ABSTRACT

El ciberespacio[1] nos expone a una serie de nuevas amenazas[2]: las ciberamenazas, que son la intromisión de terceros en los sistemas informáticos, filtraciones de información, robo y pérdida de datos, extorsiones cibernéticas, fraude. Se advierte en este escenario que el elemento motivacional no sólo se suscribe a los objetivos y amenazas de ciberdelincuentes con la finalidad de obtener rédito económico sino que se amplía actos de venganza de empleados por despidos, al desafío intelectual de poder perpetrar un ataque exitoso. Frente a contingencias de esta naturaleza el seguro de riesgos cibernéticos se convierte en un mecanismo de respuesta sumamente necesario.

Palabras claves: riesgos cibernéticos, seguros cibernéticos, póliza de seguro cibernético, ciberamenazas, seguridad de la información, daño informático, incidente de seguridad, protección de datos personales.

SEGURO DE RIESGOS CIBERNÉTICOS, LA PÓLIZA OBLIGATORIA[3]

Según la 23º edición del Internet Security Threat Report (ISTR), informe anual de seguridad de Symantec que analiza 157 países, Argentina es el cuarto país con más ataques y amenazas cibernéticas de América latina. El podio en la región lo ocupan Brasil, México y Venezuela.

En cuanto a la metodología de las ciberamenazas, Argentina ocupa el segundo lugar regional en phishing y ataques por internet, así como el tercero en malware, spam, bots y criptojacking y el quinto en ataques a la red y ransomware. A su vez, se encuentra en el Top 10 mundial de países amenazados por spam, ocupando el octavo puesto.[4]

Hoy la Gestión del Riesgo Cibernético es innegociable y demanda una toma de conciencia de la real exposición a los ciberdelitos a la que están expuestas nuestras actividades en la red. Los incidentes cibernéticos informados en el 2019 arrojan un 37% en el Top 10 de riesgos empresariales, en primer lugar por encima de catástrofes naturales (28%)[5]. Por tal razón, tanto la responsabilidad frente a terceros, como las pérdidas propias por actos maliciosos, o por fallas en la gestión requieren de una póliza que nos respalde frente a estas contingencias.

---

1 Nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información incluida Internet, las redes y los siste-mas de información y de telecomunicaciones. Estrategia de ciberseguridad nacional, 2013.

2 Condición o actividad capaz de ocasionar que, intencional o accidentalmente, la información o recursos para el procesamiento de la información se pierdan, modifiquen, queden expuestos o vuelvan inaccesibles; o que sean afectados de algún otro modo en detrimento de la organización. Obtenido de: http://es.pcisecuritystandards.org

3 Un seguro es un contrato, denominado póliza de seguro, por el que una Compañía de Seguros (el asegurador) se obliga, mediante el cobro de una prima y para el caso de que se produzca el evento cuyo riesgo es objeto de cobertura a indemnizar, dentro de los límites pactados, el daño producido al asegurado; bien a través de un capital, una renta, o a través de la prestación de un servicio. Obtenido de: https://es.wikipedia.org/wiki/Seguro

4 Obtenido de: https://www.infotechnology.com/online/Las-estafas-online-no-paran-de-crecer-como-protegerse-20191021-0008.html

5 Obtenido de: iprofesional

Como dato de color, las fuerzas de seguridad han sufrido diferentes ataques en estos cuatro años: desde el deface (cambio en las portadas de sus sitios web) a organismos como Gendarmería, Ejército Argentino y Policía Federal hasta filtración de datos de agentes poniendo en riesgo la vida de ellos con la causa denominada GorraLeaks, a diversos casos de phishing que permitió el acceso a cuentas de correo del Ministerio de Seguridad o bien a la cuenta de Twitter de la Ministra.

¿Cómo se ve afectada una empresa si recibe un ciberataque?

