Preventiva
Grupo

POLÍTICA DE SEGURIDAD DE INFORMACIÓN

ÍNDICE

1. INTRODUCCIÓN

Esta política ha sido adaptada para alinearse con los requisitos de la ISO 27001:2022, estableciendo un Sistema de Gestión de Seguridad de la Información (SGSI) que considere el contexto interno y externo de la organización, así como las necesidades de las partes interesadas.

La política define, por tanto, los principios de seguridad de la información para proteger la confidencialidad, integridad y disponibilidad de la información en el ámbito definido por el Sistema de Gestión de Seguridad de la Información (SGSI), cuyo alcance cubre todas las operaciones, activos, y sistemas gestionados por la organización, de acuerdo con la ISO 27001:2022.

- Principios básicos y compromisos asumidos
- Elementos de la estructura operativa del sistema de gobierno para tic
- Estrategia de tic y gestión de operaciones
- Asignación de responsabilidades
- Procesos de información
- Otros aspectos relevantes

La presente política recoge los aspectos fundamentales y los compromisos de Preventiva Compañía de Seguros y Reaseguros, S.A., (o en adelante Preventiva o la Entidad) que permitan a la Entidad disponer de un marco de gobierno eficaz para el correcto gobierno de las actividades relacionadas con seguridad de las tecnologías de la información y de las comunicaciones (en adelante, también TIC).

La presente política está alineada con lo establecido en normativa de transposición de la Directiva Solvencia II y en particular con lo siguiente:

-Ley 20/2015, de 14 de julio, de Ordenación, Supervisión y Solvencia de las Entidades Aseguradoras y Reaseguradoras.

-Real Decreto 1060/2015, de 20 de noviembre, de Ordenación, Supervisión y Solvencia de las Entidades Aseguradoras y Reaseguradoras.

-Reglamento Delegado (UE) 2015/25 de la Comisión de 10 de octubre de 2014 así como en aquello que resultase de sus actualizaciones (UE) 2019/981 y 2021/1256 de la Comisión de 8 de marzo de 2019 y de 21 de abril de 2021, respectivamente.

-Directrices sobre sobre gobernanza y seguridad de las tecnologías de la información y de las comunicaciones publicadas por EIOPA y adoptadas por la Dirección General de Seguros durante 2021.

Adicionalmente la presente política estará en consonancia con lo establecido en el Reglamento Delegado (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero que, si bien ha entrado en vigor en 2023, será aplicable a partir del 17 de enero de 2025.

Sin perjuicio a las referencias explícitas a la sociedad Preventiva Compañía de Seguros y Reaseguros S.A. esta política será igualmente aplicable, cambiando lo que se deba cambiar, a Expertia, Seguros de Decesos, S.A., (o en adelante Expertia) y al Grupo de entidades integrado por la empresa participante Preventiva Compañía de Seguros y Reaseguros, S.A., (o en adelante Grupo Preventiva o Grupo), acorde a la naturaleza, el volumen y la complejidad de los riesgos inherentes a la actividad de las mismas.

La presente Política ha sido aprobada por el Consejo de Administración de la Entidad y es objeto de revisión periódica.

2. OBJETIVO

El objetivo de esta política es, como ya se ha introducido, definir los principios de seguridad de la información para proteger la confidencialidad, integridad y disponibilidad de la información en el ámbito definido por el Sistema de Gestión de Seguridad de la Información (SGSI), cuyo alcance cubre todas las operaciones, activos, y sistemas gestionados por la organización, de acuerdo con la ISO 27001:2022.

La presente política de seguridad de la información definirá los principios de alto nivel y las normas para proteger la confidencialidad, la integridad y la disponibilidad de la información de la Entidad a fin de respaldar la aplicación de la estrategia de TIC.

La política incluirá una descripción de las principales funciones y responsabilidades para la gestión de la seguridad de la información y en ella se habrán de establecer los requisitos del personal, los procesos y la tecnología en relación con la seguridad de la información.

3. PRINCIPIOS BÁSICOS Y COMPROMISOS ASUMIDOS

Los principios asumidos para garantizar una adecuada seguridad de las tecnologías de la información y comunicación, a fin de facilitar una gestión prudente y adecuada de la actividad que faciliten el proceso de supervisión por parte de las autoridades competentes, se determinarán con el establecimiento de un conjunto de procesos, procedimientos, controles y demás acciones necesarias para asegurar este fin.

