BN SOCIEDAD CORREDORA DE SEGUROS, S. A.

N.° 299

Costa Rica, martes ocho de febrero del dos mil veintidós, a las nueve horas con cinco minutos.

SESIÓN ORDINARIA

Asistencia:

Directivos:	Sra. Ruth Alfaro Jara, presidenta
	Sra. Jeannette Ruiz Delgado, vicepresidenta
	MBA. Rosaysella Ulloa Villalobos, secretaria
	Sr. Mario Carazo Zeledón, tesorero
	Sra. Andrea Vindas Lara, vocal
Fiscal:	Lcda. Jessica Borbón Guevara
Gerente General:	Lic. José Alfredo Barrientos Solano
Auditoría Interna:	M.Sc. Gabriela Sánchez Quirós
Asesor Legal de la Junta Directiva General del BNCR:	Lic. Rafael Brenes Villalobos
Subsecretaria General:	Lcda. Sofía Zúñiga Chacón

ARTÍCULO 1.°

Se dejó constancia de que, dada la declaratoria de estado de emergencia nacional emitida por el Gobierno de la República, ante la situación sanitaria provocada por la Covid-19, la presente sesión se desarrolló vía la herramienta Microsoft Teams, garantizando la simultaneidad, interactividad e integralidad entre la comunicación de todos los participantes.

ARTÍCULO 2.°

La presidenta de este directorio, señora Ruth Alfaro Jara, sometió a votación el orden del día de la presente sesión ordinaria número 299 de BN Sociedad Corredora de Seguros, S. A. Sobre el particular, solicitó que en temas de Presidencia se realice un receso, para comentar un punto específico del orden del día, de previo a su discusión. Los directores mostraron su anuencia en aprobar el orden del día, con la alteración propuesta en esta oportunidad.

Resolución

POR VOTACIÓN NOMINAL Y UNÁNIME SE ACORDÓ: aprobar el orden del día de la presente sesión ordinaria 299 de BN Sociedad Corredora de Seguros, S. A., con la alteración propuesta en esta ocasión, en el sentido de que en el apartado *Temas*

de Presidencia, Directores y/o Gerente General se realice un receso, para comentar un punto específico del orden del día.

(R.A.J.)

ARTÍCULO 3.°

La directora señora Ruth Alfaro Jara sometió a aprobación el acta de la sesión ordinaria número 298, celebrada el 20 de enero del 2022.

Sobre el particular, indicó: "Doña Gabriela remitió unas observaciones de forma, que fueron enviadas a la Secretaría. ¿Alguna observación? Si no, les solicito la aprobación".

Los directivos no hicieron observaciones y expresaron su anuencia a aprobar el acta.

Resolución

POR VOTACIÓN NOMINAL Y UNÁNIME SE ACORDÓ: aprobar el acta de la sesión ordinaria número 298, celebrada el 20 de enero del 2022, considerando las observaciones de forma realizadas por la auditora interna, señora Gabriela Sánchez Quirós, las cuales fueron remitidas a la Secretaría General del Banco Nacional.

Nota: se dejo constancia que después del conocimiento del asunto consignado en el presente artículo la Presidenta del directorio decretó un receso.

(R.A.J.)

ARTÍCULO 6.°

En cumplimiento del plan de capacitación dirigido a la Junta Directiva de BN Sociedad Corredora de Seguros, S. A., para el periodo 2021, aprobado en el artículo 6.°, sesión 297 del 11 de enero del 2022, el gerente general, señor José Alfredo Barrientos Solano, informó de que invitó a los señores Giancarlo Caamaño Lizano, Fernando López Lizano y Erika Mendoza Alvarado, personeros de la firma ASSA Compañía de Seguros, con el propósito de que desarrollen la capacitación denominada ***Cyber Insurance, Seguro de Protección de Datos***.

Con la venia de la Presidencia, se incorporaron a esta sesión virtual los señores Giancarlo Caamaño Lizano, Fernando López Lizano y Erika Mendoza Alvarado, así como los señores Antonio Mora Alfaro, director comercial; Esteban Umaña Lizano, director de Estrategia Digital y Operaciones; Kathia Castro Gamboa, jefe de la Unidad de Riesgo y Control Interno, y Rocío Pérez Calvo, funcionaria de BN Corredora de Seguros, S. A., a quienes los miembros de este órgano colegiado brindaron una cordial bienvenida.

