REPÚBLICA DE PANAMÁ
SUPERINTENDENCIA DE SEGUROS Y REASEGUROS DE PANAMÁ

ACUERDO N° 4
De 15 de octubre de 2026

"Por el cual se dictan las disposiciones sobre la gobernanza y gestión de la tecnología de la información y comunicación, la seguridad de la información y ciberseguridad; y la gestión de sus riesgos"

LA JUNTA DIRECTIVA DE LA SUPERINTENDENCIA DE SEGUROS Y REASEGUROS DE PANAMÁ

En uso de sus facultades legales,

CONSIDERANDO:

Que la Ley No. 12 de 3 de abril de 2012 "Que regula la actividad de seguros y dicta otras disposiciones" reconoce a la Superintendencia de Seguros y Reaseguros de Panamá, como organismo autónomo del Estado, con la autoridad de regulación, reglamentación, supervisión, control y fiscalización de las empresas, entidades y personas sujetas al ámbito de aplicación de dicha excerta legal.

Con base en el Acuerdo 01 de 7 de enero de 2015 "Por medio del cual crea un Sistema de Control Interno", se dictan las disposiciones que se deben aplicar para simplificar y minimizar riesgos, así como la obligación de contar con un conjunto de políticas, procedimientos y técnicas de control para proveer una seguridad razonable, salvaguardar los activos y lograr una adecuada organización administrativa y eficiencia operativa, confiabilidad de los reportes que fluyen de sus sistemas de información.

Conforme al Acuerdo 03 de 19 de junio de 2025 "Por medio del cual se dictan disposiciones sobre Gobierno Corporativo, es fundamental establecer parámetros para que todas las empresas aseguradoras y reaseguradoras, mantengan en sus organizaciones principios cónsonos con un buen Gobierno Corporativo, estableciendo controles dentro de la organización para asegurar que las estrategias y decisiones adoptadas por la Junta Directiva, en beneficio de las partes interesadas, sean implementadas eficazmente.

Que de conformidad con el Acuerdo 06 de 23 de octubre de 2025 "Que adopta el marco de referencia para la Supervisión Basada en Riesgo de seguros y reaseguros", establece entre las categorías el riesgo tecnológico y de ciberseguridad, los cuales pueden impactar las operaciones y la continuidad del negocio.

Que la tecnología de la información y la comunicación (TIC) forman parte de la continua transformación, soporte y operaciones de negocio del sector de seguros, incidiendo de manera profunda y transversal en la continuidad del negocio, y dejando claramente establecido que la tecnología es un componente fundamental e inseparable para garantizarla, lo cual conlleva la aparición de nuevos riesgos que pueden impactar tanto de forma financiera, como reputacional a este sector. Por lo cual, se hace necesario la reglamentación para la implementación de un marco base para la gestión del riesgo tecnológico y cibernético, la gobernanza y gestión de la tecnología de la información, la seguridad de la información y la ciberseguridad.

Que con fundamento en lo establecido en el numeral 19 del Artículo 20 de la Ley No. 12 de 2012, son funciones de la Junta Directiva de la Superintendencia de Seguros y Reaseguros de Panamá reglamentar mediante acuerdo de sus miembros las disposiciones técnicas de la mencionada Ley.

Que, en virtud de lo antes expuesto, la Junta Directiva de la Superintendencia de Seguros y Reaseguros, en ejercicio de sus funciones,

ACUERDA:

ARTÍCULO 1. ÁMBITO DE APLICACIÓN: Este acuerdo es aplicable y de obligatorio cumplimiento para toda compañía de seguros y reaseguros, reguladas y supervisadas por la Superintendencia de Seguros y Reaseguros de Panamá.

ARTÍCULO 2. OBJETIVO. Establecer los requisitos mínimos para la gobernanza y gestión de la tecnología de la información y comunicación, la seguridad de la información y ciberseguridad, la gestión de proveedores y terceros críticos y la resiliencia operativa digital; bajo un enfoque prudencial.

ARTÍCULO 3. DEFINICIONES: Para los efectos del presente Acuerdo, los siguientes términos se entenderán así:

