Paseo de la Reforma #342, Ciudad de México
01 55 5326 9000
www.mnyl.com.mx

SEGUROS MONTERREY

POLÍTICA CORPORATIVA

Protección de datos personales

DOCUMENTO PÚBLICO
VERSIÓN 4.0

Preparado por: Sánchez Cantoral José Ramón

Área: Ética y Cumplimiento

Departamento: Ética y Cumplimiento

Fecha de publicación: 07/04/2020

Código: 14-02-01-03-033-A

CONTENIDO

1. BITÁCORA DE CAMBIOS Y MEJORAS

NO.	VERSIÓN	FECHA	ÁREA RESPONSABLE	DESCRIPCIÓN DEL CAMBIO
0	0.0	15/05/2012	Compliance	Emisión inicial
0	0.0	13/02/2015	Compliance	Última revisión
1	1.0	06/07/2017	Compliance	Cambio en formato actual
2	2.0	01/06/2018	Ética y Cumplimiento	Se actualiza el nombre del área responsable, se modifica la definición de Desduplicación, se agregar definiciones de REUS, Fines mercadotécnicos y publicitarios y se ajusta la sección 10.6 en el apartado de Fines mercadotécnicos y publicitarios; se lista en la sección de Documentos Relacionados el Instructivo: Desduplicación y validación de consentimiento. Se agregan firmantes de enterado
3	2.1	01/09/2019	Ética y Cumplimiento	Se cambia el nombre de documento relaciona "Visión y Alcance" por "Proceso de Análisis de Negocio TI" y se señalan las personas responsables de cumplir con las obligaciones marcadas en la sección 1.6, inciso d).
4	3.0	28/02/2020	Ética y Cumplimiento	Se modifica la sección 1.6. "Del Tratamiento de Datos Personales" para incluir información relativa a la extracción de información de los Sistemas Automatizados de Tratamiento de la Información. Actualización de código Sustituye al documento 01-02-04-01-001-A
5	4.0	7/4/2020	Ética y Cumplimiento	Se modificó la clasificación del documento, ya que estaba clasificado conforme a la Política de Clasificación de la Información

2. OBJETIVO

Establecer los requerimientos y lineamientos mínimos necesarios a los que todos los Colaboradores y Directivos de Seguros Monterrey New York Life (en adelante "la Compañía") deberán apegarse con el fin de proteger los datos personales en su posesión para dar cumplimiento a lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante la "Ley"), publicada en el Diario Oficial de la Federación el 5 de julio del 2010.
Establecer el compromiso de cumplir con la legislación en protección de datos personales por parte de todos los involucrados en el tratamiento a los datos personales que son tratados en la Compañía dentro de los distintos procesos y finalidades.

3. ALCANCE

Este documento es obligatorio y aplica a todos los Colaboradores incluyendo directores, subdirectores, gerentes; personal temporal y becarios; así como Terceros que actúan en representación de Seguros Monterrey.

4. ÁREA RESPONSABLE

El Oficial de Privacidad es responsable de la elaboración, revisión, modificación y derogación de este documento.

5. ENLACE CON DOCUMENTOS RELACIONADOS

CÓDIGO	TIPO	NOMBRE DEL DOCUMENTO CONTROLADO
01-02-04-02-001-B	Procedimiento	Atención de derechos Arco
01-02-04-03-001-B	Procedimiento	Políticas asociadas a la LFPDPPP en el DLP
04-04-01-01-001-A	Política	Política Corporativa de Seguridad de la Información
03-04-01-01-001-A	Política	Seguridad de la Información Documental.
04-04-03-06-005-A	Política	Política de Clasificación de la Información
04-04-03-05-002-D	Instructivo	Roles y responsabilidades de seguridad
03-04-01-04-001-B	Procedimiento	Inventario de Activos de Información Documental
03-04-01-02-001-B	Procedimiento	Manejo de la Información documental
04-04-03-06-015-D	Instructivo	Estándares de administración de Riesgos de Información Compartida con Terceros
04-03-01-07-001-B	Procedimiento	Análisis de Negocio TI
01-02-04-01-028-D	Instructivo	Desduplicación y validación de consentimiento
04-03-01-03-001-B	Procedimiento	Ofuscamiento de Datos
14-02-01-01-034-B	Procedimiento	Extracción de Información de los Sistemas Automatizados de Tratamiento de Información.

6. ENTRADA EN VIGOR

La entrada en vigor del presente documento será a partir del 21 de abril de 2020.

7. FRECUENCIA DE LA REVISIÓN

Este documento debe ser revisado y, en caso necesario, actualizado a más tardar el 07 de abril 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".**

8. VOCABULARIO

- **Activo.** Es aquello que tiene algún valor para la organización y por tanto debe protegerse.
- **Activo de Información.** Es aquel elemento que contiene o manipula información. Conjunto de documentos que se almacenan por lineamientos o procesos internos y/o externos, por un periodo de tiempo en un lugar específico.
- **Aviso de Privacidad**. Documento físico, electrónico o en cualquier otro formato, que detalla la información que se recaba, los fines, transferencias, procedimiento para ejercicio de Derechos ARCO, entre otros. Este documento es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con el artículo 15 de la Ley. El Aviso de Privacidad de SMNYL se puede encontrar en la siguiente liga: https://www.mnyl.com.mx/aviso-de-privacidad.aspx
- **Agentes.** Aquellas personas físicas y morales que tienen una cédula emitida por la Comisión Nacional de Seguros y Fianzas y un contrato mercantil firmado por la compañía para poder realizar la comercialización de productos de seguros.
- **Base de datos.** El conjunto ordenado de datos personales referentes a una persona identificada o identificable.
- **Bloqueo.** Tiene como propósito impedir el tratamiento o posible acceso por persona alguna a la información, a excepción del almacenamiento y/o que alguna disposición legal prevea lo contrario; de esta manera, el periodo de bloqueo será hasta finalizado el plazo de prescripción legal o contractual correspondiente.

  Durante este periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.
- **Colaborador.** Toda persona que se encuentra empleada por la Compañía y que realiza funciones específicas en alguna de las diferentes áreas.
- **Cómputo en la Nube.** Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente.
- **Consentimiento.** Manifestación de la voluntad del dueño de la información (titular) para que el responsable efectúe el tratamiento de datos.
- Criterio de Minimización: Procura que los datos personales tratados sean los mínimos necesarios de acuerdo con la finalidad del tratamiento que se les dará.
- **Datos.** Conjunto de datos personales, datos personales sensibles y datos financieros y patrimoniales.