El señor Barrientos Solano mencionó: "Este tema que vamos a ver hoy es muy importante por todo lo que está ocurriendo a nivel mundial en materia de ciberseguridad y el seguro relacionado es un aspecto muy importante. De hecho, nosotros tenemos una propuesta para emitir un seguro asociado no solo a

ciberseguridad, sino a robo y fraude para el uso de las tarjetas de crédito, transferencias electrónicas, compras en comercios electrónicos, etc., las cuales son situaciones que hoy se están materializando como riesgos, por lo que la Corredora, como institución financiera, está desarrollando dos propuestas: una de robo y fraude, en la que, incluso, doña Rosaysella nos ha estado ayudando en el proceso y que se encuentra en el análisis final, y el otro aspecto se enfoca en ciberseguridad. Entonces, espero que podamos sacarle mucho provecho a esta charla, ya que ellos son expertos en esta materia, así como en todo el tema de bases de datos, que hoy está en boga".

Inicialmente, el señor Caamaño Lizano brindó un agradecimiento a esta Junta Directiva por el espacio y la confianza que tienen en ASSA. Luego, indicó que la idea es llevar a cabo una presentación que pueda ser aprovechada como parte de la capacitación y expansión de conocimientos en materia de seguros, los cuales están latentes en el diario vivir.

Seguidamente, el señor López Lizano igualmente agradeció el espacio brindado para referirse en esta oportunidad al ciberseguro. Don Fernando mencionó que ASSA Compañía de Seguros es pionera en Costa Rica en el ofrecimiento del seguro de cibernético, ya que fue hace cuatro cuando registró este producto ante la Sugese y ya cuentan con una cartera importante de empresas grandes que han suscrito este seguro con ASSA. Comentó que el ciberseguro todavía no es muy conocido en el país; sin embargo, expresó que en otras latitudes se opera desde hace varios años y prácticamente es obligatorio el que las empresas lo contraten, esto debido a que a partir de la pandemia el riesgo cibernético ha sufrido un incremento importante en todo el mundo. Además, comentó que la compañía de seguros a Allianz, que es una de las más grandes del mundo (*top* cinco), emite todos los años un barómetro de riesgos, en el que se incluyen los principales riesgos a los que están expuestas las empresas cada año. Sobre este aspecto, don Fernando presentó un diagrama que detalla los riesgos más importantes que componen el citado barómetro para el presente año, los cuales son: incidentes cibernéticos, interrupción de negocios, catástrofes naturales, brote pandémico, cambios regulatorios y cambios climáticos. Apuntó que tradicionalmente se piensa que lo más probable o que lo primero que habría que asegurar es a los edificios, lo cual está bien, dado que el riesgo de incendio o desastres naturales está latente; pero, dijo que, en la actualidad, desde el punto de vista estadístico, la mayor probabilidad y cantidad de pérdidas que las compañías están sufriendo, no solo en Costa Rica, sino en el mundo, se deriva de incidentes cibernéticos, por lo que siempre que se analiza cuáles son las necesidades de cobertura de las compañías o instituciones se debe pensar en que estos incidentes son uno de los principales riesgos que se deben proteger. Luego, expresó que es importante establecer la diferencia entre crímenes por computadora y el riesgo cibernético, especialmente en las entidades bancarias, tomando en cuenta que la mayoría mantiene pólizas de fidelidad que cubren crímenes por computadora. Mencionó que este tipo de crímenes se materializan cuando un *hacker* ingresa a los sistemas del Banco para sustraer dinero, mientras que el riesgo cibernético se

relaciona con la sustracción de datos o de un daño a los datos. Dijo que en seguros existe un vacío, porque la mayoría de las pólizas no cubren el robo de datos y que, a raíz de esta situación, surgió la necesidad de contar con un seguro de este tipo, con el objetivo de estar protegidos ante la posibilidad de que un *hacker*, virus o *malware* ingrese a los sistemas de la empresa a robar datos. También, recalcó que la razón de ser del seguro cibernético es cubrir las bases de datos que, ante un robo, podrían acarrear otras pérdidas secuenciales.

La directora Ruiz Delgado dijo: "Este tema es importante, actual; pero, además, bastante complejo. Quiero saber si hablamos solamente de pérdida de datos estamos hablando de la entidad financiera o de los clientes, porque normalmente cuando hay un robo de datos de los clientes puede tener varias razones de ser: el robo de dinero, uso de la información del cliente para luego utilizarla en otro tipo de delito; sin embargo, en todo caso, casi siempre el objetivo primario es el robo de dinero. Entonces, mi pregunta va en la línea de si ese seguro es para la entidad financiera o para los clientes".

El señor López Lizano respondió: "El principal objetivo del seguro es cubrir la entidad financiera, que puede ser declarada responsable o tener que responder ante sus clientes por el robo de datos y por el perjuicio que el robo de datos le ocasione a los clientes de la entidad. A raíz del robo de datos un *hacker* puede extorsionar a los clientes y podría divulgar datos que son sensibles. La mera destrucción de los datos, por medio de un virus o *software* malicioso, también puede acarrear responsabilidades de la entidad hacia sus clientes porque no puedan accesar, por ejemplo, sus cuentas bancarias, porque se desapareció su usuario de banca en línea. Entonces, cualquier consecuencia que tenga para la entidad la pérdida, destrucción o divulgación de esos datos ante terceros, eso es lo que vamos a cubrirle a la entidad, lo que la entidad va a tener que responder a terceros y también algunos gastos propios".

