Gobierno de Puerto Rico

OFICINA DEL COMISIONADO DE SEGUROS

San Juan, Puerto Rico

REGLA NÚM. 108

"NORMAS DE CIBERSEGURIDAD PARA LA INDUSTRIA DE SEGUROS"

Gobierno de Puerto Rico
OFICINA DEL COMISIONADO DE SEGUROS
San Juan, Puerto Rico

ÍNDICE

REGLA NÚM. 108

"NORMAS DE CIBERSEGURIDAD PARA LA INDUSTRIA DE SEGUROS"

TABLA DE CONTENIDO

Gobierno de Puerto Rico
OFICINA DEL COMISIONADO DE SEGUROS
San Juan, Puerto Rico

REGLA NÚM. 108

NORMAS DE CIBERSEGURIDAD PARA LA INDUSTRIA DE SEGUROS

ARTÍCULO 1. – TÍTULO

Esta Regla se conocerá como "Normas de Ciberseguridad para la Industria de Seguros".

ARTICULO 2. – BASE LEGAL

Esta Regla se promulga de conformidad con el Artículo 2.030 de la Ley Núm. 77 de 19 de junio de 1957, según enmendada, conocida como "Código de Seguros de Puerto Rico" y la Ley Núm. 38-2017, según enmendada, conocida como la "Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico".

ARTÍCULO 3. – PROPÓSITO

Esta Regla tiene el propósito de establecer las normas de ciberseguridad en la industria de seguros y las normas para la investigación y notificación al Comisionado de un incidente de Ciberseguridad relacionada con el negocio de un Regulado, conforme dispone esta Regla.

ARTÍCULO 4. – RESUMEN EJECUTIVO

La presente Regla surge por la creciente necesidad de crear las salvaguardas necesarias para minimizar los riegos de acceso no autorizado a sistemas de información que comprometa datos e información no pública relacionada con el negocio de seguros de un Regulado. La adopción de esta Regla refleja el compromiso de la Oficina del Comisionado de Seguros de Puerto Rico con establecer un marco de regulación idóneo de ciberseguridad para salvaguardar información sensitiva de los consumidores recopilada como parte de los procesos de suscripción y reclamos en el negocio de seguro, cónsono con los principios del *National Association of Insurance Commissioners* (NAIC) establecidos en "Insurance Data Security Law".

Para garantizar la continuidad y relevancia de esta Regla se utiliza como principio rector los estándares del *U.S. National Institute of Standards and Technology* (NIST) cuyo marco proporciona los estándares, pautas y prácticas adecuadas para asistir a los Regulados en la gestión de sus riesgos cibernéticos.

A. Para lograr la ciberseguridad de la industria de seguros esta Regla requiere que los Regulados:

(1) desarrollen, implementen y mantengan un Programa de Ciberseguridad;

(2) investiguen cualquier evento de ciberseguridad; y

(3) notifiquen al Comisionado de los eventos de ciberseguridad.

ARTÍCULO 5. – INTERPRETACIÓN

No se podrá interpretar que esta Regla crea una causa de acción judicial por la violación de sus disposiciones ni se podrá interpretar que impida ejercer alguna otra causa de acción judicial que de otra manera exista.

De surgir algún conflicto entre lo establecido en esta Regla y cualquier otra legislación, la interpretación que prevalecerá será aquella que resulte más favorable para salvaguardar los derechos de los asegurados.

ARTÍCULO 6. – APLICABILIDAD

Las disposiciones de esta Regla aplicarán a toda persona que ostente una licencia o autorización para contratar negocio de seguros, debidamente emitida por la Oficina del Comisionado de Seguros de Puerto Rico ("OCS") y que a su vez utilice un Sistema de Información, según se define en esta Regla.

ARTÍCULO 7. – DEFINICIONES

Para fines de esta Regla y excepto para aquellos artículos donde se provea una definición más específica, los siguientes términos tendrán el significado que se indica a continuación:

A. "**Autenticación multifactorial**": significa autenticación mediante la verificación de al menos dos (2) de los siguientes factores de autenticación:

(1) Factores de conocimiento, como una contraseña; o

(2) Factores de propiedad, como un "token" o mensaje de texto en un teléfono móvil; o

(3) Factores inherentes, como una característica biométrica.

B. "**Código**": significa el Código de Seguros de Puerto Rico, Ley Núm. 77 de 19 de junio de 1957, según enmendada, 26 L.P.R.A., *et seq*.

C. "**Comisionado**": significa el Comisionado de Seguros de Puerto Rico.

D. "**Consumidor**": significa una persona, natural o jurídica, incluidos, sin que se

limiten a éstos, los solicitantes, tenedores de póliza, asegurados, beneficiarios, reclamantes y tenedores de certificados que residan en Puerto Rico o que poseen bienes asegurados en Puerto Rico, y cuya Información No-Pública está en las manos del Regulado o bajo su custodia o control.