- **Datos personales.** Cualquier información concerniente a una persona física identificada o identificable.
- **Datos personales sensibles.** Son aquellos datos que afectan a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.
- **Datos financieros y patrimoniales.** Conjunto de datos pertenecientes a una persona que especifican sus bienes y derechos, finanzas, ingresos, gastos.
- **Derechos ARCO.** Son las facultades que otorga la Ley para que cada individuo decida a quién proporciona su información y controlar cómo y para qué es utilizada. Estos derechos permiten a todos los individuos de Acceder, Rectificar, Cancelar y Oponerse al tratamiento de su información personal.
- **Desduplicación.** Proceso por medio del cual se hace un filtrado y limpiado de las bases de datos que se tienen en la Compañía con el propósito de no realizar contacto con personas que han sido incorporadas a las listas: Derecho Oposición y REUS.
- **Disociación.** Procedimiento mediante el cual se separan los datos personales de tal manera que cuando los usuarios realicen una consulta no se pueda identificar al titular de los mismos.
- **Dueño de la información.** Responsable de la protección de la información que maneja un área, aplicación o proceso de negocio contra acceso, divulgación o uso no autorizados, así como daño, alteración o modificación además de asegurar la disponibilidad de la información para la continuidad de la operación de la Compañía.
- **Encargado.** Persona física o moral que sola o conjuntamente con otras trate datos personales por cuenta del responsable, para la Compañía dentro de esta categoría se encuentran agentes y proveedores de servicios en general.
- **Expectativa razonable de privacidad.** La confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta Ley
- **Fines mercadotécnicos o publicitarios:** la utilización de la información del Usuario o el ofrecimiento de productos y servicios financieros realizado directamente por la Institución Financiera, o a través de prestadores de servicios contratados por ellas, mediante alguno de los siguientes medios:
    - **Publicidad:** la comunicación directa dirigida a los Usuarios y clientes potenciales de las Instituciones Financieras, que tiene por objeto informar, divulgar noticias o anuncios de carácter comercial con el propósito de comunicarles las características generales de los productos y/o servicios de las Instituciones Financieras.
    - **Promoción:** la comunicación directa dirigida a los Usuarios y clientes potenciales de las Instituciones Financieras, que tiene por objeto hacer de su conocimiento beneficios adicionales o asociados a la contratación de nuevos productos y/o servicios de la Institución Financiera tales como descuentos, bonificaciones, programas continuos, concursos y sorteos.
    - **Telemarketing:** la publicidad que se lleva a cabo mediante la comunicación vía telefónica que entabla la Institución Financiera directamente o por conducto de sus prestadores de servicios con los Usuarios o clientes potenciales de la misma, con el objeto de ofrecer productos y/o servicios.

- **La Compañía.** Seguros Monterrey New York Life S.A de C.V., sus filiales y subsidiarias.
- **Ley.** Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- **INAI.** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Es el organismo de la Administración Pública Federal encargado de proteger los datos personales en posesión de los particulares.
- **Inventario de Información Documental.** Aplicación que resguarda el inventario de activos de la información de la Compañía.
- **Medidas de seguridad**. Se entenderá por control o grupo de controles de seguridad para proteger los datos personales. Se pueden clasificar en: Medidas de seguridad administrativas, Medidas de seguridad físicas, Medidas de seguridad técnicas.
- **Medidas de seguridad administrativas.** Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales.
- **Medidas de seguridad físicas**. Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología para protección de Datos personales y el acceso a estas.
- **Medidas de seguridad técnicas**. Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que:

  a) El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados;

  b) El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

  c) Se incluyan acciones para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros, y

  d) Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales.

- **Mesa de Ayuda (911).** Área donde los usuarios pueden reportar sus incidentes y requerimientos de Tecnología de Información.
- **Oficial de Privacidad.** Figura designada en la Compañía para asegurar la protección de datos personales, gestionar y monitorear el cumplimiento del programa de privacidad en los términos que señala la Ley, así como verificar la atención en tiempo y forma de las solicitudes para el ejercicio de los derechos ARCO.
- **Oficial de Seguridad.** Responsable de asegurar la implementación de controles que garanticen la confidencialidad, integridad y disponibilidad de la información.
- **Remisión.** La comunicación de datos personales entre el responsable y el encargado, dentro o fuera del territorio mexicano.
- **Representante legal.** ejerce la facultad de **ocuparse de obligaciones y hasta derechos** de su representado, de acuerdo con las condiciones acordadas en el momento de crearse la representación. Se otorga este

carácter mediante instrumento notarial de acuerdo a la facultad que se le quiera otorgar: actos de administración, dominio, poder especial para el trámite en específico.

- **Responsable.** Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.
- **REUS:** Registro Único de Usuarios de Servicios Financieros, El Registro Público de Usuarios que no deseen que su información sea utilizada para Fines mercadotécnicos o publicitarios;
- **Sistema ARCO.** Sistema empleado por la Compañía para atender las peticiones de ejercicio de Derechos ARCO mencionados en la Ley.
- **Sistema Automatizado de Tratamiento de Información (SATI)**: De acuerdo con el Glosario de términos de Seguridad de la Información, es todo aquel Activo de TI que ha sido desarrollado y/o implementado para cumplir con una función específica de negocio que implica el tratamiento, resguardo o concentración de información (con y sin Datos Personales), por ejemplo Tecnisys, Caja.Net, SMNYL Central, Success Factors (Nuestra Red de Talento), Data Landing, entre otros. Aquellos Activos de TI, entre otros apps, paquetería, sistemas de mensajería instantánea, que solo tienen el propósito de servir como medio de comunicación o transferencia de información, o como herramienta administrativa de los colaboradores y que no tiene como propósito una función específica de negocio, no deberá considerarse dentro de esta definición y en consecuencia la información que se encuentre en ellos se considerará fuera de los Sistemas Automatizados para Tratamiento Información, por ejemplo: el correo electrónico (Outlook), Microsoft Office (Word, Excel, PowerPoint, SharePoint, Teams, etc.)
- **Tercero.** La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos.
- **Titular.** La persona física a quien corresponden los datos personales.
- **Tratamiento.** La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.
- **Transferencia.** Toda comunicación de datos realizada a una persona distinta del responsable o encargado del tratamiento.
- **TI.** Tecnología de Información.

Nota: En caso de que tengas dudas con la interpretación de alguna de las definiciones te pedimos contactar al área de Ética y Cumplimiento para revisarlo.

9. ESPECIFICACIONES

1.1 CLASIFICACIÓN DE LA INFORMACIÓN

La Ley aplica a cualquier persona física o moral que obtenga, trate, almacene o transfiera datos personales de terceros, los cuales se dividen en:

Datos personales. De manera enunciativa mas no limitativa podemos 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 académicos: Trayectoria educativa, escolaridad, títulos obtenidos, cédula profesional, certificados y reconocimientos.

Datos personales sensibles. De manera enunciativa más no limitativa podemos 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 y biométrica: ADN, información celular, huellas dactilares, retina, iris, patrones faciales, voz, firma, geometría de la mano, tipo de sangre.
- 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.).
- Datos de características físicas: Género, color de cabello, señas particulares, estatura, peso, complexión, discapacidades.