La directora Ruiz Delgado preguntó: "¿Cuando los servicios son tercerizados hay algún seguro que pueda cubrir la relación contractual entre la entidad financiera y el prestador de ese servicio tercerizado hacia la entidad financiera?".

El señor López Lizano contestó: "Sí, este mismo seguro. Ahora en la explicación de las coberturas van a ver que dentro de las coberturas básicas incluimos también a terceros subcontratados por el asegurado para la custodia o manejo de los datos".

El señor Barrientos Solano dijo: "Viendo como lo explica y la importancia que están teniendo hoy los riesgos cibernéticos, normalmente, lo que a veces ocurre es que la Administración entra en exceso de confianza y, finalmente, decimos: *tenemos todos los mecanismos, nunca nos va a pasar*. Quiero que se refiera un poco a la importancia del seguro, porque cuando falla todo para eso está conceptualizado el seguro. Mucho de lo que se vive algunas veces es que nosotros mismos en la Administración creemos que nunca va a pasar; pero, este tipo de temas son de mucho interés en países desarrollados, porque ya han vivido situaciones muy complejas. No sé si se puede referir un poco a eso".

La directora Vindas Lara externó: “Si fuera destrucción de información, la entidad financiera se da cuenta rápidamente de que tiene archivos en blanco, por decirlo de alguna manera, entonces, en ese caso, es muy visible que hubo un secuestro de datos y una eliminación de datos. En el caso de que copien archivos, ¿quién ve la afectación?, porque si es un robo de archivos; pero, la copia de archivos, ¿quién detecta que eso se da? Cuando hay un robo la afectación a clientes no necesariamente es inmediata, la afectación puede ser en un plazo medio, porque no necesariamente tienen toda la habilidad o logística para afectar a todos los clientes de inmediato, de igual forma. Entonces, quiero saber cuánto tiempo es la cobertura de este seguro y quién se da cuenta de cuánta es la afectación y la magnitud de la afectación, porque podría ser que no necesariamente todos los clientes planteen la queja, debido a que se da de diferentes formas o, por ejemplo, puede afectarnos extrayendo bases de datos para hacernos todas esas llamadas dirigidas a temas muy específicos y uno no sabe realmente de dónde procede la información sensible que uno no ha autorizado para que terceros la utilicen”.

El señor López Lizano respondió: “Muy buenas las preguntas. Voy a comenzar explicando sobre el ámbito temporal de la cobertura, o sea, por cuánto tiempo cubre. Estas pólizas cubren sobre la base de las reclamaciones que se hagan durante el periodo de póliza. Entonces, la póliza es anual, renovable cada doce meses y lo que va a cubrir son los reclamos que terceros le hagan a la entidad durante el periodo de póliza. Esas reclamaciones sin distingo de la fecha en que ocurrió realmente la sustracción de la *data*, la base va a ser la fecha de la reclamación, siempre y cuando se haya dado durante el periodo de vigencia de la póliza. Es muy importante que se comprenda que este tipo de pólizas que operan sobre la base de reclamación tienen una retroactividad, que es la primera fecha de emisión de la póliza, entonces, si la póliza se emitió el 1.° de enero yo voy a cubrir todas las reclamaciones que reciba la entidad desde el 1.° de enero hasta el 31 de diciembre. Si el año que sigue renueva la póliza con nosotros, entonces, cubriremos las reclamaciones que se den entre el 1.° de enero y el 31 de diciembre; pero, incluso, si el hackeo de los datos se llega a determinar que ocurrió en una fecha anterior, siempre y cuando no sea previa a la primera fecha de emisión de la póliza, que sería el 1.° de enero del 2022, la base será que la reclamación contra el asegurado se dé durante el periodo de vigencia y puede ser que se cubran casos. Incluso, aunque el hackeo de datos se haya dado en una fecha previa, siempre y cuando en esa fecha previa el seguro estuviera suscrito con la compañía, el monto de la pérdida lo determina el perjuicio que se haya causado a terceros y que se determine que la entidad sea responsable o que tenga que responder por ese perjuicio. En esencia, este es un seguro de responsabilidad civil, es como cuando compramos la póliza de daños a terceros del carro que tenemos, en la que este tendrá que hacer la demostración del perjuicio y si hay duda, si es necesario que lo tenga que llevar a la vía judicial para que un juez determine con exactitud la cuantía de ese perjuicio, entonces, el juez lo va a determinar y la entidad va a tener que pagar esa sentencia; por lo tanto, este seguro funciona de esa manera. Si el perjuicio es muy evidente, a la