1. Activo de Información: se refiere a la información, en cualquier medio o formato, que posee valor y requiere protección para preservar su confidencialidad, integridad y disponibilidad.
2. Activo Tecnológico: un componente de software, hardware, bases de datos, dispositivos, servicios tecnológicos, redes, infraestructura y otros recursos tecnológicos y de comunicación utilizados.
3. Amenaza: es un evento, circunstancia con el potencial de explotar una vulnerabilidad y afectar la confidencialidad, integridad y disponibilidad de los activos tecnológicos y de la información.
4. Computación en la Nube: corresponde a un modelo de prestación de servicios tecnológicos que permite el acceso bajo demanda, a recursos informáticos administrados por un proveedor incluyendo servicios de infraestructura, plataforma, software y demás modalidades de servicios en la nube.
5. Función crítica: actividad, proceso o servicio cuya interrupción puede afectar las operaciones del negocio, el cumplimiento de sus obligaciones o la atención de los consumidores de seguros.
   La identificación y clasificación de las funciones críticas corresponderá a cada compañía, de acuerdo con la naturaleza, complejidad y perfil de riesgo de sus operaciones, la cual deberá estar debidamente documentada.
6. Gobierno de la Tecnología de la Información y Comunicación (Gobierno TIC): conjunto de políticas, procesos, estructura organizacional y responsabilidades, el cual establece cómo se gestiona la tecnología de la información y comunicación, mediante las cuales la Junta Directiva y la Alta Gerencia dirigen, coordinan y supervisan el uso de la tecnología de la información; para apoyar los objetivos estratégicos de la compañía.
7. Incidente de Ciberseguridad: evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de la información, los sistemas o los servicios tecnológicos.
8. Incidente Tecnológico: evento que afecta la operación normal de la infraestructura tecnológica, aplicaciones o servicios tecnológicos.
9. Proveedor o Tercero Crítico: persona natural o jurídica que presta servicios cuya interrupción o falla puede afectar de manera significativa las funciones y procesos críticos, la seguridad o la continuidad operativa de la empresa.
10. Vulnerabilidad: debilidad en un activo, proceso, sistema o control que puede ser aprovechada por una amenaza.

11. Resiliencia Operativa Digital: es la capacidad de resistir, responder, recuperarse y adaptarse ante interrupciones tecnológicas o incidentes de ciberseguridad asegurando la continuidad de las funciones críticas.
12. TI: tecnología de la información.
13. TIC: tecnología de la información y comunicación.
14. KPI: indicador clave de desempeño.
15. KRI: indicador clave de riesgo.
16. Principio de proporcionalidad: principio mediante el cual las empresas de seguros y reaseguros deberán cumplir con la totalidad de las obligaciones establecidas en el presente Acuerdo, acorde con su naturaleza, complejidad de las operaciones, perfil de riesgo al aplicar los requisitos establecidos, sin que ello implique la exclusión, modificación o inaplicabilidad de ninguna de dichas obligaciones.
17. Inteligencia Artificial (IA): conjunto de tecnologías y técnicas que permiten a los sistemas computacionales procesar datos e información para generar resultados con distintos niveles de autonomía, los cuales están destinados a apoyar o ejecutar actividades, procesos o toma de decisiones de las compañías de seguros y reaseguros

ARTÍCULO 4. RESPONSABILIDADES DE LA JUNTA DIRECTIVA. La Junta Directiva de las compañías de seguros y reaseguros tendrá, entre sus responsabilidades para la adecuada gestión del riesgo tecnológico y cibernético, la gobernanza y gestión de la tecnología de la información, la seguridad de la información y la ciberseguridad y la resiliencia operativa digital, las siguientes:

1. Aprobar la estrategia de tecnología de la información y ciberseguridad.
2. Aprobar el conjunto de políticas y procedimientos para la gobernanza y gestión de la TIC, seguridad de la información, resiliencia operativa digital y la ciberseguridad, así como el marco normativo para el uso adecuado de la inteligencia artificial, el cual deberá contemplar la identificación de sus riesgos materiales y exigir mecanismos de supervisión y validación humana (Human-in-the-Loop) en aquellos procesos, sistemas o decisiones automatizadas de alto impacto o criticidad para el negocio y los asegurados.
3. Aprobar el plan, marco o procedimiento para la gestión y manejo de crisis tecnológicas y de ciberseguridad, incluyendo los mecanismos de activación, escalamiento, comunicación, respuesta y recuperación.
4. Aprobar el apetito y tolerancia al riesgo tecnológico y cibernético.
5. Aprobar los riesgos relacionados con la tercerización de servicios de tecnología y de ciberseguridad, basado en el apetito y tolerancia al riesgo tecnológico y cibernético de la compañía.
6. Aprobar las prioridades de inversión de TI y de seguridad de la información, ciberseguridad; así como propiciar la resiliencia operativa digital.
7. Aprobar los indicadores de riesgo tecnológico y cibernético.
8. Aprobar el reglamento del Comité de Tecnología.
9. Aprobar el presupuesto de TI y de Ciberseguridad.

TÍTULO PRIMERO

GOBERNANZA Y GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN

ARTÍCULO 5. GOBIERNO DE LA TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN. Toda compañía de seguros y reaseguros deberá contar con una estructura organizacional que atienda la tecnología de la información y comunicación, la cual deberá establecer como parte del gobierno corporativo su conjunto de políticas, procedimientos y lineamientos; con una adecuada definición y separación de funciones,

El Gobierno de TI, como parte del sistema de Gobierno Corporativo, debe establecer, implementar y mantener políticas, procedimientos, estándares, lineamientos y controles suficientes para la gestión de los recursos de TI; los cuales deberán estar debidamente documentados, aprobados y actualizados acorde a lo establecido en la normativa de Gobierno Corporativo emitida por esta Superintendencia de Seguros y Reaseguros.

