REQUISITOS DE ACCESIBILIDAD Y VALIDACION PARA VENTA DIGITAL DE SEGUROS

El motivo de este cuadro comparativo de normas legales es porque en Perú se ha aprobado recientemente un nuevo reglamento de seguridad de la información y ciberseguridad transversal a la industria bancaria, seguros y administradora de fondos de pensiones, siendo que el extremo referido a la venta de productos a distancia y digitalmente ha establecido requisitos de autentificación y enrolamiento, incluyendo criterios reforzados para ciertos supuestos, los cuales resultan excesivos para el caso de seguros.

Países que han brindado una respuesta a la consulta realizada:

1) Argentina: pendiente el adjunto
2) España
3) Bolivia
4) México
5) Ecuador
6) República Dominicana
7) Chile
8) Brasil
9) Venezuela
10) Costa Rica
11) Perú
12) Guatemala
13) Honduras
14) Panamá

Países que no han brindado una respuesta a la consulta realizada:

1) Estados Unidos
2) Colombia
3) El Salvador
4) Nicaragua
5) Paraguay
6) Uruguay

PERÚ	Resolución SBS N° 504.2021 de fecha 19 de febrero de 2021 Reglamento para la gestión de la seguridad de la información y la ciberseguridad I Subcapítulo III AUTENTICACIÓN	***"Artículo 17. Implementación de los procesos autenticación*** *17.1 La empresa debe implementar procesos de autenticación, conforme a la definición establecida en este Reglamento, para controlar el acceso a los servicios que provea a sus usuarios por canales digitales, previo a lo cual debe evaluar formalmente y tomar medidas sobre:* *a) El o los factores de autenticación que serán requeridos.* *b) Estándares criptográficos vigentes, basados en software o en hardware, y sus prestaciones de confidencialidad o integridad esperadas.* *c) Plazos y condiciones en las que será obligatorio requerir al usuario volver a autenticarse, lo que incluye y no se limita a casos por periodo de inactividad o sesiones de uso prolongado de sistemas.* *d) Línea base de controles de seguridad de la información requerida para prevenir las amenazas a que esté expuesto el proceso de autenticación, lo que incluye, y no se restringe, al número límite de intentos fallidos de autenticación, la prevención de ataques de interceptación y manipulación de mensajes.* *e) Lineamientos para la retención de registros de auditoría para la detección de amenazas conocidas y eventos de seguridad de la información.* *17.2 Los procesos de autenticación deben ser reevaluados siempre que la tecnología utilizada para su implementación deje de contar con el soporte del fabricante, o tras el descubrimiento de nuevas vulnerabilidades que pueden exponerlos.* *17.3 La empresa debe mantener y proteger los registros detallados de lo actuado en cada enrolamiento de usuario, intento de autenticación y cada operación que requiera de autenticación previa.* *17.4 La empresa debe contar con herramientas y procedimientos para implementar el monitoreo de transacciones que permita tomar medidas de reducción de la posibilidad de operaciones fraudulentas, que incorpore los escenarios de fraude ya conocidos, y el robo o compromiso de los elementos utilizados para la autenticación.* ***Artículo 18. Enrolamiento del usuario en servicios provistos por canal digital*** *18.1 El enrolamiento de un usuario en un canal digital requiere por lo menos:* *a) Verificar la identidad del usuario y tomar las medidas necesarias para reducir la posibilidad de suplantación de identidad, lo que incluye el uso de dos factores independientes de categorías diferentes, según el literal j) del artículo 2 de este Reglamento.* *b) Generar las credenciales y asignarlas al usuario.* *18.2 La empresa debe gestionar el ciclo de vida de las credenciales que genere y asigne a sus usuarios, para lo cual debe prever los*

		procedimientos para su activación, suspensión, reemplazo, renovación y revocación; así también, cuando corresponda, asegurar su confidencialidad e integridad. ***Artículo 19. Autenticación reforzada para operaciones por canal digital*** *Se requiere de autenticación reforzada para aquellas acciones que puedan originar operaciones fraudulentas u otro abuso del servicio en perjuicio del cliente, como las operaciones a través de un canal digital que impliquen pagos o transferencia de fondos a terceros, registro de un beneficiario de confianza, modificación en los productos de seguro ahorro/inversión contratados, la contratación de un producto o servicio, modificación de límites y condiciones, para lo cual se requiere:* *a) Utilizar una combinación de factores de autenticación, según el literal j) del artículo 2 del presente Reglamento que, por lo menos, correspondan a dos categorías distintas y que sean independientes uno del otro.* *b) Generar un código de autenticación mediante métodos criptográficos, a partir de los datos específicos de cada operación, el cual debe utilizarse por única vez.* *c) Cuando la operación sea exitosa, notificar los datos de la operación al usuario."*