luz de lo que cubre la póliza, nosotros no vamos a esperar a que haya un proceso o una resolución judicial, sino que vamos a tratar de resolver en la vía administrativa; pero, si el mismo perjudicado no logra demostrar fehacientemente ese perjuicio, probablemente, le va a tocar llevarlo a la vía judicial para que sea un juez el que determine si realmente la entidad es responsable y cuánto es la cuantía de esa responsabilidad. La póliza lo que va a cubrir no es el valor dato, sino la consecuencia. Los riesgos cibernéticos (virus, destrucción) están cubiertos en la póliza, así como errores, accesos no autorizados, pérdida de datos o infidelidad, porque puede ser un empleado el que robe o destruya datos; pero, lo que vamos a cubrir acá es la consecuencia, el daño a la reputación de las personas, los reclamos de terceros, la extorción que le hagan a la misma entidad, porque ya tuvimos un caso en Costa Rica (entidad bancaria); además, la pérdida de ingreso, sanciones que tengamos que pagar. Todas esas consecuencias son las que vamos a cubrir en la póliza".

La directora Vindas Lara consultó: "¿Han visto que esto funciona bien? ¿Qué periodos hay para el pago de los reclamos? ¿El diseño funciona rápidamente o es una póliza de lento trámite para llegar hacia el final? ¿Cómo ha sido la operativa?".

El señor López Lizano contestó: "En Costa Rica no hemos tenido todavía experiencia con pérdidas; pero, en otras latitudes hay mucha experiencia, porque este es un seguro que tiene un par de décadas de existir a nivel mundial. En Europa 37% de las empresas tienen un seguro cibernético, entonces, sí hay mucha experiencia en el extranjero. La respuesta es dependiendo del tipo de caso que se dé y dependiendo de qué tan evidente es el perjuicio. Entonces, acá visualizamos las coberturas, que ya ahorita las voy a explicar más a fondo, y, por ejemplo, está la cobertura de extorsión. Cuando hay una cobertura de extorsión, lo que vamos a necesitar es una respuesta rápida, porque estamos siendo extorsionados por un *hacker* o por *software* malicioso, que nos está bloqueando nuestras bases de datos, nuestra página web y nos está pidiendo rescate. Esta cobertura va a pagar ese rescate. Ahí la respuesta probablemente va a ser muy rápida. Cuando tenemos un caso de una persona que le está reclamando a la entidad, porque hackearon bases de datos de la entidad y divulgaron información sensible, puede ser que la determinación del perjuicio sí tenga que ir a vía judicial, si no es tan evidente. Nosotros, como les mencionaba, en los seguros que tienen coberturas de responsabilidad civil, procuramos resolver en vía administrativa, ya que eso abarata el costo del reclamo, hace más rápida la resolución y tenemos obviamente a nuestro asegurado más satisfecho por una pronta resolución y también el afectado va a quedar más satisfecho de que se le haya resuelto rápido. Si no es tan evidente el perjuicio y la cuantificación de este, el perjudicado va a tener que acudir a la vía judicial para demostrar ese perjuicio y que sea un juez el que determine realmente cuánto es lo que corresponde indemnizar. Yo siempre menciono, ustedes lo recordarán, el caso de hace dos o tres años, de la señora que llamó a un *call center* de una cablera y ese audio de la llamada se divulgó y se hizo viral. Esa es una divulgación de datos y son datos sensibles y confidenciales, porque, si la señora llama al *call center,* es una llamada cliente con su entidad y, obviamente, ella no quería que

eso se divulgara y que saliera en redes sociales. Bueno, ese es un caso justamente de divulgación de datos. Y aquí voy a mencionar un tema muy interesante: el dato. ¿Qué es un dato para nosotros? No es solamente un número de cédula o una dirección de una persona. Un dato puede ser un archivo de audio, como el de esta señora que llamó al *call center*. Puede ser también un video de una cámara de seguridad de un banco, puede ser un contrato o información de salud de las personas, porque, por ejemplo, la entidad bancaria tiene una corredora de seguros que posee expedientes de pólizas de gastos médicos y ahí hay información de salud sensible. Podría ser información de una persona pública, como de un candidato, por ejemplo, de la República del que se divulgue información sensible o de sus deudas. Entonces, también hay un daño reputacional de por medio, que está cubierto en la póliza". Luego, don Fernando explicó de manera amplia cómo se estructuran los tres tipos de coberturas, a saber: i) básica, que incluye responsabilidad por datos personales, datos corporativos, empresas subcontratadas y seguridad de datos; ii) extensión de cobertura, la cual comprende sanción administrativa, gastos de investigación, datos electrónicos, restitución de imagen de la sociedad y las personas, y notificación y monitoreo; iii) opcional, que incorpora extorsión de la web, interrupción de la red y contenidos multimedia. De seguido, expresó que está póliza opera tanto si el que causa el perjuicio es un empleado como si lo causa alguien ajeno a la entidad. Añadió que se considera que siete de cada 10 ataques cibernéticos a las empresas tienen la participación voluntaria o involuntaria de un empleado. Brindó ejemplos.