Datos financieros y patrimoniales. De manera enunciativa más no limitativa podemos 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, información fiscal, buró de crédito, seguros, afores, fianzas, sueldos y salarios, número de tarjeta bancaria de crédito y/o débito

1.2 DERECHOS ARCO

Son los derechos que otorga la Ley para que los titulares decidan a quién proporcionan su información y controlar cómo y para qué es utilizada. Cualquier titular, o en su caso su representante legal, podrá ejercer estos derechos, y son:

a) Acceso: El titular puede solicitar a la Compañía que le informe si tiene información personal, en caso de ser así, la Compañía deberá proporcionarle dicha información.

b) Rectificación: El titular puede solicitar a la Compañía que se corrijan, completen o actualicen sus Datos según sea el caso.

c) Cancelación: El titular podrá solicitar a la Compañía que se cancele (suprimir o bloquear) sus datos personales. Esta solicitud procederá cuando dicha información ya no sea necesaria para la relación

comercial existente y haya expirado su periodo de guarda y custodia conforme a lo que marca la Ley que corresponda.

El proceso de Cancelación pasa por dos fases: bloqueo y supresión. Cuando la información se encuentre en bloqueo y sea requerida por una instancia gubernamental, se deberá solicitar autorización del Oficial de Privacidad para poder desbloquear la información (devolverla a su estado original), una vez concluido el uso específico, la información volverá a ser bloqueada.

Supresión que consistente en eliminar, borrar o destruir el o los datos personales, una vez concluido el periodo de bloqueo, bajo las medidas de seguridad previamente establecidas.

d) Oposición: Este Derecho, podrá ser utilizado por el titular cuando quiera que la Compañía se abstenga de utilizar sus datos personales para Fines mercadotécnicos y publicitarios y/o de intercambio de datos con terceros.

El "Sistema ARCO" es un módulo dentro de WebFlow que se comunica con los sistemas de la Compañía para poder realizar el ejercicio de los Derechos ARCO de los titulares. Para conocer más de este proceso consulta Procedimiento para la atención de Derechos ARCO ubicado en: Intranet.

De la obtención de los Datos

a) De forma personal. - Cuando el titular proporciona los datos personales al responsable o a la persona física designada ejemplo cuando el titular acude a un consultorio médico (responsable) y ahí mismo proporciona sus datos personales

b) De manera directa. - Cuando el titular proporciona los datos personales por algún medio que permite su entrega directa al responsable, entre ellos, medios electrónicos, ópticos, sonoros, visuales o cualquier otra tecnología, como correo postal, Internet o vía electrónica, entre otros. Por ejemplo, cuando el titular envía sus datos por correo electrónico o cuando los comunica vía telefónica al responsable; o bien,

c) De manera indirecta. - Cuando el responsable obtiene los datos personales sin que el titular se los haya proporcionado de forma personal o directa, como podría ser a través de transferencias o fuentes de acceso público.

1.3 TIPOS DE CONSENTIMIENTO

a) Consentimiento Tácito: Utilizado para información en general y datos personales, puede ser recabado de manera verbal.

b) Consentimiento Expreso: Utilizado al recabar datos financieros o patrimoniales, puede ser recabado de manera verbal, escrita o por medios electrónicos.
Se considera que el consentimiento expreso se otorgó verbalmente cuando el titular lo externa oralmente de manera presencial o mediante el uso de cualquier tecnología que permita la interlocución oral.

c) Consentimiento Expreso y por escrito: Se considerará que el consentimiento expreso se otorgó por escrito cuando el titular lo externe mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por la normativa aplicable. Tratándose del entorno digital, podrán utilizarse firma electrónica o cualquier mecanismo o procedimiento que al efecto se establezca y permita identificar al titular y recabar su consentimiento.

1.4 PRINCIPIOS

Para cumplir con los principios rectores de la protección de datos personales que establece Ley, la Compañía y sus colaboradores deben:

Principio de licitud

- Recabar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley y demás normativa aplicable.
- Tratar con apego y cumplimiento a lo dispuesto en las policitas de la Compañía.
- Respetar en todo momento la expectativa razonable de privacidad de los titulares, privilegiando su protección en el tratamiento de sus datos personales

Principio de consentimiento

- Contar con el consentimiento del titular para el tratamiento de sus datos personales.
- Sujetar el tratamiento de datos personales al consentimiento del titular siempre en apego a la finalidad o finalidades previstas en el Aviso de Privacidad.
- Solicitar el consentimiento expreso para los datos personales financieros o patrimoniales, y el expreso y por escrito para los datos personales sensibles.
- Dar a conocer al titular el Aviso de Privacidad previo a la obtención del consentimiento.
- Llevar un control para identificar a los titulares que negaron su consentimiento.

Principio de lealtad

- Establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.
- No obtener los datos personales a través de medios fraudulentos.
- Respetar la expectativa razonable de privacidad del titular.
- Tratar los datos personales para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que se hubiese recabado de origen los datos personales y que hayan sido previstas en el Aviso de Privacidad.

Principio de información

- Informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del Aviso de Privacidad.
- Poner a disposición del titular el Aviso de Privacidad al primer contacto que se tenga con éste, cuando los datos personales se hayan obtenido de una transferencia consentida, de una que no requiera el consentimiento, o bien de una fuente de acceso público.
- Redactar el Aviso de Privacidad de manera que sea claro, comprensible y con una estructura y diseño que facilite su entendimiento.
- Ubicar el Aviso de Privacidad en un lugar visible y que facilite su consulta.
- Hacer del conocimiento el Aviso de Privacidad a encargados y terceros a los que se remitan o transfieran datos personales.
- Incluir todos los elementos informativos por tipo de Aviso de Privacidad utilizado.

Principio de proporcionalidad

- Tratar los menos datos personales posibles, y sólo aquéllos que resulten necesarios, adecuados y relevantes en relación con las finalidades previstas en el Aviso de Privacidad.
- Limitar al mínimo posible el periodo de tratamiento de datos personales sensibles.

Principio de finalidad

- Limitar el tratamiento de los datos personales al cumplimiento de las finalidades previstas en el Aviso de Privacidad.
- No condicionar el tratamiento para finalidades primarias, a que se puedan llevar a cabo las finalidades secundarias.

Principio de calidad

- Procurar que los datos personales tratados sean correctos y actualizados.
- Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el Aviso de Privacidad y para las cuales se obtuvieron.
- Tratar datos personales estrictamente el tiempo necesario para propósitos legales, regulatorios o legítimos organizacionales.
- Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo de bloqueo.
- Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación.

Principio de responsabilidad

- Velar por el cumplimiento de estos principios y adoptar las medidas necesarias para su aplicación.

1.5 PROHIBICIONES

Con el objeto de proteger los datos personales y la información de la Compañía, queda estrictamente prohibido:

- Dejar cualquier documento que contenga Datos o cualquier otra información no pública sobre el escritorio cuando el colaborador se ausente del lugar de trabajo.
- "Reciclar" o reutilizar hojas o documentos que contengan datos personales (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 de Desduplicación. Lo anterior tiene por objeto no contactar a los clientes que hayan ejercido su Derecho Oposición y/o estén inscritos en las listas REUS.
- Tratar y recabar datos personales de manera ilícita.
- Actuar con dolo, mala fe o negligencia respecto de la información proporcionada al titular sobre el tratamiento.
- Vulnerar de forma dolosa o de mala fe, la expectativa razonable de privacidad del titular.
- Transferir, compartir, enviar información y/o documentación a terceros sin asegurarse que se cuentan con las facultades y autorizaciones correspondientes.
- Notificar al titular finalidades distintas a las informadas en el Aviso de Privacidad.
- Obtener datos personales a través de medios engañosos o fraudulentos.