E. "**Contratista de Servicios**": significa una Persona, que no se define como Regulado, que el Regulado contrata para mantener, procesar, almacenar o de otra manera se le permite acceso a la Información No-Pública mediante los servicios que presta al Regulado.

F. "**Documento original**": significa el documento en papel o digital que se utilizó para crear el documento en formato electrónico.

G. "**Encriptado**": significa la transformación de la información en un formato que resulta en disminuir la probabilidad de que se descubra su significada sin usar un proceso de protección o clave. Para efectos de esta Regla, el encriptado requerido debe cumplir como mínimo con el estándar más alto de la industria de seguridad cibernética, según establecido por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (*U.S. National Institute of Standards and Technology, "NIST"*).

H. "**Estado**": significa el Gobierno de Puerto Rico.

I. "**Evaluación de riesgos**": significa la evaluación de riesgos que se requiere que haga cada Regulado conforme al Artículo 8 (C) de esta Regla.

J. "**Incidente de Ciberseguridad**": significa un evento que resulte en el acceso no autorizado, la interrupción o el uso no autorizado de un sistema de información o información almacenada en dicho sistema. Los Incidentes de Ciberseguridad no incluyen los eventos en que el Regulado haya determinado, utilizando evidencia documentable o mediante un tercero cualificado en respuesta a incidentes de seguridad cibernética, que cualquier Información No-Pública que haya sido accedida por una persona no autorizada no ha sido usada, modificada, cifrada, divulgada ni exfiltrada.

K. "**Información Pública**": significa toda información que el Regulado razonablemente pueda entender que estaría legalmente disponible al público en

general conforme a: registros federales, estatales o del gobierno local; medios de difusión masiva; o divulgaciones al público que se requieren por leyes federales, estatales o locales.

Para fines de esta definición, el Regulado tendrá un fundamento razonable para creer que la información se divulga legalmente al público general si el Regulado ha tomado medidas para determinar:

(1) Que la información es del tipo que está disponible al público en general y;

(2) Si un consumidor tiene potestad para que la información no se haga disponible al público en general y no ejerció dicho derecho.

L. "**Información No-Pública**": significa información que no está disponible al público y que consta de:

(1) Información relacionada con el negocio de un Regulado, el cual, si fuera intervenido o divulgado sin autorización o se diera acceso o uso al mismo, causaría un impacto adverso significativo al negocio, las operaciones o la seguridad del Regulado;

(2) Toda información relacionada con un Consumidor, en el cual, debido al nombre, número, marca u otro elemento identificador, se podría usar para identificar al Consumidor, en combinación de uno o más de los siguientes elementos:

(a) Número de seguro social,

(b) Licencia de conducir o tarjeta de identificación alterna para personas que no son conductores,

(c) Número de cuenta, número de tarjeta de crédito o de débito,

(d) Todo código de seguridad, código de acceso o contraseña que permitiría el acceso a una cuenta financiera del Consumidor o

(e) Registros biométricos.

(3) Toda información o dato, excepto la edad o el sexo, en cualquier formato o medio creado por o derivado de un proveedor de cuidado de

la salud o un consumidor y que esté relacionado con:

(a) La salud o condición física, mental o conductual de un Consumidor o miembro de la familia del Consumidor, en el pasado, el presente o el futuro;

(b) Servicios de cuidad de salud prestados a un Consumidor; o

(c) Pagos por el cuidado de la salud de un Consumidor.

M. "**Persona**": significa un individuo o entidad jurídica no gubernamental lo cual incluye, entre otros, toda sociedad, corporación, sucursal, agencia o asociación no gubernamental.

N. "**Persona autorizada**": significa una persona conocida y comprobada por el Regulado y que se ha determinado que es necesario y adecuado que acceda a la Información No-Pública mantenida por el Regulado y sus sistemas de información.

O. **"Programa de Ciberseguridad":** significa las salvaguardas administrativas, técnicas y físicas que usa el Regulado para acceder, recopilar, distribuir, procesar, proteger, almacenar, usar, transmitir, disponer o de otra manera manejar los datos en Sistemas de Información.

P. "**Regulado**": significa toda persona, natural o jurídica, que posea una licencia, autorización o certificado de autoridad para tramitar negocios de seguros en Puerto Rico o está registrada o se requiere que tenga licencia o autorización o esté registrada según dispuesto en el Código de Seguros de Puerto Rico. Ello no incluye un grupo de compras o grupo de control de riesgos que se haya establecido y obtenido una licencia en otro estado, o un Regulado que actúe como reasegurador y que esté domiciliado en otro estado o jurisdicción.