La directora Alfaro Jara indicó: "Don Fernando, perdón que lo interrumpa; pero, voy a leer la filmina que está en pantalla. Dice: *Aproximadamente 7 de cada 10 ataques cibernéticos a las empresas son perpetrados con la participación o facilitación de un empleado, sea en forma intencional, por simple error o por ser víctima del phishing o ingeniería social.* Esto es sumamente delicado y mi pregunta es cómo llegaron a esta conclusión".

El señor López Lizano respondió: "Son estadísticas que no son de Costa Rica, son a nivel mundial. Hay muchas empresas que generan reportes sobre la cantidad de ataques cibernéticos que se dan en un país. ¿Cuáles son las causas de esos ataques cibernéticos? Como mencionaba, muchos de los ataques cibernéticos se dan ya sea porque una entidad participe en forma voluntaria o por descuidos de los empleados. Cualquiera de nosotros puede recibir un correo electrónico en el trabajo y que parece ser un *mail* inofensivo, el correo nos envía a dar clic a un enlace y cualquier empleado de la empresa por desconocimiento o por ignorancia va y hace clic y lo lleva a un virus que puede ser la entrada a los sistemas de la empresa. Eso sucede todos los días, porque alguno de nosotros recibió un correo electrónico que parece ser de un banco o de trabajo y damos clic y resulta que no era de trabajo, era un virus o un *malware* o *ransomware,* que son los *software* que utilizan los extorsionadores para ingresar a los sistemas de la empresa y generar un daño; esto realmente sucede todos los días. Se dice que en Costa Rica cada trimestre la cantidad de ataques que se dan son millones, cada minuto hay un intento de hackeo a alguna persona o a alguna empresa en Costa

Rica y en el mundo con mucha más razón". Luego, continuó la presentación refiriéndose a los eventos que no cubre el seguro cibernético, a saber: i) pérdida de, o daño a, cualquier propiedad física; ii) actos intencionales o fraude de un socio o a directivos de alta gerencia, iii) brechas o fallas que comenzaron antes de la fecha de retroactividad; iv) actualizaciones o mejoras del sistema, y v) crimen financiero-robo de dinero o valores.

La directora Alfaro Jara indicó: "Don Fernando, perdón que lo interrumpa nuevamente; pero, doña Gabriela está pidiendo la palabra. Tal vez le atendemos la consulta a ella y luego podemos continuar".

La señora Sánchez Quirós externó: "Gracias, doña Ruth. Gracias, don Fernando, excelente presentación. Mi consulta es muy puntual. En ese punto de actualizaciones de sistemas, sabemos y hemos visto en los últimos meses vulnerabilidades que ya traen los sistemas operativos, como el *log4j* que trae Windows. ¿Qué pasa en esos casos? Porque, si bien es cierto es un tema de actualización y propio del sistema, no es una responsabilidad directa de la empresa. ¿Cómo se tratan esos temas en las pólizas? La segunda consulta, también, muy específica: ¿cuáles son los deducibles? ¿Es porcentual o es un monto fijo? ¿Cómo están definidos?".

El señor López Lizano respondió: "Muchas gracias. Comienzo por la primera. ¿Qué pasa con las actualizaciones y las pulgas que tienen los *softwares* que adquirimos? Eso no sería objeto de cobertura, lo que vamos a cubrir nosotros acá son ataques externos al *software*. Entonces, hablamos de un virus, *malware*, troyano, *ransomware,* o sea, cualquier ataque externo, un acceso no autorizado, obviamente. También, puede ser un acceso físico, o sea, si alguien dejó su sesión de Windows abierta, un empleado del Banco, y viene otra persona y se sienta en la *laptop* y empieza a travesear, ese acceso no autorizado está cubierto, cualquier agente externo que ataque el *software* y la *data* es lo que va a estar cubierto; pero, las propias pulgas que tenga el *software,* aunque sea adquirido no lo vamos a cubrir. Otra cosa muy importante que aprovecho para mencionar es que la *data* que está en la nube también está cubierta".