Cuando las funciones relacionadas con la gobernanza y gestión de las TIC sean efectuadas por otras compañías del grupo; deberá existir un contrato o acuerdo de servicio debidamente formalizado y aprobado por la Junta Directiva. Este contrato o acuerdo de servicio, debe establecer de forma clara, detallada y específica cada uno de los aspectos que se gestionan. El acuerdo de servicio firmado entre la empresa de seguro o reaseguro con las empresas del grupo no las exime de sus obligaciones y responsabilidades propias.

La información relacionada con las políticas, procedimientos y otros controles utilizados para la gobernanza y gestión de la TIC; debe estar a disposición de esta Superintendencia de Seguros y Reaseguros cuando así lo requiera como parte de la supervisión continua a la compañía.

ARTÍCULO 6. COMITÉ DE TECNOLOGÍA. Las compañías de seguros y reaseguros deben establecer un Comité de Tecnología como órgano de apoyo a la Junta Directiva, en el seguimiento, coordinación y supervisión de la gobernanza y gestión de la tecnología de la información y comunicación, seguridad de la información y ciberseguridad, así como en la resiliencia operativa digital.

Los miembros del Comité de Tecnología deberán contar con conocimientos y experiencia adecuados para el cumplimiento de las responsabilidades del Comité. El Comité deberá estar integrado, como mínimo, por dos miembros de la Junta Directiva, de los cuales uno deberá ostentar la condición de director independiente y no deben participar en la gestión diaria de la compañía de seguros o reaseguros. Asimismo, deberán integrarlo representantes de la alta gerencia, el ejecutivo responsable de tecnología, el ejecutivo responsable de seguridad de la información y ciberseguridad, y los ejecutivos de las áreas comerciales. La entidad deberá establecer el número total de integrantes atendiendo al tamaño, la naturaleza y la complejidad de sus operaciones.

Este Comité deberá reunirse trimestralmente, como mínimo.

Las funciones mínimas del Comité de Tecnología serán las siguientes:

1. Revisar y presentar a la Junta Directiva, para su aprobación, la estrategia y el plan estratégico de tecnología.
2. Revisar y presentar a la Junta Directiva para su aprobación, las políticas, procedimientos y los lineamientos relacionados con tecnología, seguridad de la información, ciberseguridad y resiliencia operativa digital.
3. Dar seguimiento al perfil de riesgo tecnológico y cibernético, así como a los indicadores de riesgo y desempeño.
4. Supervisar el riesgo relacionado con la tercerización de servicios de tecnología y de ciberseguridad.
5. Diseñar, implementar y mantener actualizado el plan, marco o procedimiento para la gestión y manejo de crisis tecnológicas y de ciberseguridad, incluyendo los mecanismos de activación, escalamiento, comunicación, respuesta y recuperación.
6. Definir, calcular y actualizar los indicadores de riesgo tecnológico y cibernético.
7. Dar seguimiento a la gestión de proveedores y terceros críticos, así como a los riesgos de concentración y dependencia tecnológica.
8. Dar seguimiento a los proyectos de TI e inversiones relevantes.
9. Dar seguimiento a los planes de acción derivados de auditorías, evaluaciones de riesgos, pruebas de seguridad e incidentes.

10. Dar seguimiento a los incidentes de TI y de ciberseguridad significativos o críticos, así como a las acciones de respuesta, recuperación y remediación.
11. Revisar la situación actual de la resiliencia operativa digital, la continuidad de TI y la recuperación ante desastres.
12. Recomendar las prioridades de inversión de TI y de seguridad de la información, ciberseguridad; así como propiciar la resiliencia operativa digital.
13. Presentar a la Junta Directiva, de manera trimestral, un informe sobre el estado de la gestión de tecnología, los principales riesgos tecnológicos y cibernéticos, incidentes relevantes. Así como informes extraordinarios, cuando sea necesario, por algún evento o riesgo significativo detectado.

El Comité debe contar con un reglamento aprobado por la Junta Directiva, que establezca su organización, funciones, responsabilidades, periodicidad de las reuniones, políticas y procedimientos. Las actas del Comité deberán estar a disposición de esta Superintendencia acorde a las disposiciones del Acuerdo sobre Gobierno Corporativo.

Parágrafo: En caso de subsidiarias, las funciones del Comité de Tecnología podrán ser practicadas por el Comité de Tecnología de su casa matriz o grupo, previa notificación de dicho actuar ante la Superintendencia, cuando se conforme dicho Comité; si esta a su vez, determina que tal función es a su juicio insuficiente, requerirá a la subsidiaria, la constitución de un comité separado de la casa matriz, para dar cumplimiento a lo establecido en el presente Acuerdo.

ARTÍCULO 7. ESTRATEGIA O PLAN ESTRATÉGICO DE TI. Las compañías de seguros y reaseguros deben establecer e implementar una estrategia de tecnología de la información y comunicación, la cual se encuentre alineada con los objetivos y estrategias; considerando el apetito de riesgo y las necesidades del negocio para su operación.