Q. "**Sistema de Información**": significa un conjunto demarcado de recursos de información electrónica que se organiza para recopilar, almacenar, reproducir, procesar, mantener, usar, compartir, divulgar o disponer de datos públicos o no públicos, además de todo sistema especializado tales como los sistemas de controles industriales y de procesos, sistemas de conmutación telefónica y sistemas PBX (*Private Branch Exchange*) y sistemas de control ambiental.

ARTÍCULO 8. – PROGRAMA DE CIBERSEGURIDAD

A. Implementación de un Programa de Ciberseguridad:

Según el tamaño y la complejidad del Regulado, la naturaleza y alcance de las actividades del Regulado, incluido el uso de Contratistas de Servicios y la sensibilidad de la Información No-Pública usada por el Regulado o en su posesión, custodia o control, cada Regulado deberá desarrollar, implementar, mantener y documentar un programa integral de seguridad de su información digital por escrito, basado en la evaluación de riesgos del Regulado y que contenga las salvaguardas administrativas, técnicas y físicas para la protección de la Información No-Pública y el sistema de información del Regulado.

B. Objetivos del Programa de Ciberseguridad:

El Regulado diseñará el Programa de Ciberseguridad para:

(1) Proteger y asegurar la confidencialidad, integridad y disponibilidad de la Información No-Pública almacenada en los Sistemas de Información, y velar por la seguridad del Sistema de Información;

(2) Proteger en contra del acceso o uso no autorizado de la Información No-Pública, y minimizar la posibilidad de daño a algún Consumidor; y

(3) Definir y periódicamente reevaluar el período de retención de la Información No-Pública y un mecanismo para destruirla cuando ya no sea necesaria.

C. El Regulado realizará una evaluación de riesgos en la cual:

(1) Designará a uno o más empleados, afiliados, suplidor externo o Contratista de Servicios designado para actuar a nombre del Regulado para que sea responsable del Programa de Ciberseguridad;

(2) Identificará amenazas internas o externas que sean razonablemente previsibles, que resultarían en el acceso, transmisión, divulgación, alteración, destrucción o uso no autorizado de Información No-Pública, incluida la seguridad de los Sistemas de Información y la Información No-Pública a los que tienen acceso o están en posesión de los Contratistas de Servicio;

(3) Evaluará la posibilidad y daño potencial de estas amenazas, tomando en

consideración la sensibilidad de la Información No-Pública;

(4) Diseñará y evaluará la suficiencia de las políticas, procedimientos, Sistemas de Información y otras salvaguardas establecidas para manejar estas amenazas, incluida la consideración de amenazas en cada área relevante a las operaciones del Regulado, incluyendo:

(a) El adiestramiento y la administración de los empleados;

(b) Los sistemas de información, incluido el diseño de la red y los programas, además de la clasificación de datos, la gobernanza, el procesamiento, el almacenaje electrónico, la transmisión y la disposición; y

(c) Detectar, prevenir y responder a los ataques, intrusiones u otros fallos de los sistemas.

(5) Implementará salvaguardas de la información para manejar las amenazas identificadas en la evaluación continua, y al menos una vez al año evaluará la eficacia de los controles claves, los sistemas y los procedimientos de las salvaguardas.

(6) De haber adoptado algoritmos, programas o tecnología de inteligencia artificial (IA), evaluará las políticas y procesos correspondientes, con el fin de:

(a) Garantizar que los datos que utilice la IA se accedan y se procesen de manera segura, protegiendo particularmente la Información No-Pública, incluido el acceso no autorizado a los modelos predictivos según sea necesario;

(b) Obedecer las políticas de privacidad y de seguridad del Regulado, así como los requisitos de cumplimiento con cualquier agencia, corporación o instrumentalidad gubernamental, agencia reguladora u otra entidad supervisora conforme a alguna ley estatal o federal; y

(c) Medir el desempeño de la IA regularmente para validar el buen funcionamiento con relación a la confidencialidad, integridad y

disponibilidad de los datos, según aplique.

D. Manejo de riesgos:

A base de la evaluación de riesgos, el Regulado debe:

(1) Diseñar su Programa Ciberseguridad para mitigar los riesgos identificados, según el tamaño y la complejidad de las actividades del Regulado, incluidos el uso de Contratistas de Servicios y la sensibilidad de la Información No-Pública usada por el Regulado o en la posesión, custodia o control de este.

(2) Implementar las siguientes medidas de seguridad, según lo amerite su infraestructura, plantilla, operación y sistemas de información:

(a) Mantener un programa formal de entrenamientos sobre las modalidades de riesgo cibernético para su personal, y llevar récord del desempeño del empleado en el programa.