La señora Sánchez Quirós acotó: "Gracias, don Fernando. Mi duda es si por medio de estas vulnerabilidades que tiene Windows se logran infiltrar a los datos de la empresa y nos instalan un *ransomware* y nos secuestran información, ¿eso sí está cubierto o dado que la fuente de la vulnerabilidad es un tema de *software* no se cubre?".

El señor López Lizano manifestó: "Sí se cubre. Por eso es muy importante que la empresa tome todas las medidas necesarias dentro de lo razonable para evitar que esto suceda. Aprovecho para mencionar que cuando se adquiere el seguro hay una etapa en la cual nosotros vamos a analizar y a medir el grado de seguridad cibernética que tiene la entidad, vamos a hacer un análisis y eso también va a ser un valor agregado para ustedes, porque nosotros del análisis que hacemos vamos a determinar dónde vemos que hay vulnerabilidades y si consideramos que esas vulnerabilidades tienen que ser corregidas antes de poder emitir la póliza. Hemos tenido casos de clientes donde les hemos dicho: *usted no califica todavía para poder darle la póliza,*

porque tiene que mejorar estos problemas que tienen su seguridad cibernética; pero, esencialmente respondiendo a su pregunta, si el ataque se da y ya la póliza está suscrita siendo el ataque de un virus, *malware*, de un hacker o un acceso no autorizado va a estar cubierto, porque obviamente ya se dio la cobertura".

La señora Mendoza Alvarado agregó: "Es importante mencionar que estos análisis los hacen expertos en la materia, que estos seguros generalmente se colocan en el mercado internacional donde hay todo un *staff* de informáticos expertos en seguridad de la información que hacen el análisis de ese cuestionario y no lo hace la compañía de seguros. Entonces, para que ustedes sepan que esto representa un valor agregado, completar el cuestionario de forma transparente y toda esta información obviamente es tratada con la debida confidencialidad".

El señor López Lizano acotó: "Muchas gracias. De hecho, tenemos un cliente que tiene asegurado con nosotros todas sus operaciones en Centroamérica con el seguro cibernético y gracias a esta póliza se le hizo un test de vulnerabilidad y esto es que tenemos gente experta en informática que ponen a prueba la vulnerabilidad cibernética del cliente para ver qué tan robusto es su seguridad informática. Entonces, de esto se generan reportes que entregamos al cliente, a nuestro asegurado para que le sirva de retroalimentación y también le sirva para identificar dónde están los puntos de mejora en su seguridad cibernética. Entonces, solo el hecho del proceso de cotizar la póliza genera un valor agregado muy importante, y yo siempre he dicho: pedir cotización es gratis. Entonces, solo el hecho de hacer ese ejercicio ya es una retroalimentación importante para la entidad". Posteriormente, presentó un ejemplo real de la empresa Target (tienda en línea). Mencionó que unos cibercriminales lograron acceder a los sistemas informáticos de los grandes almacenes de dicha empresa y robaron datos financieros y personales de 110 millones de clientes. Resaltó que representa una indemnización de US$90 millones con un deducible de US$10 millones. Después, agregó lo siguiente: "Perdón, se me quedó la pregunta que me hicieron sobre los deducibles. Lo primero es ¿cuánto debo comprar de cobertura? Eso es un factor que va a influir en la determinación de los deducibles, porque no es lo mismo una empresa pequeña que me compra una póliza de US$1 millón de cobertura a una empresa del tamaño del Banco Nacional que probablemente US$1 millón no le va a ser suficiente, sino que va a necesitar comprar mucha más cobertura. Entonces, el tamaño de la póliza tiene que ver con el deducible también; pero, los deducibles siempre van a ser un porcentaje, por ejemplo, 5% o 10% de la suma asegurada o un límite en monto; sin embargo, es muy variable porque dependerá de la entidad, del análisis de riesgo realizado y del tamaño de la póliza". De seguido, continuó explicando que estas pólizas se suscriben caso por caso, por lo que no hay dos pólizas iguales; es decir, que la póliza del Banco Nacional no va a ser igual a la póliza que va a tener otro banco, a pesar de que sea una institución similar o de igual tamaño, dado que se debe aplicar el análisis de riesgo por parte de expertos en TI y determinar el nivel de riesgo para establecer las condiciones y el costo de la póliza. Retomó el ejemplo expuesto anteriormente y reiteró que en el caso de Target se indemnizaron