Al menos podemos decir (sin que tenga carácter excluyente) que la afectación inmediata tiene que ver con la pérdida de ingresos como consecuencia de la interrupción de la actividad, la pérdida de información empresarial sensible, lesiones a su reputación y a la confianza de sus clientes sin dejar de mencionar las sanciones de los entes de control a los que quedan expuestos (inhabilitaciones, suspensiones de licencias para operar en la actividad) y reclamos o demandas por daños provocados a terceros fruto de un ciberataque.

El costo de las pérdidas derivadas de un ataque o falla cibernética varían de un caso a otro y de país a país. Por ejemplo, en Estados Unidos, este costo asciende a 5 billones de dólares, mientras que en Australia suma poco más de la mitad, 2.9 billones de dólares. Sin embargo, un aspecto irreparable como consecuencia de un daño cibernético es la reputación de la empresa afectada, especialmente si se gestionan datos de identidad de terceros que pueden verse vulnerados, razón por la cual además de contar con protocolos internos de prevención, es adquirir un seguro que brinde protección ante este tipo de amenazas y sus distintas repercusiones.

Un seguro puede ser el factor determinante cuando la privacidad de una empresa o sus operaciones regulares se ven vulneradas. No solo hay una pérdida patrimonial por gastos de abogado, perjuicios generados a terceros, costos de reemplazo de la información o sistemas y la misma utilidad dejada de percibir por la interrupción del negocio, sino también el costo de expertos necesarios para recuperarse de la situación.

Concepto y caracteres distintivos del Riesgo Cibernético:

A la luz de los acontecimientos comentados anteriormente se advierte una mutación en el concepto tradicional de riesgo, con lo que podemos afirmar que "riesgo cibernético" es todo riesgo que exponga a individuos, entidades públicas y privadas al peligro de sufrir daños sobre los activos digitales, la reputación online, la marca comercial, al fraude cometido por robo de información e incluso el daño físico producto del uso de la información y medios electrónicos o más conocidas como TICs mayormente a consecuencia de un incidente de seguridad[6].

Como características salientes del Riesgo Cibernético podemos decir que es **incierto y eventual**, está sujeto a un acontecimiento impreciso,

6 Suceso (inesperado o no deseado) con consecuencias en detrimento de la seguridad del sistema de información. [UNE-71504:2008]. Obtenido de: www.ccn-cert.cni.es

prácticamente impredecible; es **aleatorio** en el sentido de que desconoce límites geográficos, culturales, económicos y puede tomar como víctima tanto a personas físicas como entidades públicas o privadas y como consecuencia de lo anterior es **posible**, aun cuando pongamos toda la diligencia necesaria para que no ocurra y por su propia definición, la potencialidad dañosa de que se puedan afectar bienes o personas está siempre latente; es **relativamente previsible**, sabemos que actualmente por el sólo hecho de la navegación en Internet o intranet existen ciertos riesgos implícitos en su uso y debemos tomar recaudos y ser diligentes al exponer o manipular nuestros datos; implica un **peligro actual e inminente o un peligro futuro** para los internautas o usuarios de intranet; es **concreto**, el daño ocasionado por el mismo a la víctima se puede valorar cuantitativamente y cualitativamente; deriva de actos considerados **ilícitos** para el derecho interno e internacional; está vinculado a un **interés asegurable**, el estado debe poner los medios y los recursos para su protección; puede **afectar derechos** de contenido patrimonial propios o de tercero e incluso es extensivo a los de contenido moral; se desarrolla tanto en entorno **online** como **offline**; es **dinámico**, las técnicas de ataque están en constante evolución; es **complejo**, por estar compuesto de muchos aspectos y finalmente, puede desatar **consecuencias legales desfavorables** para quien es víctima de un incidente de seguridad informática ya que lo hace responsable por su acción u omisión. [7]

Riesgo Cibernético Asegurable[8]

Según se expuso en líneas preliminares el riesgo asegurable es la posibilidad de sufrir una pérdida o un daño, es una eventualidad, algo que tiene la posibilidad de suceder, un acontecimiento incierto que, de ocurrir, traerá como consecuencia un desequilibrio económico para la persona o entidad que lo sufre. Pero si agregamos a esto el condimento de lo "cibernético" se amplifica el factor riesgo y las consecuencias debido a la imprudencia, negligencia y/o impericia en el manejo de la ciberseguridad y datos personales.