La estrategia o plan estratégico de TI, debe ser debidamente documentada y actualizada en base a los cambios relevantes de la estrategia del negocio, regulatorios, y/o apetito de riesgo de la compañía. Esta estrategia debe considerar los objetivos y prioridades tecnológicas, suficiencias de recursos de la transformación digital, sistemas implementados heredados y/o obsolescencia, ciberseguridad, arquitectura tecnológica, proveedores y terceros tecnológicos, recursos humanos y presupuesto, ciberseguridad; así como la resiliencia operativa digital.

ARTÍCULO 8. GESTIÓN DE LA TI. Las compañías deberán establecer, mantener y actualizar un marco de control para la gestión de los recursos TIC, el cual esté alineado y le permita dar soporte a las necesidades del negocio, asegure brindar la continuidad del negocio, la seguridad de la información y la resiliencia operativa digital. El marco debe contemplar los siguientes aspectos:

a. Plan estratégico de TI, alineado con los objetivos estratégicos del negocio.
b. Estructura organizacional, con la debida definición de funciones, responsabilidades, una adecuada segregación y planes de continuidad operativa del recurso humano y tercerizado.
c. El detalle de la arquitectura empresarial y tecnológica alineada con las necesidades del negocio.
d. La gestión de los proyectos y aquellos que soportan los procesos y objetivos del negocio.
e. Gestión del ciclo de vida de los activos tecnológicos; contemplando su adquisición, mantenimiento, actualización y retiro.
f. La gestión adecuada para la adquisición, desarrollo, configuración, implementación y mantenimiento de aplicaciones y plataformas tecnológicas.
g. Mecanismos que le permitan identificar de forma oportuna los riesgos asociados a los activos tecnológicos que se encuentran obsoletos, hayan llegado a su fin de vida útil o se encuentren sin soporte y mantenimiento por parte de sus proveedores fabricantes.

h. La gestión de cambios en la infraestructura, aplicaciones y otros componentes tecnológicos.
i. Inventario de activos tecnológicos clasificados, con su debida identificación de propietario, criticidad, ubicación y dependencias.
j. Gobernanza y gestión de los datos durante todo su ciclo de vida.
k. Mecanismos que permitan el monitoreo y mejora continua de los procesos de TI.
l. Definición de indicadores de desempeño y de riesgo (KPI y KRI) que permitan evaluar la disponibilidad, capacidad, eficacia y eficiencia, calidad de los servicios de tecnología, resiliencia y seguridad. Los mismos deben ser monitoreados de forma continua y ser utilizados para la toma de decisiones de manera oportuna.

TÍTULO SEGUNDO

GESTIÓN DE RIESGO TECNOLÓGICO Y CIBERNÉTICO

ARTÍCULO 9. GESTIÓN DE RIESGO TECNOLÓGICO Y CIBERNÉTICO. Las compañías de seguros y reaseguros deben establecer una metodología con sus respectivos manuales de políticas y procedimientos, para la gestión del riesgo tecnológico y cibernético.

Esta metodología deberá contemplar la identificación, evaluación, tratamiento, monitoreo y comunicación de los riesgos, el cual debe estar integrado al sistema de gestión integral de riesgos.

Las evaluaciones de riesgo deben efectuarse de manera continua y de forma adicional ante cambios significativos, nuevos productos y servicios, tecnologías emergentes; así como cambios en las amenazas cibernéticas.

El marco de gestión de riesgo tecnológico y cibernético debe establecer como mínimo lo siguiente:

a. Políticas y procedimientos, los cuales deben ser revisados/actualizados una vez al año.
b. Establecimiento del apetito y tolerancia al riesgo.
c. Identificación de los procesos críticos de los cuales mantiene dependencia con proveedores y terceros de TI.
d. Gestión de los riesgos relacionados con los proveedores y terceros de servicios críticos.
e. Monitoreo continuo de los controles de los riesgos tecnológicos y cibernéticos y comunicación oportuna en caso de desviación en cuanto al impacto y ocurrencia del riesgo.
f. Comunicación de los riesgos al Comité de Riesgos de manera oportuna.
g. Auditoría Interna debe verificar la eficacia y efectividad del marco de gestión de riesgo tecnológico y cibernético; así como efectuar auditorías enfocadas a la revisión de los controles de la gobernanza y gestión de tecnología de la información, y de seguridad de la información y ciberseguridad; de conformidad con sus funciones y responsabilidades independientes.
h. El Comité de Riesgo debe comunicar a la Junta Directiva el nivel de riesgo tecnológico y cibernético, así como los riesgos en esta materia a los que se expone la compañía, de manera trimestral.

TÍTULO TERCERO

SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

ARTÍCULO 10. GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD. Las entidades deberán contar con un área a cargo de la seguridad de la información y ciberseguridad, con la suficiente jerarquía e independencia para coordinar

y supervisar la implementación de los controles de seguridad de la información y ciberseguridad que se defina en el programa de seguridad de la información y ciberseguridad.

