

Política de Outsourcing

OHIO NATIONAL SEGUROS DE VIDA S.A.

Historial de versiones.

Versión	Fecha	Modificado por	Descripción breve
V0.1	09.2018	Gerencia de Riesgos	Borrador Política de Outsourcing
V0.1	12.2018	Gerencia legal	Borrador Política de Outsourcing
V0.1.	02.2019	Gerencia Legal	Borrador Procedimiento
V.01	02.2019	Gerencia de Finanzas y Administración	Borrador Procedimiento
V02	04.2020	Gerencia Legal/ Área de Cumplimiento	Modificación y Actualización
V03	04.2021	Gerencia Legal/ Área de Cumplimiento	Modificación y Actualización
V.04	04.2022	Gerencia Legal/ Área de Cumplimiento	Modificación y Actualización
	04.2022	Gerencia de Riesgos/ Of. Seguridad Información	Revisión
V.05	05.2023	Gerencia Legal/ Área de Cumplimiento	Modificación y Actualización
	05.2023	Gerencia de Riesgos/ Of. Seguridad Información	Revisión
V.06	05.2024	Gerencia Legal/ Área de Cumplimiento	Modificación y Actualización
	05.2024	Gerencia de Riesgos/ Of. Seguridad Información	Revisión

Aprobada por Directorio 30/05/2024

Copyright © Ohio National Seguros de Vida S.A. Todos los derechos reservados.
Su uso requiere la autorización expresa de Ohio National Seguros de Vida S.A.

Indice

1.	Introducción	3
2.	Objetivos y Alcance	3
3.	Marco de Externalización de Servicios	3
4.	Condiciones generales para la externalización de Servicios	4
5.	Contrato de prestación de Servicios	6
6.	Roles y Responsabilidades	7
7.	Aprobaciones y actualizaciones	7
8.	Distribución de la Política	7

Anexo: Servicios en la Nube

1. Introducción

Ohio National Seguros de Vida (ONSV), en adelante indistintamente Ohio National o la Compañía, está comprometida en fortalecer su Gobierno Corporativo a través de establecimiento e implementación de prácticas, políticas, procedimientos, medidas y controles que permitan robustecer su Sistema de Gestión de Riesgos, como asimismo está comprometida con el desarrollo de una estrategia de negocio que incorpore las diferentes dimensiones en materia de sustentabilidad, las que se engloban bajo el concepto ASG. ASG y/o ESG por sus siglas en inglés.

Una sólida gestión de riesgos y de compliance se basa en la existencia de una adecuada estructura de gobierno, un marco con políticas, normas y procedimientos, así como un entorno que permita identificar, evaluar, controlar, mitigar, monitorear y reportar los riesgos más relevantes asociados al Outsourcing de actividades.

Outsourcing es el proceso mediante el cual la empresa externaliza una parte de su actividad, es decir, contrata a una empresa externa especializada para gestionar una parte de la compañía, con el objetivo de lograr una mayor eficiencia, reducción de costos, acceso a nuevas tecnologías, fines estratégicos, etc. La externalización de servicios puede ser implementada en diferentes materias, niveles y áreas de la Compañía.

2. Objetivos y Alcance

2.1 Objetivo

El objetivo de este documento es definir los lineamientos que permitan regular adecuadamente la externalización de servicios (Outsourcing) por parte de Ohio National Seguros de Vida S.A., como también las condiciones que permitan gestionar adecuadamente el riesgo operacional, de ciberseguridad, estratégico, reputacional y legal asociado.

2.2 Alcance

El alcance de este documento está relacionado con las actividades que realiza la Compañía para la contratación de proveedores de servicios externos, con el objeto de que éstos realicen una o más actividades operativas que podrían ser también efectuadas internamente por la Compañía con sus propios recursos, tanto humanos como tecnológicos. Las disposiciones de este documento no son aplicables a aquellos servicios que la Compañía no puede proveerse a sí misma, tales como los servicios básicos o aquellos donde una ley ha definido que deben ser prestados por entidades de giro exclusivo.

3. Marco de Externalización de Servicios

Por regla general Ohio National no externalizará actividades o procesos significativos o estratégicos, es decir, procesos críticos.

Se entiende por proceso crítico, aquellas actividades de importancia en las que cualquier debilidad o falla en la provisión o ejecución del servicio tiene un efecto significativo sobre el cumplimiento normativo, continuidad del negocio, seguridad de la información y Ciberseguridad (propia o de los clientes), la calidad de los servicios, productos, información e imagen de la compañía, como también, cualquier actividad que involucre el procesamiento de datos de carácter personal o sensible, y cualquier actividad que tenga impacto significativo en la gestión de riesgos.

