Activamos soluciones legales
para vidas reales

ISPL1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ONLYGAL SEGUROS

Contenido:	Este documento define los principios de seguridad de la información para onLygal Seguros y onLygal Servicios
Ámbito de aplicación	onLygal Seguros y onLygal Servicios
Versión:	3.4
Fecha vigor:	01/12/2025
Realizado por:	Roger Martinez
Aprobado por:	Consejo de Administración
Estado:	Aprobado
Clasificación:	Uso interno
Período de retención:	6 años

Índice

1 Objetivo

La seguridad de la información –confidencialidad (no divulgación de información no autorizada), integridad (no realización de cambios sin autorización), y disponibilidad (disponibilidad de la información en concordancia con los requerimientos de los procesos de negocio) es un factor clave de éxito para onLygal Seguros y onLygal Servicios y se está volviendo cada vez más importante debido a la digitalización de nuestro negocio. Al mismo tiempo, cada vez es más difícil garantizar la seguridad de la información. Como resultado de esto, se deben abordar riesgos adicionales. Esto se relaciona, entre otras cosas, con el uso de nuevas infraestructuras, como la computación en la nube, sin mencionar el creciente número de ciberataques cada vez más agresivos y sofisticados.

Además, la información sobre clientes, productos y procesos de onLygal Seguros y onLygal Servicios no solo se guarda en los ordenadores. Por lo tanto, también los documentos impresos, las notas manuscritas o las conversaciones deben estar adecuadamente protegidos. Esto no solo se aplica a onLygal Seguros y onLygal Servicios sino a toda la economía y a la sociedad, y se refleja en un número cada vez mayor de requisitos reglamentarios y legales.

Por esta razón, el Consejo de Administración de onLygal Seguros ha decidido establecer un Sistema de Gestión de Seguridad de la Información (ISMS en inglés) en onLygal Seguros y onLygal Servicios con el fin de alcanzar y mantener los niveles adecuados de seguridad de la información. El ISMS está orientado hacia la norma internacionalmente reconocida ISO / IEC 27001: 2022. Además, tiene en cuenta las directrices sobre gobernanza y seguridad de las tecnologías de la información de EIOPA (en adelante DGSEIOPA).

Este documento define los principios de seguridad de la información para onLygal Seguros y onLygal Servicios y por lo tanto toma en cuenta los requisitos legales y regulatorios aplicables.

La política sirve como base para la administración de la seguridad de la información y para regulaciones específicas a fin de proteger la confidencialidad, integridad (que incluye además el concepto de autenticidad) y disponibilidad de la información dentro de onLygal Seguros y onLygal Servicios contra amenazas internas o externas, ya sean intencionales o no.

Además, la 'Política de Continuidad de Negocio' establece los requisitos mínimos, los objetivos, las responsabilidades, los procesos y los procedimientos de información para la Gestión de la Continuidad del Negocio (BCM en inglés) de acuerdo a lo establecido en las directrices 19, 21, 22 y 23 de DGSEIOPA.

Por lo tanto, ISMS y BCM respaldan a onLygal Seguros y onLygal Servicios en la protección de la información, así como en la recuperación de negocios de situaciones de emergencia y crisis.

2 Alcance

Empresas y empleados a los que se dirige:

La Política de Seguridad de la Información será aplicable a todos los trabajadores de **onLygal Seguros y onLygal Servicios** sean o no empleados indefinidos, temporales o de ETT’s, incluyendo cualquier persona ajena a **onLygal Seguros y onLygal Servicios** que tenga acceso a

la información gestionada o propiedad de la misma. La Política también será aplicable a toda la información en soporte digital y a los sistemas de Información propiedad de **onLygal Seguros** o gestionados para **onLygal Seguros**.

Normas con las que está relacionada:

Este documento está relacionado con los siguientes:

- Política corporativa de seguridad de la información.

Objeto de la norma:

Este documento define los principios de seguridad de la información para onLygal Seguros y onLygal Servicios, por lo tanto toma en cuenta los requisitos legales y regulatorios aplicables, de acuerdo a lo establecido en la directriz 6 de DGSEIOPA. La política sirve como base para la administración de la seguridad de la información y para regulaciones específicas a fin de proteger la confidencialidad, integridad (que incluye además el concepto de autenticidad) y disponibilidad de la información dentro de onLygal Seguros y onLygal Servicios contra amenazas internas o externas, ya sean intencionales o no, con el fin de asegurar todas las actividades ligadas al diseño y a la contratación de los seguros, la gestión de los siniestros y los servicios de asesoría jurídica.