- Crear bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue la Compañía.
- Llevar a cabo tratamientos para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que hubiese recabado de origen los datos personales y que hayan sido previstas en el Aviso de Privacidad.
- Entregar, enviar, compartir, modificar, imprimir cualquier información o documentación, 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.

1.6 DEL TRATAMIENTO DE DATOS PERSONALES

GENERALES

a) Servicios telefónicos y otros medios de sistemas. - Al recabar información personal ya sea de clientes prospecto, clientes, empleados, candidatos a empleados, entre otros se deberá poner a disposición del Titular el Aviso de Privacidad (Ver: Anexo 1 "Aviso de Privacidad") de la Compañía y en caso necesario solicitar su Consentimiento (Ver: Anexo 2 "Consentimientos").

b) Fines estadísticos: La información deberá estar disociada, es decir, no se deberá poder realizar la identificación del individuo.

c) Fines mercadotécnicos y publicitarios: Las bases de datos obtenidas o generadas por SMNYL a utilizar ya sea por un Colaborador o por proveedores que proporcionen servicios de Publicidad, Promoción o Telemarketing deberán ser Desduplicadas contra el catálogo de individuos que ejercieron su Derecho de Oposición y REUS, para obtener detalle de como cumplir con lo establecido en este apartado, consultar el Instructivo Desduplicación y validación del consentimiento 01-02-04-01-028-D.

d) Implementación de nuevos sistemas o mejoras: Asegurarse de realiza el Análisis de Protección de Datos En la especificación funcional a que hace relación el documento "Proceso de Análisis de Negocio TI". El Business Partner TI / Analista de Negocio y la persona responsable del área de negocio involucrada tendrán la responsabilidad de informar al Oficial de Privacidad sobre dicha herramienta. En caso de ser necesario, el dueño del nuevo sistema deberá levantar una iniciativa de complemento para incluirlo dentro del Sistema ARCO.

e) Realización de Pruebas: Si vas a realizar pruebas ya sea de sistemas existentes o nuevos, deberás asegurarte de que la información a utilizar en tu ambiente de pruebas contenga Datos disociados y/u ofuscados según corresponda; de la misma manera, será tu responsabilidad mantener las bases de datos de tus pruebas sin ningún tipo de Dato real. En caso de requerir en tus pruebas Datos, deberás acudir al Gerente de Pruebas para seguir el proceso correspondiente.

f) Transferencias de datos personales: Revisar si dicha transferencia se encuentra contemplada en el Aviso de Privacidad de la Compañía, y en su caso contar con el consentimiento correspondiente para realizarla. En caso de no estar contemplado, informar al Oficial de Privacidad justificando y documentando las necesidades de la transferencia. Revisar las medidas de seguridad aplicables al caso en concreto.

g) Las transferencias internacionales de datos personales serán posibles cuando el receptor de los datos personales asuma las mismas obligaciones que corresponden a la Compañía como responsable o encargado de los datos personales.

h) Envío de información fuera de la infraestructura tecnológica de la Compañía: A través de ciertas herramientas tecnológicas nos apoyamos para dar cumplimiento a la Ley, por lo que si por las funciones y puesto a desempeñar, se requiere enviar información que contenga datos personales a agentes, promotores, proveedores o cualquier otro tercero o encargado , se deberá seguir la "Política de Seguridad de las Comunicaciones Electrónicas"; y deberá ser revisada y autorizada por el Gerente (o la persona que el Subdirector o Director designe), Subdirector o Director del área correspondiente.

i) Proyectos que involucren gestión o manejo de información fuera de la infraestructura tecnológica de la Compañía (ej. Computo en la nube, servidores externos, etc.): Asegurarse que el externo cumpla con las medidas de seguridad y privacidad exigidas por Ley.

j) El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el Aviso de Privacidad.

k) No se podrá llevar a cabo tratamientos para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que hubiese recabado de origen los datos personales y datos personales sensibles y que hayan sido previstas en el Aviso de Privacidad.

l) Remisión: Las remisiones nacionales e internacionales de datos personales entre la Compañía y un encargado no requerirán ser informadas al titular ni contar con su consentimiento.

m) El receptor de los datos personales en su carácter de responsable deberá tratar los datos personales conforme a lo convenido en el Aviso de Privacidad que le comunique la Compañía.

n) Extracción de información de los Sistemas Automatizados de Tratamiento de Información (SATI): Se recomienda que el tratamiento de los datos personales se realice dentro de los SATI's 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 SATI, para lo cual se deberán atender los siguientes Lineamientos para Información con Datos Personales fuera de los Sistemas Automatizados de Tratamiento de Información:

    a. La información deberá atender solo un propósito específico de negocio, esto significa que una base de datos utilizada para cumplir con el requerimiento "A" no deberá ser reciclada o reutilizada para otro propósito diferente del inicial.

    b. No deberá contener datos que no se justifiquen por el propósito especifico de negocio que se solicitó la información, Criterio de Minimización.

    c. No deberá ser compartida con ningún tercero, colaborador, proveedor o cualquier otra persona que no tenga necesidad de conocerla.

    d. El Dueño del Proceso que origina la necesidad de extraer la información se convertirá en el Dueño de la Información y con ello, adquirirá las responsabilidades de dicha función.

    e. Si por necesidades de negocio o regulatorias la información debe salir de la infraestructura de la Compañía se deberán seguir todos los lineamientos y recomendaciones estipulados en la presente políticas y los de Seguridad de la Información, que sean aplicables, principalmente al decidir el mecanismo más seguro para compartir la información.

    f. Por regla general, la información extraída de los sistemas de tratamiento deberá 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, este deberá ser controlado, seguro y documentado en políticas y/o procedimientos del área responsable.

g. Todo tratamiento de Información con Datos Personales fuera de los SATIs que sea recurrente, deberá estar documentado en los procedimientos correspondientes donde se indique claramente todo el ciclo de tratamiento desde la obtención de la información, su aprovechamiento, propósito, método y ruta de resguardo, así como el proceso de destrucción.

h. Todos los Dueños de Procesos que requieran el tratamiento de información con Datos Personales fuera de los SATIs, deberán 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.

i. Los Especialistas de Soporte y Mantenimiento de aplicaciones u otras áreas, que, por sus funciones y responsabilidades formalizadas, sólo participen como intermediario entre el Sistema de Tratamiento y el Dueño del Proceso, que requieren la información con Datos Personales, no deberán ni podrán resguardar la información una vez que haya sido entregada el Dueño del Proceso.

j. Todos los usuarios que gestionen extracciones de información de los SATIs, a través de la Mesa de Ayuda (911), deberán seguir lo estipulado en el procedimiento: 14-02-01-01-034-B Extracción de Información de los Sistemas Automatizados de Tratamiento de Información**.**