La unidad a cargo de la gestión de la seguridad de la información y ciberseguridad deberá establecer, implementar las políticas, procedimientos y controles suficientes para la debida protección de los activos tecnológicos y de la información. Como parte del gobierno corporativo, las políticas y procedimientos deben ser revisados y actualizados acorde con las disposiciones establecidas en la normativa vigente.

En el caso que los servicios de seguridad de la información sean brindados por compañías del grupo y/o subsidiarias, la aseguradora o reaseguradora deberá establecer un contrato o acuerdo de servicio en el que se detalle el alcance y responsables de los servicios. El acuerdo de servicio firmado entre la empresa de seguro o reaseguro con las empresas del grupo no las exime de sus obligaciones y responsabilidades propias.

La información relacionada con las políticas, procedimientos y otros controles utilizados para la gobernanza y gestión de la seguridad de la información y ciberseguridad de la aseguradora o reaseguradora, debe estar a disposición de esta Superintendencia cuando esta así lo requiera como parte de la supervisión continua.

La unidad responsable de seguridad de la información y ciberseguridad deberá coordinar sus actividades con el área de gestión de riesgos y otras áreas de control, con la debida segregación de responsabilidades.

ARTÍCULO 11. RESPONSABLE DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD. Las compañías deberán contar con una unidad responsable para la gobernanza y gestión de la seguridad de la información y ciberseguridad, la cual tenga la suficiente jerarquía e independencia de las áreas operativas del negocio y funciones de control.

Entre las responsabilidades mínimas tendrá las siguientes:

1. Implementar y mantener actualizado el marco de gestión de seguridad de la información y ciberseguridad.
2. Mantener actualizado y proponer para su aprobación las políticas, procedimientos y demás instrumentos relacionados en esta materia.
3. Coordinar junto al área de gestión de riesgos, la identificación, evaluación, tratamiento y monitoreo de los riesgos de seguridad de la información y ciberseguridad, de acuerdo con sus responsabilidades.
4. Coordinar las actividades de respuesta y recuperación ante incidentes de ciberseguridad.
5. Mantener programas de concienciación continua para todo el personal incluyendo la Alta gerencia y Junta Directiva.
6. Velar por la ejecución de análisis de vulnerabilidades de manera continua y su debida remediación/control.

ARTÍCULO 12. POLÍTICAS Y PROCEDIMIENTOS. Las compañías deben establecer, implementar y mantener actualizado como mínimo las siguientes políticas y procedimientos para la gobernanza y gestión de la seguridad de la información y ciberseguridad: gestión de activos tecnológicos de la información, gestión de vulnerabilidades, clasificación y protección de la información, gestión de incidentes de seguridad de la información, gestión de identidades y accesos, gestión de configuraciones seguras, protección contra código malicioso, monitoreo, registro y detección de eventos de seguridad, gestión de cambios tecnológicos, uso aceptables de los activos tecnológicos, adquisición y desarrollo seguro de soluciones tecnológicas, de respaldo y restauración; y cualquiera otra que sea requerida por esta Superintendencia como parte de su proceso de supervisión continua.

Las políticas y procedimientos deben ser revisadas al menos una vez al año y actualizarse cuando ocurran cambios en el entorno tecnológico, el perfil de riesgos, los procesos del negocio y amenazas cibernéticas.

ARTÍCULO 13. GESTIÓN DE LA CIBERSEGURIDAD. Las compañías deben implementar un programa de ciberseguridad basado en riesgo que le permita gobernar, identificar, proteger, detectar, responder y recuperarse ante eventos e incidentes que pudiesen comprometer sus sistemas, información y servicios. El programa debe contener como mínimo los siguientes aspectos:

1. Identificación y gestión de activos tecnológicos y de la información: las compañías deben identificar y mantener actualizado un inventario de los activos de la información y tecnológicos que soporte sus procesos de negocio, los cuales deberán estar clasificados de acuerdo con su criticidad, sensibilidad, con la identificación de sus propietarios y responsables.

2. Gestión de identidades y acceso: debe gestionar el ciclo de vida de las identidades y derechos de acceso bajo los principios de mínimo privilegio, segregación de funciones y necesidad de conocimiento.

3. Autenticación fuerte: contar con mecanismos de autenticación multifactorial para accesos privilegiados, remotos, sistemas y aplicaciones críticas, así como para aquellos accesos de riesgo significativo.

4. Gestión de vulnerabilidades y actualizaciones: debe establecer procesos continuos para la identificación, evaluación, priorización y remediación de vulnerabilidades.

   En caso de no poder corregir de forma oportuna las vulnerabilidades identificadas, deberá establecer los controles compensatorios, como medida alternativa que mitiga el riesgo cuando el control o corrección principal no puede implementarse oportunamente.