De conformidad con lo anterior, se considerará necesaria la asunción de los siguientes aspectos:

- Las actividades de gestión de TIC y su seguridad continuada, cuyo máximo responsable es el Consejo de Administración de la Entidad, se llevará a la práctica de forma estructurada, con medios humanos y materiales suficientes acorde a un modelo de gestión que se articulará entorno una dirección de área o departamento que será el responsable de los procesos asociados a esta operativa.

  La práctica de este departamento se enmarcará dentro de la estructura organizativa establecida por la Entidad para la gestión de los riesgos, una estructura o modelo basado en tres líneas de defensa donde el control de los departamentos o direcciones de área es la primera línea de defensa en la gestión de riesgos, las distintas funciones de supervisión de riesgos, controles y cumplimiento establecidas por el Consejo de Administración son la segunda línea de defensa, y la evaluación independiente del modelo, la función de control de auditoría interna, es la tercera línea de defensa.

- Adicionalmente con independencia de la existencia de un departamento responsable de seguridad de TIC, el resto de los departamentos cuya colaboración sea requerida en este ámbito se enmarcarán también bajo esta estructura organizativa y se les proporcionarán los recursos humanos y técnicos adecuados para el cumplimiento de los objetivos propuestos.

- Asimismo, la práctica de los departamentos involucrados en la elaboración de la información estratégica tendrá en consideración los siguientes principios de actuación:
    - La práctica se realizará con la adecuada competencia profesional, cuidado y diligencia, manteniendo un comportamiento integro en aras de reforzar la objetividad de la actividad y la correcta gestión de cualquier posible conflicto de intereses.
    - La práctica se realizará acorde al principio de proporcionalidad, graduando los requisitos atendiendo a la naturaleza, volumen y complejidad de las operaciones de la Entidad.
    - La práctica se realizará acorde a los principios de eficacia y eficiencia.
    - La práctica estará integrada en la estructura y en los procesos de toma de decisiones de la Entidad, acorde a los procesos internos de gestión.

4. ELEMENTOS DE LA ESTRUCTURA OPERATIVA DEL SISTEMA DE GOBIERNO PARA TIC

El Sistema de Gobierno se diseñará para contemplar los elementos recogidos a continuación y cumplir, entre otros, los siguientes requisitos:

Gestión de riesgos TIC

La Entidad dispondrá de un sistema eficaz para gestionar los riesgos de TIC y seguridad como parte del sistema global de gestión de riesgos de la empresa. Esto incluye la determinación de la tolerancia a tales riesgos, de conformidad con la estrategia sobre riesgos de la empresa, así como información periódica sobre el resultado de este proceso dirigido al Consejo de Administración.

Este Sistema de Gestión de Riesgos global comprenderá por tanto las estrategias, los procesos y los procedimientos de información necesarios que permitan identificar, medir, vigilar, gestionar y notificar de forma continua los riesgos TIC a los que la Entidad este expuesta en cada momento y sus interdependencias.

Incidentes de seguridad TIC

La Entidad establecerá un proceso para la gestión de incidentes de seguridad de TIC, definiendo roles y responsabilidades para la gestión de incidentes. A su vez, se implementarán las medidas para la contención, erradicación y recuperación de incidentes, así como protocolos para la comunicación de incidentes a las autoridades competentes cuando sea necesario.

Pruebas de recuperación de desastres y planes de continuidad del negocio

Se mantendrá por la Entidad un plan de pruebas de recuperación de desastres, que se desarrollará para evaluar la capacidad de la Entidad para restaurar sus operaciones en caso de un incidente.

Adicionalmente, en consonancia con lo dispuesto en la Política de Continuidad de las Actividades, se desarrollarán y mantendrán planes de continuidad del negocio en el ámbito TIC para garantizar la continuidad de las actividades críticas en caso de una interrupción.

Gestión de proveedores de servicios de TIC

Complementando lo dispuesto en la Política de Externalización de la Entidad y otros procedimientos descritos en el área de servicios generales, se implementarán procesos vinculados a la diligencia debida para la selección de proveedores de servicios de TIC.

En este sentido, y también tomando como referencia la Política de Externalización, también se considerará para los contratos con determinados proveedores de servicios TIC el contenido contractual estipulado que garantice una adecuada seguridad de información, así como se desarrollen procesos para la supervisión continua de su desempeño.

Auditoría Interna

Entre las atribuciones de la Función de Auditoría Interna se encontrará la responsabilidad de auditar de manera periódica, eficaz, independiente y acorde a su planificación la gobernanza, los sistemas y los procesos de las empresas para sus riesgos de TIC y seguridad.

