMNYL. • Abstenerse de transferir los Datos salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.

- El encargado, será considerado responsable con las obligaciones propias de éste, cuando:
- *Destine o utilice los Datos Personales con una finalidad distinta a la autorizada por el responsable, o efectúe una transferencia, incumpliendo las instrucciones del responsable.*
- *El Encargado no incurrirá en responsabilidad cuando, previa indicación expresa de SMNYL, remita los Datos a otro Encargado designado por este último, al que hubiera encomendado la prestación de un servicio, o transfiera los Datos a otro responsable conforme a lo previsto en este documento.*

8. Activos de Información

En la siguiente matriz debes listar los Activos de Información relacionados con este documento, tal cual con los nombres que han sido o serán reportados en el Inventario de Activos de Información, con el objetivo de mantener los registros exactos y actualizados.

Folio del activo de Información	Nombre del activo de Información
N/A	N/A