BRASIL	No es una regulación similar	En el ámbito del regulador de seguros privados (Susep), existe el normativo acerca de medios remotos (CNSP 294 - https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/11355), que está siendo revisado por el regulador para incorporar criterios más flexibles. En Brasil, no existe una regulación de ciberseguridad específica para comercializar productos de seguros de forma digital. Sin embargo, existe un requisito reglamentario para la gestión de riesgos desde 2015 (Susep 521 / Capitulo II - https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/14370). En 2020 el tema se discutió en Brasil. Se realizó una encuesta sobre riesgos cibernéticos con el mercado supervisado, motivada principalmente por la migración masiva a las actividades de teletrabajo durante la pandemia. La iniciativa tenía como objetivo evaluar la estructura de gestión de riesgos, así como fomentar la reflexión sobre el riesgo de ciberataques. En el plan de regulación de la SUSEP 2021 (Resolución 243 - https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/24063) se prevé establecer condiciones y criterios para la definición de la política de ciberseguridad de las empresas supervisadas. Además, este tema también es un pilar para la implementación de *Open Insurance*, por lo que la expectativa es una consulta pública próximamente. Cabe mencionar para el sector bancario, el tema fue regulado en 2018, y este año se revisó y reeditó la norma, esta es la Resolución 4893 de 2021 - https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=48934893 Ninguna de las normas hace referencia a la autenticación y validación en la venta de productos a distancia.
ARGENTINA	No se regula	La Superintendencia de Seguros de la Nación Argentina no requiere el cumplimiento de lo establecido en la normativa peruana.
ESPAÑA	Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera regularon la “autenticación reforzada de clientes”	En España la venta a distancia de seguros está regulada en la Ley 22/2017 sobre comercialización a distancia de servicios financieros, sin perjuicio de la aplicación general de la normativa de protección a los consumidores (incluida la relativa al comercio electrónico) y lo dispuesto en la normativa sectorial de seguros. Al respecto, es importante precisar que no se señala nada respecto a la autenticación // No se regula nada acerca de la autenticación y validación. En el tráfico bancario los requisitos de autenticación reforzada de clientes se regulan a nivel europeo en la segunda directiva de servicios de pago (Directiva PSD2 “Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE”) y la correspondiente norma española de trasposición (Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera regularon la “autenticación reforzada de clientes”. **(No es una norma que haga referencia de forma explícita a las Compañías de Seguros).** https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:72015L2366ESP_265274&from=EN “*Artículo 68. Autenticación.*

