Consulta FIDES:

¿Existe en sus respectivos países alguna normativa escrita por parte del regulador de la actividad aseguradora o financiera, alguna regulación encuadrada dentro de Gobierno Corporativo de las empresas que establezca requisitos mínimos sobre temas de Ciberseguridad?

Colombia	Adjunta la normativa colombiana en la materia
Costa Rica	Se comparte el proyecto de reforma integral al Reglamento General de Gestión de Tecnologías de Información, CONASSIF 5-17, que actualmente se encuentra en consulta a todo el sector financiero, incluido aseguradoras y corredores de seguros. Dicho proyecto se tramita desde el regulador, con el fin de alcanzar dos propósitos principales, no cubiertos por la versión vigente: a. Reforzar las funciones de los Órganos de Dirección, Alta Gerencia y Órganos de Control con relación al marco de gobierno y de gestión de TI, incluyendo responsabilidades sobre la seguridad de la información, la seguridad cibernética y la resiliencia operativa digital. b. Actualizar el marco de gobierno y de gestión de TI e incorporar disposiciones sobre tecnologías emergentes, gobierno y gestión de la seguridad de la información, seguridad cibernética, incidentes de seguridad de la información, incidentes de seguridad cibernética, tercerización de bienes y servicios de TI, computación en la nube, el tratamiento del uso y acceso de los datos y de los activos de información. En documento adjunto se resumen las principales disposiciones en materia de seguridad de la información y ciberseguridad que contempla este proyecto normativo. Asimismo, se adjunta copia del proyecto reglamentario y sus lineamientos por cualquier detalle puntual que se quiera consultar.
Ecuador	La regulación vigente de Ecuador, no cuenta con normativa específica sobre temas de ciberseguridad.

EEUU	Regarding cybersecurity governance: The NAIC has its Insurance Data Security Model Law: https://content.naic.org/sites/default/files/inline-files/MDL-668.pdf The law 'establish standards for data security and standards for the investigation of and notification to the Commissioner of a Cybersecurity Event applicable to Licensees'. As of January, 2024, the law has been adopted in 23 states. The NAIC has put together an excellent one-pager on the issue that can be publicly viewed here: https://content.naic.org/sites/default/files/government-affairs-brief-data-security-model-law.pdf
El Salvador	Para el caso de El Salvador sí existe, estas disposiciones se recogen en las Normas Técnicas para la Gestión de la Seguridad de la Información, que tienen por objeto establecer los criterios mínimos para la gestión de la seguridad de la información y la ciberseguridad de la misma, acordes a las mejores prácticas internacionales, naturaleza, tamaño, perfil de riesgo de las entidades y volumen de sus operaciones. Adjunto las Normas Técnicas en cuestión para mayor detalle.
España	Desde enero del 2023, las entidades financieras europeas están obligadas a adaptarse a las previsiones del reglamento (UE) 2022/2554, del Parlamento Europeo y del Consejo, de 14 de diciembre del 2022, sobre la resiliencia operativa digital del sector financiero. Este reglamento, que es de obligado cumplimiento en los países UE desde su publicación (es decir, no es objeto de trasposición a la legislación nacional), suele conocerse como reglamento DORA, siglas de Digital Operational Resilience Act. DORA es de aplicación a todas las entidades aseguradoras sometidas a Solvencia II (que son prácticamente todas, salvo algunas de muy pequeño tamaño), así como a los intermediarios de seguros que no sean micro, pequeñas y medianas empresas. El reglamento DORA, cuyo texto adjunto en el presente correo, establece el marco de actuación en el que las entidades financieras deben generar sus procesos y funciones para el control del riesgo tecnológico, con inclusión de elementos de gobernanza, política de activos TIC (Tecnologías de la Información y las Comunicaciones), procesos de autenticación, parches, política de seguridad de la información, desarrollos de software y hardware, mapeo de recursos y riesgos y planes de continuidad de negocio, entre otros. Asimismo,