(b) Adiestrar y asignarle responsabilidades del Programa de Ciberseguridad a los empleados;

(c) Establecer controles de acceso efectivos en los Sistemas de Información, incluidos los controles para autenticar (tales como la autenticación multifactorial) y permitir acceso solamente a personas autorizadas, para proteger contra la adquisición, alteración, divulgación o destrucción no autorizada de la Información No-Pública;

(d) Mantener un programa de supervisión a proveedores de servicios con acceso a Información No-Pública, que incluya acuerdos de servicio y requiera controles de seguridad cibernética;

(e) Identificar y administrar la información, el personal, los dispositivos, los sistemas, e instalaciones que permitan que el Regulado logre sus propósitos empresariales conforme a su importancia relativa a los objetivos empresariales y la estrategia de manejo de riesgos de la organización;

(f) Restringir el acceso físico a las áreas donde se encuentre la Información No-Pública, para que sea únicamente accesible a las personas autorizadas;

(g) Proteger mediante encriptación u otros medios adecuados, toda la Información No-Pública mientras se transmite en una red externa y toda Información No-Pública guardada en una computadora portátil u otro dispositivo o medio portátil de computación o almacenaje electrónico;

(h) Adoptar prácticas seguras de desarrollo para todas las aplicaciones que se desarrollen internamente para el uso del Regulado y procedimientos para evaluar, valorar o comprobar la seguridad de aplicaciones desarrolladas por recursos externos utilizados por el Regulado;

(i) Modificar el Sistema de Información conforme al Programa de Ciberseguridad del Regulado;

(j) Regularmente probar y monitorear los sistemas y procedimientos para detectar los ataques efectuados e intentados, o intrusiones en el Sistema de Información, así como en la red, así como documentar el resultado de estas pruebas;

(k) Incluir procesos de respaldo, resguardo y gestión de registros ("*Audit logs*") dentro del Programa de Ciberseguridad diseñados para detectar y responder a los Incidentes de Ciberseguridad y para reconstruir las transacciones financieras significativas de manera que se provea un apoyo adecuado a las operaciones normales y obligaciones del Regulado;

(l) Implementar medidas de protección en contra de la destrucción, pérdida o daño de la Información No-Pública debido a peligros ambientales, tales como daños por incendio y agua u otras catástrofes o fallos tecnológicos; y

(m) Desarrollar, implementar y mantener procedimientos para la

disposición segura de la Información No-Pública en todo tipo de formato.

(3) Incluir los riegos de ciberseguridad en el proceso de manejo de riesgos empresariales del Regulado y en los informes requeridos en los Artículos 32.040, 44.050 y 53.070 del Código de Seguros de Puerto Rico y la Regla 104 sobre Gobernanza Corporativa.

(4) Mantenerse informado con respecto a las nuevas amenazas o vulnerabilidades y utilizar medidas razonables de seguridad al compartir información según la manera del intercambio y el tipo de información compartida.

(5) Realizar pruebas de vulnerabilidad regularmente en sus Sistemas de Información.

E. Supervisión por la Junta de Directores:

Si el Regulado tiene una Junta de Directores, la Junta o un comité apropiado de la Junta, como mínimo:

(1) Requerirá que la gerencia ejecutiva del Regulado o la persona delegada por la gerencia, desarrolle, implemente y mantenga el Programa Ciberseguridad del Regulado.

(2) Requerirá que la gerencia ejecutiva del Regulado o la persona delegada por la gerencia del Regulado, presente un informe, para la aprobación y firma de la Junta de Directores, al menos una (1) vez al año sobre lo siguiente:

(a) La condición general del Programa de Ciberseguridad y el cumplimiento por parte del Regulado con esta Regla; y

(b) Asuntos relevantes o significativos relacionados con el Programa de Ciberseguridad que atiendan la evaluación de riesgos, el manejo de riesgos y las decisiones de control, las relaciones con Contratistas de Servicios, los resultados de pruebas realizadas, los Incidente de Ciberseguridad o violaciones y la respuesta de la gerencia a los mismos, y las

recomendaciones para cambios a realizarse en el Programa de Ciberseguridad.

(3) Si la gerencia ejecutiva del Regulado delega alguna de sus responsabilidades conforme al Artículo 8 de esta Regla, deberá supervisar el desarrollo, la implementación y el mantenimiento del Programa de Ciberseguridad del Regulado preparado por la persona delegada y recibirá un informe del mismo que cumpla con los requisitos de informar a la Junta de Directores indicados anteriormente.

F. Supervisión de las relaciones con los Contratistas de Servicios:

(1) El Regulado efectuará la debida diligencia al seleccionar el Contratista de Servicios, y

(2) Requerirá mediante contrato o acuerdo de servicio que el Contratista de Servicios implemente las medidas administrativas, técnicas y físicas adecuadas para proteger y asegurar los Sistemas de Información y la Información No-Pública que sean accesibles por el Contratista de Servicios o estén en posesión de éste.