Función de Seguridad de la Información

La Entidad tiene establecida, dentro de su sistema de gobernanza y de acuerdo con el principio de proporcionalidad, una función de seguridad de la información dependiente del Consejo de Administración. Dicha función está asociada al Oficial de Riesgo de Ciberseguridad ya nombrado en la Entidad, y se han desarrollado los procesos y principios necesarios que garanticen la independencia y objetividad de la función de seguridad de la información y la separen de forma adecuada de los procesos de desarrollo y operaciones de TIC.

Asimismo, se establecerá entorno a esta figura, un marco de gobernanza específico para la gestión del riesgo operacional digital, desarrollando cuantos procedimientos se consideren para este objetivo. Del mismo modo se asignarán responsabilidades claras para la gestión de dicho riesgo operacional digital, así como se proporcionará formación y concienciación sobre el riesgo operacional digital a todo el personal de la Entidad.

Elementos de Seguridad

Se establecerán procesos de actuación, revisión y autorización adecuados para proveer una seguridad razonable en relación con el logro de los objetivos fijados para desarrollo y operaciones de TIC, focalizándose en los siguientes ámbitos:

i. Seguridad lógica
ii. Seguridad física
iii. Seguridad de las operaciones de TIC
iv. Supervisión de la seguridad
v. Revisión, evaluación y prueba de la seguridad de la información
vi. Formación y sensibilización sobre seguridad de la información
vii. Adquisición, desarrollo y mantenimiento de sistemas de TIC

Se mantendrá por la Entidad un registro de las aplicaciones que apoyan funciones o procesos comerciales esenciales. De la misma manera, se establecerá un proceso de gestión de cambios de TIC para garantizar que todos los cambios en los sistemas de TIC se registren, evalúen, prueben, aprueben, autoricen y apliquen de forma controlada.

Gestión de Proyectos y Transformación

Coordinado por la Responsable de Proyectos y Transformación, se realizará un seguimiento apropiado de la cartera de proyectos de TIC, considerando también los riesgos que puedan resultar de las interdependencias entre proyectos distintos y de las dependencias de varios proyectos de los mismos recursos o conocimientos técnicos.

Gestión de la Continuidad del Negocio

Formando parte del marco de la política global de continuidad del negocio de la Entidad, se establece un ámbito relacionado con la continuidad de TIC, la cual se comunica adecuadamente en el seno de la Entidad y aplica a todo el personal pertinente y, en su caso, a los proveedores de servicios.

En relación con gestión de la continuidad de TIC, y teniendo en cuenta la proporcionalidad que acontezca, habrá procesos y metodología que velen por el desarrollo de aspectos tales como:

- Análisis de impacto en el negocio
- Planificación de la continuidad del negocio.
- Planes de respuesta y recuperación
- Pruebas de los Planes
- Comunicaciones de crisis

Externalización de los servicios y sistemas de TIC

Formando parte de la política general de externalizaciones de la entidad, y en caso de externalización de funciones importantes o esenciales, se adoptarán procesos con el fin de controlar y obtener garantías del nivel de cumplimiento de los objetivos de seguridad, las medidas y los objetivos de rendimiento por parte de los proveedores de servicios.

5. ESTRATEGIA DE TIC Y GESTION DE OPERACIONES

I. Estrategia de TIC

El Consejo de Administración es responsable de aprobar la estrategia de TIC de la Entidad, así como supervisar su comunicación y aplicación.

La estrategia de TIC está definida en el marco de la estrategia empresarial general y en consonancia con esta, de forma que cubra los siguientes aspectos:

a) cómo deben evolucionar las TIC de la Entidad para apoyar y aplicar con eficacia su estrategia empresarial.
b) la evolución de la arquitectura de TIC, incluidas las dependencias con proveedores de servicios; y
c) unos objetivos de seguridad de la información claros, centrados en los sistemas y los servicios, el personal y los procesos de TIC.

Dicha estrategia TIC se aplica, adopta y comunica a todo el personal y los proveedores de servicios pertinentes, según sea aplicable y relevante, de manera oportuna.

Alineado con la renovación del Plan Estratégico, la Entidad también establece un proceso para realizar un seguimiento y medir la eficacia de la aplicación de la estrategia de TIC. Dicho proceso es objeto de revisiones periódicas (al menos cada tres años) y actualizaciones en caso de considerarse necesario.