3 Requisitos mínimos y responsabilidades correspondientes

El Consejo de Administración de onLygal Seguros encarga al Director de Organización y TI, en su función de Responsable de seguridad de la información (ISO), que establezca la estrategia de seguridad de la información y defina, dirija, supervise y desarrolle aún más el sistema de gestión de seguridad de la información (directriz 7 de DGSEIOPA).

El ISO define y mantiene los requisitos de seguridad de la información para todo el grupo y los desarrolla en forma más. El papel del ISO es parte de la función de gestión de riesgos independiente (2da línea de defensa - 2nd LoD). En esta función, el ISO establece disposiciones para la identificación y control consistentes de los riesgos de seguridad de la información y que la organización del ISMS está estandarizada. El ISO puede escalar, si es necesario, temas relevantes de seguridad de la información directamente al miembro responsable para la seguridad de la información del Consejo de Administración del Grupo Mutua de Propietarios.

La gestión operativa (1st Line of Defense - 1st LoD) es responsable de definir, implementar y controlar las medidas de seguridad de la información para el manejo de riesgos y el cumplimiento de los requisitos de seguridad de la información.

Cada empleado, contratista y usuario externo de onLygal Seguros y onLygal Servicios (por ejemplo, un socio de ventas) garantiza dentro de su área de responsabilidad que la información del cliente y de la empresa esté protegida de manera apropiada.

4 Principios de la seguridad de la información

4.1 Gobierno basado en riesgo de seguridad de la información

No es posible proporcionar seguridad total para toda la información. Además, no toda la información requiere la misma protección. onLygal Seguros y onLygal Servicios, por lo tanto, gestionan la seguridad de la información basado en el riesgo (directriz 4 de DGSEIOPA). Esto hace posible que onLygal Seguros y onLygal Servicios faciliten y usen recursos en las áreas donde más urgentemente se requieren. El ISO, por esta razón, define los requisitos unificados para la gestión de los riesgos de seguridad de la información y, por lo tanto, facilita y supervisa las decisiones basadas en el riesgo.

4.2 Cada empleado es conocedor de su responsabilidad individual en la seguridad de la información

Tanto los empleados internos como externos de onLygal Seguros y onLygal Servicios se encuentran entre los factores de éxito más importantes para garantizar los niveles de seguridad de la información requeridos. Numerosas medidas de seguridad solo pueden implementarse eficazmente si los empleados internos y externos son suficientemente conscientes de la seguridad de la información y tienen suficientes habilidades en el campo de la seguridad de la información. El ISO, por lo tanto, desarrolla un concepto que sirve como base para definir las medidas de concientización y capacitación centradas en los grupos objetivo que luego son proporcionadas por onLygal Seguros y onLygal Servicios (directriz 13 de DGSEIOPA).

4.3 Cumplimiento de requisitos mínimos unificados de seguridad de la información

El nivel de seguridad de la información que se requiere en todo el Grupo solo puede garantizarse mediante requisitos mínimos unificados y vinculantes y sus características locales. Por esta razón, hay tres niveles de política de seguridad de la información (ISPL en inglés) basados el uno en el otro:

- Esta Política de Seguridad de la Información (ISPL1) describe en el nivel superior los principios y objetivos de la seguridad de la información del onLygal Seguros y onLygal Servicios.
- Los documentos ISPL3 (consulte el anexo 1) establecen en detalle los requisitos de seguridad para todo el grupo teniendo en cuenta los condicionantes legales que puedan ser de aplicación en cada caso.
- Los documentos ISPL4 describen las instrucciones específicas para los procesos de seguridad de la información, los procedimientos de seguridad de la información y las medidas de seguridad de la información para cumplir con los requisitos de los documentos ISPL3.

El ISO crea y mantiene la Política de Seguridad de la Información y los documentos ISPL3 para todos los servicios compartidos por el Grupo. Los documentos ISPL4 son creados y mantenidos por las unidades funcionales responsables respectivamente.