   De igual manera, deberá contar con los mecanismos de documentación y aprobación de excepciones, para aquellas vulnerabilidades que no sean subsanadas luego del análisis correspondiente y debida aceptación del riesgo. No obstante, deberá establecer los controles que le permita monitorear los indicadores de riesgo relacionados con la posible explotación de la vulnerabilidad.

5. Protección contra código malicioso: deben implementar los mecanismos o controles para la prevención, detección y respuesta ante código malicioso y otras amenazas.

6. Monitoreo y detección de eventos: deben contar con herramientas, capacidades de monitoreo que le permitan identificar de manera oportuna comportamiento anómalo, eventos de seguridad y posibles incidentes.

7. Seguridad de redes: las compañías deben implementar controles para la protección de sus redes e infraestructura, considerando, la segmentación de redes, segmentación del perímetro, gestión segura de accesos remoto, seguridad de las comunicaciones y el monitoreo continuo del tráfico de red.

8. Administración de registros (logs): las compañías deberán generar, proteger y conservar los registros de eventos de seguridad que les permita detectar actividades anómalas, apoyar la investigación de incidentes y mantener la

trazabilidad de las acciones efectuadas sobre los activos tecnológicos y de la información.

9. Cifrado: las compañías deben implementar mecanismos de cifrados adecuados para la proteger la integridad y confidencialidad de la información, durante su estado de reposo y transmisión, de acuerdo con sus políticas de clasificación de la información y nivel de riesgo.

10. Evaluaciones de seguridad: las compañías deberán efectuar evaluaciones de seguridad, incluyendo análisis de vulnerabilidades, pruebas de intrusión y otras evaluaciones técnicas que le permitan verificar la efectividad de los controles implementados.

    Las pruebas de intrusión deben realizarse de manera periódica, de acuerdo con la naturaleza, complejidad y perfil de riesgo de la entidad.

11. Incorporar requisitos de seguridad de la información y ciberseguridad desde el diseño, adquisición, desarrollo, implementación y modificación de los sistemas de información, activos tecnológicos y de la información.

12. Mantenerse informadas sobre las amenazas emergentes que puedan impactar su perfil de riesgo.

13. Las compañías deben efectuar, al menos una vez al año, un proceso de autoevaluación del nivel de madurez en materia de ciberseguridad y definir el nivel esperado con la respectiva estrategia para su implementación.

ARTÍCULO 14. GESTIÓN DE INCIDENTES. Las compañías deben establecer un proceso para la gestión de los incidentes de ciberseguridad que contemple la identificación, registro, análisis, clasificación, priorización, escalamiento, contención, respuesta, recuperación y cierre, que les permita minimizar el impacto sobre las operaciones, la información y las funciones críticas.

El proceso deberá incluir como mínimo lo siguiente:

a. Definición de roles, responsabilidades y nivel de autoridad para la gestión de incidentes.
b. Criterios para la clasificación y priorización de los incidentes, tomando en cuenta la criticidad, impacto sobre las operaciones del negocio, los asegurados, la información, los terceros y el cumplimiento regulatorio.
c. Procedimiento para la comunicación, escalamiento y coordinación durante la atención del incidente.
d. Ejecución de las acciones de contención, erradicación, recuperación y restablecimiento de los servicios afectados.
e. Análisis de la causa raíz, lecciones aprendidas y planes de acción para reducir la probabilidad de ocurrencia.
f. Mantener un registro actualizado de los incidentes tecnológicos y de ciberseguridad, que le permita identificar las tendencias y contribuir a la mejora continua.

Las compañías deberán notificar a la Superintendencia de Seguros y Reaseguros de Panamá, los incidentes significativos o críticos, tanto de ciberseguridad como tecnológicos; dentro de las primeras cuarenta y ocho (48) horas luego de que la compañía tenga conocimiento. La ausencia del conocimiento de la causa raíz, impacto o cualquier otro elemento que requiera de investigación o definición de los planes de acción no debe retrasar la notificación inicial.

Para efectos de la notificación inicial dentro de las primeras cuarenta y ocho (48) horas de haber tenido conocimiento del incidente se considerarán, entre otros, aquellos eventos que:

a. Afecten de manera significativa la disponibilidad de servicios, procesos o sistemas tecnológicos críticos para la operación de la empresa de seguro o reaseguro.
b. Afecte a contratantes, asegurados, beneficiarios o terceros.
c. Comprometan la confidencialidad, integridad o disponibilidad de la información.
d. Afecten o puedan afectar de manera significativa la integridad financiera de las operaciones de la empresa.

Posteriormente a la notificación inicial, esta Superintendencia podrá requerir en cualquier momento, a la compañía la remisión de actualizaciones sobre la evolución y gestión del incidente, las cuales deberán ser presentadas dentro del plazo que determine la Superintendencia, y hasta tanto se reciba la notificación correspondiente al cierre del incidente.

Una vez resuelto y cerrado el incidente, y finalizada la investigación y el análisis correspondiente, la compañía deberá remitir un reporte final que incluya como mínimo: la causa raíz, impacto definitivo, las acciones de remediación y las lecciones aprendidas. La Superintendencia podrá requerir información adicional que considere necesaria para el adecuado seguimiento y evaluación del incidente. El reporte final debe enviarse dentro de los siguientes 30 días calendarios luego de cerrado el incidente.

