Programa de Seguridad de la Información y Ciberseguridad de Seguros Monterrey New York Life (SMNYL)

SMNYL comprometido a mantener seguros tus Datos.

La Seguridad y protección de los Datos de nuestros clientes, colaboradores y socios comerciales es prioridad en SMNYL. Estamos comprometidos a mantener un entorno seguro para todos los aspectos de nuestras operaciones porque reconocemos la importancia crítica de la ciberseguridad en el mundo digital actual. Como compañía de seguros y parte de nuestro programa, cumplimos con todas las leyes y regulaciones correspondientes.

A través de esta postura pública, queremos comunicar nuestros principios fundamentales en cuanto a ciberseguridad:

1. Compromiso con la Seguridad:

SMNYL está comprometido con mantener los más altos estándares de seguridad cibernética (ISO27001, NIST, PCI, entre otros). Invertimos de manera continua en la actualización de nuestras tecnologías y procesos para proteger los Datos Personales y la Información Confidencial de nuestros clientes, colaboradores y socios comerciales.

2. Cumplimiento Normativo:

Cumplimos con todas las leyes y regulaciones aplicables en México relacionadas con la ciberseguridad. En SMNYL trabajamos y estamos comprometidos con llevar a cabo las mejores prácticas de la industria y adaptarnos a los cambios regulatorios.

3. Educación y Concienciación:

Creemos que la educación es esencial para la prevención de amenazas cibernéticas. El área de Seguridad de la Información tiene programas continuos de capacitación y concientización sobre seguridad para informar al personal (colaboradores, agentes y promotores) sobre cómo estar alerta y protegerse contra posibles violaciones de seguridad y divulgaciones no autorizadas, para ayudar a identificar y mitigar riesgos.

4. Protección de Datos:

Salvaguardamos los Datos de nuestros clientes con medidas de seguridad robustas basadas en marcos de referencia como ISO27001 o PCI. Utilizamos controles como cifrado, autenticación de múltiples factores y políticas de acceso restringidas para proteger la información.

5. Respuesta ante Incidentes:

Contamos con un equipo de respuesta a incidentes para actuar en caso de una violación de seguridad. Mantenemos planes de continuidad del negocio para minimizar el impacto en nuestros servicios en caso de un incidente.

6. Evaluación Periódica:

Realizamos evaluaciones regulares de riesgos y auditorías de seguridad para garantizar que nuestras políticas y prácticas de ciberseguridad estén actualizadas y sean efectivas.

7. Reporte:

Los agentes y promotores cuentan con un canal de comunicación a través del cual ellos pueden reportar preocupaciones, dudas o sugerencias con base en lo que enfrentan en su día a día y así poder fortalecer la ciberseguridad en toda la cadena de valor de SMNYL.

De manera constante, **SMNYL mejora su Programa de Seguridad de la Información y Ciberseguridad.** Para determinar el nivel adecuado de controles de seguridad, se realizan evaluaciones periódicamente que tienen en cuenta los avances tecnológicos, las amenazas emergentes y nuestra dirección estratégica general, entre otros factores. Además, el plan anual de la Dirección de Auditoría Interna de SMNYL incluye auditorías de los controles de Seguridad de la Información.

Asimismo, para garantizar una gestión y supervisión efectivas de los riesgos y un camino claro para su escalada, **contamos con una estructura de gobernanza de riesgos** que evalúa periódicamente la efectividad de los controles de implementados en colaboración con las distintas líneas de defensa.

En SMNYL se ha desarrollado un modelo de seguridad de múltiples capas que se basa en los estándares de seguridad de la industria reconocidos internacionalmente como ISO 27001, NIST-CSF y COBIT, y ofrece una forma coherente de administrar capacidades, actividades y riesgos.

El Programa de Seguridad de la Información y Ciberseguridad de SMNYL se basa en políticas y estándares formalizados y difundidos entre los colaboradores y proveedores. **El Programa tiene como objetivo** mantener la confidencialidad, la integridad y la disponibilidad de nuestros Activos de Información.

En SMNYL el modelo de defensa consiste en una serie de capas de procesos y tecnologías que **ayudan a prevenir, detectar y responder a las amenazas,** es el núcleo del programa. Para desviar las amenazas cibernéticas antes de que se conviertan en incidentes, se utilizan tecnologías preventivas como el bloqueo de correo electrónico malicioso y puntos de entrada seguros a la red en las capas externas de este modelo, es decir, el uso de comunicaciones seguras tipo VPN y controles de acceso remoto. así como tecnologías de monitoreo de eventos que están disponibles las 24 horas del día, los siete días de la semana, los 365 días del año para detectar y responder a intentos de intrusión potenciales y generar alertas que se gestionan de acuerdo con el protocolo de respuesta establecido.

Las fuerzas del orden (policía cibernética) y otros líderes globales en la comunidad de ciberseguridad pueden colaborar en cualquier momento con SMNYL para mejorar la protección de nuestros sistemas, estas relaciones, además de las notificaciones diarias de inteligencia de seguridad de múltiples fuentes, nos ayudan a recibir alertas sobre amenazas emergentes, ataques y tendencias de vulnerabilidad.

Finalmente es **importante señalar que después de implementar estos controles y protecciones,** entendemos que la naturaleza cambiante del entorno de ciberseguridad nos obliga a evaluar y mejorar continuamente estas protecciones, mejorando nuestros controles, procesos y herramientas cuando sea necesario. A pesar de que ningún método de seguridad puede garantizar completamente la protección contra todas las amenazas, SMNYL ha creado e implementado un Programa de Seguridad de la Información y Ciberseguridad sólido que se centra en proteger nuestros sistemas y Datos de nuestros clientes, colaboradores y socios comerciales.

NEW YORK LIFE SEGUROS MONTERREY