En Argentina, las principales problemáticas que podemos encontrar hoy en materia de seguridad informática a nivel estatal son: falta de control del tráfico de datos, redes inseguras, utilización de emails personales y/o gratuitos, códigos inseguros y servidores desactualizados, inexistencia de backups y políticas de disaster recovery, y no hay nada ni nadie que ante un evento de ciberdelito actúe brindando una solución en tiempo y forma, tanto para un civil, un organismo o una fuerza de seguridad.[9]

Contrato de Seguro de Riesgos Cibernéticos: objeto, consentimiento de las partes, las actividades comprendidas, cobertura y suma asegurada:

7 Características esenciales del riesgo asegurable en los seguros tradicionales: debe ser incierto y aleatorio, posible, concreto, interés lícito, fortuito, contenido económico y extraño a la voluntad de las partes. La coexistencia de los mismos dan virtualidad al riesgo asegurable entendiendo éste último como elemento indispensable para la existencia de un contrato de seguro.

8 Para el desarrollo de la temática se tomaron conceptos del Manual de principios técnicos del seguro - CENTRO DE CAPACITACIÓN FEDERAL, Páginas 19 a 29.

9 Obtenido de: https://www.lapoliticaonline.com/nota/ciberseguridad/

Actualmente en nuestro país son cuatros las aseguradoras que ofrecen paquetes de seguro de riesgos cibernéticos de las que expondré brevemente a continuación los elementos comunes y los rubros a los que dan cobertura y a los que no.

Siguiendo los preceptos del Art. 2 de nuestra Ley de Seguros 17418, en cuanto al **objeto** de contrato de seguro, el mismo puede incluir toda clase de riesgos siempre que exista interés asegurable, salvo prohibición expresa de la ley, extremos claramente presentes en este moderno esquema del "riesgo cibernético".

Como todo contrato, el de seguro de riesgos cibernéticos requiere el **consentimiento** de las partes al suscribirlo. Las partes interesadas en protegerse de estos siniestros abarcan: en las empresas o pymes a los administradores, directivos o socios, el responsable de seguridad, director de cumplimiento o director de la asesoría jurídica interna de la sociedad, los empleados; al Estado todas sus reparticiones y los particulares aunque en menor medida. Todo esto con las limitaciones o restricciones que estipule la póliza para cada caso en particular siempre que tengan cobertura. Valga la aclaración que las aseguradoras que fueron consultadas para el presente trabajo han focalizado su interés es las Pymes y la oferta de diferentes paquetes de seguros las toma como su eje.

La lista de **actividades económicas asegurables** suele ser muy extensa y excede los objetivos de este trabajo por lo cual me limitaré a citar las más destacadas. Con nivel de riesgo alto: agencias y organizadores de viajes; actividades de asistencia a turistas, actividades inmobiliarias (compra y venta, arriendo, etc.,); escuelas, colegios, universidades, academias, centros educativos en general; hoteles, moteles y hospedajes; sedes políticas; servicios jurídicos y notariales; suministro de electricidad, gas y agua (incluyendo generación); venta de electrodomésticos, equipos eléctricos, electrónicos y sus accesorios. Con nivel de riesgo medio: agencias de noticias y publicidad; empresas de encomiendas y transportadoras; imprentas, litografías, tipografías, editoriales; organizaciones empresariales, profesionales y de empleadores (colegios profesionales, organizaciones empresariales, sindicatos, etc.); salas de cine y teatros. Con nivel de riesgo bajo: bibliotecas y museos; fabricación de equipos eléctricos y electrónicos; restaurantes, heladerías, cafeterías, salones de té y comidas rápidas. Seguramente el lector se estará preguntado que quedó afuera y la respuesta es que dentro de los riesgos no asegurables se encuentran las siguientes actividades: Institución Financiera, "Big Four", Call Center, Telecomunicaciones, Servicios Informáticos, Administración Pública, Casinos y Juegos de Azar, Salas de Internet y Cabinas Telefónicas, Laboratorios Clínicos y Clínicas Médicas; las que tienen ingresos mayores a USD 5.000.000 o su equivalente en Pesos Argentinos; las actividades que requieran más de 200 empleados y por último (según la aseguradora) no tengan siniestralidad en los últimos tres años.