II. Gestión de operaciones, incidentes y problemas TIC

Las Operaciones TIC serán gestionadas de acuerdo con la Estrategia previamente definida y su nivel de relevancia.

Con el fin de tenerlos claramente identificados, se mantendrá un inventario de los activos TIC. Dichos activos serán gestionados acorde a su ciclo de vida de forma que se garantice que satisfacen las necesidades del negocio y se evalúe su obsolescencia.

Asimismo, formarán parte de la gestión de operaciones, el seguimiento de capacidades y rendimientos, así como el mantener un entorno de copias de seguridad y restauración adecuado.

En este sentido se establecerá una metodología de gestión de incidentes, adoptando criterios, umbrales y alertas que los clasifiquen y favorezcan su control, seguimiento y planes de respuesta y comunicación, manteniendo informado en última instancia al Consejo de Administración en caso de que se den sucesos significativos.

6. ASIGNACIÓN DE RESPONSABILIDADES

Las funciones y responsabilidades asumidas para el cumplimiento de los objetivos propuestos se concretan, aunque no están limitadas por las mismas, en las siguientes:

Consejo de Administración

Órgano responsable del sistema de gobierno de la Entidad, entre las funciones y responsabilidades relativas a esta política se encuentran las siguientes:

- Establecer la política de seguridad de la información, acorde a la estrategia TIC diseñada por el propio Consejo de Administración y la tolerancia al riesgo TIC de la Entidad, también definida por el Consejo.
- Establecer una estructura operativa y organizativa relativa a seguridad de TIC en la Entidad.
- Supervisar el adecuado funcionamiento del modelo conforme a lo establecido en la presente política.

Comisión de Auditoría

Órgano encargado en asesorar y prestar ayuda especializada al Consejo de Administración, entre sus responsabilidades relativas a esta política se encuentran:

- Supervisar periódicamente la efectividad del sistema de control interno, la auditoría interna y los sistemas de gestión de riesgos.
- Informar y asesorar periódicamente al Consejo de Administración sobre las conclusiones del sistema de gestión de riesgos, control interno y auditoría interna.

Función de Seguridad de la Información (también responsable del SGSI)

Los principales cometidos de la función de seguridad de la información serán:

- Apoyar al Consejo de Administración a definir y mantener la presente política y controlar su implantación.
- Informar y aconsejar al Consejo de Administración periódicamente y en momentos puntuales sobre la situación de seguridad de la información y su evolución.
- Supervisar y revisar la aplicación de las medidas de seguridad de la información.
- Asegurarse de que al utilizar proveedores de servicios se cumplen los requisitos de seguridad de la información.
- Asegurarse de que todos los empleados y proveedores de servicios que acceden a la información y los sistemas son adecuadamente informados de la política de seguridad de la información, bien sea mediante sesiones de formación o mediante sensibilización al respecto.
- Coordinar el análisis de los incidentes operativos o de seguridad y comunicar los más relevantes al Consejo de Administración.

Departamento de Informática

Área responsable de los sistemas e infraestructuras de Tecnologías de Información y Comunicación en la Entidad, y de la Seguridad de la Información, entendida como la preservación de la confidencialidad, integridad y disponibilidad de la a información o los sistemas de información. Encargado de la gestión de aspectos relacionados con Activos, Proyectos y Proveedores de servicios TIC.

Función de Gestión de Riesgos

Función de control responsable de la coordinación del sistema de gestión de riesgo, entre sus responsabilidades y funciones relativas a esta política se encuentran:

-Responsable de coordinar y desarrollar los procesos de identificación de riesgos TIC.

-Responsable de coordinar y desarrollar los procesos de evaluación y medición de los riesgos TIC.

-Responsable de coordinar y desarrollar los procesos de seguimiento del riesgo TIC.

-Confección de información periódica destinada al Consejo de Administración en relación con la integración de riesgos TIC en el sistema global de riesgos de la Entidad.

Comité de Sistemas de Gestión de Seguridad de la Información (SGSI)

Órgano formado por perfiles transversales de la Entidad e integrado en el Sistema de Gestión de Riesgos de la Organización, cuya función fundamental será velar por el cumplimiento continuado de la normativa ISO 27001, mediante la acreditación anual de dicho cumplimiento.

Otros Departamentos o Direcciones de Área

Áreas responsables de la gestión y dirección de los distintos ámbitos relativos a la actividad de la Entidad, entre sus responsabilidades relativas a esta política se encontrará la ejecución y control de los procedimientos de la seguridad de la información de relativos a su área.