TRATAMIENTO ESPECÍFICO

Contratación de terceros:

a. Cumplir con la Política Corporativa para Proveedores y Adquisiciones, incluyendo el proceso de Due Diligence.

b. Solicitar a la Dirección Jurídica la revisión del contrato correspondiente a efecto de validar que dicho contrato contenga todas las cláusulas que se describen en el "Anexo 3 Cláusulas" de esta Política.

c. En caso de ser un sistema, plataforma o cualquier tipo de servicio tecnológico, informar a Seguridad de la Información para que apoye en la revisión de la seguridad e indique que medidas se requiere tomar.

d. Informar al Oficial de Privacidad para que proporcione consideraciones adicionales para cumplir con la Ley en los casos que así lo ameriten.

e. Solicitar a la Dirección Jurídica la revisión del contrato correspondiente a efecto de validar que dicho contrato contenga todas las cláusulas que se describen en el "Anexo 3 Cláusulas" de esta Política.

•

Subcontrataciones:

o) Toda subcontratación de servicios por parte de un tercero o un encargado que implique el tratamiento de datos personales deberá ser autorizada por el Oficial de Privacidad.

p) Cuando las cláusulas contractuales o los instrumentos jurídicos mediante los cuales se haya formalizado la relación entre el responsable y el tercero o un 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 proveedores, se debe contar en el contrato respectivo con la cláusula vigente de Protección de Datos Personales.

q) Solicitar a la Dirección Jurídica la revisión del contrato correspondiente a efecto de validar que dicho contrato contenga todas las cláusulas que se describen en el "Anexo 3 Cláusulas" de esta Política.

r) La persona física o moral subcontratada asumirá las mismas obligaciones que se establezcan para el tercero o encargado en la Ley, el Reglamento y demás disposiciones aplicables.

s) La obligación de acreditar que la subcontratación se realizó con autorización de la Compañía corresponderá al encargado.

t) Dicha subcontratación deberá cumplir con la Política Corporativa para Proveedores y Adquisiciones, incluyendo el proceso de Due Diligence.

CÓMPUTO EN LA NUBE

Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el cómputo en la nube, en los que el responsable o encargado se adhiera a los mismos mediante condiciones o cláusulas generales de contratación establecidos por la Compañía, el área de seguridad de la información velara por utilizar aquellos servicios en los que el proveedor cumple con al menos los siguientes:

a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y el presente Reglamento.

b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio.

c) 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.

d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.

e) 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 personales sobre los que se presta el servicio.
   - Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio.
   - Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos.
   - Impedir el acceso a los datos personales 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.

El área de Seguridad Informática establecerá los lineamientos de cómputo en la nube siempre en consideración sobre protección, privacidad y seguridad de datos personales y datos sensibles.

DE LA VULNERACIÓN DE DATOS PERSONALES.

El responsable del área de Seguridad deberá notificar al Oficial de Privacidad cuando corresponda a un incidente relativo a datos personales o datos sensibles, tomando en cuenta la siguiente información

- Datos personales o datos personales sensibles comprometidos

- Nivel de Riesgo por tipo de Dato
- Titular de los datos vulnerados
- Tipo de incidente:
    a) Uso o tratamiento indebido de información.
    b) Divulgación no autorizada de información y/o documentación.
    c) Acceso o intento de acceso de información.
    d) Pérdida o destrucción o daño no autorizado de información y/o documentación.
    e) Envío de información y/o documentación no autorizada.
    f) Robo o copia o extravío o pérdida o alteración de documentación o información.

Una vez identificada la vulneración, el oficial de privacidad en conjunto con las áreas involucradas deberán 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.

1.7 SEGURIDAD DE LA INFORMACIÓN EN LA COMPAÑÍA

La materia de protección de Datos se encuentra incluido en el ámbito de la seguridad de la información a través de:

a. Política corporativa de Protección de Datos Personales (esta política) la cual define y desarrolla lineamientos específicos para cubrir los requerimientos de la Ley que garanticen la seguridad de la información evitando el uso indebido o ilícito.

b. La "Política Corporativa de Seguridad de la Información" ofrece un marco normativo orientado a proteger toda la información de la Compañía para garantizar su confidencialidad, integridad y disponibilidad.

c. Programa de seguridad de la información

d. Otras políticas, procedimientos, lineamientos y estándares específicos que complementan a los dos anteriores.

1.8 GENERALES

MONITOREO

El área de Ética y Cumplimiento realizará los monitoreos que considere necesarios con el fin de validar el cumplimiento de lo establecido en la presente política.

CAPACITACIÓN

Con el fin de asegurar el cumplimiento de esta Política y de la Ley, se deberán emprender las siguientes acciones:

- Al inicio de la relación laboral cada colaborador deberá presentar la Capacitación en Línea de "Protección de Datos Personales" (Incluida en la de Código de Conducta) y acreditarla con una calificación mínima de 80 puntos.
- Podrá estar disponible para los Asesores en el portal correspondiente.
- Todos los Colaboradores deberán recibir capacitación periódica ya sea en línea o presencial por parte del área de Ética y Cumplimiento de conformidad con los calendarios que de forma anual se establezcan.

- Ética y Cumplimiento podrá impartir capacitaciones específicas a aquellas áreas que por sus funciones así lo considere.

LINEAMIENTOS DE GESTIÓN DE DATOS

Es obligación de todos los colaboradores de SMNYL que traten datos personales o datos personales sensibles aplicar las policías y procedimientos en cumplimiento a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento, y así como a cualquier normatividad aplicable.

a) Cumplir con los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, conforme a lo que señala la propia Ley, su Reglamento y demás normatividad aplicable.
b) Tratar y recabar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley y demás normativa aplicable.
c) Recabar los datos personales y datos personales sensibles siempre mediante el consentimiento del titular.
d) Sujetar el tratamiento de datos personales al consentimiento del titular, salvo las excepciones previstas por la Ley.
e) Informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.
f) Procurar que los datos personales tratados sean correctos y actualizados.
g) Notificar a los titulares de los datos: la información que se recaba y los fines del tratamiento mediante los avisos de privacidad difundidos por SMNYL en los canales o medios predeterminados para tal fin.
h) Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y para las cuales se obtuvieron.
i) Tratar datos personales estrictamente el tiempo necesario para propósitos legales, regulatorios o legítimos organizacionales.
j) Limitar el tratamiento de los datos personales al cumplimiento de las finalidades previstas en el aviso de privacidad.
k) No obtener los datos personales a través de medios fraudulentos.
l) Respetar la expectativa razonable de privacidad del titular.
m) Tratar los menos datos personales posibles, y sólo aquéllos que resulten necesarios, adecuados y relevantes en relación con las finalidades previstas en el aviso de privacidad.
n) Guardar la confidencialidad de los datos personales.
o) Respetar los derechos de los titulares en relación con sus datos personales.
p) Cumplir con los controles de seguridad emitidos por SMNYL, Seguridad TI y Seguridad Corporativa.
q) Reportar cualquier incidencia o vulneración a los datos personales de acuerdo a las políticas emitidas por Seguridad TI.