Según lo expuesto previamente estamos en condiciones de abordar la cuestión de la **cobertura** que con sutiles diferencias entre compañías reposa sobre tres pilares, cuales son:

1) Por daños propios: recuperación de información digital, interrupción de su actividad empresarial, extorsión cibernética, transacciones bancarias fraudulentas, gastos para proteger su reputación.

2) Por daños a otros: responsabilidad por violación de información confidencial o datos personales, responsabilidad por software malicioso o virus informático, publicación en medios digitales, gastos de defensa-Judiciales.

3) Manejo de Crisis: gastos forenses, gastos de defensa-Autoridades Administrativas, gastos sin previa autorización.

En cada caso, las aseguradoras se encargan de orquestar los medios técnicos (brindando asistencia calificada), económicos (al pagar o reembolsar gastos o los perjuicios ocasionados) y legales (proporcionando asistencia letrada en caso de demandas por daños), para contrarrestar la contingencia sufrida, el siniestro o incidente de seguridad siempre que estén **razonablemente a su alcance** y permita restablecer la situación a su estado anterior a la brevedad posible.

Entonces, ¿qué no estaría cubierto?: multas o sanciones pecuniarias, administrativas o de cualquier naturaleza, y los daños punitivos o ejemplarizantes; lesiones personales, muerte o enfermedades; trastornos emocionales ocasionados a terceros; el deterioro, destrucción o pérdida de bienes tangibles; una interrupción global del servicio de internet; incumplimiento de obligaciones contractuales excepto la derivada de la seguridad de la información; una responsabilidad profesional; los daños ocasionados por terceros contratados por su proveedor de servicio.[10]

Una adecuada gestión del riesgo[11] cibernético debería contemplar y poder responder los siguientes interrogantes[12]:

¿Demostramos la debida diligencia, propiedad, y la gestión efectiva del riesgo cibernético? ¿Cómo nuestro programa de riesgo cibernético y capacidades se alinean a los estándares de la industria y se pone a la par de nuestros competidores? ¿Tenemos una mentalidad cibernéticamente enfocada y una cultura de consciencia cibernética en toda la organización? ¿Qué hemos hecho para proteger a la organización contra riesgos cibernéticos de terceras partes? ¿Podemos contener daños rápidamente y movilizar diversos recursos de respuesta cuando un incidente cibernético ocurra? ¿Cómo evaluamos la efectividad del programa de riesgo cibernético de nuestra organización? Esto se denomina "compliance"[13], entendido como el conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención,

10 Tomado textualmente de Sura SA, expresamente pautado en formato publicitario.

11 Actividades coordinadas para dirigir y controlar una organización, con respecto al riesgo. [ISO Guía 73:2010]. Obtenido de: www.ccn-cert.cni.es.

12 Gestionando el riesgo cibernético: Preguntas críticas para la junta directiva y la alta gerencia, Deloitte 2018. Deloitte presta servicios de auditoría, consultoría, asesoramiento financiero, gestión de riesgos, impuestos, legal, y servicios relacionados a organizaciones públicas y privadas de diversas industrias.