En el evento de que Ohio National decida externalizar una actividad o proceso crítico, además de cumplir con los requerimientos que se establecen en la presente política y en el "Procedimiento de evaluación selección y

contratación de proveedores”, deberá contar con una evaluación de riesgos específica, y con la autorización previa del Directorio de la compañía.

4. Condiciones Generales para la externalización de servicios

- a) Toda Contratación de un proveedor, sea crítico o no se regirá por el “Procedimiento de evaluación selección y contratación de proveedores”
- b) La administración, a través de la Gerencia que solicite la externalización de un servicio, deberá:
 - Velar por que el proveedor y el personal a cargo de los servicios contratados posean adecuados conocimientos y experiencia.
 - Velar por que el proveedor posea buenas prácticas en temas laborales, salud y seguridad de sus empleados, y realice esfuerzos para la protección del medio ambiente y conservación de recursos.
 - Verificar que el proveedor cuenta con mecanismos que permitan prevenir que acciones realizadas por otros clientes afecten negativamente el servicio contratado.
- c) La Gerencia Legal deberá vigilar el debido cumplimiento de aquellos aspectos regulatorios y legales que pudiesen afectar la provisión de los servicios contratados en los respectivos contratos. Asimismo, llevará el catastro y seguimiento de toda la documentación legal relacionada con el proveedor y los contratos a través del Sistema de Gestión Registro y Seguimiento de Contratos.
- d) La Gerencia de Riesgo deberá revisar el debido cumplimiento de la política y procedimientos que digan relación con protección de datos, seguridad de la información y ciberseguridad.
- e) La Gerencia de Inversiones y Finanzas deberá mantener un listado de proveedores que permita ejecutar los controles y seguimientos para la validación de los pagos con las respectivas órdenes de compra y/o contratos respectivos.
- f) El Comité de Auditoría del Directorio velará por que existan auditorías independientes al proceso de selección, contratación y seguimiento de los proveedores.
- g) En el evento de que el servicio externalizado revista un riesgo operacional evaluado como medio alto, se deberá asegurar que el proveedor realice periódicamente informes de auditoría interna o revisiones independientes de sus servicios, conforme con su estructura y el tamaño de su organización, debiendo compartir oportunamente con la institución los hallazgos que le sean pertinentes.

4.1 Selección del proveedor de Servicios

Ohio National debe evaluar las propuestas recibidas de acuerdo con sus requerimientos y llevar a cabo un “due diligence” que sustente la información recibida de los posibles proveedores, lo cual comprende la declaración de conflictos de interés y la aplicación del Manual LAFT de Ohio National.

Asimismo deberá considerar las políticas o prácticas que el proveedor tenga en materia de sustentabilidad, tales como prácticas laborales, de inclusión, diversidad y equidad, cuidado del medio ambiente, responsabilidad social, entre otros, para lo cual se aplicará un cuestionario sobre lineamientos que pueda tener el proveedor en materia ASG.

En el caso de que se contrate un servicio con una entidad relacionada, se deberá dar cumplimiento a la “Política para las Transacciones u Operaciones con Accionistas, directores, Principales Ejecutivos y Partes Relacionadas

y Acceso a Información Privilegiada” y en el “Procedimiento de Administración de Información Privilegiada y Transacciones entre Partes Relacionadas” de Ohio National.

4.2 Continuidad del Negocio

Ohio National debe verificar que sus proveedores de servicios críticos cuenten con planes apropiados que aseguren la continuidad de los servicios contratados (BCP), y con un proceso formal y sistemático de gestión frente a los incidentes que pudieran interrumpir o afectar la provisión de los productos, servicios o actividades. De igual forma se debe verificar que sus proveedores críticos aseguren que los servicios subcontratados por éstos cuentan con apropiados planes de continuidad del negocio.

Esos planes deben ser probados al menos una vez al año incluyendo, cuando corresponda, el escenario de desastre de sus distintos sitios de procesamiento, debiendo Ohio National tomar conocimiento de dicha actividad y verificar los resultados obtenidos.

Adicionalmente, Ohio National también debe disponer de planes, igualmente probados, para asegurar la continuidad operacional ante la contingencia de no contar con dicho servicio externo.

Estas verificaciones y actividades serán realizadas por la Gerencia de Operaciones y Sistemas en conjunto con la Gerencia de Riesgos y la Gerencia a la cual se encuentra asociada la actividad a externalizar, debiendo dejar evidencia escrita de la actividad realizada.

Finalmente, Ohio National debe contar con cláusulas de salida en el evento de incumplimientos de los proveedores en esta materia que consideren el término anticipado de la relación contractual y que permitan retomar la operación, ya sea por cuenta propia o mediante otro proveedor.