La Superintendencia de Seguros y Reaseguros de Panamá, establecerá los formatos para cada uno de los reportes requeridos.

ARTÍCULO 15. CAPACITACIÓN Y CONCIENCIACIÓN. Las compañías deberán establecer y mantener programas de capacitación a todo el personal en materia de seguridad de la información y ciberseguridad. El área de recursos humanos en conjunto con seguridad de la información será responsable de la planificación anual del programa de concienciación relacionado con las amenazas cibernéticas; así como los riesgos de ciberseguridad a los que se expone la entidad en caso de materializarse un incidente.

El personal técnico a cargo de la gestión de la ciberseguridad y seguridad de la información deberá recibir capacitación especializada en esta materia a fin de mantener un recurso humano capacitado y actualizado.

ARTÍCULO 16. RESPALDO Y RESTAURACIÓN DE SISTEMAS Y DATOS. Las empresas de seguro y reaseguros, deberán establecer e implementar las políticas y procedimientos para la debida protección, conservación, verificación y restauración de los respaldos de la información y de sus sistemas críticos; incluyendo pruebas periódicas de restauración y medidas para proteger los respaldos de alteración o cifrado no autorizado. La criticidad de la información y sistemas debe estar definida por la compañía bajo su metodología de riesgo para la clasificación de activos y procesos críticos del negocio.

En el caso que identifique durante el proceso de supervisión continua que la compañía no mantiene los respaldos o realiza pruebas de restauración a aquellos datos y sistemas críticos, la Superintendencia de Seguros y Reaseguros, podrá requerir a las compañías efectuar respaldos y restauración a los sistemas y datos que identifique como críticos o necesarios para una adecuada continuidad de sus operaciones y resiliencia.

TÍTULO CUARTO

RESILIENCIA OPERATIVA DIGITAL Y CONTINUIDAD

ARTÍCULO 17. RESILIENCIA OPERATIVA DIGITAL. Las compañías deben establecer capacidades que le permitan mantener o recuperar de manera oportuna, ante

servicios o funciones críticas ante la ocurrencia de interrupciones tecnológicas y ciber incidentes.

Le corresponde a la compañía identificar sus servicios y funciones críticas, recursos tecnológicos, dependencia, los tiempos tolerables de interrupción y objetivos de recuperación.

De igual manera, deberán identificar las dependencias tecnológicas críticas necesarias para la prestación de sus servicios esenciales, incluyendo a sus proveedores y terceros tecnológicos, servicios en la nube, centro de datos, telecomunicaciones y demás componentes que soporten las funciones críticas. Esta identificación tiene como objetivo de asegurarse que la interrupción de estos servicios no comprometa la continuidad de las funciones y servicios críticos.

Cuando las funciones relacionadas con resiliencia operativa digital sean gestionadas de manera corporativa o por una empresa del grupo; deberá existir un contrato o acuerdo de servicio debidamente formalizado y aprobado por la Junta Directiva. Este contrato o acuerdo de servicio, debe establecer de forma clara, detallada y específica cada uno de los aspectos que se gestionan. El acuerdo de servicio firmado entre la empresa de seguro o reaseguro con las empresas del grupo no las exime de sus obligaciones y responsabilidades propias.

ARTÍCULO 18. PLAN DE CONTINUIDAD Y RECUPERACIÓN ANTE DESASTRES. Las compañías deberán establecer y mantener un Plan de Continuidad de TI y un Plan de Recuperación ante Desastres en los que se definan los roles, responsabilidades, procedimientos de respuesta y recuperación, tiempo objetivo de recuperación, punto objetivo de recuperación, recursos necesarios, comunicaciones, dependencias críticas y mecanismos de actualización y prueba periódica.

ARTÍCULO 19. PRUEBAS DE RESILIENCIA OPERATIVA DIGITAL. Las compañías deben establecer un programa de pruebas de resiliencia operativa digital basado en riesgos, el cual le permita evaluar los controles y mecanismos implementados para recuperación y respuesta ante interrupciones tecnológicas y ataques cibernéticos.

Las pruebas deben considerar escenarios de ransomware, indisponibilidad del centro de datos, interrupción de servicios en la nube, falla de telecomunicaciones y otros escenarios relevantes. Los resultados deben documentarse, incluyendo las lecciones aprendidas, acciones correctivas y de seguimiento.

Las pruebas de resiliencia operativa digital deben efectuarse al menos una vez al año y acorde con el perfil de riesgos, criticidad de los servicios y nivel de dependencia tecnológica de la empresa.