4.4 Cooperación orientada a la seguridad con partes externas

La cooperación con proveedores y socios de servicios externos no debe reducir el nivel de seguridad de la información de onLygal Seguros y onLygal Servicios. Por esta razón, los

proveedores y los socios de servicios externos solo pueden tener acceso a la información de onLygal Seguros y onLygal Servicios y los recursos de TI una vez que onLygal Seguros y onLygal Servicios haya evaluado y clasificado los niveles de seguridad de la información de los proveedores y socios de servicios externos según corresponda. Además, onLygal Seguros y onLygal Servicios solo otorgan acceso a información y recursos de TI que son necesarios para la cooperación (principio de necesidad de conocer). El ISO, por lo tanto, define los requisitos unificados para la cooperación orientada a la seguridad con partes externas.

4.5 Desempeñar una parte activa en mantener el nivel de protección

Los niveles de seguridad de la información requeridos deben verificarse, monitorearse y evaluarse de manera independiente para poder mantenerlos y optimizarlos continuamente (directriz 12 de DGSEIOPA). Esto también se apoya en el área de Gestión de la seguridad de la información a través del "Modelo de tres líneas de defensa".

- 1ra línea de defensa (1st LoD en inglés)
  La 1st LoD está compuesta por la gestión operativa y es responsable de la definición, implementación y control de las medidas de seguridad de la información para el manejo de riesgos y el cumplimiento de los requisitos de seguridad de la información.
- 2da línea de defensa (2nd LoD en inglés)
  La segunda LoD está en manos del ISO y la unidad de la seguridad de la información del onLygal Seguros y onLygal Servicios, con el apoyo de las funciones de gestión de riesgos establecidas localmente. El 2nd LoD define los requisitos de seguridad de la información y supervisa la definición, implementación y control de las medidas de seguridad de la información a través del 1st LoD.

- 3ra línea de defensa (3rd LoD en inglés)
  La auditoría interna actúa como una unidad independiente como 3rd LoD. El 3er LoD evalúa la efectividad de las primeras dos líneas de defensa. Las auditorías deberán realizarse de forma periódica y en consonancia con su correspondiente plan de auditoría por unos auditores dotados de unos conocimientos, unas competencias y una experiencia suficientes en riesgos de TIC y seguridad, a fin de garantizar de manera independiente su eficacia (directriz 5 de DGSEIOPA)

5 Actualización de la política

Esta política se revisará de forma anual por el Consejo de Administración de onLygal Seguros. Para ello, el responsable de la norma en onLygal Seguros reportará al Consejo cualquier problema relacionado con esta norma y le recomendará las acciones a llevar a cabo.

El documento deberá actualizarse, en particular, en los siguientes casos:

- Cambios legales relacionados con el contenido de esta política.
- Cambios significativos en la estrategia y/o en las actividades de la empresa, especialmente si éstos tienen un impacto en la política de seguridad de la información
- Cambios significativos en la organización estructural y/o de procesos.
- La existencia de una infracción grave de cumplimiento relevante para el contenido de la normativa o

- Una debilidad detectada en el curso de una auditoría interna o externa.

Las decisiones adoptadas por el Consejo como resultado de la revisión deben estar justificadas claramente, debiendo quedar documentada la decisión adoptada y la justificación.

La modificación que se efectúe deberá quedar debidamente documentada en el apartado Historial de Cambios, indicando quién realizó el cambio y el motivo.

Anexo 1: Políticas de seguridad de la información de nivel 3

Los siguientes documentos definen los requisitos mínimos de seguridad de la información de onLygal Seguros y onLygal Servicios, de acuerdo con lo establecido en las directrices 6, 13, 14, 15, 16, 17 18 de DGSEIOPA.

- ISPL3 Seguridad en la nube
- ISPL3 Criptografía
- ISPL3 Seguridad de Recursos Humanos
- ISPL3 Gestión de identidad y accesos
- ISPL3 Clasificación de información
- ISPL3 Cumplimiento con Seguridad de la información
- ISPL3 Gestión y respuesta de incidentes de seguridad de la información
- ISPL3 Organización de ISMS
- ISPL3 Gestión de activos TI
- ISPL3 Desarrollo de software seguro
- ISPL3 Sistema de TI y operaciones de red
- ISPL3 Gestión de las especificaciones de seguridad de la información
- ISPL3 Seguridad móvil
- ISPL3 Seguridad física
- ISPL3 Gestión de proveedores y compras
- ISPL3 Documento de alcance
- ISPL3 Uso seguro de la información y TI

Anexo 2: Contacto para partes interesadas externas

En caso de necesitar una versión completa de la política, pueden dirigir sus peticiones al correo siguiente: direccion.informatica@onlygal.es