4.3 Seguridad de la Información y Ciberseguridad

Ohio National debe cerciorarse que el proveedor de servicio mantiene un programa de seguridad de la información que le permita asegurar la confidencialidad, integridad, trazabilidad y disponibilidad de sus activos de información y la de sus clientes, en especial la protección de datos personales. Dicho programa deberá cumplir los estándares mínimos que determine Ohio National, y será incorporado al contrato de prestación de servicios.

Para estos efectos Ohio National contará con un **Protocolo de Seguridad de la Información para Proveedores**, en el que clasificará a sus proveedores de acuerdo al nivel de información confidencial que manejan a fin de definir distintos niveles y requerimientos específicos de seguridad asociado a cada uno de ellos.

Ohio National debe controlar y monitorear la infraestructura de seguridad de la información dispuesta por el proveedor, con el objeto de proteger los activos de información presentes en los servicios críticos externalizados, independientes de los controles dispuestos por el proveedor. De igual forma, debe controlar y monitorear: la conexión de acceso a la red, la gestión de identidades, control de accesos a la información referida a dichos servicios críticos. Para estos efectos en el **Protocolo de Seguridad de la Información para Proveedores** se establecerán los controles específicos a realizar por la Compañía y su periodicidad.

Las conexiones de comunicaciones entre Ohio National y el proveedor de servicios deben contar con un nivel de cifrado que asegure la confidencialidad y la integridad de los datos de punta a punta (end to end).

Ohio National debe asegurarse que el proveedor disponga de medidas efectivas de control y protección sobre ataques externos que persigan la indisponibilidad de los servicios contratados, como, por ejemplo, los de denegación de servicios. Adicionalmente, para los servicios críticos externalizados, Ohio National deberá

controlar la realización periódica por parte del proveedor de evaluaciones de vulnerabilidades de su infraestructura tecnológica y tests de penetración.

Esta actividad estará a cargo de la Gerencia de Operaciones y Sistemas, a través del Departamento de Infraestructura.

Los proveedores de servicios proporcionarán a Ohio National, siempre que sea requerido, un listado actualizado con la relación de personal, perfiles, funciones y responsabilidades asociados al servicio prestado a la compañía, e informará de manera oportuna cualquier modificación (ingresos, salidas, reemplazo o cambio de funciones o responsabilidades) que se produzca en dicha relación.

En el caso de procesamiento de documentación física, Ohio National deberá contar con procedimientos de control que velen por el debido cumplimiento de las condiciones señaladas precedentemente. Junto a lo anterior, se deben establecer los procedimientos que aseguren el adecuado traspaso de información a Ohio National por parte del proveedor, y que éste en ningún caso mantenga información en su poder después de finalizada la relación contractual.

Los proveedores de servicios, mediante el documento “**Protocolo de Ciberseguridad para Proveedores de Bienes y Servicios**”, se comprometen a comunicar de manera oportuna cualquier incidente, debilidad, vulnerabilidad o amenaza (observada, identificada o sospechada) que pudiera afectar los recursos o información propiedad de Ohio National, de sus clientes y/o asegurados.

Dicho protocolo establece lineamientos e instrucciones para notificar estos incidentes, lo que permitirá coordinar acciones de comunicación, contención y mitigación. Para la apropiada gestión de comunicación del incidente el proveedor deberá señalar, a los menos, la persona de contacto, así como el número de teléfono y/o correo electrónico.

4.4 Criterios ASG

Ohio National al momento de evaluar y seleccionar a un proveedor de servicios, privilegiará en la medida de lo posible a aquel que cuente con políticas o prácticas en materia de sostenibilidad, en su compromiso de implementar una estrategia de sustentabilidad que involucre a todos sus proveedores en el mediano plazo.

5. Contrato de prestación de Servicios

Ohio National debe asegurarse que el contrato defina claramente los derechos y obligaciones de ambas partes, conteniendo acuerdos de niveles claros y medibles de los servicios contratados, cláusulas de término anticipado de la relación contractual, así como también un método de fijación de precios adecuado para el contrato específico. En caso de que se adquiera más de un servicio por un precio único, debe tenerse el detalle del cobro por cada uno de tales servicios.

También se deben incluir cláusulas de Probidad, Modelo de Prevención de Delitos, Continuidad del Negocio, Seguridad de la Información y Ciberseguridad, especialmente aquella que se refiere a la propiedad, protección de datos personales y confidencialidad de la información, tanto propia como de sus clientes; restricciones sobre el uso de software; eliminación segura de los datos del cliente, cuando corresponda; además de establecer una autorización permanente que permita a Ohio National examinar in situ, o en forma remota, según se disponga, en cualquier momento, todos los aspectos relacionados con el servicio contratado.