G. Ajustes en el programa:

El Regulado monitoreará, evaluará y ajustará, según sea indicado, el Programa de Ciberseguridad conforme a todo cambio pertinente en la tecnología, la sensibilidad de la Información No-Pública, las amenazas internas o externas a la información y los cambios en las relaciones comerciales del Regulado, tales como las fusiones y las adquisiciones, las alianzas y empresas conjuntas, arreglos de subcontratación y cambios en los Sistemas de Información.

H. Plan de Respuesta a Incidentes:

(1) Como parte de su Programa de Ciberseguridad, cada Regulado deberá establecer un plan escrito de respuesta a incidentes que contemple la respuesta rápida y recuperación en caso de un Incidente de Ciberseguridad que comprometa la confidencialidad, integridad o disponibilidad de la Información No-Pública que posea, los Sistemas

de Información del Regulado o la funcionalidad continua de cualquier aspecto del negocio o las operaciones del Regulado.

(2) El plan de respuesta a los incidentes deberá atender a lo siguiente:

(a) El proceso interno de respuesta a un Incidente de Ciberseguridad;

(b) Los objetivos del plan de respuesta a incidentes;

(c) La definición clara de los roles, responsabilidades y niveles de autoridad para tomar decisiones, incluyendo nombres de empleados y proveedores de respuesta a incidentes;

(d) Comunicaciones externas e internas y la manera en que se comparte información;

(e) Identificación de requisitos para la remediación de toda debilidad identificada en los Sistemas de Información y controles asociados;

(f) Documentación y preparación de informes relacionados con los Incidentes de Ciberseguridad y las actividades correspondientes de respuesta; y

(g) La evaluación y revisión del plan de respuesta a incidentes, según fuera necesario después de un Incidente de Ciberseguridad.

I. Certificación anual al Comisionado

A más tardar el 1 de junio de cada año, todos los Regulados con domicilio en Puerto Rico deberán presentar ante el Comisionado, una declaración escrita en la que se certifique que ha cumplido con los requisitos dispuestos en el Artículo 8 de esta Regla. No obstante, la primera certificación deberá ser presentada ante el Comisionado no mas tarde del último día del doceavo mes luego de la vigencia de esta Regla.

Todo Regulado mantendrá para inspección por el Comisionado, todos los registros, planillas y datos en que se basa dicha certificación por un periodo de cinco (5) años. Los Regulados deberán presentar ante el Comisionado el resultado de sus pruebas externas de vulnerabilidad cada noventa (90) días. En tanto que el Regulado haya identificado áreas,

sistemas o procesos que requieran mejoras significativas, actualización o rediseño, el Regulado documentará la identificación y los esfuerzos de remediación planificados e implementados para atender dichas áreas, sistemas o procesos. Dicha documentación estará disponible al Comisionado para inspección.

ARTÍCULO 9. – INVESTIGACIÓN DE UN INCIDENTE DE CIBERSEGURIDAD

A. Si el Regulado se percatara que ha ocurrido o pudiera haber ocurrido un Incidente de Ciberseguridad, el Regulado o el suplidor externo y/o Contratista de Servicios designado a actuar a nombre del Regulado llevará a cabo una investigación a la mayor brevedad posible y preparará un reporte escrito de la misma.

B. Durante la investigación el Regulado o el suplidor externo y/o Contratista de Servicios designado a actuar a nombre del Regulado, deberá como mínimo:

(1) Determinar si ha ocurrido un Incidente de Ciberseguridad;

(2) Evaluar la naturaleza y alcance del Incidente de Ciberseguridad;

(3) Identificar toda Información No-Pública que pudiera haber estado afectada en el Incidente de Ciberseguridad; y

(4) Efectuar o supervisar medidas razonables para restaurar la seguridad de los Sistemas de Información afectados en el Incidente de Ciberseguridad para impedir que se continúe adquiriendo, divulgando o usando la Información No-Pública en posesión, custodia o control del Regulado.

C. Si el Regulado se percata que el Incidente de Ciberseguridad ha ocurrido o pudiera haber ocurrido en un sistema mantenido por un Contratista de Servicios, el Regulado completará los pasos indicados en el inciso B o confirmará y documentará que el Contratista de Servicios haya completado dichos pasos.

D. El Regulado mantendrá registros de todos los Incidentes de Ciberseguridad al menos por cinco (5) años de la fecha del incidente y presentará dichos registros al Comisionado si este se lo requiere.