DE LOS MEDIOS DE ALMACENAMIENTO

Para definir los métodos de borrado, es necesario establecer la naturaleza de los activos, es decir, si los datos personales se almacenan en un medio de almacenamiento físico o un medio de almacenamiento electrónico.

a) **Físico.** Es todo recurso inteligible a simple vista y con el que se puede interactuar sin la necesidad de ningún aparato que procese su contenido para examinar, modificar o almacenar datos personales, de manera enunciativa más no limitativa pueden ser: Archiveros, Gavetas, Closets, Cajones, Bodegas, Cajas, Estantes, Carpetas, Documentos, oficinas.

b) **Electrónico.** Es todo recurso al que se puede acceder sólo mediante el uso de un equipo de cómputo que procese su contenido para examinar, modificar o almacenar los datos personales, de manera enunciativa

más no limitativa pueden ser: equipo de cómputo, memorias extraíbles como USB o SD, CDs, tarjetas de memoria, computo en la nube, disco duro, cintas magnéticas.

La Política de Uso Aceptable de Recursos Informáticos establece que los usuarios no deben almacenar información de la Compañía en recursos informáticos personales (por ejemplo: cuentas de correo personales, configurar el correo corporativo en un dispositivo móvil personal no autorizado, memorias USB, discos duros externos, etc.)

LINEAMIENTO DEL BORRADO SEGURO DE LA INFORMACIÓN

Una parte importante respecto a la gestión de los datos, son aquellas medidas que propicien el ciclo completo de vida de la información de forma segura, implementando políticas y mecanismos para garantizar el nivel de confidencialidad de la información y en consecuencia un adecuado borrado de la misma.

Se pueden encontrar diversos motivos para eliminar la información que se mantiene bajo nuestro encargo, sin embargo, se deberá velar por la adecuada gestión de los datos personales: estratégicos, legales o contables, etc., pero sobre todo se deberá conservar esta información y estos datos durante un periodo de tiempo estipulado por la legislación aplicable para tales casos.

El borrado seguro es la medida de seguridad mediante la cual se establecen métodos y técnicas para la eliminación definitiva de los datos personales, de modo que la probabilidad de recuperarlos sea mínima.

El momento indicado para eliminar los datos personales depende del plazo de conservación de los mismos, el cual se fija a partir de las disposiciones legales aplicables en la materia de que se trate: administrativos, contables, fiscales, jurídicos e históricos de la información (establecidos en la Política de Clasificación de la Información) y el periodo de bloqueo que corresponda, es por ello que SMNYL cuenta con políticas y procedimientos básicos para el cumplimiento.

Adicional a las políticas y procedimientos emitidos por La Compañía para el borrado de información, se deberán considerar:

a) A un primer proceso de reflexión interna para analizar la forma en la que eliminan los datos o entregan los dispositivos a terceros (y por tanto, ceden el control de la información).

b) Cuando se utilizan métodos de borrado dispuestos por el propio sistema operativo como con la opción «eliminar» o la tecla «Supr» o «Delete», se realiza el borrado exclusivamente en la «lista de archivos» sin que se elimine realmente el contenido del archivo, que permanece en la zona de almacenamiento hasta que se reutilice este espacio con un nuevo archivo.

   Por tanto, toda aquella acción que no conlleve la eliminación, tanto de la información de la «lista de archivos» como del contenido del mismo, no consigue destruir eficazmente dicha información.

c) Validar los métodos más eficaces que evitan completamente la recuperación de los datos contenidos en los dispositivos de almacenamiento.

d) Considerar la Guía de Destrucción de Información de SMNYL, los medios eficaces que evitan completamente la recuperación de los datos contenidos en los dispositivos de almacenamiento digital y físico como:

   - la desmagnetización. Este método expone a los dispositivos de almacenamiento a un campo magnético a través de un dispositivo denominado desmagnetizador. Debido a las fuerzas físicas del

proceso, es posible que el hardware donde se encuentra la información se vuelva inoperable, por lo que se recomienda aplicar este método si no se volverá a utilizar el medio de almacenamiento.

- Se considera más segura que algunos procesos de destrucción física, ya que altera directamente el contenido de información y no al medio de almacenamiento en sí mismo.
- la destrucción. Esta técnica busca que no sea posible recuperar la información tanto física como electrónica y evitan que personas no autorizadas puedan tener acceso a los datos.
- la sobreescritura. Consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.
- Trituración. Uno de los procesos más intuitivos para la destrucción de activos, tales como documentos, carpetas o archivo, con ello se evita la recuperación de los fragmentos y su posible reensamble.
- Incineración. Consiste en su destrucción a través del uso del fuego. (No es muy recomendable por cuestiones relacionadas con el cuidado del medio ambiente)

LINEAMIENTOS Y RECOMENDACIONES GENERALES PARA LA SALIDA DE INFORMACIÓN

1.- La entrega de datos y documentación siempre deberá ser a solicitud del titular o a través de su representante legal.

NOTA. Esta figura, se otorga mediante instrumento notarial de acuerdo a la facultad que se le requiera, por ejemplo: pleitos y cobranzas, actos de administración, dominio etc. o en su caso un poder especial para el trámite en específico.

2.- No deberás sugerir, comentar o asesorar a un cliente, asesor, agente, proveedor, representante legal, o titular de los datos el ejercer un Derecho de Acceso para la obtención de documentación.

3.- Identificar si el solicitante realmente quiere ejercer cualquier Derecho ARCO y no promuevas esta ley como un servicio adicional de SMNYL.

4.- Para entregar cualquier documento (Físicos) deberás asegurarte de que sea la persona correcta para recibir cualquier información y/o documentación que te solicite. Deberá acreditar su personalidad en caso de ser representante legal.

5.- Para la entrega o envío de datos, documentos, información a terceros:

Antes de enviar información a un tercero por cualquier medio (correo electrónico, mensajería) o almacenarla en cuentas de cómputo en la nube o publicarla en un sitio web, se debe evaluar si esta acción no está poniendo en riesgo a titulares y en su caso al personal de la organización.

Se deben tomar en cuenta los Estándares de Administración de Riesgos de Seguridad de la Información compartida con Terceros de SMNYL ya que el envío erróneo o intercepción de mensajes electrónicos (correo, mensajería instantánea, redes sociales, mensajes de texto a celular, entre otros) representa una grave fuga de información que puede perjudicar seriamente a los titulares y a SMNYL.

1.- Validación del destinatario de una comunicación.

ESPECIFICACIONES

- Con el fin de evitar fugado de información o documentación a terceros debido a la transmisión errónea de mensajes electrónicos como correos electrónicos, mensajería, etc. se debe tener total certeza antes de enviar el mensaje que se realiza al destinatario correcto y autorizado.
- Cuando se envíe un mensaje electrónico a varios destinatarios se debe revisar el método de envío 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.
- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún colaborador tercero, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- 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.