Adicionalmente, Ohio National podrá considerar cláusulas de veto en la selección de subcontratación de terceros por parte del proveedor principal o a lo menos de notificación obligatoria con cláusula de salida. Contractualmente debe quedar claramente establecido todo lo relacionado con la idoneidad y responsabilidad

del personal de la empresa proveedora del servicio, así como también todos los aspectos legales y laborales que imperen en el país o en el extranjero, aplicables a estas contrataciones.

Por último, todos los contratos, subcontratos y sus respectivos anexos, deberán estar en idioma español, o bien traducidos a este idioma, y con las correspondientes rúbricas de las partes.

El área legal será responsable de velar por el contenido del contrato y darle una final aprobación.

6. Roles y responsabilidades

Sin perjuicio de lo establecido en los puntos precedentes de esta política, a continuación, se detallan los roles y responsabilidades desde el punto de vista del Gobierno Corporativo, relacionados con la Externalización de Servicios en la Compañía:

- **Directorio**
 - Velar y supervisar el cumplimiento de los lineamientos generales para la externalización de servicios que realiza ONSV.
 - Aprobar la externalización de servicios críticos.
 - Aprobar la política y sus modificaciones.
- **Gerencia General**
 - Velar y supervisar el cumplimiento de los lineamientos generales para la externalización de servicios que realiza ONSV.
 - Aprobar la externalización de servicios no críticos
- **Área de Cumplimiento**
 - Asegurar el cumplimiento de la presente política en toda externalización de servicios que lleve a cabo la compañía.
- **Área de Auditoría Interna**
 - Auditar el cumplimiento de la presente política y procedimientos asociados, y evaluar su efectividad.
- **Gerencia de Riesgos**
 - Mantener actualizado el apetito de riesgo y evaluar el riesgo asociado a cada servicio externalizado, particularmente aquellos que representen un riesgo medio-alto y superior, y aquellos que revistan la calidad de servicios críticos.
 - Velar por que se dé cumplimiento a los procedimientos de Ciberseguridad.

7. Aprobaciones y actualizaciones

Este documento debe ser aprobado por el Directorio, y será revisado a lo menos una vez al año o cada vez que exista un cambio significativo en las condiciones internas y cuando ocurran cambios normativos. La revisión de la presente política estará a cargo de la Gerencia Legal.

8. Distribución de la Política

Toda modificación y actualización de la presente política será notificada y difundida al personal mediante correo electrónico y publicada en la intranet de la compañía.

ANEXO SERVICIOS EN LA NUBE

La computación en la nube o *cloud computing* engloba la evolución de varios ámbitos de las tecnologías de la información, tales como las redes de telecomunicaciones y los microprocesadores, siendo la virtualización o abstracción del *hardware* una de las más relevante.

Por la variedad de servicios que es posible acceder a través de la nube, como de infraestructura, plataforma o incluso de *software*, se advierte una modificación en la dinámica de los riesgos asociados a los actuales modelos tecnológicos de la empresa.

Para efectos de contratar cualquier tipo de servicio a través de la modalidad denominada nube, el Directorio deberá pronunciarse sobre la tolerancia al riesgo que está dispuesto a asumir en este tipo de externalizaciones a lo menos anualmente. Este pronunciamiento deberá considerar un análisis de los datos a almacenar o procesar bajo esta modalidad y su ubicación.

En el evento que la entidad evalúe la contratación de un servicio en la nube para una actividad considerada estratégica o crítica, Ohio National deberá realizar una diligencia reforzada del proveedor y del servicio, que al menos considere lo siguiente:

- a) El proveedor dispone de reconocido prestigio y experiencia en el servicio que otorga.
- b) El proveedor contratado cuenta con certificaciones independientes reconocidas internacionalmente, en términos de gestión de la seguridad de la información, la continuidad del negocio y la calidad de servicios que recojan las mejores prácticas vigentes.
- c) Los contratos de externalización de servicios son celebrados directamente entre la Compañía y los proveedores, con la finalidad de minimizar los riesgos que podría aportar el rol de intermediario en este tipo de servicios.
- d) Revisar la regulación sobre privacidad y acceso a la información existentes en jurisdicciones donde se esté llevando a cabo el servicio.
- e) Se aplicará el procedimiento de debida diligencia al proveedor de acuerdo a lo establecido en el Manual LAFT.
- f) El Proveedor cuente con adecuados mecanismos de seguridad, tanto físicos como lógicos, que permitan aislar los componentes de la infraestructura nube que la entidad comparte con otros clientes del proveedor, de manera de prevenir fugas de información o eventos que puedan afectar la disponibilidad, confidencialidad e integridad de los datos de la entidad.
- g) Identificación de los datos que por su naturaleza y sensibilidad deben contar con mecanismos fuertes de encriptación.

Toda la documentación que respalda lo señalado precedentemente deberá estar disponible para presentarla a la entidad supervisora en caso de fiscalización.