ARTICULO 10. – NOTIFICACIÓN DE INCIDENTE DE CIBERSEGURIDAD

A. Notificación al Comisionado

El Regulado notificará al Comisionado un Incidente de Ciberseguridad tan pronto sea posible, pero dentro de las 72 horas después del momento en que se haya determinado que ocurrió un Incidente de Ciberseguridad, cuando se cumpla alguno los siguientes criterios:

(1) El Regulado entiende razonablemente que el Incidente de Ciberseguridad:

(a) Impacta al Regulado de manera que requiere notificación a alguna agencia, corporación o instrumentalidad gubernamental, agencia reguladora u otra entidad supervisora conforme a alguna ley estatal o federal, o

(b) Tiene la probabilidad razonable de causarle daño sustancial a:

i. Consumidores que residen en Puerto Rico, o

ii. Ha algún aspecto importante de las operaciones normales del Regulado.

B. El Regulado proveerá la mayor cantidad posible de la información que se detalla a continuación, en formato electrónico, según lo indique el Comisionado. El Regulado tendrá la obligación de actualizar y proveer información adicional con respecto a las notificaciones iniciales y posteriores al Comisionado relacionadas con el Incidente de Ciberseguridad.

(1) Fecha del Incidente de Ciberseguridad;

(2) Descripción de cómo la información se reveló, perdió, robó o cómo se llevó a cabo la intrusión en la seguridad para acceder la misma, lo cual incluirá los roles y responsabilidades en específico de los Contratistas de Servicios, si alguno;

(3) Cómo se descubrió el Incidente de Ciberseguridad;

(4) Si se ha recuperado alguna información perdida o robada o afectada por una intrusión de seguridad y si se recuperó, cómo se hizo;

(5) La identidad de la fuente del Incidente de Ciberseguridad;

(6) Si el Regulado presentó una querella a la policía o ha notificado a alguna agencia reguladora, gubernamental o de orden público, y si lo hizo, cuándo se presentó la notificación;

(7) Descripción de las categorías específicas de datos adquiridos sin autorización. Las categorías específicas de datos, por ejemplo, información médica, información financiera o información que permite identificar al Consumidor;

(8) El periodo durante el cual el Sistema de Información se vio comprometido por el Incidente de Ciberseguridad;

(9) La cantidad total de consumidores en Puerto Rico afectados o que pudieran estar afectados por el Incidente de Ciberseguridad. El Regulado proveerá el mejor estimado en el informe inicial al Comisionado y actualizará el estimado en cada informe subsiguiente al Comisionado a tenor con este Artículo;

(10) Los resultados de toda indagación interna en que se haya identificado un fallo en los controles automatizados o procedimientos internos o se haya confirmado que todos los controles automatizados y procedimientos internos se cumplieron;

(11) Descripción de los esfuerzos para remediar la situación que permitió que ocurriera el Incidente de Ciberseguridad;

(12) Copia de la política de privacidad del Regulado y una declaración en que se detallan las medidas que tomará el Regulado para investigar y notificar a los consumidores afectados por el Incidente de Ciberseguridad; y

(13) El nombre de una persona de contacto que tenga conocimiento del Incidente de Ciberseguridad y está autorizada a actuar a nombre del Regulado.

C. Notificación a los Consumidores.

El Regulado cumplirá con la Ley de Información al Ciudadano sobre la Seguridad de Bancos de Información, Ley Núm. 111-2005, según enmendada, según fuera aplicable, y proveerá al Comisionado una copia de la notificación enviada a los Consumidores, según dispuesto por ley cuando se requiera que el Regulado notifique al Comisionado conforme al inciso A de este artículo. La notificación conforme a la Ley Núm. 111-2005 se realizará independientemente de si la información personal estuviera o no protegida con claves criptográficas o encriptada. En aquellos casos que parte o toda la información divulgada estuviese protegida, la notificación deberá indicar el nivel de encriptación utilizado.

D. Notificación sobre Incidente de Ciberseguridad de los Contratistas de Servicios:

(1) Si el Regulado adviene en conocimiento de un Incidente de Ciberseguridad en un sistema mantenido por un Contratista de Servicios, tratará dicho incidente como se dispone en el inciso A de este artículo.

(2) La fecha límite para la notificación por el Regulado se calculará a partir del día después que el Contratista de Servicios haya notificado al Regulado del Incidente de Ciberseguridad o el Regulado advenga en conocimiento del Incidente de Ciberseguridad, cual ocurra primero.

(3) Ninguna disposición de esta Regla impedirá o menoscabará los acuerdos entre un Regulado y otro, entre el Regulado y un Contratista de Servicios o el Regulado con cualquier otra persona para llevar a cabo la investigación que se dispone en el Artículo 9 de esta Regla o cumplir con los requisitos de notificación dispuestos en este artículo.