TÍTULO QUINTO

GESTIÓN DE PROVEEDORES Y TERCEROS

ARTÍCULO 20. GESTIÓN DE RIESGOS DE PROVEEDORES Y TERCEROS. Las compañías deberán establecer un marco de control para la gestión de sus terceros tecnológicos y de ciberseguridad que contemple como requisitos mínimos los siguientes:

1. Clasificación de sus proveedores y terceros tecnológicos de acuerdo con la naturaleza de los servicios prestados, dependencia tecnológica, impacto en caso de interrupción o falla, acceso a la información y criticidad de las funciones o servicios soportados.
2. Las compañías deben monitorear de forma periódica el desempeño de sus proveedores y terceros, el cumplimiento de los niveles de servicios establecidos, capacidad, seguridad y su perfil de riesgo. Asimismo, deberán realizar evaluaciones periódicas de la seguridad y continuidad de los proveedores relevantes, de acuerdo con el riesgo y criticidad de los servicios contratados.

3. La gestión debe contemplar la planificación de la selección, proceso de debida diligencia, contratación, implementación, monitoreo, renovación, modificación y finalización del contrato.
4. Las compañías deben identificar y gestionar los riesgos inherentes o producto de la subcontratación de servicios por parte de sus proveedores y terceros.
   Los contratos deberán establecer las condiciones aplicables a la subcontratación, incluyendo la obligación del proveedor de tecnología de informar oportunamente a la compañía sobre cualquier incorporación, sustitución o eliminación de subcontratistas que participen en la prestación del servicio, así como sobre cualquier cambio relevante en la cadena de prestación del servicio.

   Deben establecer planes de contingencia en conjunto para garantizar la continuidad del servicio. Los planes deben ser probados en conjunto con los proveedores o terceros para asegurarse de la efectividad de este. Asegurarse de establecer en los contratos los requisitos de seguridad y ciberseguridad, alineados con el marco establecido en la compañía.

   Cuando los subcontratistas participen en la prestación de servicios críticos, las compañías deberán identificar a aquellos subcontratistas críticos y dependencias relevantes dentro de la cadena de prestación, y evaluar los riesgos asociados cuando una interrupción pueda afectar sus funciones críticas.

5. Establecer estrategias de salida para los servicios tecnológicos críticos que les permita remplazar al proveedor o migrar los servicios sin afectar la continuidad de las operaciones, de acuerdo con el riesgo y la criticidad del proveedor o servicios contratado.
6. Identificar los servicios que mantiene con un mismo proveedor o tercero y gestionar los riesgos de concentración de servicios tecnológicos.
7. Las compañías deberán asegurarse de tener acceso a la información relacionada con el servicio y producto contratado.
8. La compañía debe asegurarse que la contratación de servicios no impida el proceso de supervisión que debe ejecutar la Superintendencia de Seguros y Reaseguros de Panamá, en cuanto a la obtención de la información necesaria para la evaluación a la empresa de seguro o reaseguro

ARTÍCULO 21. GESTIÓN DE SERVICIOS DE COMPUTACIÓN EN LA NUBE. Las compañías aseguradoras y reaseguradoras que utilicen servicios de computación en la nube deben establecer políticas, procedimientos y controles, así como los mecanismos para la identificación, evaluación, gestión y monitoreo de los riesgos derivados de estos servicios durante todo su ciclo de vida; considerando su criticidad, dependencias tecnológicas, la continuidad de los servicios y la capacidad para responder y recuperarse ante interrupciones.

La utilización de los servicios de computación en la nube no exime a la compañía de seguro o reaseguro de su responsabilidad de gestionar los riesgos tecnológicos, cibernéticos, ni de garantizar la continuidad de sus funciones críticas.

TÍTULO SEXTO

PROCESO SANCIONADOR

ARTÍCULO 22. SANCIONES. La Superintendencia de Seguros y Reaseguros de Panamá impondrá sanciones a todas aquellas personas que no cumplan con lo señalado en el presente Acuerdo, con base a lo dispuesto en el artículo 280 de la Ley N° 12 de 3 de abril de 2012, sin perjuicio del derecho que tienen las empresas aseguradoras y reaseguradoras de utilizar los recursos legales que contempla la ley en su defensa.

ARTÍCULO 23. VIGENCIA. El presente Acuerdo comenzará a regir a partir de su promulgación en la Gaceta Oficial de la República de Panamá y su aplicación entrará en vigor a partir del 1 de abril de 2027.

Dado en la ciudad de Panamá, a los quince (16) días del mes de octubre de dos mil veintiséis (2026).

PUBLÍQUESE Y CÚMPLASE,

Glorianna De Luca Quesada
Presidenta

Fernando Sucre
Secretario Ad Hoc

REPÚBLICA DE PANAMÁ SUPERINTENDENCIA DE SEGUROS Y REASEGUROS JUNTA DIRECTIVA

REPÚBLICA DE PANAMÁ SUPERINTENDENCIA DE SEGUROS Y REASEGUROS SUPERINTENDENCIA

SUPERINTENDENCIA DE SEGUROS Y REASEGUROS
ES COPIA AUTÉNTICA DE SU ORIGINAL
Panamá 27 de octubre 20 26