2.- Información enviada y recibida.

Cuando se envía información importante a través de mensajes electrónicos, ésta no se debería incluir bajo ninguna circunstancia en el cuerpo del mensaje, así como no establecer información que revele el contenido del o los archivos adjuntos.

Cuando se recibe información en un mensaje electrónico, sin importar quien lo haya enviado, se debe ser cuidadoso con los archivos y ligas adjuntas cuando éstas no son esperadas, por ejemplo, un mensaje de un proveedor que pide revisar una cotización no solicitada abriendo un archivo adjunto o dando clic a una liga específica.

En tal caso hay que verificar con el remitente del mensaje y/o utilizar herramientas antimalware para verificar el contenido.

En caso de efectuar un incidente de Seguridad de la Información o Una Violación de la Privacidad de Datos debes llevar a cabo lo establecido por la Política de Respuesta a Incidentes de Seguridad de la Información y ser escalados de acuerdo al Procedimiento de Administración de Incidentes de Seguridad.

3.- Información solicitada vía Telefónica.

Solo las áreas de Atención a Clientes (Oficinas regionales y CASA, cuya atención en ocasiones es vía telefónica) y Call Center podrán atender solicitudes que impliquen compartir información personal vía telefónica siempre y cuando utilicen algún mecanismo de autenticación, el resto de las áreas no podrán compartir información por este medio, en el caso que por razones de negocio se requiera compartir información por este medio se tendrán que canalizar a las áreas antes mencionadas, además de apegarse a la Matriz de servicios / información a través de atención telefónica, deberán seguir las siguientes recomendaciones:

- Validar que el solicitante tenga la capacidad para solicitar información o documentación, esto es que el solicitante sea el titular de los datos o de la documentación o en su caso ser representante legal el cual deberá acreditar con sus poderes.
- No comentar o comunicar información sin antes sin verificar y validar la identidad de la persona que está del otro lado de la línea.

  Por lo que se podrá solicitar información adicional que pueda corroborar su identidad como, por ejemplo: RFC, Correo electrónico, algo que no dé lugar a dudas de su real identidad.

- Si no se está seguro de poder identificar a la persona solicitante de información, solicita que entregue un escrito libre con la información y documentación que requiere en la ventanilla u oficina regional más cercana.
- Nunca comentar información sin antes haber validado la identificación del solicitante por este u otro medio (como el correo electrónico).
- Mantener la información clasificada con estricta confidencialidad y no divulgarla a ningún tercero.
- Ningún individuo diferente al Usuario Autorizado puede tener acceso a información clasificada como secreta, privada o confidencial*.

*Existen algunos servicios telefónicos en donde por emergencia del asegurado se puede corroborar o confirmar información a terceros, para conocer mayor detalle consulta Matriz de servicios / información a través de Atención Telefónica del Centro de Contacto de la Dirección de Operaciones.

4.- Información o documentación solicitada a través del correo: clientes@mnyl.com.mx

La entrega de información y/o documentación se hará a petición del interesado, únicamente si es dueño de los datos de información o documentación solicitada o a través de su representante legal, o en su caso del tercero designado por este para dicha tarea.

La petición podrá ser en un escrito que será de carácter libre y deberá precisar la información o documentación que desea obtener y el medio por el que desea obtener dicha petición. Así mismo:

Si es el titular de los datos:

Acompañar el escrito con su Identificación Oficial.

Si es el representante legal:

- Deberá adjuntar el escrito libre firmado por el titular (original), Identificación oficial del titular y del representante legal, y copia de los poderes notariados que le facultan como tal.
- Se deberá validar la firma del titular, así como de las identificaciones dentro de los sistemas correspondientes al resguardo de información.
- En caso de no coincidir, se notificará por el mismo medio el rechazo, notificando el motivo.

Si es el agente o asesor:

- Deberá adjuntar el escrito libre firmado por el titular, Identificación oficial del titular y del agente o asesor.
- Se deberá validar la firma del titular, así como de las identificaciones dentro de los sistemas correspondientes al resguardo de información.
- Así mismo se deberá establecer el medio en que desea recibir dicha información o documentación. Sin esta aclaración se entenderá que es por el mismo medio.
- Dicha petición no será recibida a través de Solicitud de Derecho ARCO.

5.- Información o documentación solicitada a través del agente o promotor o asesor.

En el caso en que un agente, promotor o asesor, requiera documentación o información de un cliente, deberá adjuntar el escrito libre, el cual deberá contener el detalle de la información o documentación requerida, el medio por el cual desea recibir dicha información o documentación, así como establecer que se le ha facultado para tal acción, así como la firma del titular de los datos. Así mismo deberá adjuntar copia de identificación oficial tanto del titular de los datos como su identificación oficial.

NOTA: Como identificación oficial se entiende al documento original oficial, emitido por autoridad competente, que esté vigente a la fecha de su presentación, y en donde conste fotografía, firma del portador y en su caso, domicilio del propio cliente, considerándose válido cualquiera de los siguientes: Credencial para votar emitida por el Instituto Nacional Electoral (INE), Instituto Federal Electoral (IFE) o por el Instituto Electoral Estatal (IEE) o ; Pasaporte; Formas migratorias o documentación expedida por el Instituto Nacional de Inmigración de la Secretaría de Gobernación que en su caso acredite la calidad migratoria; Cédula profesional; Cartilla del Servicio Militar Nacional; Certificado de Matrícula Consular; Tarjeta única de Identidad Militar; Tarjeta de afiliación al Instituto Nacional de las Personas Adultas Mayores; Credenciales o carnets de afiliación expedidos por el Instituto Mexicano del Seguro Social (IMSS) o el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE); Licencia de conducir expedida en México o en los Estados Unidos de América; Credenciales de residencia expedidas por autoridades migratorias de los Estados Unidos de América (Resident Alien Card); Credenciales emitidas por autoridades federales, estatales o municipales; Credenciales de Instituciones Públicas de Educación Media Superior y Superior.

RESPONSABILIDADES Y SANCIONES

Es responsabilidad de los Colaboradores:

- Entender y cumplir esta Política y el Código de Ética.
- Asegurar que el equipo de trabajo a su cargo conozca y cumpla los lineamientos de esta Política.
- Ayudar a prevenir actos de Soborno o Corrupción, estar alertas de cualquier incumplimiento y en caso de presentarse, reportarlo inmediatamente a algunos de los canales de denuncia.
- En caso de ser responsables de relaciones con Terceros, vigilar el cumplimiento de esta política.
- Contactar a la Dirección de Ética y Cumplimiento en caso de dudas.

SANCIONES POR INCUMPLIMIENTO

Si algún Colaborador incumple esta política, traerá como consecuencia según la gravedad del caso, las sanciones previstas en el Reglamento Interior de Trabajo pudiendo derivar en amonestaciones o hasta la rescisión de la relación laboral o de cualquier otro contrato con la Compañía y si fuera aplicable las sanciones civiles y penales que esto conlleve.