un total de US$90.000.000,00, principalmente por la afectación en las coberturas de notificación y monitoreo. Señaló que se tuvo que pagar el daño a terceros por la responsabilidad de datos personales, así como los gastos de investigación y las sanciones administrativas correspondientes. Otro ejemplo que citó fue lo sucedido con el banco HSBC, sobre un ataque cibernético que afectó la banca en línea. Amplió detalles mencionando que en el momento que se dio ese ataque cibernético fue un día de pago en Inglaterra y dos días antes de la fecha límite para el pago de impuestos, en el que las coberturas que se hicieron efectivas fueron las indemnizaciones de pagos a terceros, responsabilidad por datos personales y corporativos, gastos de defensa y de investigación, sanciones administrativas, la pérdida de utilidades de la entidad por interrupción de la red y costos adicionales que se incurrieron durante la interrupción. Explicó que los datos electrónicos se asocian con los costos para reemplazar o reestablecer los programas de cómputo, además de los costos para solventar el problema. Asimismo, dijo que lo ocurrido con la empresa Merck fue un *ransomware* (*software* malicioso que tiene como objeto extorsionar la empresa), cuyas pérdidas alcanzaron los US$600.000.000,00, siendo la cobertura afectada la de extorsión, gastos de investigación, sanciones administrativas, la interrupción de la red y el costo de reemplazar y restaurar los sistemas. Mencionó que el último ejemplo al que se va a referir fue el acontecimiento ocurrido con la empresa Equifax en el año 2017, el cual consistió en un ataque cibernético que generó una pérdida de datos a 147 millones de estadounidenses y a 15 millones de habitantes en el Reino Unido. Detalló que la *data* sustraída por los *hackers* fueron fechas de nacimiento, números de identidad y de teléfono, direcciones de correo electrónico, licencia de conducir, números de identificación, datos de tarjetas de crédito, entre otros. Apuntó que este caso fue muy conocido y tuvo gran afectación entre toda la gente que labora para Equifax; además, indicó que las coberturas afectadas fueron la notificación y monitoreo, un centro de llamadas, la contratación de una firma de relaciones públicas para el manejo mediático y las indemnizaciones por gastos personales y de terceros, gastos de defensa e investigación, así como sanciones administrativas. Recordó que hace seis meses se presentó un caso en una empresa petrolera en Estados Unidos que generó la paralización del suministro de combustible en ese país; asimismo, dijo que en Costa Rica se han presentado casos similares, como es el de una cadena de hoteles que fue hackeada hace cuatro años. Finalmente, indicó que realizar una cotización del seguro a la empresa ASSA no tienen ningún costo, únicamente se deberán completar los formularios correspondientes y aportar la información requerida, a fin de medir la seguridad cibernética de la entidad.

La directora Alfaro Jara dijo: “Fernando, muchísimas gracias, sumamente interesante. Me pide la palabra doña Gabriela y luego doña Jeannette”.

La señora Sánchez Quirós expresó: “Gracias, doña Ruth. Don Fernando, tengo una duda técnica, ¿cuánto tiempo tiene la entidad para comunicar la materialización de los eventos? Esto es porque he leído que si se deja pasar mucho tiempo se pierde el rastro del acto cometido, entonces, ¿cuánto tiempo recomiendan ustedes para esa

comunicación de eventos y qué medidas tiene que tomar la empresa para no afectar la trazabilidad de lo sucedido y que no se altere la evidencia? Gracias".
El señor López Lizano respondió: "Nosotros lo que solicitamos en cualquier seguro es que el asegurado nos dé aviso tan pronto tenga el conocimiento de cualquier evento. Aquí es muy importante de lo que depende el evento, porque si es un caso de extorsión nosotros vamos a habilitar por medio del reasegurador de la póliza una empresa para recibir notificaciones 24/7. Lo más importante para nosotros es que nos den aviso tan pronto tenga conocimiento. Aquí también aprovecho para responder algo que me habían preguntado hace un ratito y es que hay casos que se detectan de inmediato y hay casos que tardan más en detectarse. Lo importante es que nos informen cuando tengan conocimiento, porque puede ser que la pérdida de datos se dio hace uno o dos años; pero, hasta ahora, puede ser que alguien los esté reclamando y en ese momento es que se dan cuenta y nos dan aviso a nosotros. Obviamente, eso no necesariamente va a significar que se va a rechazar el reclamo. Recordemos que la póliza está orientada a cubrir todas las reclamaciones que se den en el periodo de vigencia, aunque no necesariamente la pérdida de datos ocurrió en ese momento y ahí es donde se activa la cobertura".
La directora Alfaro Jara expresó: "Muchísimas gracias, don Fernando. ¿Doña Jeannette".
La directora Ruiz Delgado manifestó: "Muchas gracias, doña Ruth. Muchas gracias, don Fernando y Ericka por la presentación. Realmente, es importante y es muy actual el tema que ustedes no están presentando, por supuesto que es una necesidad que deberíamos cubrir como entidad financiera. Mi propuesta va en la línea en que don José lleve esta presentación al Comité Corporativo de Tecnología de Información, que son quienes administran toda la red, al igual que los sistemas de seguridad de la misma, para que hagan una valoración de la conveniencia y oportunidad de contar con un seguro como este. Obviamente, esto va a pasar como un tema administrativo, no es un tema de resolución nuestro; pero, sí me parece importante ponerlos en conocimiento y que esa discusión se pueda dar, ya que hoy tenemos algunas amenazas y mañana podrían ir incrementándose, porque obviamente los delincuentes cada vez se hacen muchísimo más sofisticados. Entonces, esa sería mi propuesta, doña Ruth, para que esta presentación se pueda coordinar y se pueda conocer en el seno del Comité Corporativo de Tecnología de Información. Muchas gracias".
La directora Alfaro Jara acotó: "Gracias, doña Jeannette. Es una excelente iniciativa y aquí está don Mario que es el Presidente de ese Comité y creo que él va a estar muy de acuerdo con que don Fernando lleve esta propuesta, como decía doña Jeannette, que es bastante actualizada. No sé si tienen alguna otra consulta o comentario. Si no es así, le agradecería a don Fernando, a doña Ericka y a don Giancarlo por acompañarnos esta mañana y por ofrecernos esta capacitación en temas de *cyber insurance*. Muchísimas gracias".
Finalmente, los Giancarlo Caamaño Lizano, Fernando López Lizano y Erika Mendoza Alvarado dejaron de participar en la presente sesión virtual.