Asimismo, todos los integrantes de la Entidad deberán informar sobre cualquier posible incumplimiento de esta política que fueran conocedores y que pudiera perjudicar una gestión sana y prudente de la actividad de la Entidad.

7. PROCESOS DE INFORMACIÓN

Con el fin de garantizar la transmisión de información relativa a esta política en el sistema de gobernanza se aplicarán diversos procedimientos de información que incluirán, entre otras, las comunicaciones que se detallan a continuación:

Comunicaciones internas

La Función de seguridad de la información supervisará y analizará la información interna relativa al sistema de gestión de riegos TIC previamente a su envió al Comité de Riesgos y su posterior remisión a la Comisión de Auditoría y al Consejo de Administración.

La información a reportar estará integrada en el sistema global de los riesgos a los que se enfrenta la Entidad, el modo en el que se gestionan y controlan, y la forma en la que están afectando a su actividad y resultados, facilitándose de esta manera, entre otros aspectos, la siguiente información: los eventos de riesgo acaecidos, el seguimiento de los indicadores de riesgo, el perfil de riesgo, los cambios significativos en el perfil de riesgo, las incidencias significativas de control y el seguimiento de los planes de acción implementados.

Esta información se concretará en los siguientes procesos de información:

-Informe periódico de seguimiento de riesgos claves (Emisor: Función de Gestión de Riesgos/ Receptor: Comité de Riesgos y Comité de Auditoría y Consejo de Administración).
- Informe anual de revisión de la estrategia y apetito al riesgo (Emisor: Función de Gestión de Riesgos/ Receptor: Comité de Riesgos y Comité de Auditoría y Consejo de Administración).
- Información específica que suministrará la Función de seguridad de la información tanto a Comité de Riesgos como a Consejo de Administración, y que estará supeditada al alcance y al momento en que se produzca la solicitud de esta desde estos órganos de gobierno.

Comunicaciones externas

La Función de seguridad de información supervisará y analizará las comunicaciones externas relativa al sistema de gestión de riegos previamente a su envió al Comité de Riesgos y su posterior remisión al Comité de Auditoría y Control y al Consejo de Administración.

Esta información se concretará en los siguientes procesos de información:

-Informe ORSA de evaluación interna de riesgos y solvencia. Este informe, remitido anualmente al supervisor, recoge los eventuales impactos en que riesgos emergentes tales como la ciberseguridad, suponen en las necesidades globales de solvencia calculadas por la Entidad.

-El informe público con periodicidad anual sobre la situación financiera y de solvencia y el informe periódico de supervisión (al menos cada tres años). En estos informes se incorporará en aquellos epígrafes dispuestos para ello información sobre la gestión de este riesgo.

-La información periódica a efectos de supervisión tanto de carácter anual como trimestral, y en caso de que así sea requerido en los reglamentos de ejecución por parte del Supervisor.

8. OTROS ASPECTOS RELEVANTES

Titularidad, revisiones y actualizaciones de la política

El Responsable de esta Política es la Función de Seguridad de Información y es el responsable, con la supervisión del Titular de la Función de Gestión de Riesgos, de evaluar periódicamente la necesidad de proponer modificaciones a la misma conforme a los mecanismos de revisión establecidos en el sistema de gobierno de la Entidad, siendo asesorada, en estos aspectos, por el Comité de Riesgos y/o el Comité de Auditoría.

El Consejo de Administración de la Entidad es el encargado de revisar y aprobar esta política, al menos una vez al año y siempre que sea oportuno en base a las circunstancias de cada momento para asegurarse que la misma permanece alineada con los objetivos establecidos.

De manera periódica, el Departamento de Auditoría Interna, facilitará una revisión objetiva sobre la conveniencia de la política y el adecuado cumplimiento de la misma.

Dispensas de la política

Cualquier tipo de dispensa en el cumplimiento de la presente Política deberá ser documentado y aprobado por el Comité de Auditoría, siendo este el encargado último de su comunicación periódica al Consejo de Administración.

Cualquier tipo de dispensa significativa en relación con esta Política deberá ser aprobado por el Consejo de Administración.

Desviaciones de la política

Todas las desviaciones no autorizadas de los estándares establecidos en la política deberán ser comunicados a las Funciones de Control, al Comité de Riesgos, al Comité de Auditoría y/o al Consejo de Administración.

Dependiendo de la naturaleza y gravedad de los hechos se implementarán las oportunas medidas al respecto.