REPORTE DE INCUMPLIMIENTOS A LA POLÍTICA

Los Colaboradores y/o Directivos deben reportar cualquier incumplimiento a ésta Política en la línea de integridad disponible las 24 horas del día, los 7 días de la semana a través de los siguientes medios:

- Vía telefónica:

Desde cualquier teléfono fijo, móvil o al interior de SMNYL, marca: 0001 800 658 5454 y 0001 800 462 4240

Espera en la línea para la indicación "marca el número al que deseas llamar" y digita: 866-916-1888 y selecciona la opción 2 para el idioma español.

- Portal Web

Da clic aquí o copia y pega la siguiente liga en Google Chrome. https://secure.ethicspoint.com/domain/media/en/gui/23192/index.html

- Correo Electrónico

Envía un correo al buzón electrónico: Compliance_Comunica@mnyl.com.mx

Canaliza cualquier comportamiento que pueda poner en riesgo a nuestra Compañía, recuerda que en cualquiera de los medios, tu denuncia es abordada de forma totalmente confidencial y anónima.

10. RESPONSABILIDADES

NO.	RESPONSABLE	RESPONSABILIDADES
1	Dueño de la información	• Asegurarse del cumplimiento de las obligaciones y responsabilidades a su cargo, las cuales se describen en el documento denominado "Roles y Responsabilidades de Seguridad de la Información" que se agrega como Anexo a esta Política. • Asegurar que los datos a recabar, finalidades y transferencias, según sea el caso, se encuentren cubiertos por los términos del Aviso de Privacidad (Ver: "Anexo 1") y Consentimientos a recabar (Ver: "Anexo 2 Consentimientos"), en caso contrario se deberá informar al Oficial de Privacidad antes de realizar cualquiera de las actividades antes mencionadas. • Adoptar medidas de seguridad tanto físicas como electrónicas (Numeral 10.7 "Seguridad de la información en la Compañía" de esta política) 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 personales y se implementen las medidas conducentes.

- 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.
- 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.
- Dicho procedimiento deberá contemplar un periodo de conservación de acuerdo a lo indique la Ley que corresponda, durante dicho periodo los Datos no podrán ser objeto de tratamiento.
- Al finalizar este periodo, el dueño de la información deberá garantizar la destrucción de la misma.
- Proteger del uso inapropiado, daño, pérdida, divulgación indebida o venta de los "datos" de los clientes, socios comerciales, prospectos y empleados de la Compañía conforme a las disposiciones que establece la Ley.
- Realizar el tratamiento de Datos en un espacio físico seguro para evitar que personas ajenas a su proceso tengan acceso a la misma. De igual manera, los lugares donde se almacena información personal deben tener medidas de control de acceso, para mayor información consulta el Manual de Estándares Corporativos de Seguridad de la Información
- Asegurar que se mantenga actualizado el Inventario de Clasificación de la Información, identificando al menos las siguientes características:
  - Dueño de la Información
  - Tipo de dato (datos personales, personales sensibles, financieros y/o patrimoniales)
  - Tipo de clasificación (pública, privada, secreta o confidencial)
  - Origen
  - Destino
  - Método de envío de información

RESPONSABILIDADES

		– Medio de almacenamiento (sistemas, documentos físicos). – Periodo de conservación y fecha de destrucción. • Informar al Oficial de Privacidad y/u Oficial de Seguridad de la Información sobre cualquier tipo de desviación o vulneración encontrada en los procesos en donde se recabe, utilice, o almacenen Datos. • Asegurarse que las extracciones de información de los SATIs cumplen con lo estipulado en el procedimiento correspondiente antes de dar su aprobación para que la información sea extraída. • Asegurarse de que el tratamiento de Datos, en los procesos a su cargo, se hace en cumplimiento con todas las regulaciones aplicables.
2	Encargado	Respecto del tratamiento que realice por cuenta de la Compañía: • Tratar únicamente los datos personales conforme a las instrucciones de la Compañía. • Abstenerse de tratar los datos personales 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 personales tratados. • Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. • Abstenerse de transferir los datos personales 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

RESPONSABILIDADES

		• Efectúe una transferencia, incumpliendo las instrucciones del responsable. • El encargado no incurrirá en responsabilidad cuando, previa indicación expresa de La Compañía, remita los datos personales a otro encargado designado por este último, al que hubiera encomendado la prestación de un servicio, o transfiera los datos personales a otro responsable conforme a lo previsto en las políticas de la Compañía.
3	Colaboradores	En caso de recabar datos personales y/o sensibles: ▪ Deberá 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. • Proteger del uso inapropiado, daño, pérdida, divulgación indebida o venta de los "datos" de los clientes, socios comerciales, prospectos y empleados de la Compañía conforme a las disposiciones que establece la Ley. • Clasificar y tratar todos los Datos como información privada, de acuerdo a la Política de Clasificación de la Información, la cual establece estándares mínimos de uso general para la protección de la información privada que deben ser cumplidos. • Realizar el tratamiento de Datos en un espacio físico seguro para evitar que personas ajenas a su proceso tengan acceso a la misma. De igual manera, los lugares donde se almacena información personal deben tener medidas de control de acceso, para mayor información consulta el Manual de Estándares Corporativos de Seguridad de la Información. • Cumplir con los lineamientos de la Política de seguridad de laptops y dispositivos de almacenamiento portátiles. • Recabar el consentimiento del titular cuando corresponda, conforme a lo que indica la Ley. • Asegurarse de que el tratamiento de Datos Personales, en los procesos a su cargo, se hace en cumplimiento con todas las regulaciones aplicables.

RESPONSABILIDADES

4	Seguridad Corporativa de SMNYL	• Establecerá los lineamientos básicos para el manejo de la información documental, a partir de la correcta clasificación, resguardo, archivo y destrucción corporativos.
5	Oficial de Privacidad	• Diseñar y ejecutar una política y/o prácticas de protección de datos personales al interior de la organización, o bien, adecuar y mejorar las prácticas ya existentes en el marco de la Ley. • Monitorear y evaluar los procesos internos de la organización vinculados con la obtención, uso, explotación, conservación, aprovechamiento, cancelación y transferencia de datos personales, a fin de asegurar que la información sea protegida, tratada conforme a los principios de la Ley. • Colaborar y coordinar acciones con otras áreas de la organización como legal, de tecnologías, sistemas, seguridad de la información, mercadotecnia, atención al cliente, recursos humanos, entre otras, a efecto de asegurar el debido cumplimiento de la política y/o prácticas de privacidad en sus procesos internos, formatos, avisos, recursos y gestiones que se lleven a cabo. • Asegurar que la política y/o prácticas de protección de datos personales cumplan con la Ley y demás normatividad aplicable. • 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. • Monitorear el cumplimiento de la política y/o prácticas de protección de datos personales de las sociedades subsidiarias o afiliadas bajo el control de común de la organización o cualquier sociedad del mismo grupo del responsable que opere y le sean aplicables estas prácticas. • Identificar e implementar mejores prácticas relacionadas con la protección de datos personales.

- Ser el representante de la organización en materia de protección de datos personales ante otros actores.