		1. Los proveedores de servicios de pago aplicarán la autenticación reforzada de clientes, en la forma, con el contenido y con las excepciones previstas en la correspondiente norma técnica aprobada por la Comisión Europea, cuando el ordenante: *a) acceda a su cuenta de pago en línea;* *b) inicie una operación de pago electrónico;* *c) realice por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos.* *2. En lo que se refiere a la iniciación de las operaciones de pago electrónico mencionada en el apartado 1, letra b) respecto de las operaciones remotas de pago electrónico, los proveedores de servicios de pago aplicarán una autenticación reforzada de clientes que incluya elementos que asocien dinámicamente la operación a un importe y un beneficiario determinados.* *3. En los casos a los que se refiere el apartado 1, los proveedores de servicios de pago contarán con medidas de seguridad adecuadas para proteger la confidencialidad y la integridad de las credenciales de seguridad personalizadas de los usuarios de los servicios de pago.* *4. Los apartados 2 y 3 se aplicarán asimismo cuando los pagos se inicien a través de un proveedor de servicios de iniciación de pagos. Los apartados 1 y 3 se aplicarán asimismo cuando la información se solicite a través de un proveedor de servicios de pago que preste servicios de información sobre cuentas.* *5. El proveedor de servicios de pago gestor de cuenta permitirá al proveedor de servicios de iniciación de pagos y al proveedor de servicios de pago que preste servicios de información sobre cuentas utilizar los procedimientos de autenticación facilitados al usuario de servicios de pago por el proveedor de servicios de pago gestor de cuenta de conformidad con los apartados 1 y 3 y cuando intervenga el proveedor de servicios de iniciación de pagos, de conformidad con los apartados 1, 2 y 3.* *6. No obstante, no será preciso aplicar la autenticación reforzada de clientes a la que se refiere el apartado 1 a los supuestos indicados en el artículo 98.1.b) de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015".*
BOLIVIA	No se regula	Existe un marco legal general que es la Ley N° 164 del 8 de agosto de 2011 "LEY GENERAL DE TELECOMUNICACIONES, TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN" y su Reglamento, no se tiene una norma específica para seguros. En esta norma no se señala nada acerca de autenticación y validación. Por otro lado, hay que precisar que las entidades aseguradoras han implementado canales digitales para la atención a sus asegurados por la pandemia.
MÉXICO	Ley de Instituciones de Seguros y Fianzas, en sus artículos 214 y 348 **La Circular Única de Seguros y de Fianzas en su capítulo 4.10**	En México, los instrumentos para la regulación en materia de comercio electrónico en seguros se encuentran en: • A nivel de Ley, la Ley de Instituciones de Seguros y Fianzas, en sus artículos 214 y 348. *ARTÍCULO 214.- La celebración de las operaciones y la prestación de servicios de las Instituciones, se podrán pactar mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos, estableciendo en los contratos respectivos las bases para determinar lo siguiente:* *I. Las operaciones y servicios cuya prestación se pacte;* *II. Los medios de identificación del usuario, así como las responsabilidades correspondientes a su uso, tanto para las Instituciones como para los usuarios;* ***III.*** *Los medios por los que se hagan constar la creación, transmisión, modificaciones o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate,* ***incluyendo los métodos de autenticación tales como contraseñas o claves de acceso, y***

		IV. Los mecanismos de confirmación de la realización de las operaciones celebradas a través de cualquier medio electrónico. *El uso de los medios de identificación que se establezcan conforme a lo previsto por este artículo, en sustitución de la firma autógrafa, producirá los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio.* *La instalación y el uso de los equipos y medios señalados en el primer párrafo de este artículo se sujetarán a las disposiciones de carácter general que, en su caso, emita la Comisión.* *ARTÍCULO 348.- En la celebración de las operaciones y la prestación de servicios de las Sociedades Mutualistas, será aplicable lo previsto en los artículos 109 a 113 y 214 de este ordenamiento.* • A nivel de normatividad secundaria, la Circular Única de Seguros y de Fianzas en su capítulo 4.10. En esta norma se recogen 4 categorías de autenticación: - Factor de Autenticación **Categoría 1**: Se compone de información obtenida mediante la aplicación de cuestionarios al Usuario, por parte de operadores telefónicos, en los cuales se requieran datos que el Usuario conozca. - Factor de Autenticación **Categoría 2**: Se compone de información que sólo el Usuario conozca e ingrese a través de un Dispositivo de Acceso, tales como Contraseñas y Números de Identificación Personal (NIP). - Factor de Autenticación **Categoría 3**: Se compone de información contenida o generada por medios o dispositivos electrónicos, así como la obtenida por dispositivos generadores de Contraseñas dinámicas de un solo uso. Dichos medios o dispositivos deberán ser proporcionados por las Instituciones y Sociedades Mutualistas a sus Usuarios y la información contenida o generada por ellos, deberá cumplir con las características siguientes: a) Contar con propiedades que impidan su duplicación o alteración; b) Ser información dinámica que no podrá ser utilizada en más de una ocasión; c) Tener una vigencia que no podrá exceder de dos minutos, y d) No ser conocida con anterioridad a su generación y a su uso por los funcionarios, empleados, representantes o comisionistas de la Institución o Sociedad Mutualista, o por terceros. - Factor de Autenticación **Categoría 4**: Se compone de información del Usuario derivada de sus propias características físicas, tales como huellas dactilares, geometría de la mano o patrones en iris o retina, entre otras. Las Instituciones y Sociedades