E. Notificación sobre Incidente de Ciberseguridad por los reaseguradores a los aseguradores:

(1) (a) En el caso de un Incidente de Ciberseguridad que involucre Información No-Pública usada por el Regulado que actúa como reasegurador o que está en posesión, custodia o control de un Regulado que actúa como reasegurador y que no tiene una relación contractual directa con los Consumidores afectados, el reasegurador notificará a los aseguradores cedentes afectados y al Comisionado de su estado de

domicilio dentro de 72 horas de haber determinado que haya ocurrido un Incidente de Ciberseguridad.

(b) Los aseguradores cedentes que tengan una relación contractual directa con los Consumidores afectados cumplirán con los requisitos de notificación al Consumidor dispuestos en el inciso (C) de este artículo y cualquier otro requisito relacionado con los Incidentes de Ciberseguridad dispuesto en este artículo.

(2) (a) En el caso de un Incidente de Ciberseguridad que involucre información en posesión, custodia o control de un Contratista de Servicios de un Regulado que es un reasegurador, el reasegurador notificará a los aseguradores cedentes afectados y el Comisionado de su estado de domicilio dentro de 72 horas de haber recibido la notificación de su Contratista de Servicios que haya ocurrido un Incidente de Ciberseguridad.

(b) Los aseguradores cedentes que tengan una relación contractual directa con los consumidores afectados cumplirán con los requisitos de notificación al consumidor dispuestos en el inciso (C) de este artículo y todos los demás requisitos de notificación relacionados con los Incidente de Ciberseguridad dispuesto en este artículo.

F. Notificación de Incidente de Ciberseguridad por los aseguradores u organizaciones de servicios de salud a los productores:

En el caso de un Incidente de Ciberseguridad que involucre información en posesión, custodia o control de un Regulado que es un asegurador o su Contratista de Servicios y que los servicios del asegurador fueron prestados al Consumidor por medio de un productor o intermediario de seguros, el asegurador u organización de servicios de salud notificará al productor o intermediario según sus registros, sobre todos los consumidores afectados tan pronto sea posible.

Se releva al asegurador u organización de servicios de salud de esta obligación en los casos en que no tenga la información actual sobre el productor o intermediario de seguros para determinado Consumidor.

G. Notificación de Incidente de Ciberseguridad por el Comisionado a los aseguradores y organizaciones de servicios de salud autorizados a hacer negocios en Puerto Rico:

El Comisionado, luego de recibir la notificación del Incidente de Ciberseguridad por parte del Regulado conforme al inciso A de este artículo, procederá a emitir un aviso o Advertencia de Incidente de Ciberseguridad por escrito, dirigido a todos los aseguradores y organizaciones de servicios de salud autorizados a hacer negocios en Puerto Rico, con el fin de poner en sobre aviso a la industria de seguros de posibles intrusiones a sus Sistemas de Informática. El Aviso se limitará a la información estrictamente técnica de la naturaleza del Incidente de Ciberseguridad, sin identificar al Regulado, para alertar de la vulnerabilidad a los Sistemas de Seguridad de Información Electrónica con el fin de que tomen las medidas necesarias para mantener la integridad de sus sistemas ante el tipo de intrusión observada. El Comisionado tendrá discreción para suplementar el aviso conforme a la información que subsiguientemente se reciba sobre el Incidente de Ciberseguridad.

ARTÍCULO 11. – PODERES DEL COMISIONADO

A. El Comisionado tendrá el poder de examinar e investigar a los Regulados para determinar si algún Regulado ha actuado o está actualmente actuando en violación de esta Regla. Este poder es adicional al poder del Comisionado para investigar y llevar a cabo exámenes según dispuesto en el Código de Seguros de Puerto Rico, particularmente el Capítulo 2 del Código de Seguros de Puerto Rico. Dicha investigación o examen se llevará a cabo conforme a lo dispuesto en el Artículo 2.030(12). De ser necesario la contratación de personal técnico para llevar a cabo la investigación será costeado por el Regulado. Conforme con lo dispuesto en el Artículo 2.130 del Código de Seguros de Puerto Rico, el Regulado tiene que hacer accesible al Comisionado su Programa de Seguridad de Información Digital o de

Ciberseguridad y todo documento en su poder relacionado con los protocolos e información requerida o recopilada relacionada con esta Regla.

B. Cuando el Comisionado tenga motivos para creer que un Regulado ha actuado o está actuando en violación de esta Regla, éste podrá tomar las acciones necesarias para hacer valer las disposiciones de esta Regla que incluye la imposición de sanciones como dispone esta Regla y el Código de Seguros de Puerto Rico.