13 Obtenido de:https://retos-directivos.eae.es/que-es-el-compliance-y-como-beneficia-a-las-empresas/

gestión, control y reacción frente a los mismos. El término además implica para la empresa adaptar sus recursos y funcionamiento a los estándares, reglamentaciones, regulaciones y requerimientos vigentes dados por la organización política y legal del país donde se encuentra.

Respecto a la **suma asegurada,** las compañías se vieron en el problema de elegir un criterio que permita establecer un valor a los activos intangibles puestos en riesgo ya que su mensura puede verse teñida de subjetividades. Para ello decidieron establecer cotizadores (la mayoría online) donde potenciales clientes pueden tomar de referencia un importe que finalmente verán reflejado en el valor de la póliza para cada caso. Los ítems para cotizar son: en primer lugar la actividad económica, a la que las aseguradoras le otorgan un nivel de riesgo (asegurable) alto, medio, bajo o no asegurable; la suma asegurada y deducible en dólares; los ingresos del asegurado también en dólares (para evitar calcular en base a moneda que pueda devaluar como el caso del peso) que puede oscilar en la suma escalonada de USD 0 a 100.000 en un primer tramo hasta los 5.000.000 de dólares anuales. Es decir, el interesado además de completar el cotizador con sus datos personales declara sus ingresos casi con efecto de declaración jurada (agrego yo) para poder calcular la prima[14]. Por su parte la aseguradora determina una prima técnica a partir de la información brindada por el interesado, le aplica gastos de explotación y producción para obtener la prima total a la que a su vez le aplica recargos financieros e impuestos para obtener la prima anual y la divide en 10 meses o cuotas, es decir lo que el asegurado finalmente deberá pagar.

Conexión entre seguros cibernéticos y protección de datos personales:

La Encuesta de Percepción del Riesgo Cibernético 2019, publicada por Marsh y Microsoft Corp recoge que en Latinoamérica el 73% de las organizaciones ahora clasifican el riesgo cibernético como una de sus cinco principales preocupaciones, en comparación con el 47% del 2017. Una de cada cinco organizaciones lo considera su riesgo principal. [15] El 27% de las empresas en Latinoamérica desconfían totalmente de su capacidad para responder a un evento cibernético y el 27% de las empresas en Latinoamérica desconfían totalmente de su capacidad para responder a un evento cibernético.[16]

Según la encuesta, en Latinoamérica crece el número de empresas que cuentan con un seguro cibernético, aunque la región todavía está lejos de la media global: 29% vs 47%. En el caso de las grandes empresas, el porcentaje de penetración del seguro cibernético crece hasta el 40%.

14 Precio del seguro y representa la contraprestación del riesgo asumido por el asegurador, entendido como el estricto valor del riesgo más los gastos y beneficios de gestión de la empresa aseguradora.

15 Obtenido de: https://www.microsoft.com/security/blog/2019/09/18/marsh-microsoft-2019-global-cyber-risk-perception-survey-results/ , el 18 de Septiembre de 2019.

16 "Encuesta de Percepción del Riesgo Cibernético 2019" publicada por Marsh (líder global en consultoría de riesgos y seguros) y Microsoft Corp. (líder mundial de plataformas y productividad), que recoge las respuestas de 1,500 empresas a nivel global, de las cuales 531 de ellas en Latinoamérica.

A los fines de la temática que nos compete, podemos afirmar que existe en nuestro país un proyecto de Ley de Protección de Datos Personales en el cual se asientan las bases y principios en la materia y del que surgen necesariamente vinculaciones con el seguro riesgos cibernéticos sobre todo cuando de la manipulación y tratamiento de datos se trata. Sólo me detendré en el desarrollo de algunos ítems del proyecto que por su íntima relación con los seguros requieren más atención. Por empezar:

-Principio de responsabilidad proactiva (art. 10): el **responsable o encargado del tratamiento** (de datos) debe adoptar las medidas técnicas y organizativas apropiadas a fin de garantizar un tratamiento adecuado de los datos personales y el cumplimiento de las obligaciones dispuestas por la presente Ley, y que le permitan demostrar a la autoridad de control su efectiva implementación.

-Principio de seguridad de los datos y notificación de incidentes de seguridad (art. 19): el responsable del tratamiento y, en su caso, el encargado, deben adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

El responsable del tratamiento debe adoptar las medidas de seguridad aplicables a los datos personales que trate, considerando, al menos, los siguientes factores:

a. El riesgo inherente por el tipo de dato personal;

b. El carácter sensible de los datos personales tratados;

c. El desarrollo tecnológico;

d. Las posibles consecuencias de un incidente de seguridad para los titulares de los datos;

e. Los incidentes de seguridad previos ocurridos en los sistemas de tratamiento.

-Deber de notificación de incidentes de seguridad: el art.20 prevé un plazo de 72 horas de haber tomado conocimiento del incidente para notificar a la autoridad de control.

-Delegado de Protección de Datos: el art. 43 crea esta figura y son dice que los responsables y encargados del tratamiento deben designar un **Delegado de Protección de Datos** (persona idónea, capaz y tener conocimientos específicos para sus funciones y que sólo responde ante el más alto nivel jerárquico de la organización) en cualquiera de los siguientes supuestos:

a. Cuando revistan el carácter de autoridades u organismos públicos;

b. Se realice tratamiento de datos sensibles como parte de la actividad principal del responsable o encargado del tratamiento;

c. Se realice tratamiento de datos a gran escala.

En lo referido a **sanciones**, el art. 77 del proyecto prevé para los responsables y encargados del tratamiento:

a. Apercibimiento;

b. Multa de hasta el equivalente a QUINIENTOS (500) Salarios Mínimos Vitales y Móviles vigentes al momento de la imposición de la sanción;

c. Suspensión de las actividades relacionadas con el tratamiento de datos hasta por un término de SEIS (6) meses; en el acto de suspensión se indicarán las medidas correctivas que deberán adoptarse;

d. Cierre temporal de las operaciones relacionadas con el tratamiento de datos una vez transcurrido el término de suspensión sin que se hubieren adoptado las medidas correctivas ordenadas por la autoridad de control;

e. Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.

Adviértase que tales disposiciones son aplicables a personas privadas pero el art. 78 no dice que en caso de incumplimiento de las disposiciones por parte de la autoridad pública se remitirán las actuaciones a la "autoridad que corresponda" (sin manifestar cual) para que inicie la investigación respectiva.

Finalmente la gradación de las sanciones está prevista en el art. 79 y nos dice que se realizará en base a criterios como:

a. La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente Ley;

b. El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción;

c. La reincidencia en la comisión de la infracción;

d. La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia dela autoridad de control;

e. El incumplimiento de los requerimientos u órdenes impartidas por la autoridad de control;

f. El reconocimiento o aceptación expresa que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

La designación voluntaria de un Delegado de Protección de Datos, la adopción de mecanismos de autorregulación vinculantes, la realización de una evaluación de impacto en los términos del artículo 40 y la notificación oportuna de incidentes de seguridad serán merituados como atenuantes de la sanción que corresponda, sin perjuicio de otros que pueda considerar la autoridad de control.

Los aspectos previamente señalados en el proyecto encuentran su punto de conexión con los riesgos cibernéticos que venimos desarrollando y tornan casi indispensable al contrato de seguro como herramienta preventiva sobre todo si existe posibilidad de que se ocasionen daños.

CONCLUSIONES

La ciberamenaza será cada día más grande, por lo que se requiere una gestión de riesgos diligente y acorde con las necesidades de seguridad de esta nueva era, razón por la cual contratar un seguro de riesgos cibernético ya no es cuestión para tomar a la ligera sino que a medida que pase el tiempo deberá hacerse con carácter obligatorio.