		Mutualistas que utilicen los Factores de Autenticación de esta categoría, deberán aplicar a la información de Autenticación obtenida por dispositivos biométricos, elementos que aseguren que dicha información sea distinta cada vez que sea generada, a fin de constituir Contraseñas de un solo uso, que en ningún caso puedan utilizarse nuevamente o duplicarse con la de otro Usuario. Proceso de autenticación en cada ocasión: I. Contratación de un **seguro de vida o muerte accidental**, al menos nivel 3; II. Contratación de un **seguro de daños, de accidentes y enfermedades** con excepción de la cobertura por muerte accidental o una fianza, al menos nivel 2; III. **Cancelación de un seguro o una fianza**, al menos nivel 2, salvo en seguros de vida o muerte accidental que requerirán un nivel 3; IV. Solicitud, **aceptación o emisión de endosos a los contratos**, al menos nivel 2; V. Transferencias de recursos dinerarios a cuentas de terceros u otras Instituciones o Sociedades Mutualistas, incluyendo el pago de primas, así como las autorizaciones e instrucciones de domiciliación de pago de primas al menos nivel 3. Cuando las cuentas destino, entendidas como cuentas receptoras de recursos dinerarios en operaciones monetarias, hayan sido registradas en oficinas bancarias o bien el Usuario haya solicitado que dichas cuentas se consideren como cuentas destino recurrentes, las Instituciones o Sociedades Mutualistas podrán permitir a los Usuarios realizar dichas operaciones utilizando un solo Factor de Autenticación de al menos de nivel 2,; VI. **Modificación de designación de beneficiarios**, al menos nivel 3; VII. Alta y modificación del medio de notificación al Usuario, debiendo enviarse tanto al medio de notificación anterior como al nuevo, al menos nivel 2; VIII. Consultas de estados de cuenta u otras consultas que permitan conocer información relacionada con el Usuario o los contratos que tenga celebrados con la Institución o Sociedad Mutualista, que pueda ser utilizada como información de Autenticación, al menos nivel 3; IX. Contratación de otro servicio de Operaciones Electrónicas o modificación de las condiciones para el uso del servicio previamente contratado, al menos nivel 2; X. Desbloqueo de Contraseñas o Números de Identificación Personal (NIP), así como para la reactivación del uso de los servicios respecto de otras Operaciones Electrónicas que tenga contratados, al menos nivel 1; XI. Modificación de Contraseñas o Números de Identificación Personal (NIP) por parte del Usuario, al menos nivel 2, y XII. Solicitud de pago de rescate o aplicación de valores garantizados, al menos nivel 3.
ECUADOR	No se regula	No existe regulación similar o equivalente a la que se ha propuesto en Perú, que deba ser de cumplimiento de las empresas de seguros y reaseguros.
REPÚBLICA DOMINICANA	No se regula	No existe una disposición que exija requisito para la accesibilidad y validación para la venta digital de seguros por parte del regulador.

CHILE	No hay regulación similar	La Circular 2148 del 8 de abril de 2014, regula de manera general la contratación de seguros a distancia; sin embargo, no se precia nada respecto a la autenticación. La norma especial de autenticación y acceso a distancia de asegurados aprobada por la pandemia, fue en SCOMP: la NCG 436 que Imparte instrucciones transitorias sobre el Sistema de Consultas y Ofertas de Montos de Pensión establecido por el artículo 61 bis del DL N° 3.500, de 1980. Al respecto, hay que precisar que no existe una regulación similar a la de Perú, señalando que *"La compañía de seguros deberá establecer medidas que permitan la autenticación del solicitante, como, por ejemplo, un set de preguntas"*
GUATEMALA	No se regula	No existen requerimientos
PANAMÁ	No se regula	No han modificado la ley, solo algunas circulares sobre políticas de Conoce Tu Cliente.
HONDURAS	No se regula	No existen requerimientos actualmente
VENEZUELA	No se regula	Es importante destacar que, si bien puede haber comercialización por canales digitales, la comercialización a través de Banca-Seguros está prohibida en la Ley.
COSTA RICA	No se regula	El Reglamento sobre Inclusión y Acceso al Seguro (SUGESE 11-20), que para efectos de los seguros autoexpedibles reconoce en sus artículos 3.5 y 7 el uso de medios a distancia al menos para pagos, contratación, entrega de información, asesoría, servicio posventa y presentación de reclamaciones y quejas, en adición a los medios tradicionales. No hace referencia a la autenticación y verificación.

Conclusiones:

- Los únicos países con regulación respecto a la autenticación son España y México. La regulación de este último país es amplia.
- Tras revisar las normas se advierte que no hay una regulación similar a la peruana.

Lima, 24 de mayo del 2021.