	también regula la política de comunicación obligatoria de cíber incidentes relevantes, y voluntaria de vulnerabilidades detectadas. Se regula asimismo la política de test y comprobación, incluyendo los TLPT (Threat-led Penetration Tests), o test de equipo rojo o hackeo programado. Asimismo, la norma se completa con un capítulo dedicado a la gestión de proveedores, sobre todo aquéllos soportando funciones críticas o importantes. En último lugar, el reglamento prevé un régimen de supervisión reforzada para los proveedores considerados sistémicos, es decir, aquéllos extendidos en una amplia cuota de entidades y/o considerados difícilmente sustituibles (en la práctica, las normalmente conocidas como gatekeepers o Big Tech). El reglamento DORA prevé el desarrollo de once denominados actos delegados, la mayoría de ellos RTS (Regulatory Technical Standards), aunque otros son ITS (Implementing Technical Standards) y otros guías o directrices. Estos actos delegados desarrollan aspectos del reglamento en materias como el propio sistema de control de riesgos, la política de proveedores, la realización de TLPT, la comunicación de cíber incidentes, etc. Las autoridades supervisoras financieras europeas, normalmente conocidas como las ESAs (European Supervisory Authorities) han lanzado ya para consulta dos oleadas de actos delegados que cubren todos estos mandatos. Aunque ninguno de los actos delegados está todavía formalmente publicado, los de la primera oleada han sido ya aprobados por las ESAs, y están pendientes de su aprobación por las instituciones y su publicación. Esto quiere decir que existen borradores bastante fiables de los actos delegados de la primera oleada, y en fase de consulta para los de la segunda oleada. En el caso de que desearen acceder a estos textos, no duden en pedirlos. DORA genera asimismo efectos indirectos. Por ejemplo, en el borrador de norma para la implantación de un esquema OpenFinance en Europa, normalmente conocido como FIDA, se exige, entre otras cosas, que los actores que decidan operar como FISP (Financial Information Service Providers, es decir, los Spock del sistema OpenFinance brasileño) deben cumplir con DORA. Otra normativa de interés es la Directiva (UE) 2022/2555, del Parlamento y del Consejo, también con fecha 14 de diciembre del 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión. Directiva normalmente conocida como directiva NIS2 (Network and Information Systems Directive). NIS2 es obviamente la segunda versión de la directiva NIS, encaminada a mejorar las condiciones de cíber seguridad en determinados sectores considerados críticos. NIS1 dejaba más libertad a los Estados para

	definir qué sectores estarían dentro de la aplicación de NIS; aunque la mayoría de los Estados europeos dejaron al sector asegurador fuera de dicho ámbito, otros, como Francia o España, lo situaron dentro. NIS2, sin embargo, reconoce que, con la llegada del reglamento DORA, éste debe de ser el referente normativo del sector financiero en materia de cíber seguridad (además de que es, en general, más exigente). No obstante, todavía está pendiente de ver cómo se articulará, definitivamente, la colaboración entre DORA y NIS2 cuando ésta última sea recibida en la legislación española. Adjunto el texto de la directiva NIS2. De manera ya más colateral, la UE desarrollo otro proyecto normativo, conocido como la Cyber Resilience Act, que regula, en general, las condiciones de cíber seguridad que deben de cumplir los elementos digitales que sean puestos a disposición del público (como pueda ser una app de smartphone de una aseguradora). Esta normativa es sector-agnostic, lo cual quiere decir que aplicará también al sector financiero aunque exista el reglamento DORA. Con un carácter más general, también se desarrolla la denominada Cyber Solidarity Act, que es un proyecto normativo que busca mejorar la coordinación europea y la capacidad de luchar contra las cíber amenazas. Espero que esta información les sea de utilidad.
Guatemala	En Guatemala no existe normativa.
Honduras	En Honduras, existen las Normas para la Gestión de Tecnologías de Información, emitidas en el 2022, que establecen requisitos para las áreas de IT en materia de prevención y ciberseguridad. Adicionalmente, en el 2023 se emitieron unos lineamientos para la prevención de fraude cibernético. Adjunto ambas normas
Perú	En el Perú, la Superintendencia de Banca, Seguros y AFP emitió la Resolución N°504-2021, que aprobó el Reglamento para la Gestión de la Seguridad de la Información y Ciberseguridad, la cual acompañamos a la presente comunicación al igual que sus antecedentes normativos. La resolución bajo comentario define los términos relacionados con seguridad de la información y ciberseguridad y establece la proporcionalidad entre las medidas de seguridad de la información y el tamaño de las empresas. De igual manera, establece las responsabilidades del directorio, de gerencia y del comité de riesgos.

	En esa línea, establece las exigencias mínimas que las empresas deben realizar, para cumplir con esta normativa, entre las cuales se encuentra contar con un Programa de Ciberseguridad, reportar los incidentes sobre seguridad de la información, implementar procesos de autenticación, uso de API, entre otros.
República Dominicana	NO existe por parte del regulador regulación concerniente enmarcada al Gobierno Corporativo de las empresas del sector, con requisitos mínimos de ciberseguridad.
Uruguay	En Uruguay existen exigencias básicas al respecto en los estándares mínimos de gestión (adjunto, Ver Riesgo Operacional + estándares de tecnología) https://www.bcu.gub.uy/Servicios-Financieros-SSF/Seguros/EMG_Empresas_Aseguradoras.pdf
Venezuela	No existe ninguna regulación, sin embargo, estamos actualmente en el proceso de Consulta Pública de las normas y reglamento que van a desarrollar la reciente reforma de la Ley y dentro de todas las normativas se contempla algunas previsiones en materia de Ciberseguridad para el uso de Insurtech y Fintech, así como de Seguridad de la Información en materia de auditorías, en procedimientos y trámites a través de medios electrónicos con la Superintendencia, pero como indicamos son proyectos de normas que están en consulta, no son definitivas.