En la UE, existes mecanismos mediante los cuales los ciudadanos tienen derecho a presentar reclamaciones de forma individual o colectiva si considera que el tratamiento de sus datos personales vulnera el **Reglamento General de Protección de Datos (RGPD)**. Argentina como parte de la comunidad internacional adoptó el modelo Europeo y lo puso en vigencia el 25 de mayo de 2018 y a través del Mensaje 147 del Poder Ejecutivo Nacional se envió casi a fines del mismo año un proyecto de Ley de Protección de Datos Personales al Congreso para someterlo a su consideración. Por su parte la resolución 69/2016 del Ministerio de Justicia y de Derechos Humanos, que establece el denominado “Programa Nacional contra la Criminalidad Informática” se ha buscado proveer a la justicia penal de los elementos necesarios para la investigación eficiente de esta nueva forma de criminalidad compleja que resulta de los avances de las nuevas tecnologías, además de la Ley 26388 (de delitos informáticos) que permitió adaptar la legislación Argentina interna en materia de fondo a las demandas del Convenio de Budapest de 2001 al modificar el Código Penal.

Sin embargo no se puede afirmar que las tareas hayan concluido, por el contrario el legislador nacional tiene un desafío, el de prever que en un futuro próximo nuevas modalidades delictivas se harán presentes en el ciberespacio y será él quien deba proporcionar los recursos legales para combatirlos. En similar sentido, nuestros magistrados se verán compelidos en materia de cibercrimen a migrar gradualmente de la prueba física, corpórea o tangible hacia la prueba digital, electrónica o intangible en los procesos penales lo que habla también de una necesaria adaptación procesal a la criminalidad informática actual. Los demás operadores del derecho no son la excepción, también están obligados a realizar grandes esfuerzos para estar a la altura de estos tiempos, ya sea para construir una imputación u oponerse a la misma sobre la base de una constante capacitación.

En materia estrictamente de seguros, el ordenamiento vigente va a demandar una necesaria revisión y adecuación al menos en forma general a los requisitos y elementos que hacen a la constitución del contrato de seguro de riesgos cibernéticos, sus modalidades, forma de cumplimiento en caso de existir una contingencia, y todo cuando en materia de responsabilidad corresponde a las partes al suscribirlo.

Hugo Fabián Pérez Carretta

Abogado, Técnico en sistemas

Informáticos y Hardware

BIBLIOGRAFÍA

CENTRO DE CAPACITACIÓN FEDERAL- FAPASA. (2019). *Manual de principios técnicos del seguro.* Bs AS: FAPASA.

CONGRESO ARGENTINO. (4 de JUNIO de 2008). Ley 26388 CÓDIGO PENAL. *De Delitos Informáticos*. BUENOS AIRES.

MARSH. (2019). *MARSH.* Obtenido de https://www.marsh.com/co/insights/research/marsh-microsoft-encuesta-percepcion-riesgo-cibernetico-2019.html

SEGUROS SURA S.A. (2019 de Agosto de 2019). Broshure Riesgos Cibernéticos.

WEBGRAFÍA

www.ccn-cert.cni.es

https://www.larepublica.co/analisis/santiago-castro-513871/ciberseguridad-compromiso-de-todos-2926662

https://es.wikipedia.org/wiki/Seguro

http://es.pcisecuritystandards.org

https://www.infotechnology.com/online/Las-estafas-online-no-paran-de-crecer-como-protegerse-20191021-0008.html

https://www.responsabilidadconsejerosydirectivos.com/seguro-de-riesgos-ciberneticos/

https://www.iprofesional.com/

https://www.lapoliticaonline.com/nota/ciberseguridad/

https://www.forbes.com.mx/como-se-protege-una-empresa-al-adquirir-un-seguro-de-riesgos-ciberneticos/

https://retos-directivos.eae.es/que-es-el-compliance-y-como-beneficia-a-las-empresas

https://www.microsoft.com/security/blog/2019/09/18/marsh-microsoft-2019-global-cyber-risk-perception-survey-results/, el 18 de Septiembre de 2019.