Resolución
POR VOTACIÓN NOMINAL Y UNÁNIME SE ACORDÓ: 1) dar por recibida la capacitación denominada ***Cyber Insurance, Seguro de Protección de Datos***, impartida por los señores Giancarlo Caamaño Lizano, Fernando López Lizano y Erika Mendoza Alvarado, personeros de la firma ASSA Compañía de Seguros, como parte del plan de capacitación dirigido a la Junta Directiva de BN Sociedad Corredora de Seguros, S. A., para el período 2022, aprobado en el artículo 6.°, sesión 297 del 11 de enero del 2022. **2)** De conformidad con la propuesta formulada por la directora Ruiz Delgado, **solicitar** a la Gerencia General de esta sociedad coordinar lo pertinente con el propósito de que, oportunamente, se eleve a conocimiento del Comité Corporativo de Tecnologías de Información la capacitación recibida esta oportunidad, de manera que se pueda generar una discusión sobre la conveniencia y oportunidad de contar con la cobertura de un seguro de este tipo dentro del Conglomerado Financiero Banco Nacional.
Comuníquese a Gerencia General.

(J.A.B.S.)

ARTÍCULO 8.°

El gerente general, señor José Alfredo Barrientos Solano, presentó el resumen ejecutivo del 3 de febrero del 2022, al cual se adjunta el oficio BNCS-DO-013-2022, de la misma fecha, suscrito por el señor Esteban Umaña Lizano, director de Estrategia Digital y Operaciones, mediante el cual informa sobre la solicitud de reconsideración de multa, presentada por la empresa Grupo Computación Modular Avanzada, S. A., y dirigida a la Junta Directiva de esta sociedad, en relación con el atraso en la entrega de equipos de la Licitación Abreviada 2021LA-000001-001700001, denominada *Adquisición de 117 Laptop a BN Sociedad Corredora de Seguros, S. A.* Asimismo, detalla la cronología de los actos administrativos efectuados por BN Corredora de Seguros respecto del citado atraso en la entrega de equipos.
La directora Alfaro Jara expresó: “Este tema lo vamos a dar por conocido. Ustedes tienen la información adicional y eventualmente estaríamos esperando el criterio que emitan nuestros asesores de cómo proceder, si les parece”.
Los directivos mostraron su anuencia.
Resolución
VOTACIÓN NOMINAL Y UNÁNIME SE ACORDÓ: tener por presentado el resumen ejecutivo del 3 de febrero del 2022, al cual se adjunta el oficio BNCS-DO-013-2022, de la misma fecha, suscrito por el señor Esteban Umaña Lizano, director de Estrategia Digital y Operaciones, mediante el cual informa sobre la solicitud de reconsideración de multa presentada por la empresa Grupo Computación Modular Avanzada, S. A., y dirigida a la Junta Directiva de esta sociedad, en relación con el atraso en la entrega de equipos de la Licitación Abreviada 2021LA-000001-001700001, denominada *Adquisición de 117 Laptop a BN Sociedad Corredora de*

Seguros, S. A.; asimismo, detalla la cronología de los actos administrativos efectuados por BN Corredora de Seguros respecto del citado atraso en la entrega de equipos.

Comuníquese a Gerencia General.

(J.A.B.S.)

A las once horas con cinco minutos se levantó la sesión.

PRESIDENTE	**SECRETARIA**
Sra. Ruth Alfaro Jara	MBA. Rosaysella Ulloa Villalobos