ARTÍCULO 12. – CONFIDENCIALIDAD

A. Todo documento, material u otra información en el control o posesión de la Oficina del Comisionado de Seguros que provea un Regulado o empleado o agente actuando a nombre del Regulado conforme al Artículo 8 (I), y el Artículo 10 (B)(2), (3), (4), (5), (8), (10), y (11) de esta Regla o que el Comisionado obtenga en el transcurso de una investigación o examen conforme al Artículo 8 y 10 de esta Regla, será confidencial por ley y privilegiada, no estará sujeta a la divulgación al público conforme al Artículo 2.090 del Código de Seguros, ni a divulgación mediante subpoena u orden del tribunal y no será objecto de descubrimiento ni será admisible como prueba en un pleito privado. Sin embargo, el Comisionado está autorizado a usar los documentos, materiales u otra información en toda acción reguladora o judicial instada por el Comisionado en el desempeño de sus deberes.

B. No se permitirá ni se requerirá que el Comisionado ni la persona que haya recibido los documentos, materiales u otra información mientras actuaba bajo la autoridad del Comisionado testifique en un litigio privado relacionado con los documentos, materiales, o información confidencial sujetos al inciso A.

C. En el desempeño de sus deberes, conforme a esta Regla el Comisionado podrá:

    (1) Compartir documentos, materiales u otra información, incluidos los documentos materiales o información confidenciales o privilegiados sujetos al inciso A, con otras agencias reguladoras estatales, federales e internacionales, con la Asociación Nacional de Comisionados de Seguros, sus afiliados o subsidiarias y con las autoridades de orden público estatales, federales e internacionales,

siempre y cuando la parte que reciba dichos documentos, materiales o información acuerde por escrito que mantendrá la confidencialidad y condición privilegiada de los mismos;

(2) Recibir documentos, materiales o información, incluidos los documentos, materiales o información que de otra manera serían confidenciales y privilegiados, de la Asociación Nacional de Comisionados de Seguros, sus afiliados o subsidiarias y de oficiales reguladores y de orden público de jurisdicciones nacionales o foráneas, y mantendrá como confidencial o privilegiado todo documento, material o información que se reciba con una notificación o bajo el entendimiento de que es confidencial o privilegiado conforme a las leyes de la jurisdicción de origen del documento, material, o información;

(3) Compartir documentos, materiales u otra información, sujeto a las disposiciones del inciso A de este artículo, con un consultor externo o suplidor, siempre y cuando el consultor consiente por escrito a mantener la confidencialidad y condición de privilegio del documento, material u otra información; y

(4) Hacer acuerdos para compartir y usar la información que esté en armonía con este inciso C.

D. La divulgación al Comisionado conforme a este artículo o como resultado de compartir los documentos, materiales, o información según se autoriza en el inciso C, no redundará en el relevo de la confidencialidad o condición de privilegio aplicable.

E. Esta Regla no prohíbe que el Comisionado divulgue los resultados finales de asuntos adjudicados que están sujetos a inspección pública según la dispone el Capítulo 2 del Código de Seguros de Puerto Rico, en una base de datos u otro servicio central de información mantenido por la *National Association of Insurance Commissioner* (NAIC), sus afiliados o subsidiarias.

ARTÍCULO 13. – EXCEPCIONES

A. No serán aplicables las disposiciones de esta Regla en las siguientes circunstancias:

(1) Un Regulado con quince (15) o menos empleados, incluidos los contratistas de servicios, estará exento del Artículo 8 de esta Regla;

(2) Un empleado, agente, representante o designado de un Regulado, que también es un Regulado, está exento del Artículo 8 y no necesita desarrollar su propio Programa de Ciberseguridad en la medida en que el empleado, agente, representante o designado esté cubierto por el Programa de Ciberseguridad del otro Regulado.

B. En caso de que un Regulado deje de calificar para una excepción, dicho Regulado tendrá 180 días para cumplir con esta Regla.

ARTÍCULO 14. – **SANCIONES**

Si un Regulado violara este Regla, el Comisionado le podrá imponer una sanción de hasta $10,000 por violación según faculta el Artículo 2.250 del Código de Seguros de Puerto Rico.

ARTÍCULO 15. – SEPARABILIDAD

Si cualquier artículo, parte o párrafo de esta Regla fuese declarado inconstitucional, inválido o nulo por un tribunal competente, dicha determinación no afectará la validez de las restantes disposiciones de este.

ARTÍCULO 16. – VIGENCIA

Las disposiciones de esta Regla entrarán en vigor a los treinta (30) días de su presentación con el Departamento de Estado de Puerto Rico, conforme a las disposiciones de la Ley Núm. 38-2017, supra.

_____

LCDO. ALEXANDER S. ADAMS VEGA
COMISIONADO DE SEGUROS DE PUERTO RICO

Fecha de Aprobación:

Fecha de Presentación al Departamento de Estado:

Fecha de Presentación a la Biblioteca de la Legislatura: