FACULTAD DE POSTGRADOS

MAESTRÍA EN DERECHO DIGITAL E INNOVACIÓN

TÍTULO DE LA INVESTIGACIÓN

PROPUESTA DE LINEAMIENTOS PARA UN MANEJO ADECUADO DE UNA PÓLIZA DE CIBERSEGURIDAD PARA PEQUEÑAS Y MEDIANAS COMPAÑÍAS EN ECUADOR

Docentes:

Roberto Santiago Lara Narváez

Lorena Naranjo Godoy

Autores

Claudio Andrés Coral Santos

Santiago Andrés Suárez Borja

2024

Resumen

En los últimos años, la ciberseguridad se ha vuelto esencial para la mayoría de los negocios debido a la interconexión de sistemas informáticos a través de internet. Esto ha generado amenazas que pueden causar pérdida de información valiosa, interrupciones en operaciones diarias, entre otros problemas. En respuesta, el sector de seguros ha desarrollado políticas de ciberseguridad, aunque estas suelen estar dirigidas principalmente a grandes empresas con sistemas informáticos complejos.

Esta investigación se enfoca en definir los lineamientos para políticas de ciberseguridad adaptadas a pequeñas y medianas empresas (pymes), considerando sus estructuras y capacidades económicas. El objetivo es crear un producto de seguro viable para este segmento de mercado. Las aseguradoras deben garantizar rentabilidad, por lo que los asegurados deben cumplir ciertos requisitos de protección de sistemas y conductas de sus empleados para prevenir siniestros.

La tesis examina el desarrollo de las políticas de ciberseguridad, principios de ciberseguridad, tipos de ciberdelitos y la cobertura necesaria según la normativa ecuatoriana. La metodología empleada es analítica sintética, permitiendo un análisis detallado de la investigación.

Abstract

In recent years, cybersecurity has become essential for most businesses due to the interconnection of computer systems over the Internet. This has generated threats that can cause loss of valuable information, interruptions in daily operations, among other problems. In response, the insurance sector has developed cybersecurity policies, although these tend to be aimed primarily at large companies with complex IT systems.

This research focuses on defining the guidelines for cybersecurity policies adapted to small and medium-sized companies (SMEs), considering their structures and economic capabilities. The goal is to create a viable insurance product for this market segment. Insurers must guarantee profitability, so policyholders must meet certain requirements for the protection of systems and behaviors of their employees to prevent accidents.

The thesis examines the development of cybersecurity policies, cybersecurity principles, types of cybercrimes and the necessary coverage according to Ecuadorian regulations. The methodology used is synthetic analytics, allowing a detailed analysis of the research.

Índice

1. Introducción

La ciberseguridad es un campo crucial en el contexto actual debido al aumento exponencial de las amenazas digitales. Este trabajo se centra en analizar y proponer estrategias de ciberseguridad específicas para pequeñas y medianas empresas PYMES en Ecuador. El problema principal que aborda esta investigación es la vulnerabilidad de las Pymes, frente a ciberataques y la falta de políticas en esta materia. La relevancia de este estudio radica en la creciente dependencia de las Pymes en sistemas digitales y la necesidad de proteger sus archivos y datos frente a posibles ciberataques.

1.1. Entorno Económico Ecuador

Las pequeñas y medianas empresas en el Ecuador han aportado con varias plazas de empleo para los ciudadanos ecuatorianos y han ayudado a que de alguna forma el sector productivo siga creciendo e incrementando ganancias que a su vez se liga con más negocios, igualmente generación de empleo y diferentes líneas de inversión. Estas empresas han prestado sus servicios lícitos al público en general, pero no tienen una cultura marcada de ciberseguridad que brinde los blindajes suficientes para que sus sistemas no puedan ser vulnerados por los ciberataques y que roben los datos de sus clientes.

Esto se da por la percepción de altos costos de una póliza de ciberseguridad y por lo tanto, inaccesibles para este tipo de empresas, es por eso que se pretende buscar lineamientos para este tipo de pólizas, que estén acorde a las necesidades de estas compañías y puedan brindar la cobertura que estas entidades requieren para que se cumplan los requisitos básico de protección a sus sistemas informáticos, de igual forma es vital tener en cuenta que la información una vez vulnerada por un ciberataque es muy difícil recuperarla.

1.2. Entorno tecnológico del Ecuador

En la era digital, donde la información se encuentra cada vez más expuesta, la protección de los sistemas informáticos se ha convertido en una preocupación fundamental en el ámbito personal así como corporativo. Existen varios motores para que hoy en día se tenga mayor preocupación con este tema y un ejemplo es, la entrada en vigor de la Ley de Protección de Datos en mayo de 2021 obligó a todas las empresas a tener políticas de protección de datos en especial las que manejan información importante.

Dentro de un espacio corporativo, cuando una compañía maneja información sensible con bases de datos de sus clientes, es vital que estas tengan protegidos sus sistemas contra cualquier ataque cibernético. No obstante, al existir un error que genere un ataque a sus sistemas informáticos es importante que la empresa se pueda proteger contra los daños y perjuicios que estos ataques causan. Dentro los riesgos más comunes que se pueden presentar en las estructuras digitales de una corporación están, el malware, ransomware, spyware, ciber extorsión entre otros, por lo cual, ningún sistema está libre de caer en estos problemas, se expondrá la necesidad de contar con una póliza que proteja a la compañía de estos imprevistos.

Es por este motivo, que se va a realizar en este trabajo una propuesta de lineamientos que deben contener las pólizas de ciberseguridad para una empresa, sus coberturas y cómo se va a reparar y proteger los datos de sus clientes. Todo esto con el propósito de brindar una protección ante el contingente de sufrir un ataque dentro de una empresa y que las bases de datos y su información puedan ser restituida y la reputación de la institución se vea mayormente afectada.

2.- Identificación del Objeto de Estudio

Análisis y Propuesta de lineamientos para un manejo adecuado de una póliza de ciberseguridad en Ecuador.

3.- Planteamiento del Problema

El objetivo de esta sección es definir cuál es el objeto que se debe resolver por medio de este trabajo de investigación. De la misma forma se delimitará aquellas cuestiones que deben ser respondidas por medio de todos los elementos que, en el transcurso de esta investigación deberán ser contestadas.

3.1. El problema

En el Ecuador existen varias empresas, pequeñas y medianas, las mismas que están reguladas por la Superintendencia de Economía Popular y Solidaria y la Superintendencia de Compañías Valores y Seguros, quienes manejan bases de datos con información que, la mayoría de veces es de índole personal de los clientes. Estas empresas y más aún las grandes, están expuestas todo el tiempo a que se les pueda sustraer base de datos relevantes mediante ciberataques, por lo que se deben establecer lineamientos para un adecuado manejo de esta información y así tratar de contener la sustracción de estos datos que hoy en día están muy vulnerables, no solo a nivel mundial sino también a nivel nacional. Aún es un ramo que no se ha puesto en práctica por la mayoría de aseguradoras, por la falta de cultura de seguros lo cual evitaría una llegada apreciable al mercado. Por eso, en primera instancia se debe tomar mecanismos preventivos para que esto no suceda, con el fin de proteger la estructura del banco de datos de la compañía y de sus usuarios, y si ya han restringido este sistema de protección, hay que verificar que se haya cumplido con las directrices aconsejadas, proceder con la recuperación y si es el caso con el resarcimiento de la información que fue vulnerada.

3.2.- Pregunta General de Investigación

- ¿ Cómo establecer lineamientos para un manejo adecuado de una póliza de ciberseguridad en Ecuador?

3.3.-Preguntas específicas de investigación

- ¿Cuál es el marco legal y regulatorio para las pólizas de ciberseguridad en Ecuador?
- ¿Qué debe contener la cobertura de una póliza de ciberseguridad?
- ¿Cuál es el alcance de la protección de la póliza de ciberseguridad?
- ¿Cómo lograr un buen costo- beneficio para empresas pequeñas y medianas que contraten una póliza de ciberseguridad?

3.4.- Efectos del problema

La exposición de datos confidenciales de los clientes, la desconfianza en los sistemas informáticos empresariales, las dificultades en la resolución de problemas y la comercialización de datos de clientes con sanciones económicas son desafíos que pueden causar impactos perjudiciales significativos. Estas situaciones pueden resultar en la pérdida de la confianza del cliente, afectando negativamente la reputación de la empresa y su relación con los clientes. Además, la sustracción de datos puede desencadenar casos de robo de identidad y fraudes financieros, ocasionando daños económicos a los clientes afectados. La falta de confianza en los sistemas informáticos puede traducirse en una disminución en la captación de clientes y la pérdida de oportunidades comerciales. Por otro lado, los problemas en la resolución de inconvenientes pueden generar insatisfacción entre los clientes, afectando la calidad del servicio proporcionado. En cuanto a la venta de datos de clientes con propósitos comerciales, esto puede vulnerar la privacidad de los clientes y generar preocupaciones sobre la seguridad de su información personal.

3.5.- Causas del Problema

A nivel mundial los índices de ataques cibernéticos han aumentado de forma significativa, y de igual manera la cantidad de ciberdelitos se han acrecentado en Ecuador en los últimos años. Una de las causas es la falta de cultura en cuanto al manejo y protección de sistemas informáticos, sobre todo a un nivel de pequeñas y medianas empresas. Este escenario ha generado a estos actores económicos en muchas ocasiones, estar expuestos a todos los peligros que existen hoy en día para las redes y sistemas de una organización.

El contar con métodos de protección contra ciberdelitos, como una póliza de ciberseguridad no es una prioridad para los sectores productivos pequeños y medianos, no cuentan con un producto estructurado de forma específica para ellos y que de igual forma pueda resultar viable y apetecible para la compañía de seguros.

3.6.- Escenarios

Los posibles escenarios que pueden desencadenar de una mala práctica de protección de datos en las pequeñas y medianas producto de los ciberataques es que:

En primer lugar se debe reconocer que ninguna empresa está exenta de sufrir un ataque a sus sistemas informáticos, por lo cual debe protegerse ante este contingente, el robo de esta información afectará directamente a la empresa y a los clientes, y podría desencadenar en problemas legales entre los intervinientes.

Si se llegará a producir el primer escenario y efectivamente exista la sustracción de la información se perdería la confianza al entregar información a una empresa por parte de los clientes y buscarían otras compañías que sí le puedan proveer del servicio de protección de sus datos personales, haciendo que las pequeñas y medianas empresas vayan perdiendo credibilidad y clientes.

Como nadie está exento de estos ataques y mucho menos las empresas materia de esta investigación y, si, efectivamente las compañías fueron víctimas de estos ciberataques, se debe analizar y resolver, ¿cómo se va a recuperar o restituir la información que fue vulnerada?, con esto se procura cuidar la reputación de la compañías y garantizar la protección de los datos a sus clientes.

4.- Revisión de la Literatura

Dentro del desarrollo de esta tesis se revisará literatura actual de autores muy relevantes que hablan y son especialistas en pólizas de ciberseguridad, en sus elementos, principios, definiciones y otras características que forman parte de este tipo de contrato de seguros enfocado en la protección de ciberataques que sufren las pequeñas y medianas empresa y que, ayudará al desenvolvimiento de este trabajo académico.

4.1.- CAPÍTULO I

4.2.- MARCO CONCEPTUAL

4.3.- Definición Ciberseguridad

Desde la existencia del ciberespacio se ha dado carta abierta para que dentro de la misma puedan existir varios puntos negativos, dentro ellos están los ciberdelitos, terrorismo, invasión en sistemas militares, de esta forma se ha creado un nuevo lugar que atenta contra la tranquilidad de las personas y a su vez ha obligado a todos los gobiernos a estar alerta sobre sus sistemas para que no puedan ser hackeados y de alguna forma que puedan robar información importante de cada una de las naciones. Al estar los ciberdelitos apegados a la tecnología y teniendo en cuenta que son muy dinámicas ya que se encuentran en constante cambio, la ciberseguridad y los medios para contrastarlos debe de igual forma ir adelante de cualquiera de estos delitos informáticos.

Para desarrollar más este tema se debe comenzar definiendo lo que es la ciberseguridad: ”En esencia, la ciberseguridad se dedica a la protección de todo aquello que se resguarda en el medio intangible del ciberespacio; en especial, información sensible referente a sistemas operativos, medios de comunicación, planes nacionales, innovaciones e infraestructura estratégica" (Arreola, 2019, 5).

Es así que la Ciberseguridad ha sido creada con el fin de proteger cualquier tipo de vulneración de los sistemas de tecnología y de los sistemas operativos, para ello se deberá utilizar varias herramientas tecnológicas que ayuden a que los ataques disminuyan y que no sustraigan información importante de las empresas, para esto se deberá crear varios antivirus y programas diseñados para proteger los sistemas informáticos que imposibiliten las sustracción o la invasión dentro de una base de datos.

4.3.1.- Fases de la ciberseguridad

Es decir la ciberseguridad se encarga de cuidar el ciberespacio de los delitos informáticos que se pueden presentar, esta seguridad de igual forma tiene algunas fases o procesos para realizar esta conservación de la información que se según Kassandra Ortega se desarrolla de la siguiente forma:

4.3.1.1 Prevención:

Esta etapa es importante ya que es el origen que nos permite cortar de raíz cualquier amenaza que se pueda presentar en el ciberespacio, el mismo que deberá contar con un plan de contingencia que puede disuadir un ataque fuerte a los sistemas informáticos, este debe ir de la mano con una creación de políticas de prevención para los usuarios finales y con una capacitación a las empresas o instituciones para evitar un resultado que pueda ser irreversible.

4.3.1.2.- Localización:

A pesar de que efectivamente uno de los primeros pasos es la prevención, se debe tener en cuenta que es un desafío muy grande el tratar de frenar estos ciberataques ya que las personas que son más vulnerables son los usuarios, empresas o instituciones, la gran mayoría de ellos no son expertos en ciberseguridad por lo que, para que no haya un impacto grande de estos atentados, se debe identificar de la forma más rápida posible, el origen del problema, para esto se debe contar con sistemas sofisticados que pueden eliminar inmediatamente el inconveniente que ya fue establecido.

4.3.1.3.- Reacción:

Ya que se ha hallado el problema se debe tomar decisiones inmediatas de cómo combatir la amenaza que se puede presentar, para ello, se debe seguir ciertos protocolos como; desconectar todos los sistemas, cambiar las contraseñas de todas las aplicaciones que se tengan dentro del sistemas y analizar que efectivamente el ataque se haya extinguido permanentemente, para posteriormente si es posible, recuperar los datos que se pudo haber perdido. Una vez solucionado el problema se debe instalar distintos programas como antivirus para esto no vuelva a pasar, y de igual forma se recomienda tener más cuidado en las páginas que se navegan, ya que no todas son seguras por lo que, hay que hacer mayor énfasis en las charlas y políticas de cuidado de los sistemas informáticos para que no exista esta venta de acceso a los ciberdelitos.

Es decir la ciberseguridad es un campo bastante amplio, encargado de proteger los datos de los usuarios,el objetivo principal es evitar posibles ciberataques que puedan infectar a los sistemas y robar datos importantes, para esto debe cumplir varias fases y al ser tan extenso debe abarcar varias ramas como; seguridad de los datos, seguridad de las aplicaciones, seguridad de la red, seguridad de la identidad entre otras ramas más.

4.4.- Tipos de ciberseguridad

Una vez que se ha revisado las fases de la ciberseguridad y la definición de lo que conlleva este concepto, se puede adentrar más sobre las características que debe contener un sistema de ciberseguridad para saber qué tipos de sistemas se van a proteger, dentro de los cuales se encuentran los siguientes:

4.4.1.- Ciberseguridad de Hardware

La ciberseguridad de hardware en pymes implica asegurar dispositivos físicos esenciales para las operaciones diarias. Las pólizas de seguro deben cubrir daños o pérdidas de hardware debido a ataques cibernéticos, ofreciendo protección financiera y asistencia para la reposición o reparación de equipos críticos. Hay que tener claro que el hardware es la parte de un computador o un ordenador que es perceptible al tacto humano es decir toda la parte física de un sistema operativo, en otras palabras es la estructura que contendrá todos los cables, circuitos, “carrocería”, dispositivos externos, entre otras, que cobijará al sistema intangible que es el software.

La ciberseguridad en hardware se refiere a la protección de los componentes físicos de los sistemas informáticos y dispositivos electrónicos contra amenazas cibernéticas. Esto incluye no solo las computadoras personales y servidores, sino también dispositivos integrados en la vida cotidiana, como teléfonos inteligentes, electrodomésticos conectados y sistemas industriales. (Fernández, 2023)

La protección del hardware se va a basar en el análisis previo de la construcción de las distintas estructuras y dispositivos externos a un ordenador, ver qué componentes son los que contienen que podrían facilitar la entrada de distintos ciberataques desde un alcance más íntimo, los dispositivos externos más comunes que traen virus con sigo, son las flash memories o usbs, que por lo general transmite programas malignos denominados troyanos y que al conectarlos a un computador se activan y dificultan su adecuado manejo, para evitar este tipo de ataques se deberá contar con sistemas antivirus que exploren el contenido de estos dispositivos externos y puedan lanzar una alerta que prevenga el contagio e infección de los sistemas operativos.

4.4.2.- Ciberseguridad de software

El software es el complemento perfecto del hardware para que un sistema operativo cobre vida, es decir es la parte interna de un operador, esto conlleva a una agrupación de varias herramientas y programas que cumplen órdenes específicas, para que el computador realice varías tareas que faciliten el trabajo de las personas en su vida cotidiana, de igual forma también existen ciertos sistemas y normativas ISO internacionales que han sido programados en distintos hardwares como lo son celulares o smartwatch que no solo facilitan el día a día de los seres humanos sino que también tienen otros fines como los recreacionales.

La ciberseguridad, al menos en teoría, defiende nuestros sistemas y reacciona contra los atacantes. Para defender nuestros sistemas se necesita promocionar un software seguro y, como se ha visto, para hacer softwares seguros se necesitan los puntos de vista del atacante y del usuario. Para reaccionar contra los atacantes es necesario también, como en cualquier batalla, tener en cuenta tanto el punto de vista del atacante como del defensor que en un sistema informático sería el usuario. Como se puede apreciar, en ambos casos se necesitan los dos puntos de vista. (Hidalgo, 2017)

El objetivo principal de los softwares es crear sistemas que tengan mayor seguridad y que se vayan actualizando de acuerdo a las necesidades de la persona en relación a los ataques cibernéticos que se van presentando, lo principal es que estos sistemas sean autónomos para no tener que emplear trabajo humano en ello, y que tengan el mismo dinamismo que los diferentes programas maliciosos que infectan a los ordenadores.

4.4.3.- Ciberseguridad de redes

Al igual que en los softwares y lo hardwares los ataques cibernéticos también se infiltran en los distintos sistemas de redes, especialmente en los procesos de emisión y recepción de información en donde mientras dura este proceso, los datos hasta llegar a su destino pueden tener varios percances y es ahí en donde se produce las sustracción de bases de datos, lo que produce que los datos lleguen incompletos, dañados o que no lleguen jamás a su destinatario. Estos ataques se pueden dar a entidades y organismos gubernamentales de gran importancia.

No existe ninguna tecnología capaz de hacer una red completamente segura. Una forma de reducir la exposición a pérdidas relacionadas con ciberataques es el desarrollo de planes de contingencia adecuados y probados. Además, deben establecerse planes de asistencia multimedia entre los diferentes componentes de infraestructura crítica, de modo que se reduzcan los efectos en cascada debido a su interrelación. (Puime, 2009, p.61)

Los ciberataques lo que buscan principalmente es robar la información y lo que protege la ciberseguridad de redes es eso, esta información puede ser robado o manipulado, mediante distintos virus que se pueden infiltrar en distintas redes particulares o gubernamentales que pueden afectar cierta clase de servicios, para esto se debe establecer de igual forma programas que puedan contraatacar a estos virus y tratar de impedir la sustracción de los datos informáticos y su operación.

4.4.4.- Ciberseguridad personal

Esta protección tiene una relación muy estrecha relacionada a las personas comunes y corrientes a cualquiera de las personas que usan aparatos electrónicos u ordenadores que tenga un software y que se los puede utilizar como comunicadores, los mismo que tienen mayor probabilidad de ser atacados directamentes por cualquiera de los ciberataques que, por lo general en estos casos se utiliza para el robo de los datos y la suplantación de identidad que se desarrollará posteriormente con mayor amplitud.

Análogamente, para las personas la ciberseguridad es esencial para proteger la privacidad y la seguridad financiera. Los ataques cibernéticos pueden llevar al robo de identidad, al acceso no autorizado a cuentas bancarias y al acoso en línea, lo que puede extenderse a la seguridad de las empresas, si estas no tienen prácticas adecuadas de protección de la información. (Rodriguez & Moreno, 2023, p.14)

El objetivo principal de la ciberseguridad personal es proteger los datos de las personas particulares, para estos se debe socializar una cultura de ciberproteccion y ciberseguridad que busca que las personas no entreguen su información en ningúna aplicación, ni recibir correos con contenido extraño o malicioso que pueden contener virus que pueden sustraer la información de las personas y que pueden desencadenar delitos más graves como la suplantación de identidad, pero no solo se puede robar la información sino también un hackeo de cuentas bancarias o de redes sociales, para eso se debe implementar herramientas que aseguren que sus datos no serán robados, como antivirus o aplicaciones que protejan sus correo y aplicaciones de los distintos virus que se pueden presentar.

4.4.5.- Ciberseguridad corporativa

Al igual que los particulares nadie está exento de los ciberataques mucho menos las empresas que manejan una pesada base de datos muy importante, la información que se maneja dentro de esta empresas puede tener diferente características desde lo más simple hasta lo más complejo como lo es el manejo de datos sensible y otros que no solo afectan la reputación de la empresa sino que afectan también a terceros en este caso los clientes de las compañías.

Una de las principales formas en el que los ciberdelincuentes operan es por manipular al personal de una organización; pueden engañarlos sin saberlo descargar malware en los sistemas de la empresa, abriendo a la organización hasta el control criminal, o directamente revelando información. Finalmente, y lo más descaradamente de todo, pueden persuadirlos de realizar instrucciones fraudulentas que creen han sido legítimamente dadas por sus superiores corporativos. (Quispe, 2021, p111)

De esta forma los ciberdelincuentes pretende robar la información o realizar actos que parecen reales pero son ajenos a la realidad, para prevenir estos tipos de ciberataques se deben tomar precauciones, como saber que tan seguro es descargar ciertas cosas, se recomienda que se lo haga de sitios oficiales, de igual forma que la empresa cuente con sistemas de antivirus que se encarguen de identificar los distintos virus que podrían infectar el sistema de la empresa adicionalmente se recomienda tener una persona encargada de realizar periódicamente informes de los ataques que haya recibido la empresa dentro de un periodo establecido.

4.5.- Definición de póliza de ciberseguridad

Actualmente se está dando una transformación digital que está cambiando de una forma dinámica y muy apresurada a la sociedad, en donde varios engranajes deben ir rotando a la misma velocidad, como lo es la economía, el ámbito social, la cultural y las leyes, las mismas que están entrelazadas para mejorar el desarrollo de cada una de estas. Pero no todo en este proceso de automatización es positivo ya que también existen varias amenazas a los sistemas y es por eso que se debe contar con un contingente que pueda dar respuesta a estos desafíos.

Este tipo específico de pólizas de seguro son contratos ante ciberriesgos, que vinculan y obligan legalmente a una compañía aseguradora ante la ocurrencia de determinados eventos definidos contractualmente que conlleven pérdidas, pagando una cantidad especificada (reclamación/siniestro) al asegurado. En contraprestación, el tomador del seguro paga una suma fija (prima) a la compañía aseguradora. “El contrato es firmado por ésta y el asegurado e incluye aspectos como los tipos de coberturas, límites y sublímites, exclusiones, definiciones y, en algunos casos, cómo se va a proceder a evaluar el nivel de seguridad del asegurado”. (Hernandez & Fojón, 2016, 98)

Estos contratos no son nuevos porque cumplen la misma función que los contratos tradicionales de seguros pero, se deben adaptar a los nuevos riesgos que se pueden producir en los ciberespacios. El objetivo principal de estos delitos es atacar a los sistemas informáticos de los asegurados que pueden ser personas naturales o una compañía, para realizar diferentes tipologías de delitos, la finalidad de las pólizas de ciberseguridad es transferir el riesgo a la aseguradora quien de varias formas cargará con los daños generados a raíz de estos ataques cibernéticos.

Es también importante mencionar cuando se puede activar la cobertura de este tipo de pólizas de seguro. En primer lugar, el daño que se pudiese generar por una pérdida o robo de información que provenga de manera directa por el actuar culposo o doloso de una persona no es materia en sí de este servicio de seguros. Esta aclaración proviene precisamente de la duda que se pudiese generar al revisar que la póliza habla de protección de datos personales, seguridad de la información y cobertura de daño reputacional contra los eventos que estas generen. De forma fáctica, en una póliza de seguros contra ciberdelitos, lo que se protegerá son los sistemas informáticos de una entidad, y la protección será contra ataques cibernéticos. Los ataques estarán fijados ante aquella información que contengan los sistemas informáticos de estas compañías, es así que se hablará de la mitigación de daños que devienen de la pérdida de todo aquel contenido que acumulaba una empresa de forma cibernética. No se debe confundir un acto malicioso al interior de una organización con un ataque fortuito que puedan sufrir los sistemas de las mismas.

4.5.1.- Elementos

El siguiente tema va a tratar de los elementos que tiene una póliza de seguro. A pesar de que este trabajo habla de manera específica sobre un tipo de póliza, el de ciberseguridad, los elementos son casi idénticos y muy similares entre todas las pólizas. Estos elementos son aquellos que permiten que este tipo de contratos tengan su distinción. A estos elementos se los va a abordar desde dos tipos, unos formales y otros materiales.

La formalidad en el sector de seguros, al ser muy delicado y hablar de la protección patrimonial del asegurado, suele venir de la mano de aquellos requisitos que sean estipulados por ley y por lo dictado por aquel órgano que funja como ente de control, en el caso específico de Ecuador se habla de la Superintendencia de Compañías Valores Y Seguros. Sin embargo, de forma doctrinaria y dogmática se pueden encontrar ciertos elementos que, sin distinción del lugar donde se esté suscribiendo o ejecutando una póliza de seguros, siempre van a existir.

En primer lugar va el asegurado, esta persona es la que se obligará en la póliza de seguros. Doctrinariamente se habla de la figura del tomador, que es aquella persona que al realizar la contratación con la compañía de seguros, se obliga al pago de la prima, sin embargo en Ecuador, en la Ley General De Seguros (Código Orgánico Monetario y Financiero Libro III), no existe esta figura, solo la del asegurado como aquella persona que afronta las obligaciones derivadas de la póliza de seguros. El último elemento es el beneficiario, este no contrata directamente con la compañía aseguradora, simplemente es quién en caso de una indemnización por el reclamo de un siniestro, recibirá la suma asegurada. Como elementos materiales se va a tomar a dos fundamentales, la prima y el riesgo. De estos dos se va a tratar a continuación.

4.5.2.- Bien Asegurado

El primer elemento del cual se deberá hablar es el bien asegurado. Este es el elemento que se verá protegido en la póliza de seguros. Cuando se habla de los elementos que debe tener un contrato, objeto lícito, causa lícita y capacidad; el bien asegurado vendría a ser el objeto. De esto dependerá en su totalidad la clase de póliza que se utilice, además de que se definirá la forma en la cual vayan a ser planteados los términos de esta misma y el resto de elementos de la póliza.

Este elemento al ser aquello protegido por el contrato de seguros tiene su conexión con el asegurado y la aseguradora a través de un factor vital, el riesgo. “Elemento básico entre éstos está el riesgo, es decir la probabilidad de que un evento, cuya verificación se debe al azar perjudique en determinada forma al asegurado”. (Barrientos, 2015, p.3). Así es el vínculo entre aquellas partes que suscriben la póliza de seguro, no obstante el punto central siempre será el bien asegurado. No siempre este elemento es el mismo, como se mencionó anteriormente, esto depende, es por tal motivo que es imprescindible el describir cuál es el bien asegurado en las pólizas de ciberseguridad.

En este trabajo, se habla de un modelo relativamente nuevo de seguros, el de ciberseguridad. Pero hay que tener en cuenta que el bien asegurado aquí es más que solo un cuerpo físico como una persona, un inmueble o un vehículo, igualmente es más complejo que tan solo un activo financiero como en una póliza de fianza. Aquí se protegen varios puntos, en primer lugar los sistemas de una organización, y derivado de esto viene la mitigación de todo el daño que se causa a raíz de un ataque cibernético. La información que contienen los equipos informáticos así como todo el core digital de operaciones, que hoy en día es la base para miles de negocios sean grandes o pequeños. Y un punto clave, es apaciguar el daño reputacional, pues a raíz de un ciberataque existe una emergente desconfianza de los usuarios clientes, pues tienen la visión de un eminente peligro al entregar su información personal a una empresa que no ha podido cuidarla. En conclusión, el objeto que se pretende proteger con este tipo de pólizas viene a ser un conjunto de todo lo que implica el manejo digital de las operaciones de una empresas, no es un concepto sencillo de describir al abarcar más de un tema a cubrir.

4.5.3.- Riesgo Asegurable

Una vez que se sabe el objeto sobre el cual recaerá la póliza de seguros, ahora se debe analizar lo que se está protegiendo concretamente, es decir el riesgo que existe de que suceda algún siniestro. A este elemento también se le puede llamar estado de riesgo que es “El estado del riesgo es el conjunto de circunstancias relevantes que determinan el grado de posibilidad de que ocurra el evento dañoso” (Carrión, 2021, p.11). Es este elemento donde se constituyen factores altamente relevantes como el valor asegurado, las exclusiones y las condiciones bajo las cuales actúa la póliza o va a actuar la póliza en caso de que se genere el siniestro.

Hay que tener en cuenta que una póliza de seguros y en general todo el sector asegurador gira en torno al factor de riesgo. Las compañías de seguros tienen como función tomar a cargo este factor a cambio de un pago, es decir la prima. Hoy en día este riesgo debe ser calculado, pues no todos estos valen la pena tomarse y eso marcará la existencia de un ramo, su contrato y el precio de este servicio.

Al ser el tema principal de este trabajo una póliza de ciberseguridad, se hará la revisión de este tipo de riesgo de las varias aristas por las que se pueden generar estos ataques. Hay veces que un ataque cibernético puede ser previsto y su daño podría haber sido mitigado o incluso evitado en su totalidad. En otras ocasiones, el impacto causado es imprevisible, probablemente imposible de mitigar o rehuir. Es aquí cuando se presentan las diferentes vías por las que se produce este riesgo, un correo malicioso, un malware inesperado, algún tipo de dispositivo que podría haber estado contagiado. Más adelante se revisará de forma individualizada algunos de los tipos de ciberataques más comunes y los cuales estarán dentro de la cobertura de esta póliza.

Un tema fundamental tanto para la compañía aseguradora, como para el asegurado es el análisis de riesgo. Eventualmente se tendrá que incluir dentro de los procesos relacionados con la ciberseguridad estas medidas, a fin de poder evaluar las amenazas latentes con respecto a este tema. Para los fines de este trabajo es importante señalar que se revisará este tema desde la perspectiva de la aseguradora y desde la perspectiva del asegurado.

a) Análisis de riesgo de la aseguradora.

En el sector de seguros hablar de riesgo es un tema principal, que ha venido siendo parte de su actuar por un largo periodo de tiempo. Esto se da en virtud de su función misma de trabajar con el traslado del riesgo desde el asegurado hacia la compañía de seguros, es por esto que aquí no solo se toma el factor de analizar los riesgos, las empresas de seguros y reaseguros, quienes manejan fuertes capitales, mismos que son destinados a cubrir las indemnizaciones producto de este sector financiero, realizan todo aquello que trata sobre una gestión de riesgos, que es integral.

Todo este proceso integral abarca el reconocimiento y evaluación de varios factores de la empresa. “Como sistemas integrales de gestión de riesgos se entiende el desarrollo e implementación en las organizaciones de sistemas de gestión de riesgo internos que abarquen mercados, productos y procesos, y que requieren una integración exitosa de análisis, gestión y tecnología” (Hernandez, 2013, p.65). Este tipo de procedimiento es aún más integral, es decir que el análisis de riesgos es una parte de la gestión.

Por el tipo de negocio que son los “seguros”, las empresas que se dedican a esta clase de actividad están acostumbradas a realizar un debido proceso con respecto al riesgo asumido. El ser negligente acerca del riesgo que es trasladado a una aseguradora o reaseguradora puede implicar la vida o la muerte de estas entidades. Es por esta razón que, el tener una gestión debidamente llevada es la clave para el éxito en este ramo del sector financiero, un ramo de alta peligrosidad y complejidad sin una administración correcta en lo que a peligros del giro del negocio respecta.

b) Análisis de riesgo para el asegurado

Para esta parte, la cual vendría a ser aquello que concierne y es obligación del asegurado, se tratará en general del análisis que se debe llevar con relación a la ciberseguridad. Es verdad que tener un departamento exclusivo para esta materia es un asunto prácticamente imposible para una pequeña y mediana empresa (aquellas que son materia de este trabajo), pero el personal existente dentro de estas entidades debe considerar el llevar una debida diligencia en este aspecto. Es así que, en un mundo globalizado y altamente influenciado por las TIC (tecnologías de la información y comunicación), todas las compañías, sin importar el giro de su negocio deben tener en cuenta que hay riesgo en aquello que involucra el uso de redes y sistemas informáticos.

Los factores de riesgo, así como la naturaleza de los diferentes riesgos que enfrentan las organizaciones son diversos. Por ejemplo, los riesgos son provocados por fenómenos naturales, tecnológicos, estratégicos, económicos, políticos, comerciales y sociales(…). Pero no solo las fuentes de los riesgos que enfrentan las organizaciones son variadas, sino también su carácter es muy diverso (Alonso & Berggrun, 2015, p.VII).

Todos estos aspectos son aquellos que deberán ser analizados por una empresa para una gestión de riesgos. Evidentemente el factor tecnológico es parte de esta evaluación, sin la cual no es posible que exista o quizá no debería existir el core digital de operaciones de una compañía. Como se menciona anteriormente, el tener un análisis de riesgo en cuanto a los peligros tecnológicos y ciberdelitos que estos conllevan se torna obligación de la administración de cualquier entidad comercial, sea cual sea el giro de su negocio ya que la tecnología y el uso de redes y sistemas informáticos es transversal a todas las actividades que hoy en día se realiza.

4.5.4.- Prima

Una vez que se han determinado los dos primeros elementos de la póliza de seguros, es decir el bien asegurado y el riesgo asegurable o estado de riesgo, se puede definir el precio de la póliza. A este elemento se lo llamará prima, que es “El monto establecido debe ser pagado por el tomador en las condiciones acordadas por ambas partes. Este monto puede cambiar de forma significativa de una empresa de seguros a otra y de un usuario a otro, de acuerdo con el tipo de riesgo asumido.” (Pérez, 2022, p.1). Es importante recalcar que este valor será cancelado de igual forma dependiendo del tipo de contrato, en el caso de los seguros de asistencia médica es común que el pago sea mensualizado, mientras que en un seguro como el de vehículos o seguros de inmuebles los pagos suelen ser anualizados, en el caso de fianzas es un pago mientras dura la obra.

Es vital entender que el cálculo de la prima de una póliza de seguros, es un valor que cambia de forma constante, sus variaciones no sólo se generan en virtud del tipo de póliza que se esté contratando, también se calculará la probabilidad de que se genere el siniestro, así como la frecuencia con la cual haya sucedido anteriormente.Con esto se quiere hacer entender que de este cálculo se tendrá el valor del contrato de seguro. Puede ser el mismo objeto asegurable, pero a raíz de una alta siniestralidad puede cambiar el valor de la prima, pues la compañía de seguros debe tener rentabilidad y a mayor riesgo, mayor será el precio a pagar por la prima.

La estadística nos da el precio o valor del seguro, puesto que nos da a conocer sobre cuántos eventos posibles se verificará un siniestro, ya que el valor total cobrado al neto de los gastos, debe de servir para cubrir los siniestros ocurridos (Barrientos, 2015, p.3).

Con esto se quiere hacer entender que de este cálculo se tendrá el valor del contrato de seguro. Puede ser el mismo objeto asegurable, pero a raíz de una alta siniestralidad puede cambiar el valor de la prima, pues la compañía de seguros debe tener rentabilidad y a mayor riesgo, mayor será el precio a pagar por la prima.

En una póliza de ciberseguridad el valor de la prima dependerá de varios factores, sobre todo cuando se hable de pequeñas y medianas empresas. El manejo y cuidado que se le dé a los sistemas de seguridad de estas entidades es un factor de importancia alta, pues en virtud de este punto se podrá realizar una consideración de cuán probable es que una empresa sufra un ciberataque. Y de manera fundamental, si ya ha sufrido una vulneración a los sistemas y la compañía de seguros ha indemnizado a una empresa al renovar el contrato el valor de la prima cambiará por un factor estadístico.

4.5.5.- Intervinientes

Para hablar de quienes intervienen en el contrato de seguro, hay que tener en cuenta 3 actores principales.

4.5.5.1.- La aseguradora: Dentro del sector de seguros la parte que da sentido a todo el giro de este negocio es la compañía aseguradora. “La compañía de seguros, como la entidad autorizada legalmente que asume los riesgos a cambio del pago de la prima por parte del tomador” (Giraldo, 2022. p.1). Este tipo de ente deberá estar autorizada por el órgano competente, su actuación y constitución depende de aquello mencionado en la “LEY GENERAL DE SEGUROS (CÓDIGO ORGÁNICO MONETARIO Y FINANCIERO LIBRO III)”. El rol que cumplen estas compañías es fundamental en la sociedad, transmiten el riesgo y de tal manera se encargan de proteger el patrimonio de una persona natural o jurídica. De esta forma se llega a considerar a las empresas de seguros como parte del sistema financiero de un país.

Este tipo de entes son aquellos con quien se contrata cuando existe una póliza de seguros de por medio. Las compañías de esta clase tienen como función aceptar el riesgo, o más bien dicho un porcentaje de este al suscribir un contrato de seguros. Su función dentro de una sociedad es de tal relevancia que ciertas actividades, donde el miedo de empezar cierto proyecto impide la inversión, el generar nuevas plazas de trabajo, así como el ofrecer productos nuevos, pueden ser realizadas, dando así una mejor perspectiva a los inversionistas y emprendedores.

"La externalización puede reducir los costos de transacción cuando los costos de organizar una transacción dentro de una empresa son más altos que los costos de realizar la transacción en el mercado". (Cose, 1937, p.386). Así, Ronald Cose, de manera indirecta daba una pauta para que las empresas pudiesen distribuir los riesgos inherentes a su giro del negocio. Las aseguradoras por su mismo desarrollo comercial buscan que los costos de transacción en la sociedad puedan reducirse, llegando así entes vitales en sociedades donde la industria, el comercio y su desarrollo dependen de la reducción o mitigación del riesgo.

En el caso específico de este trabajo las empresas aseguradoras son a quienes se les transfiere el riesgo por los ataques cibernéticos que pudiese sufrir los asegurados. Estas compañías no han cambiado su función de manera general a lo largo de la historia, sin embargo las amenazas que emergen con el surgimiento de nuevas actividades económicas sugiere para estas compañías y el mercado sobre todo la necesidad de trasladar los peligros que se generen. Es así que se podrá analizar en este trabajo los criterios que debe tomar una empresa de seguro al suscribir una póliza de ciberseguridad, en especial para pequeñas y medianas empresas.

4.5.5.2.- Asegurado: De manera doctrinaria, y cómo se había hablado anteriormente, se hace referencia a la figura del Tomador, en virtud de que nuestra legislación no lo menciona, se hablará únicamente del asegurado. Esta es la parte contratante con la aseguradora y quien solicita el traspaso del riesgo hacia la compañía de seguros. "El contrato de seguro frente a los derechos de los consumidores es una temática que tomó importancia a partir de que el contratante, sea asegurado o beneficiario, se lo veía como la parte "débil" del contrato frente a las compañías de seguros" (Carrión, 2021, p.2). Esto se debe a un tema de información con relación al asegurado, el asegurado, si bien es quien paga la prima, no deja de suscribir un contrato hecho por la compañía de seguros, y aunque la ley lo faculte, en la práctica existe muy poco poder del asegurado para poder negociar las cláusulas existentes en un contrato de seguros.

De este último concepto se habla de debilidad de una parte por cuanto, no solo hay información que posee la aseguradora que usualmente no tiene el asegurado, sino que este último entrega sus datos personales y en determinados casos, sensibles a esta compañía. Es evidente que la empresa de seguros no puede trabajar sin que se le sea proporcionada esta información, sin embargo el uso que hace con esta frente al cliente genera una evidente responsabilidad, los ficheros donde están asentados estos deben ser tratados con la debida responsabilidad, la cual deberá regirse por la ley.

El asegurado es sobre todo en nuestra legislación el cliente directo con la aseguradora. En muchas ocasiones este resultará beneficiario de los servicios y en caso de que vaya a existir, de la indemnización. Sin embargo, en muchas ocasiones esta parte se encarga de suscribir el contrato con la compañía de seguros, pero en caso de existir un pago por concepto de un reclamo recibido, este tendrá otra persona que reciba este mismo, a la cual se le llamará beneficiario.

4.5.5.3.- Beneficiario: La siguiente figura de la cual se va a tratar es aquella que sin necesariamente haber suscrito la póliza de seguros con la compañía aseguradora recibirá los beneficios en caso de haber existido un reclamo. “Este último es quien recibe el pago por el riesgo asegurado en caso de que pudiese haber un siniestro generado, es la parte a la cuál le corresponde la reparación por la transferencia del riesgo” (Giraldo, 2022. p.1). El beneficiario no necesariamente sufre el impacto del riesgo asegurable, no directamente en todo caso, sólo recibe la indemnización que pueda corresponder en un caso suscitado.

Es importante hacer hincapié en esta figura, sobre todo por el tipo de póliza de seguros tratada en este trabajo. La responsabilidad que tenga el asegurado, misma que podría verse plasmada en una obligación de pago a un tercero, convertiría a esta parte en el beneficiario de la póliza. No es quien adquiere el riesgo de la actividad, pero sufre las consecuencias de algún tipo.

Esta figura se vuelve de mucha relevancia en pólizas donde existe responsabilidad civil frente a terceros. Más adelante se hablará de forma más específica de la dinámica que existirá con la póliza de seguros de ciberseguridad, y este concepto del beneficiario será de alta importancia tenerlo comprendido, pues aunque no sea el asegurado, será la persona a quien se le otorgue un resarcimiento al darse un ataque cibernético del cual llegue a tener una responsabilidad la compañía.

4.5.5.4.- Tomador: Este es un elemento del cual se habla frecuentemente a nivel doctrinario, sin embargo en la legislación ecuatoriana no se habla de manera específica de la figura del tomador, sólo de asegurado y beneficiario. Aquí hay dejar en claro la diferencia entre la figura del asegurado y el beneficiario, como se dijo anteriormente, esto es de forma doctrinaria. “El tomador del seguro es aquella persona que lo contrata, es decir, el titular del mismo. En cambio, el asegurado es la persona que queda protegida por las coberturas contratadas.” (Torroba, 2023. p.1)

Es importante resaltar que el legislador ecuatoriano no consideró relevante separar la figura del tomador con el asegurado. El motivo para que se haya tomado esta decisión pudo haber sido la dificultad para separar los conceptos de asegurado y tomador. En palabras sencillas el tomador es solo la persona que suscribe el contrato. La pregunta es en qué se diferencia con asegurado cuando este puede también ser el contratante y tener a otra persona como beneficiario. De esta manera se podrá tener más claridad al entender las partes que intervienen en el contrato de seguros.

4.5.5.5.- Corredores de seguros: Los anteriores son los actores principales, y los que siempre serán parte del contrato de seguro. Sin embargo hay veces donde actúan los intermediarios de seguros o brockers, también llamados corredores de seguros. “Son corredores de seguros las empresas que se dedican exclusivamente a ofrecer seguros, promover su celebración y obtener su renovación, siendo intermediarios entre el asegurado y la compañía de seguros” (Giraldo, 2022. p.1). Aunque se debe decir que estos últimos no constituyen un elemento esencial de las de las pólizas de seguros, pues muchas veces la contratación de la póliza se dará de forma directa entre la compañía aseguradora y el asegurado.

Existen evidentes beneficios cuando hay un corredor de seguros, pues el asegurado cuenta con una compañía o una persona natural que se encargará de asesorar en caso de generarse un siniestro. Sin embargo esto no quiere decir necesariamente que es imprescindible, pero sí recomendado, en especial para aquellos usuarios que tengan poco o nulo conocimiento respecto a este tema. El corredor de seguros, al ser una empresa que tiene contacto con la aseguradora y asesora al cliente, puede ser el punto que reduzca la diferencia de información entre la aseguradora y el cliente.

Esta clase de intervinientes no son indispensables para que pueda darse el contrato de seguro, pero definitivamente son importantes para ambas partes. Por parte de la aseguradora permiten generar conexión de forma más fácil con los clientes, ayudando así a reducir gastos de publicidad y en ciertos casos comerciales. En cuanto al cliente, como se había mencionado en el párrafo permiten que el asegurado y el beneficiario tengan una adecuada asesoría de sus derechos al tener una póliza de seguros y así poder ejercer sus derechos como clientes de mejor forma.

4.6.- Principios que rigen las pólizas de seguros

Los principios son una de las fuentes del derecho que generalmente sirven como mecanismos de interpretación, que dan origen a una norma y se utilizan en las pólizas de ciberseguridad, las mismas que deben contener varios elementos sustanciales que guiarán su mejor desarrollo y control, en el Ecuador y, son los siguientes:

4.6.1.- Legalidad

La legalidad es uno de los principios que más se han usado en el campo del derecho, el objetivo principal de este es que sirve como una herramienta jurídica para interpretar el contenido de los distintos contratos, en este caso si es que existiera una controversia seria de gran apoyo al aplicarlo en la póliza de ciberseguridad y poder verificar su alcance.

Este principio se refiere a que todos los actos o contrato deben estar apegados a la normativa estatal, esto es la Constitución de 2008 y sus normas infra constitucionales, no pueden bajo ningún concepto establecer algo que sea contrario a estas y siempre deberá respetar su jerarquía normativa y a las autoridades correspondientes quienes serán las encargadas de realizar un control de acuerdo a sus competencias. (Islas, 2009, p102)

Es decir, los contratos de seguro deben cumplir todo lo que ya se encuentra establecido en las ley infraconstitucionales y en la Ley Suprema, dichos contratos no podrán estar por encima de ninguna estas normas por el contrario deben ser concordantes a las mismas y constituidos en estricto respeto al derecho y a los tratados internacionales, al igual que el caso de las pólizas de ciberseguridad, deben estar limitadas a la ley de protección de datos, su reglamento y demás normas superiores.

4.6.2.- Buena fe

La buena fe es inherente al estado de ánimo de una persona que está ejerciendo un derecho o una obligación, el mismo debe estar acorde a las buenas costumbres que establece la sociedad, es decir lo que es correcto moralmente para el resto de persona y sin la intención de causar algún daño, este principio generalmente se lo debe aplicar de forma objetiva y sin dejar espacio a interpretación de lo que se entiende por este concepto.

Este principio hace relación a la actuación tanto de la aseguradora como la del asegurado, esto en consecuencia a la información que deberá entregar el cliente de forma voluntaria y, que deberá estar acorde a la realidad de sus vida diaria tanto antes conservar el contrato cuanto después que se pueda dar un siniestro o un contingente, de igual forma la aseguradora deberá explicar con claridad el contenido del contrato de seguro. (Nuñez del Prado, 2011).

Se debe tener en cuenta y muy claro que si el asegurado faltare a la verdad al momento de entregar su información sobre cualquier tipo de contrato de seguro que vaya a firmar, la aseguradora tiene toda la libertad de dar por terminado el contrato y solicitar que dicho contrato se declare nulo, lo mismo aplica a la persona o empresa que no de toda la información veraz sobre los datos que manejan, tanto el individual como el corporativo y que clase de datos son los más importantes y su utilización

4.6.3.- Principio de interés asegurable

El interés asegurable aparte de ser una de los principios más relevantes de la póliza de ciberseguridad a su vez es un elemento material muy importante que consiste en la estrecha relación que hay entre el asegurado y bien asegurable que está expuesto a algún riesgo y que sin este elemento el contrato carecería de algún tipo de validez.

Este principio hace una relación directa entre el bien asegurable y el valor que sobre el cual se lo va a asegurar, se deben tener en cuenta varios factores para realizar este análisis en cuanto a los riesgos que el bien asegurado puede llegar a tener y la utilidad para la cual está destinado el bien. (Nuñez del Prado, 2011)

En el caso de la pólizas de ciberseguridad se debe observar plenamente los riesgos a los que pueden estar expuesto los cliente ya sean estos persona naturales o empresas y ver otros factores adicionales que estén relacionados con las bases de datos que ellos manejan de su propia cartera de clientes y sobre todo el objeto social que tiene la compañía.

4.6.4.- Principio de indemnización

Hace referencia a la cantidad que se le entrega al asegurado a cambio del bien siniestrado o que tuvo algún tipo de afectación, este monto será entregado en la moneda de curso legal, haciendo referencia al valor actual del bien que esté en litigio y se deberá tomar en cuenta algunos factores como el estado del bien, la devaluación del bien, accesorios adicionales del bien, entre otros, al igual que el principio anterior este elemento dentro de la póliza es muy importante ya que si no consta este podría acarrear la nulidad de dicho instrumento.

“El principio de indemnización norma y es la base para determinar la cantidad que se pague.” (Nuñez del Prado, 2011, p.54)

Este principio regula la esencia del contrato de seguro y cuyo objetivo principal es transferir la obligación principal del asegurado a la aseguradora, por los daños que este haya causado o por los daños que a él le han provocado, el cual deberá pagar un porcentaje de acuerdo a la prima establecida por el usuario para que se le repare los daños. (Nuñez del Prado, 2011, p.54)

Se maneja de igual forma como en cualquier tipo de póliza ya que es un principio básico, lo que se debe tener en cuenta en los casos de ciberataques es que se pagará una prima en dos situaciones, la primera en caso de recuperación de la información y en segundo lugar, en caso de restitución que deberá ser calculado acorde al costo de pérdida, es decir al impacto del daño.

4.6.5.- Principio de contribución

La contribución consiste en una estrategia que puede utilizar el asegurado, contratando dos o más empresas aseguradoras que se encarguen de asegurar un mismo bien y, que en el momento que lo necesite el asegurado, traslade la responsabilidad a las aseguradoras que haya contratado, para que sean ellas las encargadas de dividirse los pagos del siniestro o daño que se causó, es decir que se pague la indemnización y el valor de la prima.

Esta muy apegado al principio de indemnización y hace referencia a que el asegurado ha contratado varias pólizas de seguro para que aseguren a un mismo bien quienes posteriormente deberán dividirse la responsabilidad entre las demás compañías de seguro, y es el cliente quien decidirá si cobrarles la obligación a todas o solo a una aseguradora. (Lacy, 2022)

El principio de contribución tiene una relación muy estrecha en base al labor que deben tener las aseguradoras cuando el asegurado tiene contratado dos o más pólizas de seguros con distintas empresas de seguros, dentro de la cual el asegurado debe elegir cual de estas empresa debe cubrir el porcentaje principal al momento de restituir la información o recuperarla y quien será la encargada de pagar el costo de la prima de la otra empresa.

4.6.6.- Principio de Subrogación

El objetivo principal por el que las compañías contratan a una empresa de seguros, es porque se busca que protejan la base de datos de las pequeñas y medianas compañías, cuya información es muy importante y si sufren un ciberataque pueden perder la confianza de los clientes y de esta forma tener menor credibilidad, para que esta empresas tenga la tranquilidad, la aseguradora presta servicios de ciberseguridad y, de esta forma las pequeñas y medianas empresas trasladan la responsabilidad de la protección de los datos e información de sus empresas a las aseguradoras quienes serán los encargados de recuperar y restituir la información robada quienes verán la forma de realizarlo.

Este principio hace referencia a que si la aseguradora ya ha compensado por el valor asegurado del bien al asegurado principal, la aseguradora podrá tomarlo como propio dicho bien únicamente hasta el valor por el cual fue asegurado, es decir el bien pasaría a ser de propiedad de la compañía de seguros. (Lacy, 2022).

Es decir que en el caso de que ya se haya restituido o compensado de una forma distinta el valor del bien asegurable y la aseguradora haya recuperado la información o en el caso de bienes muebles e inmuebles, recuperado la propiedad y al haber ya cancelado el valor de indemnización, podrá ser el dueño de los datos o por el contrario dueño del bien mueble o inmuebles para esto la empresa de seguros podrá hacer lo que quieran con estas propiedades.

4.6.7.- Principio de minimización de pérdidas

Le corresponde a las aseguradoras brindar la información correcta, veraz y digeribles a sus asegurados, con el único fin de que sus clientes sean los principales actores en la protección de su información y base de datos para que a su vez estas pequeñas y medianas empresas sean el primer filtro de seguridad para custodiar sus bancos de datos si el daño ya se hubiese efectuado los encargados de la atención del primer filtro básico de las empresas serán quienes brinden todos los antecedentes de los hechos de la sustracción de la información.

Este principio tiene la gran parte de la responsabilidad el asegurado ya que una vez que haya ocurrido el contingente, el cliente deberá ser el encargado de no agravar más el hecho que se haya suscitado y por el contrario colaborar en todo lo que se puede presentar para evitar posibles problemas que puedan afectar al asegurado o a su vez a terceros. (Lacy, 2022)

Una vez entregada toda la información a la aseguradora y colaborando durante todo el proceso, la encargada de investigar y llegar al origen de quien o quienes robaron dicha información será la empresa de seguros quienes deberán contar con el contingente necesario para realizar todas las diligencias.

4.6.8.- Principio de causa directo

Los trabajadores de las pequeñas y medianas empresas quienes son el primer filtro de seguridad, una vez que se haya suscitado la sustracción de la información serán quienes proporcionen de manera detallada los hechos a la aseguradora para que sean ellos quienes determinen cuál fue la causa principal por la que existió este robo de información y no tener especulaciones falsas.

Se refiere a la causa de la contingencia inmediata es decir que si existe varias problemáticas dentro de un siniestro se deberá analizar cual de estos problemas es el principal que por efecto del mismo derivó en los demás problemas que por lo general se lo hace contra bienes de tercero o tambien sobre la humanidad de terceras personas. (Lacy, 2022)

Para poder aplicar este principio se debe tener con claridad y exactitud cual fue la causa principal de daño o sustracción de la base de datos para poder identificar la responsabilidad del mismo y descartar causas secundarias que hipotéticamente pudieran haber causado el daño y de esta forma retrasar el proceso de indemnización o la culpa del asegurado o terceros.

4.7.- Tipos de ciberdelitos

El punto clave dentro la póliza de ciberseguridad son justamente los ciberdelitos, es decir, son el riesgo asegurable. Aquí se va a tratar acerca de cuáles son los delitos cibernéticos más comunes hoy en día. Durante varios años, y como se había tratado previamente en este trabajo, las amenazas cibernéticas son un tema que existe desde los años setenta del siglo XX, no obstante, con el constante avance de la tecnología se puede denotar que estas amenazas avanzan a un ritmo considerablemente superior al de la ciberseguridad. Esto deja a los sistemas en un constante y evidente riesgo, de ahí viene la necesidad de protegerse de los estragos que puedan causar estos ataques, no siendo posible el evitarlos en toda situación.

A continuación se hablará de forma específica de ciertos ciberataques que hoy en día resultan más comunes. No obstante cabe mencionar que “Una primera clasificación distinguiría entre los delitos que tienen su origen en técnicas de ingeniería social y los que tratan de aprovecharse de vulnerabilidades de los sistemas. No obstante, en algunos ciberdelitos se combinan ambos orígenes” (Alcivar; Calderon; Blanc. 2016, p.39). Es por tal motivo que se va a analizar los virus que de forma violenta vulneran los sistemas informáticos de una empresa y también aquellos que llegan a causa de un engaño a alguien o de la negligencia en el manejo de la ciberseguridad.

Es de vital importancia realizar el análisis entre ataques según su origen. El realizar esta diferenciación nos ayudará a entender varios puntos importantes dentro del cuidado que debe mantener una organización en cuanto al manejo de su IT. Por ambos canales quedará expuesta la información que protege de manera digital una compañía, y existe la manera de prevenir o en realidad, de tener un cuidado mayor para que ambos se den.

4.7.1.- Malware: Cuando se habla de ciberataques, se puede encontrar varios tipos y en varios canales. Sin embargo el principal y más genérico es el malware. “La palabra define un tipo de software que tiene como objetivo infiltrarse en un equipo o sistema informático sin el consentimiento del usuario. (Pérez, 2015,p.1)

Entonces se puede ver, que de forma más usual, un ciberataque en su mayoría será un malware, pues vendrían a ser programas informáticos que de manera intencional quieren herir al usuario, simplemente dañando sus sistemas, robando su información, extorsionando a este a cambio de la devolución de su información, etc. Más adelante se va a revisar ciertos tipos de ataques digitales, los mismos que en su gran mayoría vendrán ligados a un programa que tenga por finalidad el causar un daño o incluso, llegar a ser un delito.

Es importante, al ver que el malware es el término que puede definir en sí al problema del ataque digital, definir como entre el resto de amenazas se diferencian unas de otras. Un virus siempre será un malware, pero no todo malware será un virus, pues el definir a un ataque como virus o no va de la mano con su poder de infectar y reproducirse de un sistema a otro. El término malware se torna de tal amplitud que usualmente se requiere diferenciarlo, para ver qué tipo de daño o ataque se está hablando.

Es así que la definición antes realizada entre el origen que tienen las ciberamenazas es importante realizarla, pues hay veces que el malware se dará siempre y cuando existe un engaño a una persona que se encuentre manejando un sistema informático, y en otras ocasiones el daño tendrá un origen en un sistema vulnerable, desactualizado o falta de “debida diligencia” dentro de los estándares de cuidado y protección de tecnología de la información dentro de una compañía.

4.7.2.- Phishing: Este tipo de amenaza cibernética es la forma de apoderarse de los datos personales de quien se encuentra en internet, al abrir un correo electrónico o un mensaje de alguna fuente desconocida. Evidentemente se pueden evitar teniendo la precaución de no abrir correos extraños y siempre borrando aquellos correos de los que se desconfía el destinatario. Sin embargo, la cantidad de información que se recibe a través de un correo electrónico impide tener precaución para evitar que lleguen estas amenazas a nuestros sistemas informáticos.

Es una técnica que se utiliza para duplicar una página web o manipular el diseño de correo electrónico logrando que cualquier enlace que generen los phishers parezca legítimo y así hacen creer al usuario que se encuentran en una página oficial y que el correo que reciben proviene de una identidad segura y lo utilizan generalmente en páginas de instituciones bancarias para poder tener el login y la contraseña del cliente de la institución y así poder realizar diversos delitos. (Alcivar; Calderon; Blanc, 2016, p.37).

Este es un tipo de delito que se desprende de un “engaño” a una persona. De cualquier forma aquí existe una vulneración a un sistema informático, que no proviene en sí de una disrupción en un sistema informático, de forma exclusivamente violenta de un virus. Esta clase de ciberamenazas pueden ser evitadas, no se puede decir que fácilmente y en todos los casos, pero una buena cultura de IT (tecnologías de la información), así como de ciberseguridad puede prevenir en gran escala que esta clase de molestias puedan causar daños a la información que maneja una compañía.

4.7.3.- Ransomware: Este es un ataque equivalente a un secuestro. Muy común hoy en día en sistemas vulnerables y que actúa de forma diferente al antes mencionado "phishing**",** pues en vez de suplantar la información de alguna para persona para causar el daño en sí, se apoderará de toda esta y realizará una extorsión con el fin de que los datos puedan ser recuperados. Usualmente este tipo de ataques suelen ser relacionados con terrorismo por la forma en la cual los agentes que operan con estos programas suelen interactuar"

Es un programa malicioso que cifra los archivos en la computadora infectada y los vuelve inaccesibles. Los atacantes luego le piden a la víctima el pago de un rescate (por lo general, en criptomoneda) para liberar los documentos secuestrados. (Jaimovich, 2022, p.3).

Existen diferentes consecuencias que se puedan sufrir a raíz de este ataque. Al final, quien haya realizado o propagado este ataque, de la forma que fuese, vía correo electrónico, un dispositivo infectado, un sitio web que traía este programa dañino, será quien tenga el poder de la información. Es así que, el ciberdelincuente al no contar con el rescate solicitado puede hacer uso de aquellos datos que le sean útiles, como contraseñas, nombres de usuario etc.

4.7.4.- Suplantación de identidad: A raíz de haber sufrido un ataque de phishing o un ransomware, el ciberdelincuente puede tomar los datos personales robados y dedicarse a hacer estafas con los nombres y demás datos de los usuarios que constaban en las bases de datos robadas. "Un ataque de suplantación de identidad es uno de los **riesgos digitales más frecuentes**, que afecta tanto a personas como a organizaciones. Normalmente, los delincuentes intentan obtener contraseñas, números de cuentas bancarias" (Estruga, 2021. p.1). Este es un ataque usualmente derivado de otro, sin embargo con el crecimiento de la inteligencia artificial, se puede ver que nuevos tipos de modalidades se generan, creando o simulando características de la víctima con el fin de lograr cometer este delito.

En Ecuador el delito de suplantación de identidad actualmente está tipificado en el artículo 212 del "CÓDIGO ORGÁNICO INTEGRAL PENAL". Hay que tener en consideración que una vez que de forma maliciosa se han vulnerado los sistemas informáticos de una compañía, el ciberdelincuente puede realizar varias acciones con aquella información que se encuentra en su poder. La parte fundamental para entender la suplantación de identidad es que, con aquellos datos que reposan en forma ilegítima en manos ajenas a quien deberían estar, estas personas se hacen pasar por empresas o instituciones y generar duda o confusión con uno u otro usuario con el fin de inducirlos al engaño.

Aquí se podrá generar el hecho donde el usuario entregue su información de manera intencional, pero sin conocimiento de a quien se le entrega sus datos personales. Es importante mencionar que para efectos de este trabajo, la suplantación de identidad se dará de forma tal, que la información únicamente haya sido sustraída mediante un ataque a los sistemas de la empresa asegurada. Esta información de cualquier forma será usada de la forma en la que está estipulada como delito en la legislación ecuatoriana.

4.7.5.- Ciberdelitos en la legislación ecuatoriana

Es importante hablar de la tipología de los ciberdelitos en la legislación ecuatoriana. No obstante, hay que diferenciar entre el idioma informático y el jurídico, pues dentro de la póliza usualmente se mencionan a los ataques informáticos con términos que son usados usualmente por los conocedores de IT. El objetivo es que se entienda claramente el porqué estos ataques configuran parte de una ilegalidad en el contexto ecuatoriano. También se deberá equiparar los ciberdelitos estipulados en el "Código Orgánico Integral Penal" con aquella terminología utilizada en el ámbito digital.

Los Delitos Informáticos en su mayoría son delitos tradicionales que con la ayuda de la TIC's suponen nuevas formas de delinquir, que conlleva en ciertos casos a la creación de nuevos tipos penales, y de una nueva conceptualización sobre la tendencia criminal. (Cuenca, 2022, p.17).

Como se mencionó anteriormente, los delitos informáticos, aún así estén estipulados dentro de una codificación legal estos deberán tener la capacidad de abarcar las nuevas y diferentes tipologías que se puedan generar. En un mundo que se encuentra en un constante cambio y evolución, también presupone que el delito tenga un crecimiento de esta misma naturaleza. Es por tal razón, que los ataques informáticos que se han mencionado anteriormente y de igual forma aquellos que puedan generarse o que existan y no se encuentren dentro de la póliza deberán poder ser juzgados y abarcados por aquellos ya constantes en nuestra legislación.

Los principales ciberdelitos que se encuentren en el “Código Orgánico Integral Penal”, y que se enmarcan en aquellos que puedan ser cubiertos y abarcados en esta póliza son:

1. Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones
2. Art. 190.- Apropiación fraudulenta por medios electrónicos
3. Art. 232.- Ataque a la integridad de sistemas informáticos
4. Art. 186.-Estafa, numeral 2
5. Art. 212.- Suplantación de identidad
6. Art. 178.- Violación a la intimidad. (Código Orgánico Integral Penal, 2014)

Todos estos delitos tienen que darse por un medio electrónico, y en el caso de la estafa, el numeral dos constituye un agravante el que se de de esta forma. Como se mencionó anteriormente, no es posible para quien crea la norma prever cuántos o cuáles ciberdelitos podrán generarse, los medios por los que se difundan o la magnitud del daño, sin embargo es importante que con estos artículos señalados se pueda tener claro la ilegalidad de los actos a través de medios informáticos y el bien jurídico tutelado. (Se pidió a la Fiscalía

General del Estado datos estadístico sobre los ciberdelitos que más se practican en Ecuador sin respuesta alguna como consta en los anexos 1,2,3)

4.8.- Cobertura y alcance de la póliza de ciberseguridad

Una vez que se han revisado algunas de las ciberamenazas más comunes, es importante examinar cuál será el alcance y la cobertura de una póliza de ciberseguridad. Mucho dependerá del tamaño de la compañía, y en este caso específico se dirigirá a pequeñas y medianas empresas. Para esto se debe dar una pequeña definición de lo que son estas compañías, y de esta manera poder hacer un análisis de qué será lo que se cubra.

Existen varios conceptos de Pymes (pequeñas y medianas empresas), estos dependen mucho del país o región en las que se encuentren estas. Un ejemplo es en Europa donde se define a las Pymes como "pequeñas y medianas empresas (pymes) está constituida por las empresas que ocupan a menos de 250 personas y cuyo volumen de negocios anual no excede de 50 millones EUR o cuyo balance general anual no excede de 43 millones EUR" (COMISIÓN EUROPEA, 2019,). Sin embargo, en lo que se puede estar de acuerdo es que estas compañías tienen un volumen de ventas más bajo que las grandes corporaciones, ganancias anuales igualmente inferiores y una cantidad de personal menor sin importar al sector al cual pertenezcan.

Ahora, teniendo en cuenta esta pequeña definición de lo que son las Pymes, se podrá empezar a hablar de aquellos puntos a los que deberá cubrir la una póliza de ciberseguridad dirigida a este segmento de empresas.Como primer punto se debe tener la noción de aquello que busca cubrir esta póliza. Los ciberataques deberán ser contingentes que sucedan a los sistemas de una compañía. Con esto se quiere decir que estos eventos deben provenir de manera inesperada y a pesar de todo el cuidado y la debida diligencia que pueda tener el personal de una compañía con relación al manejo de sus sistemas y la información que sea manejada dentro de estos. Evidentemente existirán exclusiones de las que se hablará más adelante, y algunas de estas tendrán que ver con una falta de prudencia o negligencia con el manejo de los medios informáticos de la compañía.

En segundo lugar, se tiene que fijar los conceptos de aquellos eventos que serán materia de la póliza. Es decir separar un daño por un ciberataque de un eventual daño de los equipos por cualquier factor que no venga de una amenaza de alguno de los ciberataques, los mismos que deberán estar claramente definidos dentro de la póliza.

Cuando se hable del monto por el cuál estará asegurada la compañía este dependerá de algunos factores provenientes de la empresa. En primer lugar, hay que verificar el tamaño de la compañía, con esto se verá el volumen de clientes que tenga y la información que se maneje de estos. Además, el monto cubierto dependerá de la calidad de sistemas que tenga la compañía y los medios de protección a estos. En relación a estos factores, de manera individualizada es que la aseguradora realizará el respectivo análisis para saber el monto asegurado, y de forma obvia el valor de la prima.

Con estos puntos se podrá tener una idea de los factores clave de la póliza de ciberseguridad, cuáles son los límites y que es lo que protege. Evidentemente este producto de seguros no está hecho para cualquier daño a los equipos informáticos de una compañía, sino que protege a los sistemas y la información que se maneja dentro de estos. No obstante, la protección no es contra actuaciones indebidas de los colaboradores de la compañía, pues existen las pólizas de infidelidad. Además si el ataque es proveniente de impericias humanas o negligencia dentro del cuidado y protección de los sistemas internos de la compañía y la información que contiene, la póliza tendrá una exclusión. Es decir, el alcance es para eventos impredecibles y que se sobreponen a todo el cuidado necesario por parte del asegurado.

También hay que entender la función de la compañía de seguros, y en sí de la póliza de seguros en general. Este tipo de empresas, son personas jurídicas que tienen por finalidad dedicarse al servicio de los seguros, de ramos generales o de vida, es decir tienen un fin de lucro. Toda vez que su objetivo es generar ganancias, deberán existir límites para la indemnización del reclamo, es así que se vuelve imperioso para estas empresas proceder según los parámetros que establezca la póliza, caso contrario no existirá forma alguna de que se genere el pago por aquello que se desea proteger.

4.9.- Adaptación y adopción a pequeñas y medianas empresas de este tipo de póliza.

Con todos los antecedentes que se han revisado se debe definir cómo se adaptará una póliza de ciberseguridad para el sector de las pymes. Claramente las pequeñas y medianas empresas tienden a descuidar sus sistemas informáticos, sin tener procesos de ciberseguridad, será importante ahondar los motivos por los que se genera este descuido. Un segundo punto es revisar las cifras de ciberdelitos que se sufre en Ecuador, cuáles son los más comunes y desde cuándo se han agudizado este tipo de amenazas. Finalmente hay que ver la cultura y modelos de comportamiento que deben tener estas compañías, es decir la “debida diligencia” que deben tener en cuanto al cuidado de sus sistemas y la mitigación de riesgos que pudiesen provenir de las ciberamenazas.

Con todos estos factores se llegará a las conclusiones de cómo llegar a la adopción de un tipo de contrato, usualmente utilizado para grandes corporaciones, con sistemas de alta tecnología como en las instituciones financieras que tienen un core con tecnología de punta que requiere una alta protección, con prevención, así como respaldo y un seguro contra ataques cibernéticos. Como se había mencionado, un problema con las pymes es su bajo o nulo cuidado con sus sistemas y la poca prevención ante ciberataques.

Desde el comienzo de la pandemia, los ciberataques aumentan en las empresas, desde las pequeñas a grandes, lo que obligó a tomar medidas de protección; sin embargo, aunque se habla del tema y las amenazas aumentan, las pequeñas empresas no ven el riesgo o consideran que no será su caso por el tamaño de su organización. (LOPEZ, 2022, p.1).

Esto quiere decir que este tipo de compañías por desconocimiento y quizá hasta por negligencia suelen dejar de lado las precauciones y debido manejo de la seguridad de sus ataques. No obstante, hasta los sistemas más fuertes y más protegidos han sido víctimas de ciberdelitos, razón por la cual un seguro contra este tipo de riesgos no deja de ser imprescindible para reducir el impacto que se genera cuando estas compañías han sido víctimas de la delincuencia digital.

Hay que tener en cuenta las cifras de ciberdelitos que han venido ocurriendo en el país en el último año. Los datos son alarmantes, pues según datos de la UNIDAD DE CIBERDELITOS DE LA POLICÍA NACIONAL, en cierto tipo de delitos como Acceso no consentido a un sistema informático, telemático o de telecomunicaciones en el año 2017 hubieron 42 denuncias, mientras que en el año 2022 se duplicaron a 84 y hasta julio del año 2023 existieron 54. Se vuelve evidente que las pequeñas y medianas empresas pueden resultar objetivos más susceptibles para los delincuentes cibernéticos, pues estas organizaciones tienen menor cuidado con sus sistemas, siendo así estas un blanco común para organizaciones criminales en línea, como se lo demuestra en el cuadro del anexo 4.

Es importante que el cuidado de una compañía sea puertas adentro. Con esto se quiere decir que la prevención contra los ciberdelitos debe provenir de la administración de las empresas, y esto es una revisión de los sistemas, una *"due diligence"*. Las compañías grandes cuentan con la figura de gerentes de tecnologías (CTO), encargado de la innovación y de tomar a cargo todo tipo de innovación necesaria, sin embargo en empresas más pequeñas, al tener un número reducido de trabajadores, quien funja de administrador o gerente general deberá tomar a su cargo las funciones del CTO, "CDO y CTO, merecen una especial atención por parte del responsable de la Due Diligence, ya que tanto en control de los datos como de las nuevas tecnologías pueden ser un factor diferencial para la compañía" (CASTELLTORT, 2022, p, 4).

Una vez entendidos ciertos factores tanto coyunturales como corporativos, se puede empezar a definir cómo adaptar una póliza de ciberseguridad hacia una pequeña o mediana compañía. Aunque fue el tercer punto, la debilitamiento diligencia o *"due diligence"* de parte de la administración es clave, pues la póliza por definición está para cubrir contingentes, eventos que no se hayan podido prever, cuando una empresa no cuenta con licencias actualizadas en sus sistemas, una auditoría constante a sus redes y equipos, deja ser un imprevisto lo que pueda generarse en cuanto a ciber riesgos, se transforma en negligencia y constituiría una exclusión en lo que concierne a la póliza de ciberseguridad. Es importante hacer mención de este punto, pues sería el punto de inflexión para que se tome en cuenta el riesgo que tiene una pyme, considerando que efectivamente cuenta con menos recursos que una empresa grande para protegerse ante ciberamenazas.

El cambio de cultura corporativa, manejo y prevención de daños hacia la IT de una organización por parte de los administradores y una correcta educación sobre este tema a los colaboradores, sería la base sobre la cual se fundamentaría la póliza. El poder demostrar mediante un manual de procedimientos, el tratamiento y manejo de las tecnologías de la información, podría ser el punto de confianza para que una empresa aseguradora tome el riesgo de asegurar al sector de las pymes.

4.10.- Restitución de datos y mitigación de daño reputacional a la empresa

Esta es una parte fundamental dentro de una póliza de ciberseguridad ya que son las soluciones a los problemas que se puedan presentar, después de haber agotado todas las vías posibles para evitar el daño del sistema del usuario, empresa o instituciones. Es decir siempre y cuando se haya intentado restablecer todos los datos de los sujetos anteriormente mencionados y al no tener resultado alguno, se les deberá reponer tanto los datos de una forma adecuada y materializados, o si no se pueden restituir los datos, se debe responder de una forma económica que simbolice la indemnización por el robo de los datos, y asi pues tambien la aseguradora será la encargada de compensar el daño reputacional que afecte al prestigio de la empresa.

En una época con nuevas vías de negocios, y con una operatividad digital, ha generado nuevas preocupaciones para las empresas y los profesionales. Al tener canales de negocios, que de forma usual funcionan a través de internet, ha permitido cambiar los conceptos tradicionales de comercio, lo cual ha traído consigo la necesidad de proteger los sistemas con los cuales se interactúa. Es así que desde el sector de seguros, nace un nuevo ramo para este requerimiento y consigo las pólizas de ciberseguridad que cubran esta demanda.

La mitigación de riesgos es la estrategia que utilizan las organizaciones para disminuir los efectos del impacto causado a raíz de algún ataque o amenaza. Es similar al proceso de reducción de riesgos, en el que se identifican las posibles amenazas empresariales antes de que la organización tome las medidas necesarias para disminuir los efectos de estos factores.

Algunas de las amenazas y riesgos a los que se enfrentan las organizaciones modernas son las amenazas de ciberseguridad, las catástrofes naturales y todo aquello que pueda causar daños en los equipos, el personal y las instalaciones de una organización. (Gentbutsu, 2023, p.1)

Es por eso que las aseguradoras deben tener un plan de contingencia para cada una de las necesidades de los usuarios, el objetivo principal es prevenir las situaciones complejas de robo de datos y, si es que el robo pasa a un segundo plano, tratar de reducir el impacto de la vulneración de los sistemas en donde se encuentran los datos de las empresas, datos que son de diferentes categorías, si es que los datos ya estarían perdidos se deben restituir utilizando sistemas sofisticados para este objetivo.

En cuanto al daño reputacional hace referencia a la persona jurídica es decir a la empresa, a la que se le haya afectado de alguna forma, en este caso que se haya afectado al sistema operativo de su compañía en donde se encuentran datos de toda clase de sus clientes. La aseguradora tiene como objetivo principal el evitar que la reputación de la compañía se manche por eso debe aplicar distintas estrategias para que esto no ocurra, entre ellas crear políticas de un manejo adecuado de los distintos sistemas empresariales, a su vez si el daño reputacional es irreversible, la aseguradora será la encargada mediante vía judicial de restablecer este daño y solicitar se aplique el derecho al olvido.

4.11.- Exclusiones de cobertura de las pólizas de ciberseguridad

Un punto fundamental dentro de toda póliza de seguros, son las exclusiones, parte medular que delimita la relación que tendrá la compañía con el asegurado o el tomador según el caso. Anteriormente se trató el tema de adaptación a pequeñas y medianas empresas, y con este punto se abrió la discusión de un cambio de cultura corporativa. El punto central para que una compañía de seguros pueda asegurar a una empresa pequeña es que exista la certeza de que un ataque será una contingencia, imprevisible y que actualmente se está llevando una debida diligencia con los sistemas informáticos. Es imprescindible, y sin menoscabar o discriminar a una empresa por su tamaño o facturación, que este tipo de compañías tengan un manejo adecuado de su IT, además por un tema cultural, aquí en Ecuador no suelen tomar las precauciones debidas con sus sistemas informáticos. Con este análisis, se podrá revisar los factores que no serán parte de la cobertura de la póliza.

Cuando se habla de un cambio de cultura corporativa se remonta a todos los cambios que se han dado dentro del manejo de las empresas y sus actitudes con los constantes modificaciones que surgen de forma legal, social y tecnológica los mercados, las personas y los países. Todas estas evoluciones se producen para tener a una compañía siempre actualizada con lo que sucede en su entorno, es así que se han podido ver estas revoluciones de compartimiento en cuanto a la visión de las corporaciones. “Es un reflejo de cómo actúan e interactúan los empleados, cómo superan los desafíos y responden al cambio, y cómo la organización se representa a sí misma como un todo hacia los grupos de interés” (Howard-Grenville; Lahnem, 2022, p.1). Al hablar de ciberseguridad se aplican los mismos criterios y lógica, simplemente adaptar a la compañía y a sus colaboradores para que innoven y con esto preserven la buena imagen de esta organización, así como todos aquellos asuntos que conllevan los nuevos modelos ligados a un cambio de cultura corporativa. Ahora se puede ahondar en el motivo por el cual se ha procedido a tratar sobre el tema anterior de cultura corporativa, y cuál es el objetivo en sí de la póliza de ciberseguridad. “Basta sólo pensar en que los seguros operan como una unidad de compensación de riesgos socialmente asumidos, que persigue legítimas utilidades para las compañías de seguros, únicamente concebibles mediante la contratación en masa” (Barrientos, 2015, P.430). Como se explica aquí, dividido en tres conceptos sencillos que son, compartir los riesgos, generar ganancias (por parte de las aseguradoras) y que sea contratado por varias personas, explica lo oneroso de este contrato. Toda vez que estos requisitos deben estar presentes para que resulte óptimo el negocio en sí, es que deberán existir ciertos parámetros que permitirán que exista la relación de asegurado-asegurador. Al ser la naturaleza del contrato de seguro aleatorio, los mencionados parámetros serán los que permitan mantener este concepto intacto en el contrato. Una vez que se ha explicado la naturaleza del contrato de seguro y también se ha hablado de qué significa el cambio de cultura corporativa es necesario entender cómo estos conceptos se deberán adaptar a las compañías para la interacción adecuando con la aseguradora cuando se contrata un ciberseguro. Hay que entender, que a partir del año 2020, como se habló anteriormente, se produjo una extensa digitalización en torno a muchos campos productivos.

Pese que la pandemia por el COVID-19 obligó a la implementación amplia del teletrabajo, la teleducación, la telemedicina y otras aplicaciones telemáticas, que surgieron como paliativos a la enfermedad, a la economía y a lo social, la cultura de ciberseguridad en el Ecuador no se ha consolidado. (Vargas, 2022, p.45)

Desde la perspectiva, inclusive de las fuerzas armadas del Ecuador, se nota que aún falta en la sociedad esta concientización. Las compañías, sean del tamaño que sean, deben tomar todo tipo de medidas necesarias con el objeto de evitar que se produzcan ciberataques. A partir de este concepto de debida diligencia informática, o más bien en el cuidado de los sistemas de una organización, es que una compañía de seguros podrá ofrecer la póliza, sabiendo que el riesgo sería eventual, imprevisible y que previo a un supuesto suceso de ataque cibernético se tomaron las medidas pertinentes y necesarias para que este pudiese ocurrir.

Finalmente hay que mencionar aquellos factores que no suelen ser parte de la cobertura de una póliza de ciberseguridad. Ya se han revisado aquellos motivos por los cuáles no toda afectación que sufran los sistemas de una compañía serán motivo de indemnización, además parte de este trabajo es proponer ciertos puntos cruciales que ayuden a la adaptación de este tipo de contratos a empresas pequeñas y medianas, siendo la contratación masiva un punto clave para que se pueda desarrollar este tipo de negocio. A continuación se puede revisar algunas de las exclusiones más relevantes con las que deberá contar una póliza de ciberseguridad para pequeñas y medianas empresas, así como un breve desarrollo de la motivación de las mismas a fin de que haya una mejor comprensión por parte del contratante, llámese tomador o asegurado en el caso de la normativa ecuatoriana.

1. **Exclusión a hechos conocidos:** La póliza de seguro al no tener un efecto de tipo retroactivo, sólo cubrirá aquellos ataques de originen posterior a la contratación de la póliza de ciberseguridad. Al igual que en muchas pólizas, las preexistencias son factores que deben ser analizados de manera previa, pues el primer riesgo que se excluye es aquel que ya existe.

2. **Daños que provengan de una actitud maliciosa y deliberada por parte del personal**: Como se ha tratado de forma extensa, la póliza es un tipo de contrato aleatorio, toda vez que sólo funciona al generarse un suceso que es fortuito e imprevisible. En virtud de esto, cualquier acto doloso por parte de los colaboradores de una empresa no podría considerarse cubierto. Además el punto de la contratación de este tipo de productos de seguros, es proteger a los sistemas con un ataque cibernético. Existen otras pólizas que cubren los actos dolosos de los trabajadores, sin embargo, aún cuando la información de la compañía sea el bien afectado, como son datos personales de los clientes, secretos empresariales, entre otros, no habrá indemnización. En este Punto se recalca que el daño a cubrir será indemnizado únicamente por daños a los sistemas por el efecto de un ciberataque.
3. **Negligencia en el cuidado, manejo o mantenimiento del sistema:** Cuando el daño que pudiese ser causado a los sistemas de la compañía contratante de la póliza de ciberseguridad, sea causado sin dolo, pero con algún grado de negligencia en cuanto a la debida diligencia con la cual se debe tratar a estos, no habrá lugar a la indemnización. A pesar de que la información que contienen los sistemas informáticos de una organización sea la que se vea afectada, y evidentemente la causa sea por motivo de un ciberataque, cuando sea comprobada la negligencia o falta de cuidado no procederá el pago por motivo de indemnización a raíz de un reclamo. Dentro de esta exclusión podrían generar otras derivadas, las mismas que podrían constar en la póliza, tales como:
    a) Software sin Licencia: Como ya se aclaró previamente, es obligación de la compañía tener un cuidado diligente y realizar el seguimiento a las medidas solicitadas de ciberseguridad.
    b) Responsabilidad por productos: Cualquier pérdida que se pueda generar por aquellos productos que son instalados o revisados por el asegurado o en nombre de él.
    c) Responsabilidad de gestión: Esta pérdida deviene por cualquier tipo de acto negligente en cuanto a la gestión del asegurado.

4. **Daños no contratados en el seguro:** La cobertura estará extendida de forma exclusiva a aquellos daños que se encuentren explícitamente contratados dentro de la póliza. Sin embargo, y al ver que el cibercrimen crece con gran fuerza, no es posible enumerar y prever cada clase de software malicioso que pudiese existir, en virtud de esto es que se realiza el debido análisis a fin de constatar que se llegue a verificar que el problema efectivamente es de aquellos enumerados y señalados de forma expresa en la póliza.

5. **Daños Materiales:** Al ser esta una póliza que protege principalmente los sistemas de una compañía, se debe separar aquellos problemas que afectan a los equipos electrónicos (hardware), de aquellos que atacan específicamente al software de los equipos y la información contenida en ellos. De manera exclusiva, aquellos daños que se pudiesen generar a un equipo electrónico, y que sean generadas por un ataque cibernético serán cubiertas en esta póliza.

6. Mejoras: La idea de la póliza de seguro es exclusivamente la protección del patrimonio ya existente, por tal razón la cobertura no podrá ir más allá de aquello que ya existe. Cualquier reparación o indemnización serán pertinentes y equivalentes a los bienes asegurados, en el caso específico de la póliza de ciberseguridad a los sistemas y la información que haya tenido la compañía al momento de sufrir un ciberataque.

7. Robo, pérdida o daño de Equipos electrónicos (hardware): El asegurado deberá tener en cuenta el objetivo y esencia de esta póliza de seguros, el cual es la protección de los sistemas de una empresa y la información que estos almacenan. Es por este motivo, que se debe aclarar que en el supuesto caso de haber sido sustraído un equipo electrónico la compañía aseguradora únicamente cubrirá de forma parcial el daño que pueda surgir del mal uso de dicha forma que hubiese contenido el hardware siempre y cuando se demuestre que este era de uso exclusivo de la compañía.

En caso de que el daño al sistema sea de tal magnitud que dañe un equipo electrónico perteneciente al asegurado, la aseguradora cubrirá los gastos que conlleven el daño generado por la pérdida de información, más no la reparación de ningún tipo del equipo informático.

Las exclusiones dependerán en cada póliza, no obstante estas son aquellas que parecen ser más necesarias de detallar. La aseguradora para suscribir este contrato podrá realizar una inspección a la empresa, constatando que los sistemas se encuentren en un estado adecuado para poder prestar el servicio de seguros contratado. Agregar ciertas exclusiones, o aumentar el contenido de las ya existentes será trabajo de la aseguradora, el cumplir con aquellos factores incluidos dentro de la póliza sería la del asegurado.

4.12.- Sujetos que intervienen en la Protección de Datos

Los sujetos que intervienen en el sistema de protección de datos son los encargados de precautelar el cuidado del tratamiento de datos hasta que se cumple el objetivo para el cual fueron recopilados, sin que durante este proceso se pueda vulnerar o sustraer alguno de ellos. Los intervinientes dentro de este proceso son los siguientes:

4.12.1.- Titular: Artículo 4: “(...)Persona natural cuyos datos son objeto de tratamiento(...)” (Ley Orgánica de Protección de Datos Personales, 2021)

Esta persona es quien entrega sus datos personales, no es una persona jurídica es decir una empresa, y es quien otorga mediante un consentimiento, que una empresa o una tercera persona realice el tratamiento de sus datos para el fin específico que fue establecido en el contenido del consentimiento, el será el titular para exigir los derechos que abarca la protección de sus datos y quien podrá ejercer cualquier tipo de acción legal, si esto no se respeta y se hace un mal uso de los mismos.

Por lo que el titular de sus datos personales deberá leer de forma detenida el contrato de consentimiento para ver cómo serán tratados sus datos y a su vez la persona que emite este documento tiene la obligación de explicar de forma clara y precisa para lo que se utilizará sus datos y que ocurrirá caso contrario sino se respeta este contrato, se debe tener en cuenta que no todas las personas tiene conocimientos jurídicos por lo que cualquier omisión que se presente sobre el tratamiento de los datos será de responsabilidad de la empresa o tercera persona a la que se le entreguen los datos.

4.12.2.- Responsable del tratamiento: Artículo 4 **"**(...)persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales(...)"**.** (Ley Orgánica de Protección de Datos Personales, 2021)

Esta persona será la responsable de los datos que le fueren conferidos del titular y quienes deben establecer cual es la finalidad de los datos que se les fue entregado, para que se los va a utilizar y entre que funcionarios ya sea de al empresa privado o pública se podrán compartir, a su vez se tiene que analizar el tipo de datos que manejan para dar un adecuado y confidencial tratamientos de los mismos.

Este responsable de los datos podrá ser cualquier entidad pública o empresa que se dedicara específicamente al tratamiento de datos de sus clientes asi tambien podra ser únicamente una persona que puede ser algún profesional como por ejemplo un médico que cabe recalcar maneja datos sensible, un abogado o un arquitecto, estos serán los encargados de decidir para qué van a ser utilizados esos datos. Bajo ningún concepto los responsables darán un mal uso de los datos que les han sido entregados y tiene la obligación de emitir informes de los datos que se trate, deben rendir cuentas a la autoridad competente si ésta los solicita.

4.12.3.- Encargado del tratamiento: Artículo 4: "(...)Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales(...)”. (Ley Orgánica de Protección de Datos Personales, 2021)

Por lo general la mayoría de las pequeñas y medianas empresas lo utilizan durante el procedimiento de tratamientos de datos o se delega a un persona natural o jurídica que sea responsable y encargado del uso de estos datos, es decir esta persona será quien esté a cargo del uso de los datos y quién puede ser totalmente ajeno a la empresa, esta persona natural o jurídica podrá actuar en nombre o a cuenta del responsable de los datos.

Es decir la empresa principal podría contratar a una tercera empresa que sea subsidiaria a la principal y que realice actividades secundarias a el objeto social de la empresa y quien será el encargado del tratamiento de datos de la empresa principal de ciertos o de la totalidad de clientes con que la compañía principal cuente, esta atribución es muy importante y debe prever que la información de los cliente no se filtre y mucho menos se sustraiga bajo ningún concepto.

4.12.4.- Destinatario: Artículo 4: “(...) Persona natural o jurídica que ha sido comunicada con datos personales(...).” (Ley Orgánica de Protección de Datos Personales, 2021)

Esta persona será a quien se le deberá entregar la información intacta del titular de los datos personales y quien será el encargado de utilizar esta información acorde el consentimientos del manejo de los datos, existirá una excepción para que el consentimiento no sea obligatorio en caso de que la autoridad competente requiera información sobre el titular.

Bajo la misma línea los datos que sean requeridos por autoridad competente con fines investigativos no serán catalogados como destinatarios del tratamientos de los datos del titular, ya que prima en estos casos el interés general de la ley, los destinatarios por el contrario, deben cumplir una finalidad con los datos que se les haya entregado, por ejemplo en el caso de los médicos al ser entregados los datos sensibles del paciente serán con la única finalidad, en el caso de exámenes realizar un diagnóstico y emitir un criterio médico que concluye que enfermedad tiene esa persona, no se podrán compartir estos datos a otras personas y mucho menos con fines comerciales.

4.12.5.- Autoridad de Protección de Datos Personales: Artículo 4 “(...) Autoridad de Protección de Datos Personales: Autoridad pública independiente encargada de supervisar la aplicación de la presente ley, reglamento y resoluciones que ella dicte, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales(...)”

Actualmente en el Ecuador ya se ha nombrado una autoridad responsable de la Superintendencia de Protección de Datos, el Ejecutivo ha enviado una terna al Consejo de Participación Ciudadana y Control Social para que sean ellos quienes designe a la nueva autoridad de protección de datos, la misma que será la encargada de supervisar, a la ley de protección de datos personales y sus normas secundarias con el fin de proteger los derechos de todos los ciudadanos, y quien fue posesionado por la Asamblea del Ecuador.

Esta autoridad tiene varias atribuciones sobre el tema de tratamientos de datos, a su vez debe trabajar de forma cooperativa con las demás instituciones del Estado ecuatoriano que lo requieran. Esta autoridad podrá en cualquier momento solicitar informes a los responsables del tratamiento de los datos para que si no ha cumplido con el reglamento sancionar a la empresa que ha incumplido, es decir también dentro de sus atribuciones está el sancionar a la o las personas natural o jurídica que incumplan.

4.12.6.- Delegado de protección de datos personales: Artículo 4 “(...) Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos(...)”

El delegado de datos es un intermediario entre la autoridad de protección de datos y los responsables o encargados de la protección de datos, es quien brindará un asesoramiento de cómo manejar los instrumentos legales dentro del tratamiento de datos de una empresa u organización, la Ley obliga a estas compañías a nombrar un delegado de protección de datos dentro de sus instituciones privadas y a su vez en el caso que se lo requiera también se nombrará en instituciones públicas.

El delegado de protección de datos tendrá cierta autonomía en la toma de decisiones ya que su nivel estará en relación a los más altos ejecutivos de empresa, este funcionario deberá estar en constante capacitación y actualización en temas que corresponde a la protección de datos y no podrán ser destituido bajo ningún concepto si ellos cumplen a cabalidad con sus funciones, siempre deberá mantener la confidencialidad que corresponde en el ejercicio de sus funciones.

Este proceso de tratamiento de datos se encuentra enmarcado en el anexo 5 uno dentro de un ordenador gráfico.

4.13.- Potenciales efectos jurídicos de las pólizas de seguridad

Para una empresa, cualquiera que fuese su tamaño el verse frente a una vulneración de sus sistemas trae consigo efectos no solo de tipo económico, sino también consecuencias de tipo legal. Cualquier persona que tenga una afectación posterior al sufrir un ciberataque a una empresa tomará medidas legales en contra de esta, lo que causará un perjuicio a la compañía. Para Roberto González, presidente ejecutivo del Banco del Pacífico en el año 2022, el gastar en seguridad es un tema de gran costo para las instituciones, es así que, por datos del mismo Banco el gasto en seguridad tanto de los espacios físicos como digitales es de alrededor del 15% de lo que gastó las institución en el año 2022, lo cual fue aproximadamente 11 millones de dólares, como consta en la publicación del diario digital premisas en el anexo 6.

Es aquí cuando la mitigación de daños que brinda la póliza de ciberseguridad, cubrirá los gastos legales que genere un posible litigio nacido de los daños y perjuicios causados por un ciberdelito. No obstante, se generarán obligaciones, anteriores y posteriores a las acciones que sufren los afectados, es decir los clientes o usuarios cuya información pudiera haber sido sustraída o vulnerada durante un posible ataque cibernético. En la actualidad muchas de las compañías, sean grandes o pequeñas tienen un “core de operaciones” relaciones a sus sistemas digitales, aquí sus clientes evidentemente consignan su información personal, motivo por el cual, es evidente que un ataque a este centro de operaciones podría desencadenar un impase en un sentido jurídico.

En este aspecto se debe tomar el primer recurso que se ve afectado cuando sucede un ataque cibernético. Esta información, dependiendo del giro del negocio de una empresa puede llegar a ser tan delicada, que el hecho de perderla puede significar una pérdida de vida o muerte para quien confía con esta a la empresa. Es así que se han conformado y se siguen afianzando instituciones jurídicas que de forma especial se encargan de la protección de datos personales. Así se podría decir que la primera obligación de una compañía con la información que guarda de sus clientes es la protección de datos personales, y con esto no solo se habla del tratamiento de los datos personales, sino del cuidado de las bases donde están asentados estos mismos.

El desarrollo social y empresarial ha tenido como consecuencia fenómenos tecnológicos que han impulsado al desarrollo del derecho en direcciones que no eran previsibles hace algunos años, de la misma manera en la cual las personas naturales han visto cómo dichos avances generan perfiles y acumulaciones de información que, en la mayoría de las ocasiones, puede considerarse lo suficiente importante para ser protegida por el derecho (Montesuma, 2019, p.3).

Cuando un ataque cibernético se genera, de la misma forma nacen obligaciones de la empresa con el dueño de la información, llámese cliente o usuario. La primera reacción que debe tener la compañía es, el notificarme que ha sucedido este impase. Se está hablando de un punto donde no es claro si la información va ser usada perniciosamente, si va a existir una extorsión o simplemente el uso que se dará a la data vulnerada, simplemente todo aquel que ha consignado sus datos personales con una compañía tiene el derecho a saber que estos mismos han sido atacados, sustraídos de la entidad a quien se los confió.

Una vez que se demuestre o que alguno de los consignatarios de la información vulnerada ha resultado afectado el efecto obvio y más grave para la empresa que ha sufrido el ataque cibernético será la responsabilidad civil y los daños. De aquí, quizá se pueda definir a la parte más relevante de la póliza de ciberseguridad, pues las pérdidas económicas que se generen podrían ser un factor para que puedan seguir o vayan a quebrar, sobre todo compañías pequeñas y medianas.

El robo de información, la caída en la disponibilidad de servicios y sistemas y los daños a su imagen ocasionados por el cibercrimen suponen pérdidas para las empresas a nivel mundial por 445,000 millones de dólares, una cantidad que se acerca a los ingresos de Walmart, la compañía que ocupa el primer lugar de la lista de Fortune 500 en el 2016, con 485,000 millones de dólares. (Riquelme, 2017, p.2)

El sufrir un ciberataque trae consecuencias verdaderamente perniciosas para toda la sociedad. Las compañías víctimas de estos delitos pueden llegar a la quiebra por varios factores, que están totalmente justificados, pues no es algo menor verse afectado por el robo de la información a una entidad a la cual se le ha confiado con nuestros datos personales o en el caso de personas jurídicas con su información de alta relevancia. En primer lugar, viene un probable paro de las actividades de una empresa, generando pérdidas económicas por la falta en sus actividades laborales. Segundo viene el daño reputacional, no hay más confianza de sus clientes pues información importante que ha sido confiada a estas compañías puede ser utilizada en contra de sus consignatarios. Como tercer punto vienen las demandas por daños, con valores difíciles o imposibles de cubrir, abogados y todo lo que conlleva costas judiciales y una posible indemnización al cliente o usuario. Por todos estos factores es imprescindible que, la información que guarde una empresa, sea cual sea, esté altamente resguardada, sí de forma imprevisible se ha llegado a vulnerar, que los gastos y pérdidas que estos generen puedan ser cubiertos, de aquí la relevancia de la póliza de ciberseguridad.

4.13.1.- Falta de conocimiento y cultura de ciberseguridad

El ciberseguro ha sido un ramo de seguros comúnmente utilizado por compañías grandes, con un core de operaciones basado ampliamente en sus sistemas informáticos, lo cual lleva a que se tenga una fuerte estructura y cultura en cuanto a la ciberseguridad. Sin embargo, las empresas pequeñas y medianas, por cuestiones culturales, no suelen poner un debido énfasis a este tema, no tienen la precaución de resguardar los sistemas que usan y que son parte muy relevante de sus funciones. Es así que por descuido, confianza y hasta negligencia muchas de estas empresas dejan como algo secundario y de poca relevancia el cuidado de sus sistemas de operaciones.

Al ámbito empresarial, donde al manejarse y utilizarse tecnologías en la mayoría de las empresas para llevar a cabo sus actividades diarias, estas se encuentran en un foco rojo dentro de su operación, ya que se vuelven entes vulnerables para ser sujetos a sufrir ciberataques. (Landgrave, 2023, p. 5)

Es en este sentido que muchas compañías aún tienen miedo y reserva de invertir en cuanto a la protección de sus sistemas. No suelen ser el objetivo más común de la delincuencia digital, sin embargo quienes cometen esta clase de ilícitos saben también que son blancos fáciles y que de la misma forma almacenan información de alta relevancia como datos personales y sensibles de sus clientes o usuarios. Siendo esta una realidad en un país con un mercado pequeño, el mismo que tardíamente se adapta a los cambios tecnológicos que propone un mundo globalizado, es vital revertir el pensamiento inocente de no creer que pueda suceder un ataque a una empresa PYME.

El crear una conciencia en el entorno laboral es el primer paso hacia mejorar el cuidado de los sistemas informáticos que maneja una compañía. El empleador, es decir el empresario pequeño y mediano es el primer sujeto que debe empezar a crear conciencia de las amenazas que surgen de un mundo globalizado y digital. El personal de la empresa de igual forma debe tener conocimiento de los riesgos existentes así como de los cuidados que deben generarse dentro de las empresas. Evidentemente estos cambios a nivel cultural no podrían generarse si es que desde la cabeza de la empresa existe la visión de un cuidado diligente de aquel “core” digital que permite enlazar a un negocio con el mundo digital que está en constante cambio.

4.13.2.- Afectaciones económicas

Con la llegada de la pandemia de Covid 19, con su origen en Asia, su paso por Europa y Estados Unidos para posteriormente llegar a Latinoamérica, trajo consigo varios puntos negativos; insalubridad, escasez económica a nivel mundial, problemas psicológicos y de salud en las personas, entre otros, pero también tuvieron puntos muy positivos que después derivaron en la creación de delitos cibernéticos, es decir, las empresas tuvieron que adaptarse a esta nueva normalidad e implementar la virtualidad en los sistemas de las distintas compañías a nivel mundial, entre estas compañías se tienen públicas y privadas que crearon plataformas para facilitar trámites en línea, obligándolos a realizar una transformación digital en todas sus plataformas.

Esta transformación vino de la mano de la creación de nuevos delitos en el ciberespacio cuyo objetivo principal es la sustracción de datos e información importante y hasta el latrocinio de dinero de las cuentas de los bancos y cooperativas de ahorro y crédito de sus usuarios, cuyo sistema de ciberseguridad casi todo el tiempo se ve vulnerado con estos ciberataques y que en algún momento podrían afectar la economía de las personas a nivel mundial. El escenario empresarial debido a la pandemia generó la proliferación de riesgos tecnológicos y financieros, ocasionando en las organizaciones la pérdida de transparencia, vulneración de controles internos, alteración de los modelos de supervisión, incumplimiento de normas de aseguramiento, pérdida de información y afectación financiera. (Ackerman, 2021)

El ciberdelito ataca a los sistemas y redes de información tanto personales, como empresariales, constituyendo un tipo de riesgo tecnológico. Es el resultado de la conducta delictiva que los perpetradores ejercen con el fin de obtener un beneficio ilícito mediante la utilización de herramientas tecnológicas como los sistemas de información en línea, redes informáticas, modificando reportes en sistemas informáticos, alterando la información, afectando la confidencialidad de datos con fines de ocultamiento, enriquecimiento ilícito, estafas financieras y generando daños a la reputación institucional. (Westerski; Kanagasabai; Narayanan; Wong, 2021)

Si no se toman las medidas adecuadas los ciberdelitos afectarán a la economía mundial pudiendo el daño será irreversible ya que estas infecciones a los sistemas pueden robar base de datos de todo tipo, inclusive información catalogada como reservada de los países. Como resultado de esto se pueden presentar fricciones internacionales que pueden dar como resultados la aplicación de barreras arancelarias a distintos productos de intercambio comercial o por el contrario bloqueos a la entrada de productos de un país al otro.

Por lo que, es de vital importancia que las persona y los gobiernos a nivel mundial puedan contar con herramientas tecnológicas para poder contener estos ciberataques y de esta forma mantener una estabilidad comercial y económica, así como también todas las personas deben tener pólizas de ciberseguridad que puedan garantizar el cuidado de su información, de la empresa y de la de sus clientes, para que las compañías y los usuarios no pierdan los datos personales y su confianza.

4.13.3.- Daño Reputacional

Una parte vital al hablar de ciberseguridad es cuidar la imagen de la organización. Al ver vulnerados los sistemas de una compañía no solo se verá perjudicada está, sino todo aquel que está involucrado o ha entregado información a la empresa. Siendo el cibercrimen una tipología del delito en crecimiento, y al ver que luego de una vulneración de los sistemas existen varios afectados, es de gran relevancia el retomar la información perdida y mitigar los perjuicios que se hubiesen generado. Una póliza de ciberseguridad, tiene como una de sus funciones que este daño reputacional pueda ser lo menos nocivo posible para la empresa y de igual manera, lograr que la reputación de la compañía pueda volver a su cauce habitual como se puede observar en el anexo 7.

La CONSERVACIÓN de la INTEGRIDAD de los datos de forma que no puedan ser alterados por usuarios sin AUTORIZACIÓN. La CONFIDENCIALIDAD de forma que únicamente aquellas personas para las que está destinada la información sean las que accedan a ella y nadie más. Y la DISPONIBILIDAD para que la información esté siempre que se requiera de una forma lícita. (De Haro, 2020, p.10)

Para entender el objetivo de la ciberseguridad y las razones por las que un cliente o usuario van a atacar a la reputación de cierta empresa empieza por entender este concepto mismo. El usuario confía en el ente al cual entrega su información personal, siendo así que, el verse afectado por cualquier mal uso de sus datos personales llevaría a este a convertir su experiencia en una red de comunicación perjudicial para la compañía involucrada. Con el auge de las redes sociales, todo aquel malestar o perjuicio que haya tenido una persona puede ser rápidamente comunicado a miles o millones más, es así que la obligación de cuidado de la información a través de la protección de los sistemas informáticos habría sido omitida por la empresa que custodiaba los datos en un primer lugar.

Con esto se retoma el concepto de “debida diligencia”, la información personal es un bien intangible preciado para una compañía y, así como uno cuida un inmueble o un vehículo, de igual forma se debe tener el cuidado con esta. El perder un activo intangible tan relevante como los datos personales de clientes o usuarios puede llevar a parte de las pérdidas económicas de una compañía, a un daño reputacional complejo de reparar. Es así que se torna de gran importancia el poder retornar a un punto donde una empresa vuelva a tener la confianza de los clientes y una llegada al mercado deseable.

La mitigación de daños es la parte donde la compañía trata de retornar a un punto inicial de seguridad hacia clientes o usuarios. Esto es un costo adicional, motivo por el cual contratar una póliza de ciberseguridad es relevante a fin de poder retornar con normalidad a las actividades de una compañía. Evidentemente no son sólo recursos económicos aquello necesario para recuperar la confianza con los diferentes actores en el mercado, el tiempo es un recurso fundamental, sin embargo el poder reducir costos económicos en este proceso es un punto que permitirá a la empresa retornar con mayor holgura y tranquilidad. Después de toda esta larga investigación y el aporte de varios autores se ha determinado los siguientes objetivos de nuestra tesis:

5.- Objetivo General

Propuesta de lineamientos para para un manejo adecuado de una póliza de ciberseguridad para pequeñas y medianas compañías en Ecuador

5.1.- Objetivos Específicos

· Analizar el marco legal y regulatorio de las pólizas de ciberseguridad en Ecuador

· Revisar que deben contener las pólizas de ciberseguridad en Ecuador

· Promover la adopción de pólizas de ciberseguridad en pequeñas y medianas empresas en Ecuador

5.2.- Justificación y aplicación de la metodología

En este acápite se mencionan aquellas formas que se utilizarán para resolver el problema planteado. Todas las preguntas que se encuentran enunciadas dentro de esta investigación han sido contestadas con apego a la metodología escogida para solventar de forma técnica y precisa a este trabajo.

5.2.1.- Nivel de estudio

5.2.2.- Tipo de Investigación:

En un primer momento, esta investigación fue de tipo exploratoria con el objetivo principal de familiarizarse con los términos, elementos y principios que rigen a las pólizas de seguros.

5.2.3.- Método de investigación: Se utilizó el método inductivo-deductivo ya que dentro del desarrollo de esta investigación se ha utilizado una estructura que contiene varios párrafos seguidos de una conclusión y también porque va de lo general a lo particular.

5.2.4.- Método analítico sintético:

La metodología analítica sintética adoptada permite un examen detallado de cada elemento de la póliza, asegurando que todas las recomendaciones estén basadas en evidencia concreta y prácticas recomendadas internacionalmente. Este método se ha utilizado para recabar información que aparentemente se encontraba aislada, por el hecho de que no existe normativa específica para las pólizas de ciberseguridad, separar y luego unir de forma racional varios elementos en una nueva totalidad y de esta manera poder entregar juntamente con una hipótesis.

5.2.5.- Instrumentos de Investigación: Dentro de esta investigación se aplicó la Observación directa ya que se revisó las pólizas de ciberseguridad creadas y ofrecidas al mercado en países como Brasil, Argentina y prototipos de pólizas realizadas por aseguradoras extranjeras que operan en Ecuador, también se utilizó el análisis de estos documentos para poder revisar las falencias que tienen e implementar directrices de manejo.

5.2.6.- Procesamiento de datos: Microsoft office Word, Power Point, Canva.

Protocolos de Investigación:

Objetivos específicos	Actividades
1.- Analizar el marco legal y regulatorio de para las pólizas de ciberseguridad dentro de Ecuador.	1. Analizar el marco legal para las pólizas de seguros en Ecuador. 2. Identificar los tipos de riesgos cibernéticos 3. Analizar qué deben contener las pólizas de ciberseguridad en sus coberturas 4. Identificar cómo se puede adoptar este tipo de pólizas para Pequeñas y medianas empresas.

	5. Identificar los actores del tratamiento de datos
2.- Revisar que deben contener las pólizas de Ciberseguridad	1. Analizar los elementos, principios e intervinientes dentro de una póliza. 2. Identificar los tipos de ciberdelitos que existen en Ecuador y se enmarcan en el marco legal. 3. Establecer las exclusiones que deberán contener las pólizas de ciberseguridad.
3.- Promover la adopción de pólizas de ciberseguridad en pequeñas y medianas empresas en el Ecuador	1. Identificar que tipo de ciberataques tienen estas compañías. 2. Promover una cultura de ciberseguridad en los empleados de estas compañías. 3. Establecer pólizas de ciberseguridad accesibles para este tipo de compañías

6.- Propuesta de solución del problema identificado

6.1.- Propuesta de lineamientos para para un manejo adecuado de una póliza de ciberseguridad para pequeñas y medianas compañías en Ecuador

En base a la investigación realizada y la revisión de varios textos académicos que permitieron ahondar en los temas de ciberseguridad y tener más conocimientos. Se ha analizado que, los potenciales clientes que van a utilizar este tipo de pólizas es decir las pequeñas y medianas empresas en el Ecuador, no cuentan con los elementos para proteger la información de la base de datos de sus empresas. Por lo que se cree que se debe tomar en consideración que, para crear las pólizas de ciberseguridad en el Ecuador se debe adoptar los siguientes lineamientos que, en base al conocimiento fruto de esta investigación y recomendación de algunos autores, se ha establecido de esta forma:

6.2.- Cuidados Preventivos

Dentro de los lineamientos en primer lugar se desarrollarán los ejes preventivos que corresponde al cincuenta por ciento del proceso de protección de ciberseguridad que se deben tener dentro de las pequeñas y medianas empresas, esta primera fase es de las más importantes porque si se detecta a tiempo un ciberataque y se cumplen todas las directrices que constan dentro de la guía práctica se podrá evitar y mitigar los riesgos de la sustracción de una base de datos o información relevante de una compañía previo una evaluación de qué tipo de información manejan estas empresas como se demuestra en el anexo 9.

6.2.1.- Guía práctica de procedimiento de ciberseguridad

Esta guía contendrá instrucciones concretas de un adecuado manejo de los sistemas digitales y de datos de las pequeñas y medianas empresas, a los cuales se brindará protección de ciberseguridad, esto se refiere a que contendrá varios sistemas de protección como antivirus, cifrados de accesos, bloqueos y actualizaciones, a su vez contendrán temas relacionados con los empleados de dichas empresas que hace referencia a las capacitaciones que van de la mano de las buenas prácticas informáticas, de igual forma se establecerán obligaciones para que los mantenimientos de los equipos se realicen en lugares avalados y homologados por la aseguradora.

Se pretende también dentro de esta guía realizar una protección a otros dispositivos que contengan bases de datos importantes relacionados con la información de los clientes de estas compañías, a su vez se quiere tener parámetros concretos sobre la protección y mantenimientos que se le deberá realizar a los sistemas de red de las empresas durante el transcurso de determinados períodos.

Esta guía va hacer creada por un miembro del personal de las pequeñas y medianas empresas, a quien se ha denominado oficial de seguridad de la información y datos, esta persona será quien una vez culminada la guía práctica de procedimientos de ciberseguridad, con previa aprobación del representante legal de la compañía, se lo presentará ante la aseguradora para que realice un análisis, negando o aprobando la cobertura de las pólizas de ciberseguridad para la empresa y en algunos casos presentando observaciones para su corrección y aprobación.

6.2.2.- Capacitación:

En cuanto al tema de formación a trabajadores de las pequeñas y medianas empresas se debe tomar en cuenta varios factores como lo son; que este tipo de capacitaciones se los dará en temas de protección de datos en este caso el tema legal y por otro lado un tema de buenas prácticas tecnológicas, como lo es verificar las páginas que pueden ser confiables o no, tener aplicaciones que permitan el cifrado de extremo a extremo, el navegar de modo incógnito pero de forma segura, cómo instalar una extensión del navegador. la utilización de cookies, entre otras, las mismas se darán en distintos lapsos periódicos, en un inicio serán recurrentes para posteriormente hacerlo de forma semestral, anual o cuando se requiera actualizaciones.

Hay que tomar en cuenta la cantidad de trabajadores que van a tener las pequeñas y medianas empresas ya que, en el tema de las pequeñas compañías se podrán presentar hasta dos empleados que trabajan únicamente dentro de una empresa, teniendo en cuenta que uno de ellos será el representante legal de la empresa y posiblemente un empleado más, y las medianas empresa podrían llegar a tener empleados que puedan sobrepasar las cincuenta a setenta personas o más, lo que conlleva que tener un oficial de seguridad de la información y un responsable de protección de datos o cualquiera de los intervinientes en el tratamientos de datos pueda generar mayores costos para estas pequeñas empresas que podría manejar datos comunes o a su vez datos que sean sensibles.

Es por eso que se pretende nombrar a una sola persona quién estará a cargo de la protección de datos y de las IT (Information Technology), a quien se denominará como oficial de seguridad de la información y datos, quien en una primera instancia será una persona con bastos conocimiento en tecnologías de la información y a quien se le capacitará en temas de protección y tratamiento de datos, un curso que podrá durar hasta seis meses. En las medianas empresas con mayor cantidad de trabajadores se podrían llegar a tener todos los intervinientes, es decir un responsable o dependiendo el caso un delegado de protección de datos y a su vez un oficial de seguridad de la información quienes trabajarán de la mano, asesorandose uno al otro en sus temas de competencia, ambos sujetos deberá brindar informes a la aseguradora, de acuerdo a su área de experticia.

Esta persona que podrá ser natural o jurídica es decir se lo podría elegir a una persona o empresa especialista en ambos temas, debera estar de forma permanente o semipermanente dentro de estas empresas para realizar auditoría periódicas sobre la seguridad de los sistemas de la empresa, y será la encargada de brindar las capacitaciones a los demás trabajadores de la empresa que manejen datos, para que tenga los cuidados necesarios, como son los respaldos, manejo de doble autenticación en sistemas de la empresa manejo de antivirus, reconocimiento de correos fraudulentos entre otros.

En un principio se harán estás capacitaciones tanto al oficial de seguridad de la información y datos como a los trabajadores en general y ya posteriormente ya se lo hará por intermedio únicamente del oficial quien será el intermediario entre la aseguradora y las pequeñas y medianas empresas que puede supervisar el cumplimientos de lo establecido dentro de esta guía práctica.

6.2.3.- Sistemas de protección actualizados y homologados Internacionalmente:

Las pequeñas y medianas empresas deben contar con un sistema en el caso de las pequeñas medianamente seguro y en el caso de las medianas de alta protección, así como también deberán tener sistemas de antivirus y sistemas anti hackeos, dentro de las capacitaciones estarán el adecuado manejo de esta es decir establecer buenas prácticas de uso de estas herramientas tecnológicas.

Los sistemas o la herramientas tecnológicas que se utilizan para estas empresas deberán cumplir con normativas internacionales que estén homologadas dentro del Estado ecuatoriano y que cumplan normas ISO 31000, normas ISO/IEC29134:2017/TIC, normas COSO, y demás, que medirán el riesgo y la vulneración a la que están expuestos los sistemas de esta compañías y quienes podrán emitir informes mensuales sobre, la seguridad que se está manteniendo dentro de la empresa referente a la calidad de los softwares que utilizan, también podrán realizar un control interno en cuanto a eficacia y eficiencia de sus herramientas tecnológicas,confiabilidad de la información financiera en el caso de las cooperativas de ahorro y crédito en cualquiera de sus niveles, entre otras.

El objetivo que cumplen estos sistemas homologados es fortalecer el eje preventivo de la ciberseguridad para el impacto del daño de los datos si se presentara no sea tan abismal, se debe tener en cuenta también que estas compañías tienen que contar también con sistema de trazabilidad, quienes podrán identificar el proceso de los datos desde que el emisor envía los mismos, hasta que el emisor los recibe, en este caso se podrá mitigar los riesgos ya que se sabrá con claridad en qué punto fue que los datos o la información se pudieron haber filtrado o sustraído.

Adicionalmente a estos sistemas de protección el oficial de seguridad de la información y datos que en primera instancia deberá estar a cargo de las TIC y deberá ser de igual forma el responsable del tratamiento de datos de la empresa dependiendo de la necesidad de la compañía, esta persona deberá realizar una evaluación de riesgo en donde deberá constar todo lo concernientes al tratamiento de datos, es decir: tipo de datos que se maneja , clasificación de los datos, el riesgo del tratamientos de datos, y cómo se evitará las amenazas que los datos y la información pueden estar teniendo, así como también la eficiencia de los programas que se están aplicando para su tratamiento dentro de las pequeñas y medianas empresas.

6.2.4.- Mantenimiento de equipo en lugares avalados por la aseguradora:

En este caso se va a operar de la misma forma que se lo hace en el tema de los autos que salen de la agencia, es decir que los mantenimientos se lo harán en los lugares acreditados por la marca a nivel nacional y en caso de algún tipo de accidente se los llevará de igual forma, sino es a la agencia de origen a lugares avalados por la marca.

Entonces, la forma que se va a realizar estos mantenimientos serán el los acreditados por la aseguradora y que sean de confianza de estas, si es que la empresa no cumple con este ítem que se encuentra establecido dentro de la guía práctica, automáticamente se perderá la indemnización si en algún momento las compañías aseguradas tiene una vulneración de sus sistemas y como resultado la sustracción o pérdida de los datos o la información.

El objetivo principal del mantenimientos es impedir la manipulación de los equipos tecnológicos, es decir de los hardware y obviamente de los software de las pequeñas y medianas empresas, por parte de personas que carecen de conocimientos en sistemas o mantenimientos, al estas personas que únicamente tienen conocimientos empíricos en su gran mayoría, manipulen los dispositivos pueden dañarlos o por el contrarios puedan sustraerse información de gran valor para la compañía, es por eso que para evitar que esto suceda se enviará a establecimientos que tenga convenios directamente con la aseguradora.

6.2.5.- Robo de hardware

Dentro del trabajo de Investigación se ha encontrado al robo del hardware como un excluyente a la cobertura de la póliza pero, ahora se lo ve como una oportunidad para que se puede prestar un servicio adicional de cobertura por parte de la aseguradora, obviamente el pago de la póliza incrementa su valor, pero el beneficio es que se prestará este nuevo servicio siempre y cuando el hardware o dispositivos como ordenadores, celulares, tablets y demás, sean de propiedad de la empresa y por ende utilicen información inherente a las mismas.

En todas las empresa desde las pequeñas hasta las grandes se utilizan materiales de oficina, herramientas que pueden ser desde un lápiz hasta el uso de computadoras, las mismas como ya lo mencionaba debe ser de propiedad de la empresa en la que se trabaja bajo relación de dependencia. Bajo esa premisa se debería establecer reglas internas laborales para el adecuado manejo de estos dispositivos electrónicos y los mismos que se lo deberá tener dentro del establecimiento de trabajo pero, en el caso de que el trabajo requiera de mayor tiempo y complejidad o que se deben llevar los trabajadores, los dispositivo a su cargo, a sus hogares se podría realizar una cobertura adicional, siempre y cuando el contenido en su totalidad de esas instrumentos tecnológicos sean temas relacionados estrictamente con el labor de la empresa.

Si estos artefactos tecnológicos son utilizado como herramientas laborales se los cubrirá, si existiera alguna vulneración a los sistemas de estos instrumentos, es decir, datos e información relacionados a la empresa o a sus clientes o si por el contrario no se da ni se ha dado la vulneración y sustracción de datos durante el transcurso de 1 a 2 años, la acción de cobertura prescribirá y no se podrá indemnizar posteriormente a este período establecido.

Se debe señalar que si los dispositivos tienen otro fin ajeno a los labores dentro de la empresa es decir acceso a redes sociales personales o correos personales, entre otros, que son un foco de entrada de ciberataques, no se cubrirá la pérdida de la información o base de datos que se manejen en eso dispositivos adicionalmente se recomienda tener en cuenta y con claridad el derecho de los trabajadores a la desconexión para que de igual forma se pueda cumplir con lo establecido dentro de del Acuerdo Ministerial 237 de Trabajo y evitar que los dispositivos puedan salir de su lugar de trabajo.

6.2.6.- Políticas de protección de datos

En el Ecuador con la entrada en vigencia de la ley de protección de datos personales desde el 26 de mayo de 2021, obliga a todas las empresas que manejan datos personales a que cuenten con políticas de protección de datos, por lo que tanto las medianas como pequeñas empresas dependiendo de la extensión y tipo de información que manejen, deberán contar dentro de sus compañías, de igual forma deberá contar con un plan de contingencia para realizar una evaluación de riesgo eficiente con estas políticas.

El contenido mínimo de las políticas de protección de datos deberán contener fundamentalmente el consentimiento expreso de los datos del titular, la finalidad para la cual van a ser utilizados estos datos, el tiempo de duración que van a tratarse estos datos, qué tipo de protección se le va a otorgar a estos datos, notificación previa si se va a modificar algo de la política de la protección del tratamiento de datos, deben tener también claramente un procedimiento administrativo establecido y que sea fácil para el acceso y rectificación de los datos y no tener que activar garantías constitucional es como el habeas data, algunos de estos son los requisitos mínimos que debe contener esta política de protección de datos adicionales a los que la ley establezca.

El objetivo de estas políticas, es la protección del tratamiento de datos y las pequeñas y medianas empresas deben prestar dicha protección a los derechos de sus clientes de acuerdo al tipo de datos que se manejen, se utilizaran programas reconocidos con normas internacionales dedicados al cuidado de estos datos como las normas ISO 27001:2022, 27001:2019 y 27001:2020 y sobre todo herramientas tecnológicas encargadas de la trazabilidad de los datos, cuyo objetivo principal es verificar el proceso de los datos, mientras los datos son enviados por emisor hasta llegar receptor, como fue la trayectoria de estos datos e identificar prematuramente si existiera una filtración de datos, una sustracción, o algún tipo de fuga, siempre irán de la mano el oficial de de seguridad de la información en el caso de las pequeñas empresa y el oficial de seguridad de la información junto con el responsable de tratamiento de datos.

6.2.7.- Oficial de seguridad de la Información y datos

La figura del oficial de seguridad de la información y datos se la ha creado desde la iniciativa de una resolución de la SEPS pero con nombre de invención propia que se encuentra en el anexo 10, se incluye como un punto obligatorio en esta póliza sobre todo por fines de control interno. Es evidente que una compañía mediana y aún peor una pequeña podrán contar con un departamento de TIC y seguridad de la información. Es por este motivo que se señala a una persona natural que pueda ejercer este cargo, rendir cuentas a la aseguradora y asegurar que se implementen las buenas prácticas corporativas en aquellos asuntos relacionados con la seguridad de los sistemas informáticos y la protección de la información que estos contienen.

Esta persona deberá tener un nombramiento por parte de la administración de la compañía, cuando se trate de empresas medianas. Cuando sean empresas pequeñas podrá ser una persona natural en relación de dependencia o con un contrato de prestación de servicios; esta deberá obligatoriamente ser presentado a la aseguradora previa la suscripción de la póliza. En el caso de empresas obligadas a contar con un delegado de protección de datos podrá ser la misma persona, (oficial de seguridad de la información y datos), sin ningún tipo de perjuicio, ya que podrá comparecer ante la autoridad de control, es decir el Superintendente de datos ya que tendría autonomía completa.

El oficial de seguridad de la información y datos como primera función tendrá la elaboración de la guía práctica de procedimientos de ciberseguridad. Esta misma deberá tener la firma del representante legal y ser remitida a la compañía de seguros. Con este documento, la aseguradora contará con una base de todos aquellos parámetros que deberían ser cumplidos, y este hecho podría marcar el pago o la negativa de un reclamo.

El oficial de seguridad de la información y datos deberá contar con ciertas horas de capacitación que requiera la compañía de seguros. Este tiempo de formación tendrá que ser por algún órgano que pueda emitir una certificación, la cual tendrá que aprobarse por la aseguradora previo a la firma de la póliza. Al ser el oficial una figura que pudiese tener otras funciones dentro de la compañía o de ser el caso sólo trabajar bajo prestación de servicios, no necesariamente será una persona con formación en protección de datos personales, sin embargo deberá presentar certificaciones que demuestren que ha adquirido al menos algún tipo de conocimiento básico en el tema.

El objetivo de que pueda presentar estas certificaciones es con el fin de que todo este conocimiento pueda servir para la elaboración de la guía en primer lugar. Como segundo punto esta persona deberá poder realizar el control de las buenas prácticas y la debida diligencia en cuanto al manejo de la seguridad de sistemas y redes. Por último, su conocimiento debe ser replicado al resto del personal de la empresa, a fin de que pueda capacitarlos o poder elegir que tipo de capacitación deben tomar y en qué temas.

Esta figura que se ha planteado crear para fines de control de ciberseguridad podría ser un importante motor de cambio dentro de las compañías pequeñas y medianas. Así mismo es de gran relevancia que, a pesar de contar con la póliza de ciberseguridad, toda compañía cuide de su core de operaciones, la afectación de este puede significar el detener la producción y no generar ingresos. Si bien es cierto que esta persona (el oficial de seguridad de la información y datos), será un parámetro de confianza para la aseguradora, puede ser de igual forma un apoyo al crecimiento y cuidado de aquellas herramientas digitales con las que una gran cantidad de empresas manejan su funcionamiento.

6.3.- Recuperación de la Información

La recuperación de la información de las pólizas de ciberseguridad es una de las fases dentro de la protección de la información y las bases de datos después de la fase preventiva, que es la principal para evitar un sustracción prematura de información o datos de las pequeñas y medianas empresas, las medidas que se tomarán dentro de esta fase son las siguientes:

6.3.1.- Asesoría legal en caso de daño

La Asesoría legal va enfocada más que nada a las pequeñas y medianas empresas en el caso de se presente alguna contingencia de sustracción de los datos de sus clientes, para que ellos a su vez sepan cómo comunicarse directamente con sus clientes y saber que decir, para no crear expectativas que puedan generar un descontento general en los demás clientes, más o menos como un silencio bancario y que no se pueda divulgar el rumor del robo de la base de datos información de algunos cliente que también podrían estar implicados.

En estos casos es fundamental identificar de forma concreta basándose en las herramientas de trazabilidad que ya utilizan estas empresas, en donde se produjo la sustracción de la información y que tan grande puede llegar a ser el impacto del robo de estas bases de datos, de que clientes no más se han producido este robo, se debe dar a conocer los derechos a los que son acreedores los titulares de los datos y qué acciones podrían iniciar en contra de estas compañías, de igual forma se les debe notificar con el problema que la sustracción de los datos con hasta 72 horas de que se haya identificado que efectivamente se produjo el problemas, lo más razonable es que la persona que entra como intermediario es un abogado especializado en protección de datos que, de la mano con el oficial de de seguridad de la información de datos y el responsable de tratamiento de datos son quienes, con conocimiento casa adentro pueden brindar una información al abogado de la aseguradora para que el pueda brindar una asesoría completa tanto a las pequeñas y medianas empresas como a los clientes.

La idea principal dentro de esto es que el asesor pueda crear un ambiente de tranquilidad y seguridad entre las compañías y los clientes para establecer ciertos acuerdos, previos a iniciar cualquier tipo de acción por parte de los clientes en contra de estas pequeñas y medianas empresas, a su vez no perder la confianza de los clientes y tratar de retribuir de alguna forma el incidente causado, con ciertos beneficios que deben considerar las empresas para enmendar esta sustracción de los datos.

6.3.2.-Uso de técnicos avalados por la aseguradora

En el eventual caso de haber sufrido un ciberataque el asegurado puede requerir de técnicos para la reparación de sus sistemas. Sobre todo al verse afectado por ataques como el “ransomware” (secuestro de información), el contratante del ciberseguro requerirá de especialista que puedan atender a las afectaciones de sus sistemas informáticos y la pronta recuperación de información. De cualquier manera, existen varios tipos de daños que pueden generarse, equipos con funcionamiento lento por ejemplo.

Al tratar con datos personales e información de alta relevancia para el asegurado y sus clientes, usuarios y hasta proveedores, es importante que el servicio técnico sea de alta calidad. La aseguradora deberá entregar al cliente un catálogo de especialistas y técnicos que puedan brindar el servicio adecuado. La cobertura en cuanto al servicio técnico posterior al ataque tendrá exclusividad para que el servicio sea brindado por aquellos que consten dentro del aval de la empresa de seguros.

Aunque pueda parecer autoritario por parte de la compañía de seguros, es importante que existan estándares de alta calidad para saber que el daño ha sido apaciguado. Además al existir una extensa oferta de este tipo de servicios, es importante que la compañía de seguros pueda contar con la certeza de que su cliente trata a sus sistemas con el personal más calificado, así este tratamiento resultará preventivo y eficiente para evitar ataques cibernéticos a futuro.

6.3.3.- Contar con respaldo de información

Como se ha mencionado extensivamente en este trabajo, el core de operaciones de muchas empresas, grandes o pequeñas está ligado ampliamente con sus sistemas informáticos. Siendo esta una realidad latente, las empresas deben saber que la información que manejan estará expuesta a los peligros de la red. Una de las formas que se requiere es un sistema de protección, donde los datos e información que se maneja en una compañía pueda tener un respaldo. Existen varias clases de servidores espejos (mirrors), y muchos de estos pueden tener un coste evidentemente alto.

Sin embargo, hay que tener en cuenta que se puede también utilizar métodos que resulten accesibles para una empresa pequeña o mediana. Un ejemplo puede ser contratar servicios de “mirroring” en la nube. La información evidentemente deberá ser actualizada de forma constante y obligatoriamente será la misma que aquella información original.

Para hablar de pequeñas y medianas empresas hay que enfocarse en aquellos métodos que resulten cómodos al momento de realizar esta inversión en seguridad. Invertir en sistemas con una fuerte infraestructura costosa no suele ser una opción viable para una empresa con prioridades como el pago de sus haberes empleados, proveedores, gastos corrientes, etc. Es así que se debe poner atención en aquellas soluciones que sean más sencillas cuando se habla en términos económicos.

Evidentemente el uso de un servidor en la nube, es una solución cómoda, sin gasto de hardware, fácil de aumentar el espacio (esto aumenta el costo) y el acceso igualmente es flexible, pues puede ser desde varios dispositivos. Sin embargo este es un problema cuando de ciberseguridad se trata, pues el acceso al servidor “espejo” debe ser restringido para el uso exclusivo de actualización del sistema, mantenimiento y obviamente en caso de una emergencia en cuanto al acceso a los sistemas informáticos que sean utilizada habitualmente por la compañía.

Por lo tanto hay que concluir que la compañía deberá obligatoriamente respaldar su información. El método podrá ser a criterio de la administración del asegurado, sin embargo el encargado de IT en caso de un ciberataque deberá rendir cuentas a nombre de la compañía en caso de una eventual falla del servidor utilizado para el mirroring. Este es un método, que si bien no es infalible es de una gran utilidad, pues evitará una pérdida completa de información o un pare temporal de actividades que resulte en pérdidas económicas y reputacionales que devengan en una situación catastrófica para la compañía.

6.4.- Mitigación de daños

Esta póliza (ciberseguridad), funciona en torno al concepto de reducir el daño que deviene de un ataque a los sistemas informáticos o al core operativo de una empresa. La afectación que sufre el asegurado es de de aquellas que pueden ser percibidas con facilidad como un daño material, es por esto que la indemnización se enfoca en en temas subjetivos por un lado, como la reputación y en factores económicos por otro como es el caso de los gastos legales o de restauración y saneamiento de los sistemas informáticos. A continuación se tocarán los temas más relevantes en cuanto a la mitigación de daños.

6.4.1.- Con cada reclamo informe del oficial de seguridad de la información y datos

Al ser una labor del oficial de seguridad de la información y datos el mantener informada a la compañía de seguros sobre cualquier asunto que pudiese devenir en un eventual reclamo, éste deberá contar con ciertos requisitos. En este caso específico la aseguradora deberá poner procedimientos más estrictos para poder evaluar el daño ocurrido, pues la afectación viene de procedimientos donde el oficial de seguridad de la información y datos debe seguir aquellos pasos establecidos en la guía. Como se ha establecido anteriormente, el daño debe ser fortuito, y en el caso de esta póliza, teniendo en cuenta que no fuese de medida devastadora para la compañía, se podría indemnizar por una sola vez a causa de impericia humana.

Es importante establecer que la aseguradora contará con un profesional en la materia (redes y sistemas) a fin de constatar las causas del problema. Es aquí donde se genera una de las obligaciones más importantes del asegurado con la compañía aseguradora. Se deberá presentar un informe de daños a raíz de un ciberataque. El informe será en su totalidad realizado por el encargado de IT con aquellos parámetros que sean requeridos por la compañía de seguros.

El informe, preliminarmente deberá contar con ciertos requisitos básicos. En primer lugar la descripción del ataque que ha sufrido el asegurado, con la mención del tipo de delito (no necesariamente de aquellos mencionados en el Código Orgánico Integral Penal, sino en términos digitales). En segundo lugar deberá especificar las causas por las que el asegurado sufrió el agravio a sus sistemas. También es importante que se haga una evaluación de los daños ocasionados, en términos económicos, reputacionales, de operaciones y todo aquello que haya sido siniestrado a causa del ciberataque y que se encuentre en la cobertura de la póliza.

Evidentemente con la evaluación del inspector se podría pedir más requisitos o una ampliación al informe. El inspector podrá pedir una entrevista con el oficial de seguridad de la información y datos a fin de revisar el informe, analizar los daños presentados en el reclamo y todo aquello que considere necesario. Al finalizar esta acción se podrá presentar oposición al reclamo y negar al mismo.

El informe deberá ser remitido dentro del término que sea establecido por la compañía aseguradora. De igual manera, deberá estar completo, previo a la revisión del inspector de la aseguradora. Evidentemente y por cuanto la aseguradora ha establecido un oficial de seguridad de la información y datos, la firma de este será imprescindible dentro del informe para empezar al análisis del pago de la indemnización o la negativa del reclamo.

6.4.2.- Profesionales del derechos otorgados por la compañía

Una de las consecuencias que más le preocupa a toda persona natural o jurídica al dedicarse a algún tipo de actividad económica son los gastos que pudiesen surgir a raíz de una demanda por daños relacionados con la prestación de sus servicios. En el caso de las pólizas de ciberseguridad la preocupación es, la afectación que pudiese existir al sufrir un ciberataque, y cómo esto puede replicar en la empresa responsable de los datos consignados por los titulares. Este es el motivo por el cual la póliza al tener por objetivo la transferencia del riesgo que pueda existir en un supuesto ciberdelito, debe encargarse de cubrir este aspecto que eventualmente podría surgir al haber sufrido una violación a los sistemas del asegurado.

La póliza de ciberseguridad, como parte de la mitigación del daño tendrá en cuenta los gastos legales que pudiesen llegar a existir. El costo de litigio y patrocinio legal, cuando sea con el equipo legal que contrate y sugiera la compañía aseguradora será cubierto en todo lo pactado menos los valores deducibles. Sin embargo, si el cliente quisiera contratar un equipo legal diferente, el costo será mayor al deducible. Evidentemente el cliente asumiría un riesgo, pues la compañía de seguro tendrá en cuenta la contratación de especialistas en la materia, quienes tendrán como cometido el preservar el bienestar del asegurado.

El proceso legal a raíz de una afectación que ya está afectando a una empresa, puede verse como un gasto doble, por un lado solucionar los daños del ciberdelitos y por otra parte encargarse de un litigio eventual. Es una situación tediosa, complicada y de alto peligro en cuestiones económicas y reputacionales para una empresa el tener que enfrentar un juicio para resarcir el daño a un cliente. Es así que un objetivo de alta relevancia en lo que concierne a la póliza de ciberseguridad será el poder relevar al cliente de esta labor incómoda y poder así disminuir la afectación que de por sí ya estaría sufriendo el asegurado.

6.4.3.- Respetar la cláusula de jurisdicción y competencia

Las pequeñas y medianas empresas al ser los asegurados directos de las compañías de seguros, la misma debe velar por los interes de ellas, es por eso para con el fin principal de llegar a un acuerdo entre el cliente y esta empresa se debe establecer cláusulas de jurisdicción y competencia en cuanto a los métodos alternativos de solución de conflicto y dentro del cual se busca utilizar otro método más amigable para llegar a un convenio entre las partes intervinientes y poder mantener de esta forma principalmente la confidencialidad del hecho ocurrido y no perder la confianza entre los clientes.

Bajo esta premisa y teniendo en cuenta que esta cláusula es muy importante en varios contratos en materia civil, se debe establecer con claridad de que en una primera instancia las partes se someterán a un centro de mediación que acuerden las voluntades esto dependerá del territorio en donde se suscriba la póliza, y dado el caso que en esta primera mediación no se pueda llegar a un acuerdo o se ha llegado a un acuerdo parcial que no progresó, se deberá someter, a un centro de arbitraje de igual forma acorde con las partes, se debe respetar el laudo arbitral emitido por este centro de arbitraje, para de esta forma no poder presentar ningun acción judicial, es decir renuncian a cualquier tipo de jurisdicción y competencia de un procedimiento judicial y penal.

La importancia de tener esta cláusula de jurisdicción y competencia dentro de una póliza de seguridad y que tanto el cliente como la pequeñas y medianas empresas sepan su objetivo, es brindar a los cliente seguridad jurídica, tener mayor eficiencia en la solución de conflicto y efectivamente al ser esto métodos más amigables tratar de llegar a convenios que satisfagan las necesidades los clientes y de las compañías aseguradas, se de saber también que el efecto de estas decisión son la de una sentencia ejecutoriada en última instancia es decir igual validez que los proceso judiciales tradicionales.

6.4.4.- Recuperación de imagen

Algo vital que busca un asegurado al contratar una póliza de ciberseguridad, es no perder su buena imagen en el mercado, o quizá no deteriorarla de forma irreversible luego de sufrir un ciberataque. El retomar las actividades básicas, aún después de que se logró sanear los sistemas y el core operativo de una empresa se encuentra en un estado óptimo para ser utilizado, puede ser un tema complejo, pues muchos clientes o usuarios se habrían alejado de la compañía. Parte vital de la mitigación de los daños es poder dar a conocer el compromiso de la compañía con sus clientes o usuarios.

La póliza de ciberseguridad al tener un objetivo integral de reparación de daños, tendrá asignado un valor específico y rentable tanto para la aseguradora como para el asegurado para que este último pueda recobrar su buena imagen. Este valor será destinado a un equipo especialista en marketing y manejo corporativo de imagen a fin de tener una evaluación preliminar donde pueda ser notoria una recuperación reputacional. Esta preocupación es el motivo para que se contraten este tipo de pólizas de seguros.

Tanto los gastos legales, así como también el daño reputacional son factores en los que el asegurado querrá tener una protección. La póliza ofrecerá a expertos que asesoran al cliente en cuanto al proceder en lo que a recuperación de imagen trata. De por sí es complicado para una empresa pequeña o mediana entrar al mercado, es así que una correcta administración de imagen resultará el poder continuar las operaciones o cerrar estas.

6.4.5.- Cálculo de la indemnización

Es vital tener en cuenta los criterios de indemnización que se tendrán en una póliza donde el bien asegurado es un activo intangible. Además, se debe considerar que en un mundo donde la tecnología es un factor transversal, el "core" de operaciones de una considerable cantidad de negocios se basa en el uso de sistemas informáticos, donde estos son los que mueven, al menos la parte operativa del negocio. Es así que el daño puede generarse desde varios puntos, siendo así que la reparación que busca la compañía tiene diferentes matices y en varios aspectos.

Un ejemplo de esto son las afectaciones reputacionales que en un eventual ataque a los sistemas informáticos de una compañía se pudiesen generar. Una empresa pequeña o mediana al no tener una representación considerable en el mercado o un historial que acredite su reputación necesitará ayuda para levantar su imagen con los usuarios o clientes.

También existe la necesidad de soporte en cuanto al factor legal. No solo son los gatos de litigio, también es la asesoría legal lo que se busca. Estos gastos pueden ser considerables, además del tiempo que se puede invertir en la búsqueda de personal calificado para llevar estos procesos. Es así que todo aquello relativo a los asuntos jurídicos son temas que deben ser considerados al momento del cálculo de la indemnización.

Un tercer punto a considerar es el saneamiento y reparación de los sistemas. Como se mencionó anteriormente, la parte operativa suele estar ampliamente ligada al uso de sistemas informáticos, y el hecho de parar las actividades por el daño a estos representan pérdidas prácticamente imposibles de cubrir. A parte de esto el cubrir estos costos resultan onerosos sin perjuicio del hecho de no estar generando ningún tipo de ingreso.

Todos estos factores son aquellos que se deberán cubrir con la póliza de ciberseguridad para pequeñas y medianas empresas. Estos parámetros son los que se deben considerar al momento de señalar la cobertura, el deducible, el copago y el resto de criterios técnicos propios de una póliza de seguros. El propósito de estos lineamientos es señalar aquellos factores para tener en consideración cuando se suscribe la póliza, se realiza el reclamo, la inspección y finalmente la indemnización.

6.5.- Análisis de Riesgo Post Ataque

Dentro del pago de la indemnización por la existencia de un siniestro (ciberataque en este caso), es fundamental para la aseguradora el inspeccionar las causas y cumplimiento de la póliza por parte del asegurado. Al suscribir el contrato de seguros, se estipulan exclusiones al pago de indemnización, derecho de la aseguradora y criterio fundamental para la existencia de un producto de seguros. La compañía de seguros, con personal experto en la materia realizará el análisis correspondiente a fin de proceder a la aprobación o negativa del reclamo.

6.5.1.- Verificación del cumplimiento del manual

Para la verificación del cumplimiento del manual se necesita del apoyo del intermediario entre la pequeñas y medianas empresas y la aseguradora, en este caso se necesita de la entrega de la información mediante informes que debe presentar el oficial de seguridad de la información y datos, en periodos mensuales dentro del cual debe contener evaluación de riesgo en donde la aseguradora pueda ver que ataques se han producido actualmente, cual es el riesgo que la base de datos podría presentar, de igual forma se deben presentar la eficiencia y eficacia de los programas homologados para la protección de los datos en cumpliento con los estandares internacionales que ya han sido mencionadas.

Se realizarán dentro del primer año auditorías para verificar y constatar que efectivamente se estaba cumpliendo con los establecido dentro de la guía práctica, en un primer momento en dos ocasiones dentro del primer año se lo hará cada seis meses y posteriormente al primer año se los realizará por una sola ocasión de forma anual, la aseguradora podrá realizar en cualquier momento esta auditoría previo a notificación con quince a treinta días de anticipación y la empresa deberá constar con toda la documentación a esta fecha no podrá existir una prórroga para la realización de esta auditoría salva caso fortuito o fuerza mayor.

El incumplimiento a la guía práctica de procedimiento de ciberseguridad podrá acarrear efectos legales como la terminación unilateral por parte de la aseguradora si el caso amerita, se analizará si algunas situación se podría subsanar pero solo se lo hará por una ocasión ya que, el eje preventivo dentro de este proceso es una de las fases más importante y fundamental para la protección de la ciberseguridad de los datos en las empresas, es por eso que la aseguradora en cualquier momento podrá solicitar el envío de informes del área o del tema que vea que tiene mayor debilidad siempre ampara de la evaluación de riesgo que será obligatorio realizarlo.

6.5.2.- Investigación al oficial de seguridad de la información y datos

Luego de que se haya producido un ciberataque a un asegurado, la compañía de seguros iniciará su proceso de inspección. Cuando se procedan a revisar las causas de esta vulneración a los sistemas de un cliente, la persona que rendirá cuentas será el oficial de seguridad de la información y datos. Por parte de la aseguradora, esta figura será imprescindible y no puede haber emisión, suscripción, reclamo o indemnización de una póliza de ciberseguridad para pequeñas y medianas empresas sin esta persona.

El inspector de la aseguradora en primer lugar deberá constatar todo lo que consta en la guía práctica de procedimiento de ciberseguridad. Una vez que se haya revisado esta guía, se debe revisar que dentro de la compañía todos estos procedimientos sean cumplidos a cabalidad. Es así que se realizará una auditoría del cumplimiento de la debida diligencia en cuanto al manejo de la seguridad de la información acorde a lo descrito en la guía.

El resultado de este proceso es lo que determinará si se justifica el pago del reclamo o su negativa. La compañía de seguros al tener su ente de control (Superintendencia de Compañías Valores y Seguros), debe justificar con la debida motivación toda negativa a los reclamos realizados por los clientes, y en este caso, al estar estipulado que el incumplimiento reiterado de la guía, la falta de control en uno o más puntos de esta es una causal directa de negativa, cuando haya sucedido por segunda vez. El oficial de seguridad de la información y datos, no podrá seguir cumpliendo con esta función cuando se haya producido un ciberataque por negligencia o falta de vigilancia y control por más de una vez.

6.5.3.- Restauración de sistemas

Al culminar la fase de revisión e inspección por parte de la compañía aseguradora se generará el informe para el pago de la indemnización bajo los procedimientos establecidos dentro de los anexos 11, 12, 13. Al evaluar las pérdidas y daños se tendrá en cuenta aquello que sin lugar a dudas queda afectado, y son los sistemas informáticos de la compañía. Se ha establecido en reiteradas ocasiones en este trabajo que el centro o core de operaciones de estas compañías serán sus sistemas informáticos, en consecuencia han contratado una póliza de seguros de ciberseguridad.

La aseguradora debe hacer en su informe de evaluación de daños aquellos campos que requerirán de la cobertura. Sin perjuicio de todo aquello que deba ser indemnizado, lo primero será restablecer la correcta funcionalidad de los sistemas. Esto permitirá que el asegurado pueda volver de la manera más rápida al cauce normal de sus operaciones.

Los sistemas luego del ataque deben retornar a tal estado que no exista un riesgo latente o residual de la vulneración a la cual fueron expuestos. De la misma forma se debe certificar al asegurado que sus sistemas han sido saneados de manera correcta, permitiendo así que haga conocer a sus clientes que en cuanto a la funcionalidad del lado informático todo ha retornado a un estado estable y propicio para retomar sus funciones. Sin que este punto quede resuelto no existe la más mínima posibilidad de poder ayudar a un cliente que ha sufrido un ciberataque a levantar nuevamente sus operaciones luego de haber sufrido un ciberdelito que perjudicó a sus sistemas.

7.- Conclusiones y Recomendaciones

7.1.- Conclusiones:

Después de Investigar a varios autores en diferentes espacios y tiempos y que han aportado para el desarrollo de este trabajo académico se ha llegado a las siguientes conclusiones:

7.1.2.- Al ver que algunas compañías catalogadas como pequeñas y medianas, en Ecuador, no cuentan con los debidos protocolos en cuanto a seguridad de sus sistemas, información y datos. Al verse vulnerables en un entorno en el cual la base de operaciones se centra en los sistemas informáticos e internet, se crea la necesidad de una protección a aquella información que manejan, incluyendo datos de clientes, empleados y todas sus bases de datos corporativas.

7.1.3.- Las Pólizas de ciberseguridad dirigidas para las pequeñas y medianas empresas tienen altos costos en algunos casos no son proporcionales para el tipo de información que manejan estas compañías, es por eso que para que las aseguradoras no pierdan, se trabajaran con partners que, al nosotros publicitar sus sistemas ellos nos otorgaran un porcentaje por la venta de una de sus herramientas digitales y así las aseguradoras poder ofrecer precios accesibles y razonables.

7.1.4.- Tras revisar el marco legal de las pólizas de ciberseguridad, es evidente que las regulaciones ecuatorianas proporcionan un fundamento sólido para la protección de datos. Sin embargo, la implementación de estas pólizas en las pymes requiere un enfoque adaptado que considere tanto la viabilidad económica como las especificidades operativas de estas empresas.

7.1.5.- Dentro de la Investigación se concluyó que, el objetivo de la compañía de seguros es obtener rentabilidad con aquellos productos que saca al mercado. Por esta situación es que se ha previsto figuras como el oficial de seguridad de la Información y datos, así como todas las exclusiones para este tipo de pólizas. Así la compañía de seguros precautela que el asegurado cumpla con la debida diligencia en ciberseguridad y protección de datos personales.

7.1.6.- El establecer la figura de "Oficial de seguridad de la Información y datos", es vital para que exista la certeza del cumplimiento de parámetros básicos de la seguridad de los sistemas y la protección de la información que estos contienen. Además, al no poder sustentar el gasto de un departamento específico de IT, las empresas pequeñas y medianas deberán contar con una persona que pueda responder en caso de algún tipo de falla o vulneración a sus sistemas. Esta persona es un intermediario que tiene el rol de crear seguridad ante la empresa de seguros y en relación al cumplimiento de los parámetros de seguridad con los que deberán contar los asegurados. Es importante que pueda existir control interno con la finalidad de evitar que se produzcan ataques, pues una póliza de seguros es de carácter preventivo y en situaciones aleatorias.

7.1.7.- La elaboración de una guía práctica de procedimiento de ciberseguridad es un método que facilita el manejo de la póliza para ambas partes. En cuanto a la aseguradora, tiene los parámetros para demostrar si el Oficial de seguridad de la Información y datos ha puesto en práctica la debida diligencia mencionada en la guía, lo cual es el punto para justificar el pago o negativa del reclamo. En cuanto a los asegurados, genera una cultura de buenas prácticas en el manejo de ciberseguridad, establece lineamientos para renovación de licencias y equipos, y ayuda a evitar siniestralidad en cuanto a ciberdelitos. Teniendo una base digital en la operación de los negocios de los asegurados, estos deben facilitar el cuidado de aquellas herramientas que permiten una mejora en cuanto al servicio y productividad, la guía son las directrices para llegar a que se cumplan estos objetivos.

7.2.- Recomendaciones

7.2.1.- Se recomienda la adaptación de la guía práctica de procedimientos de ciberseguridad, en un lenguaje sencillo y que tenga una rápida comprensión para todas las personas que lo manejen además de llegar a ser parte de la cultura de los trabajadores dentro de las pequeñas y medianas empresas.

7.2.2.- Revisar y actualizar la póliza anualmente o en caso de cambios significativos en la empresa o en el panorama de amenazas con el fin de poder realizar una nueva evaluación de riesgos en relación al caso de cada compañía. Esto ayudaría a revisar el costo de la prima, monto asegurado y el riesgo asegurable, y poder adoptar un nuevo plan de estrategias para una mejor diligencia en los procesos de tratamientos de datos.

7.2.3.- La compañía de seguros con la que se contrate una póliza de ciberseguridad deberá asesorar al asegurado de manera integral cuando este haya sufrido un ataque a sus sistemas. Esto quiere decir que, en la evaluación de daños se deberá tener en cuenta los aspectos vulnerados, tanto en sus sistemas informáticos, como daño reputacional o gastos legales. De igual manera se debe dejar una reserva en cuanto a posibles afectaciones futuras que se pudiesen generar. En este último caso en términos de daño reputacional o gastos de litigio.

7.2.4.- La compañía de seguros al culminar con la indemnización debe facilitar al asegurado una certificación de saneamiento de los sistemas. Esto sirve para poder acreditar ante cualquier cliente, proveedor o acreedor del asegurado que la información que mantiene con esta empresa, se mantiene en un estado debido de vigilancia y cuidado. Así mismo servirá en el caso de una futura y posible auditoría del ente de control en cuanto a protección de datos personales.

7.2.5.- Para ilustrar la aplicación de nuestras recomendaciones, se tiene el caso específico de Banco del Pacífico en el cual se indica, en una institución "grande" como un banco que el gasto en cuanto a seguridad representa aproximadamente el 15% del gasto anual de esta entidad. Esto demuestra la necesidad de esta inversión con fines de protección, tanto física como virtual. Es altamente necesario en un entorno con una creciente tasa de ciberdelincuencia el contar con una póliza que traslade el riesgo en caso de un siniestro.

8.- Referencias:

Ackerman, R. (2021). Corrupción y Covid 2019. *Eunomía. Revista en Cultura de la Legalidad*, 37. https://e-revistas.uc3m.es/index.php/EUNOM/article/view/6062/4407

Alcivar, C., Calderon, J., Blanc, G., & Duchi, B. (2016). *ANALISIS ESPACIAL DE LOS DELITOS Y APLICACIÓN DE LA NORMATIVA JURIDICA ECUATORIANA*. UNIVERSIDAD ECOTEC. https://libros.ecotec.edu.ec/index.php/editorial/catalog/view/32/29/315-1

Alonso, J. C., & Berggrun, L. (2015, 04). Introducción al Análisis de Riesgo Financiero. *Ecoe Ediciones*, 270. https://elibro.net/es/ereader/udla/126447

Arreola, A. (2019). *Ciberseguridad: ¿Por que es importante para todos?* (Primera ed.). Siglo XXI editores. https://books.google.es/books?hl=es&lr=&id=ZqHDDwAAQBAJ&oi=fnd&pg=PT5&dq=ciberseguridad+que+es&ots=yi993aZx84&sig=pD9oZNTA5jY5S--cwYvWdjaC5tw#v=onepage&q&f=false

Barrientos, M. (2015, mayo). EL DEBER PRECONTRACTUAL DE INFORMACIÓN EN EL CONTRATO DE SEGURO, UN PRODUCTO FINANCIERO Y DE CONSUMO. ESTUDIO DE SUS FUENTES / PRECONTRACTUAL DUTY OF INFORMATION IN INSURANCE AS A FINANCIAL PRODUCT. A STUDY OF HISTORICAL LEGAL SOURCES. *Revista Chilena de Derecho*, 3. https://www-jstor-org.bibliotecavirtual.udla.edu.ec/stable/42776128?searchText=Conceptos+Generales+del+Seguro+y+la+Naturaleza+del+Contrato&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3DConceptos%2BGenerales%2Bdel%2BSeguro%2By%2Bla%2BNaturaleza%2Bdel%2BCont

Carrión, C. (2021). *El contrato de seguro en el Ecuador – conceptos básicos y análisis de la reticencia, falsa declaración y acuerdos transaccionales*. https://revistas.ecotec.edu.ec/index.php/rnv/article/view/539

CASTELLTORT, I. (2022). *El papel de las tecnologías de la información en el proceso de Due Diligence*. Universitat Rovira i Virgili. https://accid.org/wp-content/uploads/2023/06/El-papel-de-las-tecnologias-de-la-informacion-en-el-proceso-de-Due-Diligence_watermark.pdf

Código orgánico Integral Penal. (2014). *Suplemento del Registro Oficial No. 180*.

Código Orgánico Integral Penal. (2014, 02 10). *Registro Oficial suplemento 180*. https://www.igualdadgenero.gob.ec/wp-content/uploads/2023/03/CODIGO-ORGANICO-INTEGRAL-PENAL-COIP.pdf

Código Orgánico Monetario y Financiero. (2017, 12 29). *Registro Oficial Suplemento 403*. https://www.cosede.gob.ec/wp-content/uploads/2019/08/LEY-GENERAL-SEGUROS.pdf

Comisión Europea, Dirección General de Mercado Interior, Industria, Emprendimiento y Pymes. (2019, SEPTIEMBRE). Guía del usuario sobre la definición del concepto de pyme. *Oficina de Publicaciones de la Unión Europea*, 39. https://op.europa.eu/es/publication-detail/-/publication/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1

Cose, R. (1937). The Nature of the Firm. https://www.loc.gov/item/2017732143/

Cuenca, H. A. (2022). In *Articulación de la Fiscalía General del Estado para la persecución de delitos cibernéticos* (p. 44). INSTITUTO DE ALTOS ESTUDIOS NACIONALES LA UNIVERSIDAD DE POSTGRADO DEL ESTADO. https://repositorio.iaen.edu.ec/bitstream/handle/24000/6045/TRABAJO%20DE%20TITULACI%C3%93N%20HUGO%20CUENCA%20ESPINOSA.pdf?sequence=1&isAllowed=y

De Haro, F. J. (2020, 11 25). Crimen, cibercrimen y an´alisis forense inform´atico. *I.E.S Celia Viñas*, 18. https://dialnet.unirioja.es/descarga/articulo/8180667.pdf

Estruga, N. (2021, October 11). *Qué son y cómo funcionan los ataques de suplantación de identidad*. EALDE Business School. Retrieved January 3, 2024, from https://www.ealde.es/ataques-de-suplantacion-de-identidad/

Fernández, L. (2023, September 22). *Ciberseguridad y Hardware: Otra perspectiva en la seguridad. – Rawson BPO*. Rawson BPO. Retrieved March 5, 2024, from https://rawsonbpo.com/ciberseguridad-y-hardware/

Gentbutsu, G. (2023, March 27). *Mitigación de riesgos: Genchi Genbutsu I SafetyCulture*. Safety Culture. Retrieved January 4, 2024, from https://safetyculture.com/es/temas/mitigacion-de-riesgos/

Giraldo, A. (2022, March 25). *¿Qué partes intervienen en un contrato de seguros?* WTW. Retrieved December 21, 2023, from https://www.wtwco.com/es-co/insights/2022/03/que-partes-intervienen-en-un-contrato-de-seguros

Hernandez, A., & Fojón, E. (2016, junio). Ciberseguros: la ultima linea de defensa. *transferencia de riesgos*, (120), 98. https://www.thiber.org/wp-content/uploads/2016/06/sic120-ciberseguros.pdf

Hernandez, R. (2013). Los riesgos de las entidades aseguradoras en el Marco del Enterprise Risk Management (ERM) y el control interno. *Revista Innovar Journal*. https://www-jstor-org.bibliotecavirtual.udla.edu.ec/stable/43786405?searchText=analisis+de+riesgo+en+seguros&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3Danalisis%2Bde%2Briesgo%2Ben%2Bseguros%26so%3Drel&ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&refreqid

Hidalgo, J. (2017, November 9). *INGENIERÍA DEL SOFTWARE Y CIBERSEGURIDAD*. YouTube: Home. Retrieved March 5, 2024, from https://www.ieee.es/en/Galerias/fichero/docs_opinion/2014/DIEEEO88-2014_Ingenieria_Software_Ciberseguridad_HidalgoTarrero.pdf

Howard-Grenville, J., & Lahnem, B. (2022, marzo 03). La cultura organizacional como una herramienta de cambio. *Stanford Social Innovation Review en*

Español. https://ssires.tec.mx/es/noticia/la-cultura-organizacional-como-una-herramienta-de-cambio

Islas, R. (2009). Sobre el principio de legalidad. In *Anuario de derecho Constitucional Latinoamericano* (p. 102). https://www.corteidh.or.cr/tablas/r23516.pdf

Jaimovich, D. (2022, July 29). Los cinco ciberdelitos más habituales y cómo protegerse de ellos. *La Nación*. https://www.lanacion.com.ar/tecnologia/los-cinco-ciberdelitos-mas-habituales-y-como-protegerse-de-ellos-nid29072022/

Lacy, S. (2022, October 2). *PRINCIPIOS BASICOS DEL SEGURO*. . - YouTube. Retrieved December 19, 2023, from https://www.linkedin.com/pulse/principios-b%C3%A1sicos-del-seguro-luis-horacio-mander/?originalSubdomain=es

Landgrave, M. F. (2023). *CULTURA DE CIBERSEGURIDAD, PREVENCIÓN Y ATENCIÓN PARA LAS EMPRESAS MEXICANAS*. UNIVERSIDAD LA SALLE. https://repositorio.lasalle.mx/bitstream/handle/lasalle/2778/Maria%20Fernanda%20Landgrave%20Sandoval_Estudio%20de%20caso.pdf?sequence=1&isAllowed=y

Ley Orgánica de Protección de Datos Personales. (2021, mayo 26). *Registro Oficial Suplemento 459*. Quito, Pichincha, Ecuador. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

LOPEZ, E. (2022, 08 18). *Pymes no creen tener riesgos en ciberseguridad*. eleconomista.com. https://www.eleconomista.com.mx/el-empresario/Pymes-no-creen-tener-riesgos-en-ciberseguridad-20220817-0095.html

Maroto, J. (2009). El ciberespionaje y la Ciberseguridad. *La violencia del siglo XXI*. https://dialnet.unirioja.es/descarga/articulo/4549946.pdf

Montesuma, D. (2019). *La responsabilidad demostrada frente al tratamiento de datos personales y su relevancia para la graduación de la sanción al* *interior de procedimientos administrativos sancionatorios*. Pontificia Universidad Javeriana. https://repository.javeriana.edu.co/bitstream/handle/10554/47748/Trabajo%20de%20Grado.pdf?sequence=1&isAllowed=y

Nuñez del Prado, A. (2011, febrero 13). Principios Jurídicos del seguro. *Escuela de Seguros de la Asociación Peruana de Empresas de Seguros*, 6. https://revistas.javeriana.edu.co/index.php/iberoseguros/article/view/18502

Ortega, K. (2023, June 5). *Fases de la ciberseguridad*. Saint Leo University. Retrieved January 4, 2024, from https://worldcampus.saintleo.edu/noticias/cuales-son-las-fases-de-ciberseguridad

PÉREZ, M. (2022, MARZO 10). Prima de Seguro: ¿Qué es y Cuáles Factores Inciden en su Valor? *PEREZ LARA*, 2. https://perezlara.com/prima-de-seguro/

Pérez, V. (2015, December 18). *¿Cuál es la diferencia: malware, virus, gusanos, spyware, troyanos, ransomware, etc?* Computer Hoy. Retrieved January 15, 2024, from https://computerhoy.com/listas/software/cual-es-diferencia-malware-virus-gusanos-spyware-troyanos-ransomware-etc-35163

Puime, J. (2009). *EL Ciberespionaje y la Ciberseguridad*. https://www.google.com/search?q=EL+CIBERESPIONAJE+Y+LA+CIBERSEGURIDAD&rlz=1C1ONGR_esEC1083EC1083&oq=EL+CIBERESPIONAJE+Y+LA+CIBERSEGURIDAD&gs_lcrp=EgZjaHJvbWUyCQgAEEUYORiABDIKCAEQABiABBiiBDIKCAIQABiABBiiBDIKCAMQABiiBBiJBTIGCAQQRRg80gEHNzM5ajBqN6gCALACAA&sou

Puime, J. (2009). *El Ciberpionaje y la Ciberseguridad*. https://www.google.com/search?q=EL+CIBERESPIONAJE+Y+LA+CIBERSEGURIDAD&rlz=1C1ONGR_esEC1083EC1083&oq=EL+CIBERESPIONAJE+Y+LA+CIBERSEGURIDAD&gs_lcrp=EgZjaHJvbWUyCQgAEEUYORiABDIKCAEQABiABBiiBDIKCAIQABiABBiiBDIKCAMQABiiBBiJBTIGCAQQRRg80gEHNzM5ajBqN6gCALACAA&sou

Quispe, J. (2021). *Modelo de Ciberseguridad Corporativa en el Sistema Bancario*. https://www.google.com/search?q=Una+de+las+principales+formas+en+el+que+los+ciberdelincuentes+operan+es+por+manipular+al+personal+de+una+organizaci%C3%B3n%3B+pueden+enga%C3%B1arlos+sin+saberlo+descargar+malware+en+los+sistemas+de+la+empresa%2C+abriendo+a+l

Riquelme, R. (2017, 11 21). Grandes pérdidas económicas por prácticas como el robo de información, la caída en la disponibilidad de servicios y sistemas y daños a la imagen de las empresas por cibercrimen. *Noti_infosegura*. https://www.uv.mx/infosegura/general/noti_cibercriminales-44/

Rodriguez, H., & Moreno, C. (2023, Noviembre). Seguridad de la información y ciberseguridad: su importancia para los Estados, empresas y las personas, una revisión sistemática. *Corporación de Seguridad Ocupacional y Ambiental*, (29), 23. https://colpap.org/wp-content/uploads/2023/12/Articulo-de-revision-sistematica-Ciberseguridad.pdf

Torroba, J. (2023, January 9). *Diferencias entre tomador y asegurado en un contrato de seguros*. Juan Torroba. Retrieved January 15, 2024, from https://juantorroba.es/blog/diferencias-tomador-y-asegurado/

UNIVERSIDAD DE VALLADOLID. (2021). *El mercado del seguro: impacto de las nuevas tecnologías en el sector asegurador*. UNIVERSIDAD DE VALLADOLID. https://uvadoc.uva.es/bitstream/handle/10324/53259/TFG-E-1378.pdf?sequence=1&isAllowed=y

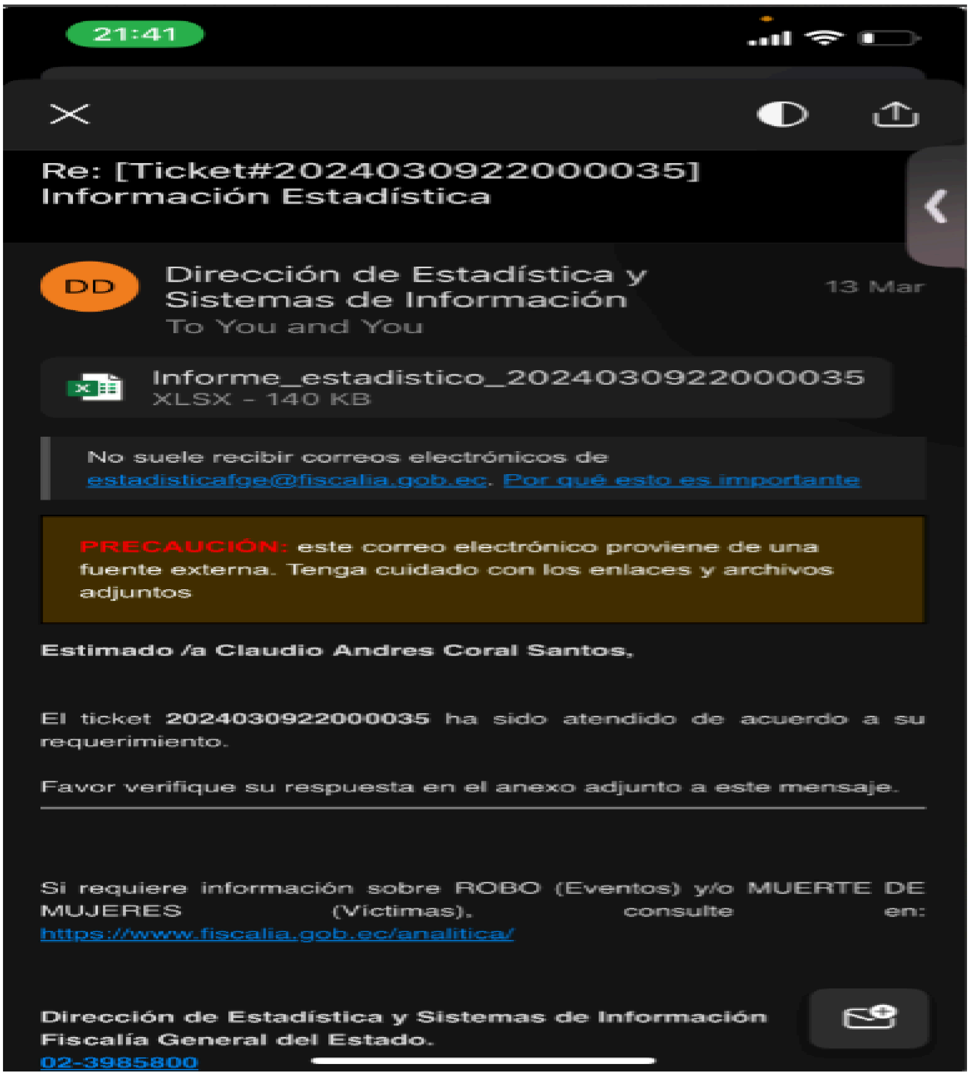
Vargas, R. (2022). CONCEPCIÓN POLÍTICO – ESTRATÉGICA DE CIBERDEFENSA. *ademic.ccffaa*, 11. https://ademic.ccffaa.mil.ec/wp-content/uploads/sites/3/2023/04/Pensamiento-Estrategico-sep-22-2021-37-47.pdf

Westerski, A., Kanagasabai, R., Narayanan, A., & Wong, J. (2021, Marzo 18). Detección de anomalías explicables para la identificación de fraudes en adquisiciones: lecciones de implementaciones prácticas. https://doi.org/10.1111/itor.12968

9.- ANEXOS

Anexo 1

Correo solicitando información estadística a Fiscalía (negativa)



Fuente: Correo enviado desde una cuenta de outlook a Fiscalía por Claudio Coral y Contesta el encargado de la Dirección de Estadísticas y Sistemas de Información Fiscalía General del Estado con una negativa.

Anexo 2

Correo solicitando información estadística a Fiscalía (negativa)

FGE
FISCALÍA GENERAL DEL ESTADO
ECUADOR

DIRECCIÓN DE ESTADÍSTICA Y SISTEMAS DE INFORMACIÓN

Informe Estadístico

Fecha de suscripción de la solicitud:	9/3/2024
Número de documento de ingreso de solicitud:	Ticket#2024030922000035
Nombre y apellido de la persona solicitante:	(Estudiante) Claudio Andres Coral Santos
Cédula de la persona solicitante:	
Correo electrónico de la persona solicitante:	claudio.coral@udla.edu.ec
Tipo del solicitante:	1
Fecha ingreso a la Dirección:	9/3/2024
Fecha de reasignación al analista:	11/3/2024
Fecha de respuesta:	12/3/2024
Tipo de medio de notificación:	Mesa de Ayuda
Número de documento de ingreso de solicitud (Memorando, Oficio):	
Detalle de la información requerida:	Noticias del Delito por Delitos Informáticos entre el 01 de enero de 2017 y el 31 de diciembre de 2023
Tipos penales:	REVELACIÓN ILEGAL DE BASE DE DATOS, INTERCEPTACIÓN ILEGAL DE DATOS, TRANSFERENCIA ELECTRÓNICA DE ACTIVO PATRIMONIAL, ATAQUE A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS, ACCESO NO CONSENTIDO A UN SISTEMA INFORMÁTICO, TELEMÁTICO O DE TELECOMUNICACIONES, FALSIFICACIÓN INFORMÁTICA, ESTAFA (numeral 2), VIOLACIÓN A LA INTIMIDAD, SUPLANTACIÓN DE IDENTIDAD, APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS
Procedimiento de extracción de información:	
· **Fuente:**	Sistema Integrado de Actuaciones Fiscales (SIAF) - ANALÍTICA FGE
· **Fecha de corte:**	8/3/2024
· **Periodo de análisis:**	01/01/2017 - 31/12/2023
· **Unidad de Análisis:**	Noticias del delito NDD (incluye en tentativa y consumados)
Elaboración:	Francisco Fonseca Villacrés
Revisión y aprobación:	Alex Santiago Tupiza Aldás
Fecha de revisión y aprobación:	13/3/2024

Se informa al peticionario que según:

La Constitución de la República del Ecuador:

Artículo 18.- Todas las personas, en forma individual o colectiva, tienen derecho a:

Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los

Fuente: Correo enviado desde una cuenta de outlook a Fiscalía por Claudio Coral y Contesta el encargado de la Dirección de Estadísticas y Sistemas de Información Fiscalía General del Estado con una negativa.

Anexo 3

Continuación del correo solicitando información estadística a Fiscalía (negativa)

La Constitución de la República del Ecuador:

Artículo 18.- Todas las personas, en forma individual o colectiva, tienen derecho a:

Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.

La Ley Orgánica de Transparencia y Acceso a la Información Pública

Artículo 1.- Principio de Publicidad de la Información Pública.- El acceso a la información pública es un derecho de las personas que garantiza el Estado.

Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema material de la información tengan participación del Estado o sean concesionaros de éste, en cualquiera de sus modalidades, conforme lo dispone la Ley Orgánica de la Contraloría General del Estado; las organizaciones de trabajadores y servidores de las instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no gubernamentales (ONGs), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley.

La Dirección de Estadística y Sistemas de Información atenderá éste pedido durante los 10 días siguientes a la recepción del mismo o, a más tardar, dentro del plazo establecido en el Artículo 9 de la Ley Orgánica de Transparencia y Acceso a la Información Pública – LOTAIP

De conformidad con el Código Orgánico Integral Penal

Artículo 472, no podrá circular libremente la siguiente información:

1) Aquella que esté protegida expresamente con una cláusula de reserva previamente establecida en la ley.

2) La información acerca de datos de carácter personal y la que provenga de las comunicaciones personales cuya difusión no haya sido autorizada expresamente por su titular, por la ley o por el juzgados.

3) La información producida por la o fiscal en el marco de una investigación previa y aquella original en la orden judicial relacionada con las técnicas especiales de investigación.

4) La información acerca de niñas, niños y adolescentes que viole sus derechos según lo establecidos en el Código Orgánico de la Niñez y Adolescencia y la Constitución.

5) La información calificada por los organismos que conforman el Sistema nacional de inteligencia.

Artículo 584

6) Las actuaciones de la Fiscalía, de la o el juzgador, del personal del Sistema especializado integral de investigación, medicina legal y ciencias forenses, la Policía Nacional, y de otras instituciones que intervienen en la investigación previa, se mantendrán en reserva, sin perjuicio del derecho de la víctima y de las personas a las cuales se investigan y sus abogados a tener acceso inmediato, efectivo y suficiente a las investigaciones, cuando lo soliciten.

7) Cuando el personal de las instituciones mencionadas, los peritos, traductores, interpretes, que han intervenido en estas actuaciones, divulguen o pongan de cualquier modo en peligro el éxito de la investigación o las difundan, atentando contra el honor y al buen nombre de las personas en general, serán sancionadas conforme con lo previsto en este Código.

Ley Orgánica de Comunicación

"Con base en al principio de responsabilidad ulterior contenido en el Artículo 19 de la Ley Orgánica de Comunicación, que establece que la responsabilidad ulterior es la obligación que tiene toda persona de asumir las consecuencias administrativas posteriores a difundir contenidos que lesiones los derechos establecidos en la Constitución y en particular los derechos de la comunicación y la seguridad pública del Estado, a través de los medios de comunicación, sin perjuicio de las acciones civiles penales o de cualquier otra índole a las que haya lugar; la FGE requiere al peticionario utilizar la información proporcionada solo para los fines específicamente establecidos en la solicitud, así como, hacer uso responsable de la misma.

Fuente: Correo enviado desde una cuenta de outlook a Fiscalía por Claudio Coral y Contesta el encargado de la Dirección de Estadísticas y Sistemas de Información Fiscalía General del Estado con una negativa.

Anexo 4

Cuadro de Delitos cibernéticos denunciados en Ecuador (desde 2017 hasta junio de 2023)

DELITO	2017	2018	2019	2020	2021	2022	2023
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	42	56	55	46	78	84	54
Acoso sexual	12	19	13	10	18	13	10
Apropiación fraudulenta por medios electrónicos	113	158	216	153	896	562	185
Ataque a la integridad de sistemas informáticos	21	16	21	19	32	36	20
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	4	14	8	7	18	15	18
Estafa	139	96	103	105	212	107	36
Intimidación	93	78	95	61	73	58	23
Pornografía con utilización de niñas, niños o adolescentes	27	33	42	35	66	42	23
Suplantación de identidad	9	13	18	10	59	59	18
Violación a la intimidad	50	58	76	101	222	120	49
OTROS DELITOS (actos de odio, abuso de confianza, robo, etc)	199	197	288	135	177	244	137
TOTAL	709	738	935	682	1851	1340	573

Fuente: Elaborado por Unidad de Ciberdelitos de la Policía Nacional del Ecuador

Anexo 5

Cuadro de Protección de Datos personales en un evento de continuidad

Fuente: Elaborado por Jorge Guerron en base a un entorno académico. (Abril, 2024)

Anexo 6

La inseguridad aumenta los costos para Bancos y Cooperativas


La inseguridad aumenta los costos para bancos y cooperativas

El aumento de los índices de violencia y de ataques informáticos ha llevado a bancos y cooperativas a invertir más en protección de cajeros y en ciberseguridad.

Autor: Gabriela Coba

Actualizada: 29 Dic 2022 - 5:25

Imagen referencial del robo de cajeros automáticos de bancos y cooperativas en Ecuador. - Foto: Policía Nacional/Twitter

LO ÚLTIMO

01 Emelec apelará sanción tras el Clásico: USD 80.000 de multa y un partido sin público

02 Precio de las entradas para U. Católica vs. Barcelona SC por LigaPro 2024

03 Guayaquil: Dos detenidos tras 'lluvia' de disparos al aire en Bastión Popular

Fuente: Elaborado por Gabriela Coba en el diario digital Primicias https://www.primicias.ec/noticias/economia/bancos-cooperativas-inseguridad-costos/

Anexo 7

Cuadro de Bussiness Impact Analysis

Fuente: Elaborado por Jorge Guerron en base a un entorno académico. (Abril, 2024)

Anexo 8

Lineamientos

8.1.- LINEAMIENTOS DE UNA PÓLIZA DE CIBERSEGURIDAD PARA PEQUEÑAS Y MEDIANAS EMPRESAS

Este trabajo de investigación ha planteado definir aquellos lineamientos que ayudarían a que una póliza de ciberseguridad para pequeñas y medianas empresas pueda volverse un producto viable en el mercado de seguros. Se han tomado cuatro puntos para definir los lineamientos, los cuales se encuentran en concordancia con las exclusiones planteadas específicamente para este tipo de póliza. Los puntos a través de los que se van a abordar los lineamientos son, en primer lugar un eje preventivo, en el cual se indica el manejo que debe llevar el asegurado con sus equipos y sistemas informáticos. Como segundo lineamiento se encuentra la recuperación de información, factor crítico, pues es el elemento que se protege en la cobertura de la póliza, le sigue la mitigación de daños, lo cual busca reducir el impacto de un eventual ciberataque. Finalmente existe la fase post ataque, aquella que verifica que se haya corregido cualquier vulnerabilidad en los sistemas y se repare el daño.

8.2.-CUIDADOS PREVENTIVOS

Se empezará hablando del punto de cuidados preventivos. El eje de prevención es crucial cuando se habla de ciberseguridad, el tener los sistemas lo suficientemente resguardados a fin de que no se produzca un eventual ciberataque. Las pequeñas y medianas empresas, de manera regular no suelen contar con un departamento de Seguridad de la Información o siquiera de sistemas, motivo por el que se ha planteado que, dentro de quienes se encuentran en nómina cumplan como Oficial de Seguridad de la Información y Datos, haciendo de esta figura un intermediario que en un eventual siniestro, rinda cuentas ante la aseguradora de todos los procesos de debida diligencia en cuanto al manejo de ciberseguridad.

Además de esta figura, se ha planteado un mecanismo que contendrá el resto de procesos de debida diligencia. Este documento es la Guía Práctica de Procedimiento de Ciberseguridad, la cual contiene aquellas operaciones sistemáticas y organizadas que debe cumplir el asegurado. De hecho, en caso de suscitarse un eventual siniestro, el criterio a manejarse por parte de la compañía aseguradora para el pago o la negativa del reclamo será mediante la revisión del cumplimiento de la Guía. El objetivo es que la cultura de seguridad de la información y cuidado de los sistemas se implemente a un nivel organizacional en los asegurados.

Aquellos punto con los que debe contar la Guía Práctica de Procedimiento de Ciberseguridad, son la capacitación al personal, el uso de sistemas de protección actualizados y homologados por la aseguradora, aquellos lugares en los que se podrá y deberá dar mantenimiento a los equipos, las políticas de protección de datos personales y los requisitos para ser Oficial de Seguridad de la Información y Datos. Estos son los factores que se han planteado de primera mano para que el asegurado pueda suscribir y tener cobertura de esta póliza de ciberseguridad.

8.3.- RECUPERACIÓN DE LA INFORMACIÓN

El segundo eje con el cual se abordan los lineamientos es la recuperación de la información en una eventualidad de sufrir un ciberataque. Uno de los temores más grandes de una compañía al sufrir un ataque a sus sistemas es la pérdida de aquella información almacenada en estos. En primer lugar se teme por las consecuencias de los datos personales de clientes y trabajadores, pero también existe información corporativa relativa al giro del negocio, lo cual puede ocasionar severas pérdidas desde varios puntos de vista. Para este efecto se ha planteado algunos puntos para contrarrestar los daños una vez que estos ya han sucedido.

En primer lugar se estableció que el asegurado al ver que ha sufrido un ataque a sus sistemas informáticos va a requerir asesoría legal. Esta ayuda es para llevar a cabo las acciones pertinentes relativas a notificaciones a los clientes, denuncia ante fiscalía y demás operaciones que puedan tener efectos jurídicos. Las etapas procesales son parte de la siguiente fase de la cual se hablará más adelante.

Con respecto a los sistemas, una vez que han sido vulnerados se requerirá saneamiento de los mismos y acciones para recobrar la data perdida o secuestrada según sea el caso. Evidentemente la aseguradora brindará al cliente los técnicos más calificados para que atiendan a sus sistemas y se pueda retornar con total normalidad a las actividades de la compañía asegurada.

8.4.- MITIGACIÓN DE DAÑOS

En este tercer punto se tratará de la mitigación de daños una vez que se ha producido una vulneración a los sistemas informáticos del asegurado. Está previsto que se brinde todo tipo de asesoría, sin embargo existirán daños más allá de los causados por el hecho del ataque. En primer lugar se tienen aquellas consecuencias legales que devienen luego del siniestro, y como segundo punto se cuenta con el daño reputacional, lo que causa pérdida de la cartera de clientes.

Desde el punto de vista legal, ahora se tienen todos los gastos litigiosos. El cliente del asegurado, al verse afectado por el robo de sus datos personales, sensibles entre otros, podrá reclamar por la vía legal todo perjuicio que haya sufrido. Es aquí donde la póliza dentro de su cobertura, asignará un equipo legal capacitado para enfrentar conjuntamente con el asegurado los procesos legales que se inicien a causa del ciberataque.

Las afectaciones pueden ir más allá del ámbito legal. Existe el daño reputacional, lo cual, como se había mencionado anteriormente lleva a la pérdida de clientes y una imagen negativa en el mercado. En compañías pequeñas y medianas su mayor patrimonio son sus consumidores, además, al estar empezando o tener un porcentaje pequeño del mercado, la imagen negativa puede llevar a la quiebra de la compañía.

Desde esta visión se concluye que parte vital dentro de la mitigación de daños es recobrar la imagen. Para este fin la póliza cubrirá gastos ligados a un “alza reputacional”. Esto quiere decir que se contratará con expertos en “marketing”, publicidad y trabajo para recobrar la confianza de los clientes, tanto afectados como aquellos que por el daño desean abandonar la gestión de la compañía.

8.5.- ANÁLISIS DE RIESGO POST ATAQUE

El último criterio con el cual se ha tratado los lineamientos es aquel que viene luego del ataque. A pesar de que se cubren gastos legales, tanto de asesoría como de litigio, mitigación del daño reputación, recuperación de datos. La compañía aseguradora, deberá realizar una verificación de algunos detalles. Primero el saneamiento de los sistemas, es importante asegurarse que se ha eliminado todo rezago del ciberataque. Se debe investigar al oficial de seguridad de información y datos y el cumplimiento del manual.

Todos estos detalles son los que permitirán que exista nuevamente la confianza necesaria para renovar la póliza. Hay que recordar siempre que el éxito de un producto de seguros en el mercado es su baja siniestralidad. Así se mantiene el objetivo de aleatoriedad del contrato de seguros y se mejora la cultura corporativa con relación al cuidado de los sistemas informáticos de una organización.

Anexo 9

Cuadro de la Información que debe contener el business Impact Analysis

Fuente: Elaborado por Jorge Guerron en base a un entorno académico. (Abril, 2024)

ANEXO 10

Resolución N SEPS-IGS-IGT-IGDO-INGINT.INTIC-INSESF-INT.DNSI-2022-02

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

RESOLUCIÓN No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002

SOFÍA MARGARITA HERNÁNDEZ NARANJO
SUPERINTENDENTE DE ECONOMÍA POPULAR Y SOLIDARIA

CONSIDERANDO:

Que, la Constitución de la República del Ecuador, en su artículo 66, numeral 19, prescribe: *"Se reconoce y garantizará a las personas: (...) 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley"*;

Que, el artículo 82 de la Norma Suprema dispone: *"El derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes"*;

Que, el artículo 226 ibídem señala: *"Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución"*;

Que, el artículo 283, inciso segundo ejusdem establece: *"(...) El sistema económico se integrará por las formas de organización económica pública, privada, mixta, popular y solidaria, y las demás que la Constitución determine. La economía popular y solidaria se regulará de acuerdo con la ley e incluirá a los sectores cooperativistas, asociativos y comunitarios"*;

Que, el Código Orgánico Monetario y Financiero regula los sistemas monetario y financiero, así como los regímenes de valores y seguros del Ecuador;

Que, el artículo 13 del Libro 1 de dicho Código crea la Junta de Política y Regulación Financiera, parte de la Función Ejecutiva, responsable de la formulación de la política y regulación, crediticia, financiera, de valores, seguros y servicios de atención integral de salud prepagada;

Que, el numeral 7 y el último inciso del artículo 62 del aludido Código, en concordancia con el último inciso del artículo 74, establece como una de las funciones de la Superintendencia de Economía Popular y Solidaria,: " *7. Velar por la estabilidad, solidez y correcto funcionamiento de las entidades sujetas a su control y, en general, vigilar que cumplan las normas que rigen su funcionamiento, las actividades financieras que presten, mediante la supervisión permanente preventiva extra situ y visitas de inspección in situ, sin restricción alguna, de acuerdo a las mejores prácticas, que permitan determinar la situación económica y financiera de las* *entidades, el manejo de sus negocios, evaluar la calidad y control de la gestión de riesgo y verificar la veracidad de la información que generan; (...)*

La superintendencia, para el cumplimiento de estas funciones, podrá expedir todos los actos y contratos que fueren necesarios. Asimismo, podrá expedir las normas en las materias propias de su competencia, sin que puedan alterar o innovar las disposiciones legales ni las regulaciones que expida la Junta de Política y Regulación Financiera";

Que, el artículo 163 del referido Código determina que las cooperativas de ahorro y crédito, las asociaciones mutualistas de ahorro y crédito para la vivienda, cajas centrales, de servicios auxiliares del sistema financiero, entre otras, forman parte del sector financiero popular y solidario;

Que, el artículo 387 del citado Código previene que es competencia de la Superintendencia de Economía Popular y Solidaria el control de las actividades financieras de las entidades del Sector Financiero Popular y Solidario y de la entidad financiera pública a la que se refiere la Ley Orgánica de Economía Popular y Solidaria;

Que, los artículos 434 y 436 ibídem en su parte pertinente, en su orden, disponen: *"**Naturaleza**. Los servicios auxiliares serán prestados por personas jurídicas no financieras constituidas como sociedades anónimas o compañías limitadas, cuya vida jurídica se regirá por las disposiciones de la Ley de Compañías. El objeto social de estas compañías será claramente determinado. (...)" "**Calificación**. Las compañías, para prestar los servicios auxiliares a las entidades del sistema financiero nacional, deberán calificarse previamente ante el organismo de control correspondiente, la que como parte de la calificación podrá disponer la reforma del estatuto social y el incremento del capital, con el propósito de asegurar su solvencia. (...)";*

Que, el artículo 444 ejusdem determina que: *"**Regulación y control.** Las entidades financieras populares y solidarias están sometidas a la regulación de la Junta de Política y Regulación Financiera y al control de la Superintendencia de Economía Popular y Solidaria, quienes en las políticas que emitan tendrán presente la naturaleza y características propias del sector financiero solidario";*

Que, la Disposición Transitoria Quincuagésima Cuarta ibídem determina: *"Régimen transitorio de Resoluciones de la Codificación de la Junta de Política y Regulación Monetaria y Financiera. Las resoluciones que constan en la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros de la Junta de Política y Regulación Monetaria y Financiera y las normas emitidas por los organismos de control, mantendrán su vigencia hasta que la Junta de Política y Regulación Monetaria y la Junta de Política y Regulación Financiera resuelvan lo que corresponda, en el ámbito de sus competencias";*

Que, el literal b), del artículo 151 de la Ley Orgánica de Economía Popular y Solidaria determina entre las atribuciones del Superintendente de Economía Popular y Solidaria, la de: *"Dictar las normas de control (...)";*

Que, el artículo 158 de la aludida Ley Orgánica crea la Corporación Nacional de Finanzas Populares y Solidarias, como una entidad financiera de derecho público;

Que, el artículo 165 del citado cuerpo legal establece que la Corporación Nacional de Finanzas Populares y Solidarias CONAFIPS estará sometida al control y supervisión de la Superintendencia de Economía Popular y Solidaria, y tendrá una unidad de auditoría interna encargada de las funciones de su control interno;

Que, en la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros, en el Libro I "Sistema Monetario y Financiero", Título II "Sistema Financiero Nacional", Capítulo XXXVII "Sector Financiero Popular y Solidario", consta la Sección III, "NORMAS PARA LA ADMINISTRACIÓN INTEGRAL DE RIESGOS EN LAS COOPERATIVAS DE AHORRO Y CRÉDITO, CAJAS CENTRALES Y ASOCIACIONES MUTUALISTAS DE AHORRO Y CRÉDITO PARA LA VIVIENDA", cuya Disposición General Cuarta determina que la Superintendencia de Economía Popular y Solidaria podrá emitir las normas de control necesarias para su aplicación;

Que, en la Codificación ibídem, en el Libro I "Sistema Monetario y Financiero", Título II "Sistema Financiero Nacional", Capítulo XXXVII "Sector Financiero Popular y Solidario", consta la Sección VIII "NORMA PARA LA ADMINISTRACIÓN INTEGRAL DE RIESGOS DE LA CORPORACIÓN NACIONAL DE FINANZAS POPULARES Y SOLIDARIAS"; cuya Disposición General Segunda determina que la Superintendencia de Economía Popular y Solidaria podrá emitir las normas de control necesarias para su aplicación;

Que, mediante Resolución No. SEPS-IGT-IR-IGJ-2018-021, de 13 de julio de 2018, la Superintendencia de Economía Popular y Solidaria emitió la *"Norma de control respecto de la seguridad física y electrónica"*, reformada por la Resolución No. SEPS-IGT-IR-IGJ-2018-0259, de 10 de octubre de 2018;

Que, mediante Resolución No. SEPS-IGT-IR-IGJ-2018-0279, de 26 de noviembre de 2018, la Superintendencia de Economía Popular y Solidaria emitió la *"Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del Sector Financiero Popular y Solidario, bajo el control de la Superintendencia de Economía Popular y Solidaria"*, reformada por las resoluciones Nos. SEPS-IGT-IR-IGJ-2018-0284 de 13 de diciembre de 2018 y SEPS-IGT-IGS-INR-INGINT-2020-0221 de 2 de junio de 2020;

Que, mediante Resolución No. SEPS-IGT-IGS-INFMR-INGINT-IGJ-2020-0153, de 12 de mayo de 2020, la Superintendencia de Economía Popular y Solidaria emitió la *"Norma de control sobre los principios y lineamientos de educación financiera"*;

Que, es necesario que la Superintendencia de Economía Popular y Solidaria expida una norma de control para la seguridad de la información que coadyuve al fortalecimiento de los procesos internos de las entidades del Sector Financiero Popular y Solidario, bajo el control de la Superintendencia de Economía Popular y Solidaria; y,

Que, en virtud de la Resolución Nro. PLE-CPCCS-T-O-081-13-08-2018, emitida por el Consejo de Participación Ciudadana y Control Social Transitorio el 13 de agosto de 2018, el pleno de la Asamblea Nacional posesionó como Superintendente de Economía Popular y Solidaria a la doctora Sofía Margarita Hernández Naranjo, el 04 de septiembre de 2018.

En ejercicio de sus atribuciones y funciones, resuelve expedir la siguiente:

NORMA DE CONTROL RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN EN LAS ENTIDADES DEL SECTOR FINANCIERO POPULAR Y SOLIDARIO BAJO CONTROL DE LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

CAPÍTULO I
ÁMBITO, OBJETO, REGÍMENES Y DEFINICIONES

Artículo 1.- Ámbito.- Las disposiciones de la presente norma, de acuerdo a su segmento, aplicarán para:

a) Las cooperativas de ahorro y crédito, asociaciones mutualistas de ahorro y crédito para la vivienda y cajas centrales, en adelante denominadas "entidad o entidades"; y, a la Corporación Nacional de Finanzas Populares y Solidarias, en lo sucesivo CONAFIPS; y,
b) Las compañías y organizaciones de servicios auxiliares que prestan servicios a las actividades financieras de las entidades y CONAFIPS, en adelante "empresas".

Artículo 2.- Objeto.- La presente norma tiene por objeto regular los niveles mínimos para la administración de seguridad de la información que las entidades, la CONAFIPS y las empresas, deben definir e implementar con el fin de resguardar y proteger sus activos de información, preservando su confidencialidad, disponibilidad e integridad.

Artículo 3.- Regímenes.- Para efectos de esta norma, se aplicarán los siguientes regímenes:

1. Régimen general: a las cooperativas de ahorro y crédito de los segmentos 1 y 2; a las asociaciones mutualistas de ahorro y crédito para la vivienda y a la CONAFIPS;
2. Régimen especial: a las cooperativas de ahorro y crédito del segmento 3; y,
3. Régimen simplificado: a las cooperativas de ahorro y crédito de los segmentos 4 y 5.

A las empresas se aplicarán los regímenes anteriores según el tipo de servicio que presten, de acuerdo con la siguiente tabla:

Tipos de Servicios Auxiliares	General	Especial	Simplificado
Software financiero y computación	x		
Transaccionales y de pago	x		
Transporte de especies monetarias y de valores		x	
Red de cajeros automáticos	x		
Cobranzas		x	
Generadoras de cartera	x		

3.

Administradoras de tarjetas	x		
Giro inmobiliario			x
Servicios contables			x

Artículo 4.- Definiciones.- Para la aplicación de esta norma, se considerarán las siguientes definiciones:

- **Activo de información:** se consideran a los servicios o herramientas creados o utilizados en medios digital, físico, electromagnético y otros; hardware o software, utilizados para el procesamiento, transferencia o almacenamiento de información; y, cualquier dato que tenga información valorada por la entidad, CONAFIPS o empresa.
- **Autorización de accesos:** acto por el cual se permite el acceso de los usuarios a zonas restringidas, a distintos equipos y/o servicios, después de haber superado el proceso de autenticación.
- **Bitácora de eventos de riesgos:** registro de eventos de riesgo durante un periodo en particular. Se registrará acorde a la "Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del Sector Financiero Popular y Solidario bajo el control de la Superintendencia de Economía Popular y Solidaria".
- **Cifrar:** es el proceso mediante el cual la información o archivos son transformados en forma lógica y controlada, con el objetivo de evitar que alguien no autorizado pueda interpretarlos, verlos o copiarlos.
- **Confidencialidad:** es la propiedad por la que se garantiza que la información es accesible solo al personal autorizado.
- **Disponibilidad:** acceso a la información en el tiempo y forma en que ésta sea requerida.
- **Información:** es cualquier forma de registro físico, electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado y distribuido.
- **Integridad:** es la cualidad de que la información se mantiene inalterada y completa.
- **ISO/IEC 27000:** Se refiere a la Norma Técnica emitida por el Servicio Ecuatoriano de Normalización, INEN, NTE INEN-ISO/IEC 27000 Cuarta edición 2016-11 TECNOLOGÍAS DE LA INFORMACIÓN — TÉCNICAS DE SEGURIDAD — SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN — DESCRIPCIÓN GENERAL Y VOCABULARIO (ISO/IEC 27000:2016, IDT)
- **Partes interesadas:** son todas las personas naturales o jurídicas que, de alguna forma, puedan verse afectadas por la actividad de la entidad, de la CONAFIPS o de la empresa.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Zonas restringidas:** son aquellas que requieren de una autorización de acceso.

CAPÍTULO II
SEGURIDAD DE LA INFORMACIÓN – RÉGIMEN GENERAL

Artículo 5.- Régimen General.- Conforman el régimen general de seguridad de la información:

a) El Consejo de Administración o el Directorio, según corresponda;
b) El Comité de Seguridad de la Información (CSI);
c) El Gerente General o Representante Legal;

M.

d) La Unidad o Departamento de Seguridad de la Información; y,
e) El Oficial de Seguridad de la Información (OSI).

Artículo 6.- Comité de Seguridad de la Información (CSI).- Las entidades, empresas y la CONAFIPS que conforman este régimen, deberán contar con un Comité de Seguridad de la Información (CSI), conformado por los siguientes miembros:

a) El presidente del Comité de Administración Integral de Riesgos, quien presidirá también el Comité de Seguridad de la Información y tendrá voto dirimente;
b) El Gerente General o representante legal;
c) El oficial de seguridad de la información, quien actuará como secretario del Comité;
d) El responsable del área de tecnología o su delegado; y,
e) Un delegado de Auditoria Interna.

El Comité podrá invitar a las sesiones a los responsables de las áreas de negocio que juzgue del caso, quienes tendrán voz pero no voto.

Artículo 7.- Sesiones del Comité de Seguridad de la Información.- Las sesiones del Comité de Seguridad de la Información (CSI), se instalarán con la asistencia de al menos tres de sus miembros, entre los cuales deberá estar presente su presidente.

El Comité sesionará de manera ordinaria al menos dos veces al año. Podrá reunirse extraordinariamente cuando el presidente lo convoque por iniciativa propia, o a petición de uno de sus miembros y/o cuando por eventos de fuerza mayor o caso fortuito lo amerite. En las sesiones extraordinarias se tratarán únicamente los puntos del orden del día.

Las decisiones serán tomadas por mayoría de votos.

Las convocatorias tendrán el orden del día y deberán ser comunicadas por el presidente con, al menos, cuarenta y ocho horas de anticipación, excepto cuando se trate de sesiones extraordinarias que podrán ser convocadas en cualquier momento.

Las sesiones podrán realizarse de manera presencial, o por cualquier medio tecnológico.

Las resoluciones constarán en las respectivas actas, las que deberá elaborar el secretario del Comité, quien además las fechará y numerará en forma secuencial, así como estarán suscritas por los asistentes. Será responsabilidad del secretario la custodia de las actas bajo principios de confidencialidad, integridad y disponibilidad de la información.

Artículo 8.- Unidad o Departamento de Seguridad de la Información.- Las entidades, empresas y la CONAFIPS que conforman este régimen, deberán contar con una Unidad o Departamento de Seguridad de la Información, liderado por el Oficial de Seguridad de la Información (OSI), quien debe tener título universitario de tercer nivel y evidenciar al menos 40 horas de capacitación en seguridad de la información en los dos años inmediatamente anteriores al ejercicio de sus funciones. Dicha Unidad o Departamento, debe estar adscrita a la Gerencia General o representante legal.

Artículo 9.- Requisitos obligatorios para el Régimen General.- Las entidades, empresas y la CONAFIPS pertenecientes a este régimen deberán contar con al menos, lo siguiente:

a) Plan Estratégico de Seguridad de la Información;

b) Plan de Recursos (técnicos, humanos, financieros) para seguridad de la información;
c) Plan de Gestión de Riesgos de Seguridad de la Información. Al efecto podrán tomar como referencia el Anexo 2 de esta resolución;
d) Plan de Concienciación y Formación de Seguridad de la Información;
e) Políticas, procesos, procedimientos, roles y responsabilidades para la gestión de seguridad de la información y del SGSI;
f) Los requerimientos señalados en el Anexo 1 de esta resolución, correspondiente al Régimen General; y,
g) Sistema de Gestión de Seguridad de la Información (SGSI).

Artículo 10.- Sistema de Gestión de Seguridad de la Información (SGSI).- Las entidades, empresas y la CONAFIPS que conforman este régimen, deberán implementar y mantener un SGSI, orientado a garantizar la adecuada gestión de seguridad de la información, con base en la serie de estándares ISO/IEC 27000, y acorde a la normativa legal vigente.

Para establecer el alcance del SGSI, además de lo previsto en el artículo anterior y la serie de estándares ISO/IEC 27000, deberán considerar:

1) Definición de tipos de información con criterios de integridad, confidencialidad y disponibilidad; y,
2) Identificación y clasificación de activos de información, que contendrá:
   a) Personas;
   b) Procesos agregadores de valor y/o catalogados como sensibles o críticos;
   c) Unidades intervinientes en los procesos;
   d) Infraestructura tecnológica;
   e) Ubicaciones físicas y puntos de atención, oficina matriz, sucursales, agencias, puntos móviles, corresponsales solidarios; y,
   f) Relaciones con personas naturales y/o jurídicas que pudieren acceder a información crítica o sensible.

Artículo 11.- Medidas de Seguridad de la Información (controles).- Las entidades, empresas y la CONAFIPS que conforman este régimen, al implementar el SGSI, deberán adoptar las medidas de seguridad de información observando los controles específicos enumerados en la norma técnica ISO/IEC 27002 o las que las sustituyan, de acuerdo al análisis de riesgos establecido. Además deberán implementar los controles obligatorios previstos para este Régimen, en el Anexo 1.

Artículo 12.- Responsabilidades de la gestión de seguridad de la información.- Los órganos internos de dichas entidades, empresas y la CONAFIPS, además de las responsabilidades previstas en la normativa legal vigente, deberán cumplir con lo descrito a continuación, para una gestión adecuada de la seguridad de la información:

1. Consejo de Administración o Directorio:

a) Aprobar el Plan Estratégico de Seguridad de la Información, el mismo que debe estar alineado al Plan Estratégico de la entidades, empresas y la CONAFIPS;
b) Aprobar los recursos humanos, técnicos y financieros que sean necesarios;
c) Aprobar políticas, procesos, procedimientos, roles y responsabilidades;
d) Aprobar el Plan de Concienciación y Formación; y,
e) Aprobar el Plan de Gestión de Riesgos de Seguridad de la Información.

2. **Comité de Seguridad de la Información (CSI).-** Deberá proponer al Consejo de Administración o al Directorio, según corresponda:

a) El Plan Estratégico de Seguridad de la Información;
b) Los recursos humanos, técnicos y financieros necesarios para la gestión de seguridad de la información y verificar que su inversión sea eficiente y eficaz para el logro de los objetivos estratégicos;
c) Las políticas, procedimientos, roles y responsabilidades para la gestión de seguridad de la información y del SGSI;
d) El Plan de Concienciación y Formación de su personal, en temas concernientes a seguridad de la información; y,
e) El Plan de Gestión de Riesgos de Seguridad de la Información y verificar que esté alineado al Plan de Administración de Riesgos.

Además de lo señalado en el numeral anterior, el Comité de Seguridad de la Información, deberá aprobar la implementación de controles de seguridad de la información, propuestos por el Oficial de Seguridad de la Información (OSI); informar los riesgos de seguridad de la información al Comité de Administración Integral de Riesgos, para su consolidación en la matriz de riesgos y su seguimiento; y, evaluar, dirigir, monitorear y supervisar la gestión de seguridad de la información y del SGSI.

3. **Gerente general o representante legal:**

a) Liderar la gestión de seguridad de la información y el SGSI, de acuerdo con las disposiciones del Consejo de Administración o del Directorio y lo dispuesto en esta norma;
b) Designar al Oficial de Seguridad de la Información (OSI); y
c) Coordinar la participación activa de todas las partes interesadas que intervienen en el SGSI y en la gestión de seguridad de la información.

4. **Oficial de Seguridad de la Información:**

Entre sus responsabilidades, tendrá las siguientes:

a) Desarrollar, gestionar y monitorear el Plan Estratégico de Seguridad de la Información y el SGSI;
b) Diseñar y proponer las políticas, procesos, procedimientos, roles y responsabilidades para la gestión de seguridad de la información y del SGSI, al Consejo de Administración;
c) Solicitar la asignación de los recursos humanos, técnicos y financieros necesarios para la gestión de seguridad de la información, y velar que los mismos sean utilizados de forma eficiente y eficaz, alineados con los objetivos estratégicos institucionales;
d) Elaborar, implementar, mantener y actualizar las políticas, procesos, procedimientos, metodologías, planes y controles concernientes a la gestión de seguridad de la información, del SGSI, su mejora continua; y, una vez aprobados, difundirlos al personal que corresponde;
e) Desarrollar y ejecutar los Planes de Concienciación y Formación a su personal, en temas concernientes a seguridad de la información;
f) Coordinar y supervisar, con los responsables de los procesos del negocio, la implementación efectiva de los controles de seguridad de la información, establecidos en el plan de gestión de riesgos;
g) Desarrollar, coordinar, ejecutar, evaluar, proponer y comunicar el Plan de Gestión de Riesgos de Seguridad de la Información;

h) Coordinar las actividades para la gestión de seguridad de la información y del SGSI, incluyendo su implementación y seguimiento;
i) Definir, ejecutar y mantener procedimientos para la gestión de incidentes de seguridad de la información;
j) Velar que los involucrados internos y/o externos cuenten con los conocimientos y capacitación necesaria para el cumplimiento de sus roles y responsabilidades para la ejecución de procedimientos de respuesta ante incidentes;
k) Ejecutar los procedimientos y lineamientos establecidos, cuando se identifiquen incidentes de seguridad de la información;
l) Informar, de acuerdo con la normativa pertinente, los incidentes de seguridad de la información catalogados como sensibles o críticos, a las instituciones públicas que correspondan;
m) Participar en la evaluación de las amenazas de seguridad de la información y proponer medidas de mitigación;
n) Asesorar en materia de seguridad de la información, a través de su participación en los proyectos que involucren el manejo de información sensible o crítica de la misma, de sus socios, clientes y usuarios;
o) Recomendar medidas correctivas adicionales en temas relacionados de seguridad de la información, alineadas al Anexo 1, Régimen General y/o alineadas a buenas prácticas;
p) Verificar que los servicios prestados por personas naturales o jurídicas cumplan con las políticas de seguridad de la información establecidas; y,
q) Generar la documentación que evidencie la gestión de la seguridad de la información y del SGSI.

5. Auditor interno:
a) Verificar la efectividad de las medidas implementadas por la Unidad de Seguridad de la información;
b) Custodiar los informes de las auditorías y/o pruebas de vulnerabilidades realizadas por la Unidad de Seguridad de la Información y ponerlos a disposición de la Superintendencia de Economía Popular y Solidaria, cuando esta lo requiera; y,
c) Recomendar medidas correctivas a la Unidad de Seguridad de la Información.

Artículo 13.- Evaluación y cumplimiento.- Las entidades, empresas y la CONAFIPS que conforman este régimen, una vez implementado el SGSI, deberán realizar evaluaciones, revisiones, pruebas, exámenes y actualizaciones, anualmente o cuando se requiera, para determinar su efectividad, mediante auditorías internas y/o de terceros. En función de los resultados deberán incorporar las mejoras o adoptar las medidas correctivas, impulsando la mejora continua del SGSI.

CAPÍTULO III
SEGURIDAD DE LA INFORMACIÓN – RÉGIMEN ESPECIAL

Artículo 14.- Régimen Especial.- Conforman el régimen especial de seguridad de la información:

a) El Consejo de Administración o Directorio;
b) El Comité de Seguridad de la Información (CSI);
c) El Gerente General o Representante Legal; y,

w.

d) El Oficial de Seguridad de la Información (OSI).

Artículo 15.- Comité de Seguridad de la Información (CSI).- Las entidades y empresas que conforman este régimen, deberán contar con un Comité de Seguridad de la Información (CSI), conformado por los siguientes miembros:

a) El presidente del Comité de Administración Integral de Riesgos, quien presidirá también el Comité de Seguridad de la Información y tendrá voto dirimente;
b) El Gerente General o representante legal;
c) El oficial de seguridad de la información, quien actuará como secretario del Comité;
d) El responsable del área de tecnología o su delegado; y,
e) Un delegado de Auditoría Interna.

El Comité podrá invitar a las sesiones a los responsables de las áreas de negocio que juzgue del caso, quienes tendrán voz pero no voto.

Artículo 16.- Sesiones del Comité de Seguridad de la Información.- Las sesiones del Comité de Seguridad de la Información (CSI), se instalarán con la asistencia de al menos tres de sus miembros entre los cuales deberá estar presente su presidente.

El Comité sesionará de manera ordinaria al menos dos veces al año. Podrá reunirse extraordinariamente cuando el presidente lo convoque por iniciativa propia, o a petición de uno de sus miembros y/o cuando existieren eventos fortuitos o casos de fuerza mayor. En las sesiones extraordinarias se tratarán únicamente los puntos del orden del día.

Las decisiones serán tomadas por mayoría de votos.

Las convocatorias tendrán el orden del día y deberán ser comunicadas por el presidente con al menos cuarenta y ocho horas de anticipación, excepto cuando se traten de sesiones extraordinarias que podrán ser convocadas en cualquier momento.

Las sesiones se podrán realizar de manera presencial o no presencial, de acuerdo al alcance de las entidades y empresas.

Las resoluciones constarán en las respectivas actas que las deberá elaborar el secretario del Comité, quien las deberá llevar fechadas y numeradas en forma secuencial y suscritas por los asistentes. Será responsabilidad del secretario la custodia de las actas bajo principios de confidencialidad, integridad y disponibilidad de la información.

Artículo 17.- Oficial de Seguridad de la Información.- Las entidades y empresas que conforman este régimen, deberán contar con un Oficial de Seguridad de la Información (OSI), que tenga conocimientos verificables y demuestre entrenamiento continuo en seguridad de la información. Dicho Oficial debe tener título universitario de tercer nivel y evidenciar al menos 40 horas de capacitación en seguridad de la información en los dos años inmediatamente anteriores al ejercicio de sus funciones. El Oficial de Seguridad de la Información deberá estar adscrito a la Gerencia General o representante legal.

Artículo 18.- Requisitos obligatorios para el Régimen Especial.- Las entidades y empresas pertenecientes a este régimen deberán contar con al menos, lo siguiente:

a) Asignación de recursos humanos, técnicos y financieros para seguridad de la información;
b) Plan de Gestión de Riesgos de Seguridad de la Información. Al efecto, las entidades y empresas podrán tomar como referencia el Anexo 2 de esta resolución;
c) Plan de Concienciación y Formación para Seguridad de la Información;
d) Políticas, procesos, procedimientos, roles y responsabilidades para la gestión de seguridad de la información;
e) Los requerimientos señalados en el Anexo 1 de esta resolución, correspondiente al Régimen Especial;
f) Clasificación e identificación de tipos de información críticos o sensibles con criterios de integridad, confidencialidad y disponibilidad; y,
g) Identificación de activos de información, tomando en cuenta que contendrá:
    1) Personas;
    2) Procesos agregadores de valor y/o catalogados como sensibles o críticos;
    3) Unidades de las entidades y empresas intervinientes en los procesos;
    4) Infraestructura tecnológica;
    5) Ubicaciones físicas y puntos de atención, oficina matriz, sucursales, agencias, puntos móviles, corresponsales solidarios; y,
    6) Relaciones con personas naturales y/o jurídicas que pudieren acceder a información crítica o sensible.

Artículo 19.- Medidas de seguridad de la información (controles).- Las entidades y empresas que conforman este régimen, para la gestión de seguridad de la información, deberán implementar los controles mínimos previstos para este Régimen en el Anexo 1.

Artículo 20.- Responsabilidades en la gestión de seguridad de la información.- Los órganos internos de dichas entidades y empresas, además de las responsabilidades previstas en la normativa legal vigente, deberán cumplir con lo descrito a continuación, para una gestión adecuada de la seguridad de la información:

1. **Consejo de Administración o Directorio:**

a) Aprobar la asignación de los recursos humanos, técnicos y financieros que sean necesarios;
b) Aprobar las políticas, procesos, procedimientos, roles y responsabilidades;
c) Aprobar los planes de concienciación y formación concernientes a seguridad de la información; y,
d) Aprobar el Plan de Gestión de Riesgos de Seguridad de la Información.

2. **Comité de Seguridad de la Información (CSI).-** Deberá proponer al Consejo de Administración:

a) La asignación de los recursos humanos, técnicos y financieros necesarios para la gestión de seguridad de la información y verificar que su inversión sea eficiente y eficaz para el logro de los objetivos estratégicos de las entidades y empresas;
b) Las políticas, procedimientos, roles y responsabilidades para la gestión de seguridad de la información;
c) Los Planes de Concienciación y Formación concernientes a seguridad de la información; y,
d) El Plan de Gestión de Riesgos de seguridad de la información y verificar que esté alineado al Plan de Administración de riesgos de las entidades y empresas.

M.

Además de lo señalado en el inciso anterior, el Comité de Seguridad de la Información, deberá aprobar la implementación de controles de seguridad de la información, propuestos por el Oficial de Seguridad de la Información (OSI) e informar los riesgos de Seguridad de la Información al Comité de Administración Integral de Riesgos, para su consolidación en la matriz de riesgos y su seguimiento.

3. **Gerente general o representante legal:**

a) Liderar la gestión de seguridad de la información de acuerdo con las disposiciones del Consejo de Administración o del Directorio y lo dispuesto en esta norma;
b) Designar un Oficial de Seguridad de la Información (OSI); y,
c) Promover la participación activa de todas las partes interesadas que intervienen en el proceso y la gestión de seguridad de la información.

4. **Oficial de Seguridad de la Información:** entre sus responsabilidades, tendrá las siguientes:

a) Definir, elaborar, supervisar la ejecución; mantener y actualizar las políticas, procesos, procedimientos, metodologías, planes y controles concernientes a la gestión de seguridad de la información, los cuales deben ser difundidos al personal correspondiente de las entidades y empresas;
b) Solicitar la asignación de los recursos humanos, técnicos y financieros necesarios para la gestión de seguridad de la información y velar que los mismos sean utilizados de forma eficiente y eficaz alineados con los objetivos estratégicos institucionales;
c) Diseñar y proponer al Consejo de Administración, las políticas, procesos, procedimientos, roles y responsabilidades, para la gestión de seguridad de la información;
d) Desarrollar y ejecutar los Planes de Concienciación y Formación a su personal, en temas concernientes a seguridad de la información;
e) Coordinar y supervisar, con los responsables de los procesos del negocio, la implementación efectiva de los controles de seguridad de la información, establecidos en el plan de gestión de riesgos; así como, desarrollar, coordinar, ejecutar, evaluar, proponer y comunicar el Plan de Gestión de Riesgos de seguridad de la información;
f) Coordinar las actividades para la gestión de seguridad de la información;
g) Ejecutar los procedimientos y lineamientos establecidos cuando se identifiquen incidentes de seguridad de la información;
h) Informar, de acuerdo con la normativa pertinente, los incidentes de seguridad de la información catalogados como sensibles o críticos, a las instituciones públicas que correspondan;
i) Participar en la evaluación de las amenazas de seguridad de la información y proponer medidas de mitigación;
j) Asesorar en materia de seguridad de la información, a través de su participación en los proyectos que involucren el manejo de información sensible o crítica de la misma, o de sus socios, clientes y usuarios;
k) Recomendar medidas correctivas adicionales en temas relacionados de seguridad de la información, alineadas al Anexo 1 y/o a buenas prácticas;
l) Verificar que los servicios brindados por personas naturales o jurídicas cumplan con las políticas de seguridad de la información establecidas; y,
m) Generar la documentación que evidencie la gestión de la seguridad de la información.

5. **Auditor interno:**

a) Verificar la efectividad de las medidas implementadas por el Oficial de Seguridad de la Información (OSI);
b) Custodiar los informes de las auditorias y/o exámenes especiales realizados por el Oficial de Seguridad de la Información (OSI) y ponerlos a disposición de la Superintendencia de Economía Popular y Solidaria, cuando esta lo requiera; y,
c) Recomendar medidas correctivas al Oficial de Seguridad de la Información (OSI).

Artículo 21.- Revisión y actualización.- Las entidades y empresas deberán revisar anualmente y actualizar cuando corresponda, la documentación referida en la presente norma.

CAPÍTULO IV
SEGURIDAD DE LA INFORMACIÓN
RÉGIMEN SIMPLIFICADO

Artículo 22.- Régimen Simplificado.- Conforman el régimen simplificado de seguridad de la información:

a) El Consejo de Administración;
b) El Gerente General o representante legal; y,
c) El Responsable de Seguridad de la Información.

Artículo 23.- Responsable de Seguridad de la Información.- Las entidades y empresas que conforman este régimen, deberán contar con un Responsable de Seguridad de la Información, quien debe tener conocimientos generales en seguridad de la información, tecnología o gestión de riesgos y reportará directamente a la Gerencia General o representante legal.

Artículo 24.- Requisitos obligatorios para el Régimen Simplificado.- Las entidades y empresas pertenecientes a este régimen deberán contar con al menos, lo siguiente:

a) Políticas, procesos, procedimientos, roles y responsabilidades para la gestión de seguridad de la información;
b) Asignación de recursos humanos, técnicos y financieros para seguridad de la información;
c) Actividades de concienciación y formación en temas concernientes en seguridad de la información;
d) Los requerimientos señalados en el Anexo 1 de esta resolución, correspondiente al Régimen Simplificado; y,
e) Registro de los eventos relacionados con seguridad de la información en la "Bitácora de Eventos de Riesgos", para lo cual podrán basarse en la metodología de riesgos que se adjunta en el Anexo 2.

Artículo 25.- Medidas de Seguridad de la Información (controles).- Las entidades y empresas que conforman este régimen, para la gestión de seguridad de la información, deberán implementar los controles mínimos previstos para este Régimen, en el Anexo 1.

Artículo 26.- Responsabilidades para la gestión de Seguridad de la Información.- Los órganos internos de dichas entidades y empresas, además de las responsabilidades previstas en la normativa legal vigente, deberán cumplir con lo descrito a continuación, para una gestión adecuada de la seguridad de la información:

1. Consejo de Administración:
a) Aprobar la asignación de los recursos humanos, técnicos y financieros necesarios; y,
b) Aprobar las políticas, procesos, procedimientos, roles y responsabilidades.

2. Gerencia General o Representante legal:
a) Liderar la gestión de la seguridad de la información de acuerdo con las disposiciones del Consejo de Administración y lo dispuesto en esta norma;
b) Designar a un funcionario en la entidad o empresa como Responsable de Seguridad de la Información;
c) Identificar y promover la participación activa de todas las partes interesadas que intervienen en la gestión de seguridad de la información y la gestión de riesgos, asociados a la seguridad de la información; y,
d) Aprobar las actividades de concientización y formación para la seguridad de información.

3. Responsable de Seguridad de la Información.- Entre sus responsabilidades, tendrá las siguientes:
a) Proponer actividades de concienciación y formación para seguridad de la información;
b) Identificar y gestionar los eventos relacionados a seguridad de la información y registrarlos en la "Bitácora de Eventos de Riesgo";
c) Elaborar los informes de pruebas y controles establecidos en temas relacionados a seguridad de la información;
d) Recomendar medidas correctivas adicionales en temas relacionados a seguridad de la información, alineadas al Anexo 1 atinente al Régimen Simplificado y/o a buenas prácticas;
e) Verificar que los servicios prestados por personas naturales o jurídicas cumplan con las políticas de seguridad de la información establecidas; y,
f) Generar la documentación que evidencie la gestión de la seguridad de la información.

4. Consejo de Vigilancia:
a) Verificar el registro y efectividad de las medidas implementadas en temas relacionados a seguridad de la información;
b) Integrar actividades relacionadas a seguridad de la información en Plan de Trabajo Anual;
c) Custodiar los informes de las pruebas y controles establecidos y ponerlos a disposición de la Superintendencia de Economía Popular y Solidaria, cuando esta lo requiera; y,
d) Recomendar medidas correctivas para la gestión de seguridad de la información.

Artículo 27.- Revisión y actualización: Las entidades y empresas que conforman este régimen, deberán revisar anualmente y actualizar cuando corresponda, la documentación referida en la presente norma.

DISPOSICIONES GENERALES

PRIMERA.- Las entidades, empresas y CONAFIPS, sin perjuicio de la información que solicite en cualquier momento este Organismo de Control, deberán reportar a la Superintendencia de Economía Popular y Solidaria, de forma inmediata, los eventos que afecten directamente a la continuidad del negocio y a la prestación de servicios financieros, incluyendo al menos la fecha del incidente, el impacto, el/los sistemas o servicios, y/o actividades afectadas, en la forma y medios que esta Superintendencia establezca para el efecto.

SEGUNDA.- Las entidades, empresas y CONAFIPS deberán solicitar al menos una vez al año a los prestadores de servicios, sean estos personas naturales o jurídicas, la documentación que demuestre que el servicio prestado cuenta con las revisiones (auditorías, exámenes especiales, certificaciones, entre otros) y controles necesarios para una adecuada administración de la seguridad de la información.

TERCERA.- Las entidades, empresas y CONAFIPS, en los contratos de prestación de servicios que celebren con personas naturales y/o jurídicas, deberán incluir cláusulas específicas por las cuales el contratista se obliga a mantener controles para la seguridad de la información y protección de datos personales, alineados a los estándares y buenas prácticas de aceptación internacional.

CUARTA.- Los casos de duda en la aplicación de la presente norma serán resueltos por la Superintendencia de Economía Popular y Solidaria.

DISPOSICIONES TRANSITORIAS

PRIMERA.- Las entidades, las empresas y la CONAFIPS implementarán esta norma dentro de los plazos previstos en el siguiente cuadro, contados a partir de la presente fecha:

Entidad, empresa y/o CONAFIPS	Segmento	Plazo para la implementación de las medidas de seguridad de la información
Cooperativas de ahorro y crédito	1	12 meses
	2	24 meses
	3	36 meses
	4 y 5	24 meses
Cajas Centrales		12 meses
Asociaciones Mutualistas de ahorro y crédito para la vivienda		12 meses
CONAFIPS		12 meses
Compañías y Organizaciones de servicios auxiliares		24 meses

SEGUNDA.- El primer oficial de seguridad de la información y el primer responsable de seguridad de la información, según corresponda, podrán acreditar el cumplimiento de los requisitos de capacitación previstos en esta norma, dentro del plazo de 6 meses contados a partir de su designación o contratación. La Superintendencia, en casos debidamente justificados y aceptados por este Organismo de Control, podrá ampliar dicho plazo por una sola vez.

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

DISPOSICIÓN FINAL.- La presente resolución entrará en vigencia a partir de la fecha de suscripción, sin perjuicio de su publicación en el Registro Oficial.

Publíquese en el portal web de la Superintendencia de Economía Popular y Solidaria.

COMUNÍQUESE.- Dado y firmado en la ciudad de San Francisco de Quito, Distrito Metropolitano, a 3 de mayo de 2022.

SOFÍA MARGARITA HERNÁNDEZ NARANJO
SUPERINTENDENTE DE ECONOMÍA POPULAR Y SOLIDARIA

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

ANEXO 1
CONTROLES OBLIGATORIOS DE SEGURIDAD DE LA INFORMACIÓN

Las entidades, empresas y/o CONAFIPS controladas, además de los requisitos exigidos en la presente norma para cada régimen, deberán desarrollar e implementar al menos los siguientes controles, los mismos que deberán ser revisados con una periodicidad mínima anual.

Controles Seguridad de la Información

Nombre / Control	Descripción	General	Especial	Simplificado
Políticas, procesos y procedimientos, roles y responsabilidades (Normativa interna de Seguridad de la Información)				
Políticas				
Seguridad de la información	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán al menos contar con el marco de políticas correctamente detallado. El contenido de las políticas deberá estar alineado a los objetivos estratégicos.	x	x	x
Clasificación de información		x	x	x
Gestión de riesgos de seguridad de la información. (Alineada a la Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del Sector Financiero Popular y Solidario bajo el control de la Superintendencia de Economía Popular y Solidaria)		x	x	x
Control de accesos físicos y tecnológicos		x	x	
Gestión de incidentes		x	x	
Gestión de software		x	x	
Gestión de infraestructura tecnológica		x	x	
Seguridad de la información para recursos humanos		x		
Seguridad física (Alineada a la Norma de control respecto de la seguridad física y electrónica emitida por la Superintendencia de		x	x	

Nombre / Control	**Descripción**	**General**	**Especial**	**Simplificado**
Economía Popular y Solidaria)				
Gestión con terceros		x	x	x
Ciberseguridad		x	x	
Procesos				
Identificación de los procesos agregadores de valor				
Documento de identificación de procesos agregadores de valor. (Alineada a la Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del Sector Financiero Popular y Solidario bajo el control de la Superintendencia de Economía Popular y Solidaria)	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda deberán disponer de un documento evidenciable en el cual se identifique y defina los procesos agregadores de valor.	x	x	x
Gestión de vulnerabilidades				
Auditorias informáticas	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán realizar auditorías, revisiones generales y/o focalizadas internas y externas.	x	x	
Pruebas de penetración	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán al menos una vez al año: a) Revisar la seguridad de sus activos mediante ejercicios prácticos y controlados, tales como ethical hacking, pentesting, entre otros, que simulen varios tipos de amenazas; y, b) Evaluar la infraestructura y aplicativos que soportan todos los servicios, en diferentes escenarios.	x		

Nombre / Control	Descripción	General	Especial	Simplificado
	Las pruebas y/o ejercicios deberán ser ejecutadas por personas naturales o jurídicas externas que acrediten experiencia en este tipo de evaluaciones.			
Plan de mitigación de los hallazgos	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán contar con un plan de mitigación de los hallazgos identificados de las auditorias o exámenes realizados. Este plan deberá incluir un análisis comparativo con los hallazgos previamente encontrados en exámenes y/o auditorias anteriores.	x	x	
Adquisición y desarrollo de software; hardware y servicios.				
Procedimiento de adquisición, desarrollo de software y mantenimiento de sistemas informáticos, hardware y servicios.	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán disponer de procedimientos para la adquisición y desarrollo de software, hardware y servicios, en los cuales se incluyan temas relacionados con controles de seguridad de la información.	x	x	
Planes de Contingencia tecnológica y continuidad del negocio				
Planes, procesos y procedimientos de Contingencia tecnológica y continuidad del negocio	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán elaborar los planes de contingencia tecnológica y continuidad del negocio. Dichos planes deberán ser evaluados periódicamente a fin de tomar acciones que correspondan.	x	x	
Cifrado				
Procedimientos de cifrado de la información sensible o Crítica	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán:	x		

Nombre / Control	Descripción	General	Especial	Simplificado
	a) Disponer de procedimientos de cifrado de sus datos sensibles o críticos, conforme al análisis de riesgos de seguridad de la información; y, b) Verificar periódicamente la vigencia de los elementos de cifrado.			
Procedimientos				
Inventario y Clasificación de información (Alineada a la Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del Sector Financiero Popular y Solidario bajo el control de la Superintendencia de Economía Popular y Solidaria)				
Identificación de tipos de información	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán disponer de un documento evidenciable en el cual se identifique y cuantifique los tipos y activos de información considerando los criterios de disponibilidad, confidencialidad e integridad así como su custodio, responsable y ubicación.	x	x	x
Inventario de activos de información.		x	x	x
Clasificación de activos de información.		x	x	x
Gestión de riesgos				
Análisis y evaluación de riesgos de las aplicaciones, servicios y activos de seguridad de la información. (Alineada a la Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del Sector Financiero Popular y Solidario bajo el control de la Superintendencia de Economía Popular y Solidaria)	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda deberán disponer de un documento evidenciable en el cual se evalúen vulnerabilidades y amenazas con el fin de determinar el nivel de riesgo. Para lo cual pueden usar cualquier método de gestión de riesgos de seguridad de la información, estructuradas y generalmente aceptadas. Podrán tomar como referencia el Anexo 2 de la presente norma.	x	x	x
Respaldos y resguardo de información sensible o crítica.				

Nombre / Control	**Descripción**	**General**	**Especial**	**Simplificado**
Procedimientos y mecanismos de resguardo de información física y digital, sensible o crítica (Alineada a la Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del Sector Financiero Popular y Solidario bajo el control de la Superintendencia de Economía Popular y Solidaria)	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán: a) Respaldar la información sensible o crítica (física y digital) en lugares y ubicaciones adecuadas, considerando la triada de seguridad de la información; y, b) Disponer al menos de un documento evidenciable que compruebe el correcto funcionamiento de los respaldos.	x	x	x
Cultura de seguridad de la información.				
Plan de capacitación de seguridad de la Información. (Alineada a la Norma de control sobre los principios y lineamientos de educación financiera)	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán: a) Evaluar periódicamente el plan de Capacitación de Seguridad de la Información; b) Definir dentro del plan de capacitación indicadores de madurez que permitan medir el nivel de aprendizaje; c) Proporcionar capacitaciones al personal, así como a proveedores, clientes, socios y usuarios.	x	x	
Gestión de accesos tecnológicos.				
Procedimiento de control de accesos	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán: Definir los perfiles y roles asignados al personal y establecer el procedimiento para su administración.	x	x	x
	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán: Implementar el registro de los accesos a los datos	x	x	

Nombre / Control	Descripción	General	Especial	Simplificado
	críticos o sensibles y las actividades que se realicen sobre estos. (Pistas de auditoría).			
Gestión de la configuración.				
Procedimiento para gestión de la configuración	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, implementarán procedimientos para la gestión de configuraciones del activo de tecnologías de información.	x	x	
Gestión de cambios, control de versiones y mantenimiento en hardware, software y servicios tecnologías de la información.				
Procedimiento para gestión de cambios y control de versiones en los servicios de tecnologías de la información.	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, implementarán procedimientos de gestión de cambios y control de versiones en el que se registren las autorizaciones, ajustes y variaciones que se realicen en los servicios de tecnología, de una manera ordenada y controlada.	x	x	

Controles tecnológicos

Nombre / Control	Descripción	General	Especial	Simplificado
Arquitectura segura	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda, deberán diseñar, implementar y gestionar, la arquitectura segura para proteger los activos digitales en función de la particularidad tecnológica. La arquitectura deberá contener al menos: a) Una estrategia de defensa en profundidad; b) Controles de flujo de información;	x	x	

Nombre / Control	Descripción	General	Especial	Simplificado
	c) Aislamiento y segmentación; d) Monitoreo y detección; y, e) Técnicas de cifrado.			
Monitoreo y detección	Las entidades, empresas y/o CONAFIPS de cada régimen según corresponda y de acuerdo a la clasificación de activos, deberán implementar sistemas que mantengan registros de logs correlacionados de la infraestructura crítica, que permitan su detección, análisis y depuración. Los registros de logs deberán incluir por lo menos: a) Hora del evento; b) Cambios en los permisos de un archivo; c) Periodo de operación; d) Acceso o salida de un usuario; e) Cambios en los datos; f) Errores y violaciones; y, g) Tareas fallidas.	x	x	

ANEXO 2
CONSIDERACIONES PARA LA METODOLOGÍA DE RIESGOS

Clasificación de Activos.

La clasificación de activos deberá:

a) Considerar al menos: aspectos del negocio, tipo de información y datos almacenados, importancia a la continuidad del servicio, consecuencias legales e impacto económico.

b) Categorizar a los activos por su privacidad en: público, uso interno y restringido; y, así valorar su proceso de custodia y control, tomando en cuenta una evaluación por activo dentro de los cuatro aspectos principales: confidencialidad, integridad, disponibilidad y privacidad, bajo el esquema de criticidad propuesto.

Gestión de riesgo.

Todas las entidades, empresas y la CONAFIPS en el análisis de riesgo institucional deberán incluir un acápite de seguridad de la información que contenga al menos los criterios básicos señalados por la norma técnica ISO/IEC 27000.

Todas las entidades, empresas y la CONAFIPS, deberán considerar al menos los siguientes aspectos dentro de su metodología:

Descripción del riesgo.

Causa, evento y consecuencia, en el siguiente orden:

a) Evento y/o amenaza: es el riesgo identificado en las tareas o actividades del proceso y/o sistema evaluado;
b) Causa y/o vulnerabilidad: es el motivo o razón que podría generar la materialización del riesgo y dar como resultado pérdidas; y,
c) Consecuencia: es la posibilidad de pérdida o materialización del evento, que puede generar un impacto financiero, por pérdidas o daños en activos, sanciones y multas por incumplimiento regulatorio y otros.

Determinación del riesgo inherente.

Riesgo intrínseco de cada actividad, tomando en cuenta el mapa de calor para determinar la criticidad así como su calificación de acuerdo con la siguiente ecuación:

CRITICO	5
ALTO	4
MEDIO	3
BAJO	2
MUY BAJO	1

$$\text{Nivel de Riesgo de Seguridad} = \text{Probabilidad x Impacto}$$

$$\text{Probabilidad} = \text{Amenaza x Vulnerabilidad}$$

Implementación de controles.

Incluir controles para la mitigación del riesgo identificado, tomando en cuenta el presupuesto y la criticidad-probabilidad del riesgo.

Evaluar la efectividad de los controles

Clasificar a los controles implementados de acuerdo con la siguiente tabla:

Efectivo	**Efectivo no formalizado**	**Inefectivo prueba**	**Inefectivo diseño**	**Control no existente**
a) Control existente bien diseñado, ejecutado adecuadamente. b) Periodicidad establecida, minimizando exposición al riesgo. c) Formalizado en norma.	a) Control existente bien diseñado, ejecutado adecuadamente. b) Periodicidad establecida, minimizando exposición al riesgo. c) No formalizado.	a) Control existente bien diseñado. b) Formalizado en norma. c) No es ejecutado adecuadamente: Falla en un número limitado de oportunidades y/o sin la periodicidad establecida.	a) Diseño del control existente, no permite mitigar adecuadamente el riesgo. b) Control débil, requiriendo acciones correctivas.	a) No se ha diseñado algún control. b) El control diseñado falla continuamente, por tanto no mitiga el riesgo relacionado.

Medición del riesgo residual.

Aquel que permanece después de que las entidades, empresas y la CONAFIPS desarrollen sus respuestas a los riesgos. El riesgo residual refleja el riesgo remanente, una vez que se ha implantado de manera eficaz las acciones planificadas. Para determinarlo se aplicará la misma ecuación del riesgo inherente.

Tratamiento del riesgo.

Las estrategias de tratamiento para los riesgos de seguridad de la información, se aplicaran a los riesgos determinados como críticos y altos; es decir, de criticidad relevante, a los cuales se los identificará y se propondrán planes de acción o controles. El responsable de proponer y darle seguimiento a la ejecución de los planes de acción, será el Oficial de Seguridad de la Información o quien hiciere sus veces. Para el tratamiento del riesgo se aplicara el siguiente esquema:

RIESGO	**Asumir** Aceptar, convivir con el riesgo y minimizar su impacto.
	Compartir Acuerdos contractuales que permiten traspasar parcialmente parte del riesgo a un tercero.
	Mitigar Tomar medidas encaminadas a impedir la materialización de los eventos de riesgo.
	Transferir Es el traspaso total del riesgo identificado a terceros.

Fuente: Elaborado por la Superintendencia de Economía Popular y Solidaria.
(2022)

Anexo 11

Cuadro de Arquitectura de continuidad de negocio

Fuente: Elaborado por Jorge Guerron en base a un entorno académico. (Abril, 2024)

Anexo 12

Cuadro del principio de continuidad

Fuente: Elaborado por Jorge Guerron en base a un entorno académico. (Abril, 2024)

Anexo 13

Cuadro de Ejercicio y Pruebas

Ejercicios y pruebas

TIPO DE EJERCICIO	¿QUÉ ES?	BENEFICIOS	DESVENTAJAS
Lista de verificación	Distribuye planes para revisión	Asegura que el plan cubra todas las actividades	No está dirigido hacia la eficacia
Recorrido estructurado	Mirada detallada a cada paso del plan de continuidad de negocio	Asegura que las actividades planificadas estén descritas correctamente en el PCN	Permite valorar ciertas capacidades de respuesta
Simulación	Escenario para representar los procedimientos de recuperación	Sesión práctica	Se tiene visibilidad limitada de algunos elementos necesarios
Paralelo	Prueba total, sin embargo, el centro de procesamiento de datos principal no es interrumpido	Asegura un alto nivel de confiabilidad, sin interrumpir las operaciones	Se debe involucrar a vario personal para identificar opciones de mejora
Interrupción Total	El desastre es replicado al punto de interrumpir las operaciones normales	Prueba confiable de funcionamiento y entrenamiento del PCN	

Fuente: Elaborado por Jorge Guerron en base a un entorno académico. (Abril, 2024)

ANEXO 14

Pólizas De Ciberseguridad

¡Bienvenido/a

Apreciado/a cliente/a:

Como director general de XXXXXXXXX es un placer darle la bienvenida a que XXXX ha agradecido la confianza depositada en nuestra compañía.

La misión de XXXX es proteger a nuestros clientes y a la sociedad en la que vivimos y trabajamos. Por ello, llevamos más de cien años en España siendo fieles a nuestro compromiso de ofrecerles los productos y servicios que mejor se adapten a sus necesidades, apoyados en nuestros principios éticos de integridad, sostenibilidad y excelencia.

Somos una aseguradora líder que presta servicio a pequeñas, medianas y grandes empresas, incluidas multinacionales, en todo el territorio nacional. Nuestra ambición es ser la mejor aseguradora a nivel global, avalada por nuestros clientes, mediadores, colaboradores y accionistas.

En este documento encontrará todo el detalle de la póliza que ha contratado. Para más información, consulte con su mediador.

XXXXXXXXXXXX

Documentación del contrato del seguro

I. Estructura de la póliza

Esta póliza está compuesta por las condiciones generales, particulares y, en su caso, especiales, que están interrelacionadas y forman parte integral del contrato de seguro.

En caso de discrepancia, las condiciones especiales prevalecerán sobre las generales y particulares, salvo que dicha discrepancia afecte al riesgo objeto de esta póliza, que deberá atenerse a lo que establecen las condiciones particulares.

II. Régimen legal, jurisdicción y competencia territorial

Asegurador y autoridad de control de su actividad

XXXXXXX es una compañía aseguradora registrada en Irlanda, con úmero de compañía XXXXX y con domicilio en XXXXXXXX. Está upervisada y registrada por Central Bank of XXXX, y autorizada para perar en España, en régimen de derecho de establecimiento, a través e su sucursal XXXXXXXX.

XXXXXX, Sucursal en España, conXXXXXXXX, y con domicilio en aseo de la XXXXXXX, está inscrita en el Registro administrativo de la irección General de Seguros y Fondos de Pensiones con la clave XXX.

n aplicación del art. 123 del Real Decreto 1060/2015, de 20 de oviembre, de ordenación, supervisión y solvencia de las entidades seguradoras y reaseguradoras, informamos de que no se aplicará la ormativa española en materia de liquidación de asegurador, sino la ormativa irlandesa.

Legislación aplicable

ste contrato de seguro, cuando no tenga la consideración legal de "Gran esgo", conforme a lo previsto en el artículo 11 de la Ley 20/2015, de 14 e julio, de ordenación, supervisión y solvencia de las entidades seguradoras y reaseguradoras, quedará sometido a las siguientes ormas:

- Ley 50/80, de 8 de octubre, de contrato de seguro.
- Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

- Ley 7/2004, de 29 de octubre, en lo relativo a la regulación del Estatuto Legal del Consorcio de Compensación de Seguros.

- Cualquier otra norma que pueda ser aplicable durante la vigencia de la póliza.

El contrato de seguro que tenga la condición legal de "Gran riesgo" conforme a lo previsto en el artículo 11 de la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras, de acuerdo a lo que dispone el artículo 107 y en el párrafo segundo del artículo 44 de la Ley 50/80, de 8 de octubre, de contrato de seguro, se regirá por:

- En primer lugar, y al amparo de lo que dispone el artículo 1.255 del Código Civil, por las cláusulas y condiciones de este contrato.

- Salvo pacto expreso, por las normas supletorias generales sobre obligaciones y contratos contenidas en el Código Civil y el Código de Comercio.

Subsidiariamente, en defecto de pacto expreso y de las normas supletorias antes indicadas, será de aplicación lo que dispone con carácter dispositivo la Ley 50/1980, de 8 de octubre, de contrato de seguro.

Jurisdicción y competencia territorial

Este contrato se regirá e interpretará conforme al derecho español o andorrano, dependiendo de que la contratación del mismo se haya hecho en España o en Andorra.

Las partes acuerdan someterse a la jurisdicción exclusiva de los juzgados y tribunales correspondientes al domicilio del asegurado.

III. Condiciones particulares

Datos identificativos

N.º de póliza: **12345678901234**
N.º de suplemento: **00000**
Producto: **Póliza de seguridad y responsabilidad de privacidad**

Periodo del seguro

Fecha de efecto: **00/00/0000 a las 00:00 h**
Fecha de vencimiento: **00/00/0000 a las 24:00 h**
Duración: **un año, renovación tácita**

Datos del tomador

Nombre o razón social: **Nombre Asegurado, S.L.**
Dirección: **C/ ejemplo, 000**
C.P.: **00000**
Población: **Ejemplo**
Provincia: **Ejemplo**
NIF/CIF: **00000000A**

Datos del mediador

Mediador: **Mediador ejemplo**
Código del mediador: **0000000000000**

Precio del seguro

Precio total del seguro	000.000.000 €
Prima neta anual	000.000.000 €
Impuestos España	000.000.000 €
Total recibo	**000.000.000 €**
Recibo n.º:	0000

Límite agregado de indemnización

Límite de indemnización: **X.XXX.000,00 €** por cada ***reclamación / pérdidas propias***.
Límite agregado de indemnización: **X.XXX.000,00 €** por ***periodo del seguro***.

En caso de ***evento ransomware:***
Límite de indemnización: **Y.YY.000,00 €** por cada ***reclamación / pérdidas propias***.
Límite agregado de indemnización: **Y.YYY.000,00 €** por ***periodo del seguro***.

Los ***gastos de defensa*** forman parte del ***límite agregado de indemnización*** y de cada ***límite de indemnización*** aquí expuesto.

Resumen de coberturas, límites, sublímites y franquicias contratadas

Este cuadro resumen de coberturas, límites, sublímites y franquicias se ha elaborado para facilitar una mejor comprensión por parte del asegurado de la información relativa a dichos conceptos. Se agrupan por secciones A, B, C y D. No obstante, cada una de las coberturas está sujeta a los términos contenidos en esta póliza, que incluyen su respectivo ámbito material, territorial y temporal de aplicación.

	Cobertura	Contratada	*Límite de indemnización*	*Franquicia* o *periodo de espera*
A.	Coberturas de respuesta a un incidente			
1.	Primera respuesta	Sí	Incluido	Sin franquicia
2.	Gastos de gestión de eventos	Sí	Incluido	Xxxx €
3.	Gastos de emergencia	Sí	10% del ***límite de Indemnización***	Xxxx €
B.	Coberturas de pérdidas propias			
4.	Pérdida de beneficios y Pérdida de beneficios derivada de proveedores			
	Periodo de restablecimiento	120 días		
	Pérdida de beneficios incurrida como consecuencia de una ***interrupción del servicio*** causada por un ***evento de seguridad, evento de privacidad*** o un ***error administrativo***	Sí	Incluido	18 horas ***periodo de espera***
	Pérdida de beneficios incurrida como consecuencia de una ***interrupción del servicio*** causada por un ***fallo del sistema***	No	No Aplicable	No Aplicable
	Pérdida de beneficios derivada de proveedores incurrida como consecuencia de una ***interrupción del servicio*** causada por un ***evento de seguridad, evento de privacidad*** o un ***error administrativo***	Sí	Incluido	18 horas ***periodo de espera***
	Pérdida de beneficios derivada de proveedores incurrida como consecuencia de una ***interrupción del servicio*** causada por un ***fallo del sistema***	No	No Aplicable	No Aplicable
5.	Gastos de reposición de activos digitales	Sí	Incluido	Xxxx €
6.	Amenaza de extorsión cibernética y pago de recompensas			
	Gastos por extorsión	Sí	Y.YY.000,00 €	Xxxx €
	Pagos por extorsión	Sí	Y.YY.000,00 €	Xxxx €
	Pago de recompensas	Sí	25.000 €	Xxxx €

	Cobertura	Contratada	*Límite de indemnización*	*Franquicia* o *periodo de espera*
C.	Coberturas de responsabilidad frente a terceros			
7.	Responsabilidad por seguridad y privacidad	Sí	Incluido	Xxxx €
8.	Procedimiento regulatorio	Sí	Incluido	Xxxx €
9.	Procedimiento del Reglamento general de protección de datos	Sí	Incluido	Xxxx €
10.	Pagos PCI-DSS	No	No Aplicable	No Aplicable
11.	Responsabilidad de publicación electrónica	Sí	Incluido	Xxxx €

D. Endosos aplicables a esta póliza

Endoso 1 Servicio de repuesta ante incidentes

Endoso 2 Renovación tácita

Ámbito

Ámbito territorial:

El *ámbito territorial* para todas estas coberturas es **mundial, excepto los Estados Unidos de América o de sus territorios o posesiones.**

Ámbito temporal:

(a) Respecto a las coberturas proporcionadas bajo la sección A. Coberturas de respuesta a un incidente, y la sección B. Coberturas de pérdidas propias del apartado IV. Condiciones de cobertura de la póliza, estas se aplicarán a cualquier ***pérdida propia*** incurrida por el ***asegurado***, **previo consentimiento por escrito del *asegurador*,** como consecuencia directa de cualquier evento contemplado bajo dichas secciones: A. Coberturas de respuesta a un incidente, y B. Coberturas de pérdidas propias que fuese descubierto por primera vez por el ***asegurado*** durante el ***periodo del seguro***.

(b) Respecto a las coberturas proporcionadas bajo la sección C. Coberturas de responsabilidad frente a terceros del apartado IV. Condiciones de cobertura de la póliza, estas se aplicarán únicamente con respecto a **cualquier *reclamación* presentada por primera vez contra el *asegurado*, o contra el *asegurador* en ejercicio de la acción directa, durante el *periodo del seguro* o, de ser aplicable, durante el *periodo adicional de declaración*,** como consecuencia **directa de un *acto incorrecto de privacidad* o un *acto incorrecto de seguridad* o un *acto incorrecto de publicación electrónica* que se hubiera producido por primera vez después de la *fecha de retroactividad* y antes de finalizar el *periodo del seguro*.**

Fecha de retroactividad:

Ilimitada

Programa internacional:

NO CONTRATADO

Periodo adicional de declaración:

Periodo:	30 días	Prima adicional:	Sin ***prima*** adicional
Periodo:	1 año	Prima adicional:	100% de la ***prima***

Servicio de respuesta ante incidentes

Las notificaciones de ***reclamaciones***, ***circunstancias*** y otros eventos asegurados bajo esta póliza, se deben dirigir al ***Servicio de respuesta a incidentes*** facilitado por el ***asegurador***.

Servicio de respuesta a incidentes	Lazarus	931 845 872

IV. Condiciones de cobertura de la póliza

Objeto del seguro

En los términos y condiciones indicados en este contrato, el asegurador asume las coberturas que más adelante se indican y que estén expresamente incluidas en las Condiciones Particulares, y su responsabilidad no excede en ningún caso de los respectivos límites de indemnización determinados en dichas condiciones particulares.

Garantías y coberturas

Las siguientes coberturas se aplicarán cuando consten como expresamente contratadas en el apartado III. Condiciones Particulares, y quedarán sujetas a todos los términos y condiciones de esta póliza, incluyendo el ***límite de indemnización***, el ***límite agregado de indemnización***, la ***franquicia*** y los ***periodos de espera*** especificados en las ***Condiciones Particulares***.

Si el apartado III. Condiciones Particulares indica que una cobertura no está contratada, esta póliza no proporcionará ninguna cobertura al respecto.

A. Coberturas de respuesta de incidentes

1. Primera respuesta

El ***asegurador*** pagará los ***gastos de gestión de eventos***, ***gastos de reposición de activos digitales***, ***incremento de gastos de operaciones***, o ***gastos de defensa*** **durante 72 horas después de que el** ***asegurado*** **descubra por primera vez** cualquier ***evento de privacidad***, ***evento de seguridad***, ***evento de publicación electrónica*** o ***interrupción del servicio*** real o sobre la que se tenga una sospecha razonable, **siempre y cuando el** ***asegurado*** **incurra dichos gastos a través del** ***Servicio de respuesta a incidentes***.

2. Gastos de gestión de eventos

El ***asegurador*** pagará los ***gastos de gestión de eventos*** incurridos de modo necesario y razonable por el ***asegurado***, **previo consentimiento por escrito del** ***asegurador***, como consecuencia directa de un ***evento de privacidad***, ***evento de seguridad*** o ***evento de publicación electrónica*** que fuese descubierto por primera vez por el ***asegurado*** durante el ***periodo del seguro***.

3. Gastos de emergencia

En el caso de que no fuese posible obtener el consentimiento por escrito del ***asegurador*** en un plazo de tiempo razonable antes de que el ***asegurado*** incurra de modo necesario y razonable en ***gastos de gestión de eventos***, ***gastos de reposición de activos digitales***, ***incremento de gastos de operaciones***, o ***gastos de defensa*** en relación con un ***evento*** cubierto o una ***reclamación***, el ***asegurador*** podrá aprobar de forma retroactiva dichos gastos.

B. Coberturas de pérdidas propias

4. Pérdida de beneficios y pérdida de beneficios derivada de proveedores

El ***asegurador*** pagará:

- la ***pérdida de beneficios***,
- la ***pérdida de beneficios derivada de proveedores***, e
- ***incremento de gastos de operaciones***,

incurridos por el ***asegurado*** durante el ***periodo de restablecimiento***, como consecuencia de una ***interrupción de servicio*** que sea descubierta por primera vez durante el ***periodo del seguro***.

5. Gastos de reposición de activos digitales

El ***asegurador*** pagará los ***gastos de reposición de activos digitales*** incurridos de modo necesario y razonable por el ***asegurado*** debido a la corrupción o destrucción de ***activos digitales*** como consecuencia de un ***evento de privacidad*** o un ***evento de seguridad*** que sea descubierto por primera vez durante el ***periodo del seguro***.

6. Amenaza de extorsión cibernética y pagos de recompensas

El ***asegurador*** pagará:

- los ***gastos por extorsión***, y
- el ***pago de recompensas***,

de igual forma, el ***asegurador*** reembolsará:

- los ***pagos por extorsión***,

incurridos de modo necesario y razonable por el ***asegurado*** como consecuencia directa de una ***amenaza de extorsión cibernética***, recibida por primera vez durante el ***periodo del seguro***, siempre y cuando:

i) un ***ejecutivo*** del ***asegurado*** apruebe el pago de dichos ***gastos por extorsión*** y/o ***pagos por extorsión***, y

ii) no se realice ningún ***pago de recompensas*** a un auditor externo del ***asegurado***, o a cualquier ***persona asegurada*** que sea un auditor interno del ***asegurado*** o que supervise o gestione a un auditor externo del ***asegurado***.

C. Coberturas de responsabilidad frente a terceros

7. Responsabilidad por seguridad y privacidad

El ***asegurador*** pagará al, o por cuenta del ***asegurado***:

- la ***pérdida*** que el ***asegurado*** esté legalmente obligado a pagar, incluyendo los costes y gastos del reclamante, y
- los ***gastos de defensa*** incurridos por el ***asegurado***,

derivados de una *reclamación* presentada por primera vez contra el *asegurado*, o contra el *asegurador* en ejercicio de la acción directa, durante el *periodo del seguro* o, de ser aplicable, durante el *periodo adicional de declaración*, como consecuencia directa de un *acto incorrecto de privacidad* o un *acto incorrecto de seguridad* que se hubiera producido por primera vez después de la *fecha de retroactividad* y antes de finalizar el *periodo del seguro*.

8. Procedimiento regulatorio

El ***asegurador*** pagará al, o por cuenta del ***asegurado***:

- las ***multas y sanciones civiles*** que el ***asegurado*** esté legalmente obligado a pagar y que sean legalmente asegurables, y
- los ***gastos de defensa*** incurridos por el ***asegurado***,

derivados de un *procedimiento regulatorio* iniciado por primera vez contra el *asegurado* durante el *periodo del seguro* o, en su caso, el *periodo adicional de declaración*, como consecuencia directa de un *evento de privacidad* o un *evento de seguridad* que se hubiera producido por primera vez después de la *fecha de retroactividad* y antes de finalizar el *periodo del seguro*.

9. Procedimiento del Reglamento general de protección de datos (procedimiento RGPD)

El ***asegurador*** pagará al, o por cuenta del ***asegurado***:

- las ***multas y sanciones civiles*** que el ***asegurado*** esté legalmente obligado a pagar y que sean legalmente asegurables, y
- los ***gastos de defensa*** incurridos por el ***asegurado***,

derivados de un *procedimiento RGPD* iniciado por primera vez contra el *asegurado* durante el *periodo del seguro* o, en su caso, el *periodo adicional de declaración*, como consecuencia directa de un *evento de privacidad* o un *evento de seguridad* que se hubiera producido por primera vez después de la *fecha de retroactividad* y antes de finalizar el *periodo del seguro*.

10. Pagos PCI-DSS (Estándar de seguridad de datos para la industria de tarjetas de pago)

El ***asegurador*** pagará al, o por cuenta del ***asegurado***:

- los ***pagos PCI-DSS*** que el ***asegurado*** esté legalmente obligado a pagar, y
- los ***gastos de defensa*** incurridos por el ***asegurado***,

derivados de una ***reclamación PCI-DSS*** presentada **por primera vez contra el *asegurado* durante el *periodo del seguro* o, en su caso, el *periodo adicional de declaración*, como consecuencia directa de un *evento de privacidad* o un *evento de seguridad* que se hubiera producido por primera vez después de la *fecha de retroactividad* y antes de finalizar el *periodo del seguro*.**

11. Responsabilidad de publicación electrónica

El ***asegurador*** pagará al, o por cuenta del ***asegurado***:

- la ***pérdida*** que el ***asegurado*** esté legalmente obligado a pagar incluyendo los costes y gastos del reclamante, y
- los ***gastos de defensa*** incurridos por el ***asegurado***,

derivados de una ***reclamación*** presentada **por primera vez contra el *asegurado* durante el *periodo del seguro* o, en su caso, el *periodo adicional de declaración*, como consecuencia directa de un *acto incorrecto de publicación electrónica* que se hubiera producido por primera vez después de la *fecha de retroactividad* y antes de finalizar el *periodo del seguro*.**

V. Definiciones

Los términos escritos en **negrita y cursiva** en esta póliza, estén en singular o en plural y con independencia de que consten en este apartado V. ("Definiciones") o definidos en otros apartados de esta póliza, tendrán el significado especificado a efectos de esta póliza.

5.1 Acceso no autorizado

Acceso no autorizado significa un acceso a, o uso de un ***sistema informático*** por cualquier persona o personas no autorizadas, o por una persona o personas autorizadas pero que accedan de una manera no autorizada.

5.2 Activos digitales

Activos digitales significa ***datos electrónicos***, ***programas informáticos***, archivos de audio y archivos de imagen almacenados en el ***sistema informático*** del ***asegurado***, **siempre y cuando los *activos digitales* no incluyan cuentas bancarias, facturas, recibos, dinero, llaves criptográficas que permitan el acceso a las monedas digitales, valores, efectos al portador o a la orden endosados en blanco, registros, documentos valiosos, escrituras, manuscritos u otros documentos**, excepto si hubieran sido convertidos en ***datos electrónicos***, en cuyo caso se considerarán únicamente bajo dicha forma electrónica.

5.3 Acto incorrecto

Acto incorrecto significa un ***acto incorrecto de seguridad***, un ***acto incorrecto de privacidad*** o un ***acto incorrecto de publicación electrónica***.

5.4 Acto incorrecto de privacidad

Acto incorrecto de privacidad significa cualquier acto, error, omisión, negligencia o incumplimiento del deber, real o supuesto, por parte del ***asegurado***, por cualquier persona por la cual el ***asegurado*** es legalmente responsable o por el ***proveedor del servicio*** del ***asegurado***, que resulte en un ***evento de privacidad***.

5.5 Acto incorrecto de publicación electrónica

Acto incorrecto de publicación electrónica significa cualquier acto, error, omisión, negligencia o incumplimiento, real o supuesto, de un deber por parte de un ***asegurado***, que resulte de un ***evento de publicación electrónica***.

5.6 Acto incorrecto de seguridad

Acto incorrecto de seguridad significa cualquier acto, error, omisión, negligencia o incumplimiento del deber, real o supuesto, por parte del ***asegurado***, así como por parte de cualquier persona por la que el ***asegurado*** sea legalmente responsable o por el ***proveedor del servicio*** del ***asegurado***, que dé lugar a un ***evento de seguridad***.

5.7 Actos incorrectos interrelacionados

Actos incorrectos interrelacionados significa todos los ***actos incorrectos*** derivados de, basados en, en relación con o de otro modo atribuibles a la misma causa o fuente de origen.

5.8 Ámbito territorial

Ámbito territorial significa mundial, **excepto los Estados Unidos de América o de sus territorios o posesiones**, salvo que se establezca lo contrario en las ***Condiciones Particulares***.

5.9 Amenaza de extorsión cibernética

Amenaza de extorsión cibernética significa:

(a) una amenaza o una serie de amenazas conexas, realizadas sin la cooperación de un ***ejecutivo*** para:

- (i) introducir ***código malicioso*** en un ***sistema informático***;
- (ii) iniciar un ***ataque de denegación de servicio***;
- (iii) difundir, divulgar o utilizar indebidamente cualquier ***información personal*** o ***información corporativa*** obtenidos como resultado de un ***acceso no autorizado*** al ***sistema informático*** del ***asegurado***, o
- (iv) cifrar o hacer inaccesibles por otros medios los ***datos electrónicos***;

salvo si se recibe un *pago por extorsión* del *asegurado* o por cuenta del *asegurado* a cambio de la eliminación, la mitigación o la retirada de dicha amenaza, y

(b) una amenaza o serie de amenazas conexas relacionadas con cualesquiera de los actos indicados en el párrafo (a) anterior que ya hayan comenzado.

5.10 Asegurado

Asegurado significa:

(a) el ***tomador del seguro***, según se indica en las ***Condiciones Particulares***;

(b) una ***empresa filial***, o

(c) una ***persona asegurada***.

5.11 Asegurador

La persona jurídica que asume la cobertura del riesgo previsto en el contrato, dentro de los límites pactados en este.

5.12 Asociación de tarjetas

Asociación de tarjetas significa un emisor de tarjetas de crédito, tarjetas de débito, tarjetas de valor depositado o tarjetas prepagadas.

5.13 Ataque de denegación de servicio

Ataque de denegación de servicio significa cualesquiera acciones o instrucciones generadas con la facultad de dañar o interferir de cualquier manera la disponibilidad, los servicios o la conectividad de redes o los sistemas de información incluyendo, pero no limitándose a, la generación de tráfico de red en exceso en direcciones de dichas redes o el aprovechamiento de deficiencias del sistema o de la red, y generación de tráfico en exceso e irreal dentro de y entre las redes.

5.14 Bienes

Bienes significa los bienes tangibles del ***asegurado*** distintos de ***dinero*** o ***valores***.

5.15 Cambio de control

Cambio de control significa un acontecimiento en el que cualquier persona, entidad o grupo:

a) adquiere más del 50% del capital social del ***tomador del seguro***;

b) adquiere la mayoría de los derechos de voto del ***tomador del seguro***;

c) asume el derecho a designar o destituir a la mayoría del consejo de administración o puestos equivalentes del ***tomador del seguro***;

d) asume el control en virtud de un acuerdo por escrito con otros accionistas relativo a la mayoría de los derechos de voto en el ***tomador del seguro***;

e) realiza una fusión por absorción del ***tomador del seguro***, o

f) es nombrado administrador o liquidador concursal (o cargo o persona equivalente en función de la jurisdicción aplicable) del ***tomador del seguro***, o el ***tomador del seguro*** se convierte en deudor en posesión (o la condición equivalente en la jurisdicción aplicable).

5.16 Campo electromagnético

Campo electromagnético significa cualquier campo de energía que esté formado por componentes eléctricos y magnéticos asociados.

5.17 Ciberterrorismo

Ciberterrorismo significa el uso de la tecnología de la información para ejecutar ataques o amenazas por cualquier persona o grupo, con independencia de que actúen solos o por cuenta de, o en relación con cualquier individuo, organización o gobierno, con la intención de:

(a) causar un daño, o

(b) intimidar a cualquier persona o entidad, o

(c) causar la destrucción o el daño de infraestructuras o datos críticos;

para promover objetivos financieros, sociales, ideológicos, religiosos o políticos, que puedan resultar en una amenaza o daño a la ***seguridad de la red*** del ***asegurado***.

5.18 Circunstancia

Circunstancia significa cualquier incidente, ocurrencia, hecho, asunto, acto u omisión que pueda dar lugar a una ***reclamación***, a un ***evento de seguridad***, a un ***evento de privacidad***, a un ***evento de publicación electrónica***, a un ***error administrativo***, a un ***fallo del sistema***, a una ***amenaza de extorsión cibernética***, a un ***procedimiento regulatorio***, a un ***procedimiento RGPD*** o una ***reclamación PCI-DSS***.

5.19 Cliente

Cliente significa cualquier entidad o individuo a quien el ***asegurado*** vende bienes o presta servicios en virtud de un contrato escrito.

5.20 Código malicioso

Código malicioso significa cualquier programa informático, código o programa no autorizado, corruptor o dañino específicamente diseñado para:

(a) borrar o corromper ***datos electrónicos***;

(b) dañar o alterar cualquier red o ***sistema informático***, o

(c) eludir cualquier producto o servicio de seguridad,

incluyendo, pero no limitado a virus informáticos, caballos de Troya, registradores de teclas (*keystroke loggers*), archivos de registro de información o rastreo (*cookies*), programas espía (*spyware*), aplicación de anuncios no deseados (*adware*), gusanos, secuestro de datos (*ransomware*) y bombas lógicas.

5.21 Condiciones Particulares

Condiciones Particulares significa las condiciones particulares adjuntas a esta póliza y aquellas modificaciones que pudieran sufrir durante el ***periodo del seguro***.

5.22 Contaminantes

Contaminantes significa cualesquiera elementos que puedan perjudicar el medio ambiente y/o a los recursos naturales, incluyendo a título enunciativo, pero no limitativo cualquier ruido, vibración, contaminación lumínica, material biológico, hongos de cualquier tipo, material radiactivo o nuclear, asbestos o cualquier producto o material que contenga asbesto en cualquier forma o cantidad, irritante térmico, sílice, contaminante sólido, líquido o gaseoso, incluyendo humo, vapor, hollín, gases, ácidos, químicos y desechos. Los desechos incluyen, pero no se limitan a, material reciclable, reacondicionable o recuperable.

5.23 Datos electrónicos

Datos electrónicos significa información almacenada o transmitida en formato digital. ***Datos electrónicos* no incluye *programas informáticos*, moneda digital ni llaves criptográficas que faciliten el acceso a los sistemas de moneda digital.**

5.24 Dinero

Dinero significa divisa, monedas o billetes de bancos en uso y con un valor nominal, o cheques de viaje, cheques registrados y giros bancarios mantenidos para la venta al público. ***Dinero* no incluye criptoactivos.**

5.25 Ejecutivo

Ejecutivo significa cualquier persona física que sea o que, durante el ***periodo del seguro*** de la póliza, llegue a ser nombrada o elegida administrador, directivo, consejero, director de operaciones, director financiero, director del departamento jurídico, director de seguridad, director de tecnología, gerente de riesgos, delegado de protección de datos, o cargo equivalente del ***asegurado***.

5.26 Electromagnetismo

Electromagnetismo significa magnetismo generado por una corriente eléctrica.

5.27 Empleado

Empleado significa cualquier persona física que:

(a) tenga un contrato laboral, de prestación de servicios o de formación con el ***asegurado***;
(b) esté bajo un programa o contrato de prácticas o similar con el ***asegurado***, o
(c) esté contratado o haya sido temporalmente cedido al ***asegurado*** por parte de otro empleador;

mientras esté bajo el control o la supervisión del ***asegurado***.

Asimismo, a los efectos de este concepto se equiparará con el mismo cualquier persona física que:

(d) sea jefe de contratación o subcontratista de obra, o aquellas personas designadas por cualesquiera de estos, o
(e) sea un trabajador autónomo,

y trabaje para el ***asegurado***, en relación con su negocio, mientras esté bajo el control o la supervisión del ***asegurado***.

5.28 Empresa filial

Empresa filial significa cualquier entidad u organización, en la cual durante, o antes de la fecha de inicio de esta póliza, el ***asegurado***, bien directa o indirectamente, a través de una o más ***empresas filiales***:

(a) controla la composición del consejo de administración para elegir o tener derecho a nombrar a la mayoría de los miembros del consejo de administración (o su equivalente en cualquier otro país);

(b) controla más del 50% de los derechos de voto de los accionistas o del capital social, u

(c) ostenta más del 50% del capital social o de las acciones emitidas.

5.29 Entidad relacionada

Entidad relacionada significa cualquier persona física o jurídica o sus ***subcontratistas*** o apoderados:

(a) que sea propietaria de, opere o gestione, total o parcialmente, al ***asegurado***;

(b) en la cual el ***asegurado*** ostente una participación superior al 20%, o

(c) que está controlada, operada o gestionada por el ***asegurado***.

5.30 Error administrativo

Error administrativo significa un acto accidental, no intencional o negligente o un error u omisión cometido por el ***asegurado*** o el ***proveedor del servicio*** durante el transcurso de:

(a) el procesamiento o tratamiento de datos, la programación, mantenimiento, servicio, conversión, modificación, manejo, desarrollo o mantenimiento de ***datos electrónicos*** o ***programas informáticos***, o

(b) la operación, mantenimiento o reparación de ***sistemas informáticos***;

incluyendo la recopilación, la compilación, el procesamiento, el almacenamiento, la extracción, el almacenaje o la gestión de datos.

5.31 Evento

Evento significa un ***evento de seguridad***, ***evento de privacidad***, ***evento de publicación electrónica***, ***amenaza de extorsión cibernética***, ***error administrativo*** y ***fallo del sistema***.

5.32 Evento de privacidad

Evento de privacidad significa:

(a) una divulgación no autorizada, real o presunta, o la pérdida de:

(i) ***información personal*** bajo el cuidado, custodia o control del ***asegurado*** o bajo el cuidado, custodia o control del ***proveedor del servicio*** del ***asegurado***, o

(ii) ***información corporativa*** bajo el cuidado, custodia o control del ***asegurado*** o bajo el cuidado, custodia o control del ***proveedor del servicio*** del ***asegurado***, que esté identificada específicamente como de carácter confidencial y protegida conforme a un acuerdo de confidencialidad o un contrato similar;

(b) un incumplimiento, real o presunto, de cualquier ***normativa de protección de datos personales*** por parte del ***asegurado***, o

(c) el incumplimiento por parte del ***asegurado*** de aquella parte de su declaración pública o de su política de tratamiento, recopilación, uso, divulgación, intercambio, difusión y corrección o suplementación de ***información personal***, y el acceso a ***información personal*** que específicamente:

(i) prohíbe o restringe la divulgación, intercambio o venta de ***información personal*** por parte del ***asegurado***;

(ii) requiere que el ***asegurado*** facilite un acceso individual a la ***información personal*** o que corrija la ***información personal*** incompleta o inexacta después de realizarse una solicitud al respecto, o

(iii) establece procedimientos y requisitos para evitar la pérdida de ***información personal***;

siempre que el *asegurado* tenga en vigor, en el momento de dicho incumplimiento, una política de tratamiento, recopilación, uso, divulgación, intercambio, difusión y corrección o suplementación de, y de acceso a la *información personal*.

5.33 Evento de publicación electrónica

Evento de publicación electrónica significa cualquier acto o supuesto acto de:

(a) injuria, calumnia, difamación comercial o desprestigio que resulte de la ***publicación electrónica*** de material que difame a una persona u organización o desprestigia los bienes, productos o servicios de una persona u organización;

(c) violación del derecho a la privacidad, derechos al honor, a la intimidad personal y familiar y a la propia imagen o el derecho de publicidad de cualquier persona distinta de una ***persona asegurada*** que resulte de la ***publicación electrónica*** de material que revele públicamente hechos privados relativos a tal persona o que se apropie comercialmente del nombre o apariencia de tal persona;

(d) incumplimiento de un derecho de autor, título, eslogan, marca registrada, nombre comercial, imagen comercial, señal, marca de servicios o nombre de servicio incluyendo, pero sin limitarse a, un incumplimiento del nombre de dominio, el empleo de enlaces profundos (*deep linking*) o *framing*, que resulten de las actividades de ***publicación electrónica*** del ***asegurado***, o

(e) uso no autorizado de encabezamientos, formatos, funciones, estilo, caracteres, gráficos u otro material protegido que resulten de las actividades de ***publicación electrónica*** del ***asegurado***,

siempre y cuando dicha cobertura no se otorgue en relación con cualquier tipo de responsabilidad que resulte directa o indirectamente de:

(i) el robo de puntos de juego de ordenador o de videojuego, premios obtenidos u otros bienes intangibles;

(ii) la carga o descarga de música, películas, programas informáticos o videojuegos digitalizados por parte de personas que supuestamente o de hecho no han obtenido licencias válidas en relación con dicha música, películas, programas informáticos o videojuegos, o

(iii) cualquier tarifa de licencia, daños y perjuicios, cuenta de ganancias o regalías (*royalties*) cuyo pago resulte ordenado o acordado por el *asegurado* conforme a una sentencia, laudo arbitral, acuerdo de liquidación u orden o acuerdo similar para el uso continuo del derecho de autor, título, eslogan, marca, nombre comercial, imagen comercial, marca de servicios o nombre de servicio u otro elemento de propiedad intelectual, de una persona o entidad.

5.34 Evento de seguridad

Evento de seguridad significa:

(a) el ***acceso no autorizado*** a;

(b) el robo físico por una persona que no sea el ***asegurado*** de;

(c) la introducción de ***código malicioso*** en, o

(d) el ***ataque de denegación de servicio*** al

Sistema informático del ***asegurado*** que cause una violación de la ***seguridad de la red*** que origine:

(i) una ***interrupción del servicio***;

(ii) el robo, la alteración, destrucción, pérdida o divulgación no autorizada de ***datos electrónicos*** en el ***sistema informático*** del ***asegurado***;

(iii) la denegación del acceso de un usuario autorizado al ***sistema informático*** del ***asegurado***, a menos que dicha denegación de acceso se deba a un fallo mecánico o eléctrico ajeno al control del ***asegurado***;

(iv) la participación del ***sistema informático*** del ***asegurado*** en un ***ataque de denegación de servicio*** o de minería de moneda digital o criptoactivos dirigido contra el ***sistema informático*** de un ***tercero***;

(v) la transmisión de ***código malicioso*** desde el ***sistema informático*** del ***asegurado*** al ***sistema informático*** de un ***tercero***;

(vi) la alteración, corrupción o destrucción de ***activos digitales*** o ***información personal***, o

(vii) la pérdida de uso de todo o parte del ***sistema informático*** del ***asegurado*** causada por la reprogramación no autorizada del ***programa informático*** que hace que dicho ***sistema informático***, o cualquier componente del mismo, no funcione o sea inútil para el propósito para el que estaba destinado.

5.35 Evento ransomware

Evento ransomware significa cualquier ***evento de privacidad***, ***evento de seguridad*** e ***interrupción del servicio*** en relación con un ***pago por extorsión*** real o supuesto. Se considerará como un ***evento ransomware*** independientemente de que se pague realmente un rescate o no, o se revele parte de los datos extraídos.

5.36 Eventos interrelacionados

Eventos interrelacionados significa todos los ***eventos*** derivados de, basados en, en relación con o de otro modo atribuibles a la misma causa o fuente de origen.

5.37 Fallo del sistema

Fallo del sistema significa la interrupción, suspensión o fallo medible, material, no intencionado y no planificado del ***sistema informático***, sea cual sea la causa. ***Fallo del sistema* no incluye *evento de seguridad***.

5.38 Fondo de compensación del consumidor

Fondo de compensación del consumidor significa cualquier suma de dinero que el ***asegurado*** está legalmente obligado a depositar o consignar para el pago de reclamaciones de consumidores, por requerimiento o resolución en su contra como consecuencia de un ***procedimiento regulatorio*** o en un ***procedimiento RGPD***.

5.39 Fecha de retroactividad

Fecha de retroactividad significa la fecha especificada como tal en las ***Condiciones Particulares***.

5.40 Franquicia

Franquicia significa el importe especificado como tal en esta póliza, en las ***Condiciones Particulares*** o en cualquier endoso, en relación con cualquier ***reclamación*** o ***evento*** o ***pérdida***, ***pérdidas propias*** y/o ***gastos de defensa*** por los que el ***asegurado*** sea responsable.

5.41 Gastos de defensa

Gastos de defensa significa:

a) los honorarios, costes, cargos y gastos incurridos por el ***asegurado***, **con el previo consentimiento por escrito del *asegurador***, necesarios para la investigación, defensa, transacción, liquidación o recursos en general de una ***reclamación*** presentado en contra del ***asegurado***; así como,

b) los gastos incurridos por el ***asegurado*** para la constitución y mantenimiento de cualquier fianza judicial o aval, que se requiera como parte de un procedimiento judicial derivado de una ***reclamación*** interpuesto contra el ***asegurado***. **Estos gastos no incluirán ni implicarán para el *asegurador* obligación alguna de obtener o tramitar la fianza o el aval ni de otorgar garantía alguna para su expedición.**

Los *gastos de defensa* no incluirán los salarios, honorarios, bonos o cualquier otra forma de remuneración de cualquier *persona asegurada*, el coste de su tiempo o costes o gastos generales del *asegurado*.

Los *gastos de defensa* tampoco incluyen cualquier *pérdida propia*.

Los *gastos de defensa* siempre formarán parte de, y no serán adicionales ni aplicarán en exceso del *límite de indemnización* aplicable, y estarán sujetos a *franquicia*.

5.42 Gastos de gestión de eventos

Gastos de gestión de eventos significa cualesquiera cargos, costes, gastos y honorarios, razonables y necesarios, incurridos por el ***asegurado*** **con el consentimiento previo por escrito del *asegurador*, dentro de los 24 meses desde que el *asegurado* tenga conocimiento por primera vez de un *evento de privacidad*, *evento de seguridad*** o un ***evento de publicación electrónica***, para contratar los servicios profesionales de un contable, asesor informático, abogado, asesor de relaciones públicas o cualquier otro profesional cualificado para:

(a) realizar un análisis informático forense en el ***sistema informático*** del ***asegurado***, para establecer la causa y el alcance de dicho ***evento de privacidad***, ***evento de seguridad*** o ***evento de publicación electrónica***;

(b) establecer las obligaciones de indemnización bajo cualquier contrato escrito en relación con un ***acto incorrecto*** cometido por un ***proveedor del servicio*** relacionado con un ***evento de privacidad***, ***evento de seguridad*** o un ***evento de publicación electrónica***;

(c) asesorar sobre la obligación del ***asegurado*** de notificar a cualquier autoridad de control, en particular a la Agencia Española de Protección de Datos, o a los individuos potencialmente afectados después de cualquier ***evento de privacidad***, ***evento de seguridad*** o ***evento de publicación electrónica***;

(d) hacer cumplir cualquier ***normativa de protección de datos personales*** aplicable más favorable a los individuos afectados del ***asegurado***. **No obstante, una vez que el cumplimiento se ha efectuado después de un *evento de privacidad*, *evento de seguridad* o un *evento de publicación electrónica*, esta póliza no cubrirá los costes para mantener el cumplimiento continuo de cualquier *normativa de protección de datos personales*;**

(e) notificar a cualquier individuo o autoridad de control competente el compromiso de cualquier ***información personal*** que surja de cualquier ***evento de privacidad***, ***evento de seguridad*** o ***evento de publicación electrónica***, con independencia de que estén o no obligados a ser notificados en virtud de la legislación aplicable. **No obstante, el *asegurado* deberá solicitar el consentimiento del *asegurador* antes de realizar cualquier notificación a un individuo o autoridad de control cuando no exista una exigencia legal o regulatoria en dicho sentido;**

(f) planificar, implementar, ejecutar y gestionar una campaña de relaciones públicas para contrarrestar o minimizar cualquier efecto adverso real o anticipado de publicidad negativa de un ***evento de privacidad***, ***evento de seguridad*** o ***evento de publicación electrónica*** para proteger o restaurar la reputación comercial del ***asegurado*** en respuesta a la publicidad negativa posterior a dicho ***evento***;

(g) proporcionar servicios de monitorización de crédito y de identificación, servicios de restauración de la identificación, y un seguro contra el robo de la identificación, siempre que el ***asegurador*** no tenga la obligación de solicitar o proporcionar dicho seguro, para las personas afectadas por la destrucción, la pérdida, la alteración, la divulgación o el acceso a la ***información personal***, o

(h) prestar servicios de centro de llamadas (call center) si son necesarios para atender a las consultas de las personas afectadas por la destrucción, la pérdida, la alteración, la divulgación o el acceso a la ***información personal***,

los *gastos de gestión de eventos* no incluyen cualesquiera:

(i) **sueldos, salarios u honorarios habituales o por horas extra de cualquier *socio comercial*, director, *ejecutivo* o *empleado*;**

(ii) **gastos de cumplir con cualquier medida cautelar u otro remedio de carácter no económico;**

(iii) **capital, intereses u otro dinero pagado o adeudado como consecuencia de cualquier préstamo, arrendamiento o ampliación o concesión de créditos,**

(iv) **impuestos, multas, sanciones o penalizaciones.**

5.43 Gastos de reposición de activos digitales

Gastos de reposición de activos digitales significa los costes y gastos razonables y necesarios incurridos por el ***asegurado*** **con el previo consentimiento por escrito del *asegurador* para**:

(a) restaurar o reconstruir los ***activos digitales*** a partir de archivos escritos, o

(b) igualar total o parcialmente los ***datos electrónicos***;

debido a su corrupción o destrucción, incluyendo, pero no limitado a, cualquier recuperación de un desastre o un trabajo de una investigación forense. **Los *gastos de reposición de activos digitales* no incluirán:**

(i) **cualquier coste y gasto incurrido hasta la fecha, reemplazo u otro tipo de actualización de *activos digitales* hasta un nivel superior a aquel que existía antes del *evento de seguridad* o de *evento de privacidad***, salvo en el caso de una ***mejora***;

(ii) **cualquier coste y gasto incurrido para identificar o remediar errores o vulnerabilidades de *programas informáticos*;**

(iii) **cualquier coste y gasto incurrido para investigar y desarrollar *activos digitales*, incluyendo *secretos comerciales*;**

(iv) **el valor económico o de mercado de *activos digitales*, incluyendo los *secretos comerciales*;**

(v) **cualquier pérdida o daño consecuencial;**

(vi) ***gastos por extorsión*, o**

(vii) ***pagos por extorsión*.**

5.44 Gastos por extorsión

Gastos por extorsión significa los gastos razonables y necesarios incurridos por el ***asegurado*** **con el consentimiento previo por escrito del *asegurador***, derivados directamente de una ***amenaza de extorsión cibernética***.

5.45 Grupo de control

Grupo de control significa el consejero delegado, director financiero, director de operaciones, director de seguridad de la información, director de información, director o delegado de protección de datos, director de tecnología, gerente de riesgos, director de seguros, director jurídico del ***tomador del seguro*** o cualquier otro director con competencias en tecnología, jurídicas o de datos.

5.46 Incremento de gastos de operaciones

Incremento de gastos de operaciones significa los gastos razonables y necesarios incurridos por el ***asegurado*** **con el consentimiento por escrito del *asegurador*** durante el ***periodo de restablecimiento*** para minimizar, evitar o reducir la ***interrupción del servicio*** o la ***pérdida de beneficios*** o la ***pérdida de beneficios derivada de proveedores*** y que:

(a) estén por encima de y superen los gastos operativos y de nómina normales del ***asegurado***, y

(b) **no excedan el importe de la pérdida que, de no haber incurrido en dichos gastos, se debería pagar como *pérdida de beneficios* o *pérdida de beneficios derivada de proveedores*.**

A estos efectos, se hace constar que el *incremento de gastos de operaciones* no incluye:

(i) **cualquier gasto o coste necesario para corregir cualquier deficiencia o problema con cualquier *sistema informático* o para identificar o remediar errores o debilidades de cualquier *programa informático;***

(ii) cualquier gasto o coste para actualizar, restaurar, remplazar o mejorar cualquier *sistema informático* o *programa informático* a un nivel por encima del existente inmediatamente antes de la *interrupción del servicio*, salvo en el caso de una *mejora*;

(iii) cualquier penalización contractual derivada de cualquier responsabilidad frente a un *tercero*;

(iv) cualquier pérdida o daño consecuencial, o

(v) cualquier otro coste, pérdida o pago específicamente definido en esta póliza y cubierta bajo cualesquiera de sus coberturas o mediante endoso específico.

5.47 Interrupción del servicio

Interrupción del servicio significa una interrupción, suspensión, fallo, degradación o retraso real y medible en el rendimiento del ***sistema informático*** del ***asegurado***, directamente derivada de un ***error administrativo***, de un ***fallo del sistema***, de un ***evento de seguridad*** o de un ***evento de privacidad***.

Interrupción del servicio también significa:

(a) un apagado voluntario del ***sistema informático*** del ***asegurado*** cuando esta acción se lleva a cabo para minimizar, evitar o mitigar un ***evento de seguridad***, o

(b) un apagado forzoso del ***sistema informático*** del ***asegurado*** cuando esta acción sea ordenada por una autoridad judicial o administrativa competente, como parte de un ***procedimiento regulatorio*** o un ***procedimiento RGPD***.

5.48 Información corporativa

Información corporativa significa cualquier información confidencial que no está disponible para el público en general, incluyendo a título enunciativo, listas de clientes, diseños, previsiones o estimaciones, procesos, informes, o documentos sujetos a protección legal que estuvieran bajo el cuidado, custodia o control de cualquier ***asegurado*** o de un ***proveedor del servicio*** del ***asegurado***.

5.49 Información personal

Información personal significa cualquier información mediante la cual una persona física pueda ser identificada de forma unívoca y fiable, incluyendo, a título de ejemplo, el nombre y apellidos, número de teléfono, número de seguridad social, datos médicos o sanitarios u otra información de salud protegida, carné de conducir o número de pasaporte, número de cuenta bancaria, número de tarjeta de crédito, número de tarjeta de débito, código de acceso o contraseña que pueda permitir el acceso a la cuenta bancaria de esa persona física o cualquier otra información personal de carácter no pública conforme a su definición en cualquier ***normativa de protección de datos personales*** aplicable a dicha persona física, en particular bajo lo previsto en el *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, y en la *Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*. ***Información personal*** no incluirá aquella información que legalmente esté a disposición del público en general por cualquier razón, incluyendo información disponible en los archivos de gobiernos nacionales, autonómicos o locales.

5.50 Instalación nuclear

Instalación nuclear significa cualquier instalación de la clase o descripción establecida por las autoridades administrativas y/o gubernamentales competentes en cada caso, a través del procedimiento legal pertinente, diseñada o adaptada para:

(a) la producción o el uso de energía atómica;

(b) la realización de cualquier proceso preparatorio o auxiliar de la producción o utilización de la energía atómica que implique o pueda provocar la emisión de radiaciones ionizantes, o

(c) el almacenamiento, el procesamiento o la eliminación de combustible nuclear o de cantidades voluminosas de otras materias radiactivas que hayan sido producidas o irradiadas en la producción o utilización de combustible nuclear.

5.51 Límite agregado de indemnización

Límite agregado de indemnización significa el importe agregado máximo indicado en las ***Condiciones Particulares*** que el ***asegurador*** pagará en relación con todas las ***reclamaciones*** o ***eventos***, en relación con ***pérdidas***, ***pérdidas propias*** y ***gastos de defensa*** cubiertos por esta póliza.

5.52 Límite de indemnización

Límite de indemnización significa el importe máximo que, una vez descontado el pago de cualquier ***franquicia*** aplicable, el ***asegurador*** pueda estar legalmente obligado a pagar bajo cada cobertura establecida en esta póliza, según se indica en las ***Condiciones Particulares***.

5.53 Mejora

Mejora significa:

(a) los inevitables avances tecnológicos estándar incluidos en cualquier ***sistema informático*** más reciente del ***asegurado***, como el aumento de la capacidad de memoria o la velocidad de procesamiento, o

(b) necesarios y razonables para instalar una versión más segura y eficiente del ***sistema informático*** afectado del ***asegurado***.

5.54 Multas y sanciones civiles

Multas y sanciones civiles significa penalizaciones económicas o monetarias de carácter exclusivamente civil o administrativo directamente impuestas a un ***asegurado*** por infracciones de cualquier disposición legal o normativa aplicable y **exclusivamente cuando:**

(a) dichas infracciones no sean conocidas por el *asegurado*, ni realizadas con carácter intencional, doloso o criminal, y

(b) dichas penalizaciones sean asegurables conforme a las leyes internas de la jurisdicción en la cual las penalizaciones fueron tramitadas o impuestas.

5.55 Normativa de protección de datos personales

Normativa de protección de datos personales significa cualquier legislación, incluyendo, pero sin limitarse al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos" (***RGPD***) y la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, promulgada para controlar el uso de ***información personal*** dentro del ***ámbito territorial*** indicado en las ***Condiciones Particulares***.

5.56 Pago de recompensas

Pago de recompensas significa cualquier cantidad ofrecida por el ***asegurado***, **con el previo consentimiento escrito del *asegurador***, por información que lleve al arresto y condena de cualquier individuo que cometa o intente cometer cualquier acto ilícito relacionado con una ***amenaza de extorsión cibernética***.

5.57 Pagos PCI-DSS

Pagos PCI-DSS significa los pagos a los que el ***asegurado*** está contractualmente obligado, tras un ***evento de privacidad*** o un ***evento de seguridad***, frente a una ***asociación de tarjetas*** o un banco a consecuencia de un incumplimiento por parte del ***asegurado*** del estándar de seguridad de datos publicado por la industria de tarjetas de pago, y que son de aplicación al ***asegurado*** en virtud del contrato.

5.58 Pagos por extorsión

Pagos por extorsión significa cualquier dinero o criptoactivos pagada por el ***asegurado***, **con el consentimiento previo por escrito del *asegurador***, a un ***tercero*** que el ***asegurado*** razonablemente considera responsable de una ***amenaza de extorsión cibernética*** a los efectos de poner fin a dicha ***amenaza de extorsión cibernética***. Para evitar cualquier duda, cualquier indemnización reembolsada por el ***asegurador*** al ***asegurado*** en concepto de ***pagos por extorsión*** se realizará en la misma moneda del ***límite de indemnización***.

5.59 Pérdida

Pérdida significa:

(a) cualquier importe, incluyendo los derivados de sentencias firmes, laudo arbitral y acuerdos extrajudiciales, incluyendo intereses devengados, que el ***asegurado*** esté legalmente obligado a pagar como consecuencia de una ***reclamación*** contra el ***asegurado***, y

(b) aquellas cantidades que el ***asegurado*** deba abonar o consignar en un ***fondo de compensación del consumidor*** o figura equivalente, exclusivamente en relación con la cobertura 8. Procedimientos regulatorios, y la cobertura 9. Procedimientos del Reglamento general de protección de datos; otorgadas bajo la sección C. Coberturas de responsabilidad frente a terceros.

Pérdida **no incluye:**

(i) *gastos de defensa*;

(ii) la pérdida, compensación, devolución de honorarios, comisiones, regalías (royalties), bonificaciones o beneficios por parte del *asegurado* o el coste de volver a prestar cualquier servicio;

(iii) el coste de cumplir con cualquier medida cautelar u otra compensación no monetaria;

(iv) la devolución, restitución o compensación de honorarios, gastos o costes pagados al *asegurado*;

(v) daños abonados en la medida en que exceden la cantidad por la cual el *asegurado* hubiera sido responsable en ausencia de dicho abono;

(vi) el coste de diseñar, actualizar, mantener o mejorar un *sistema informático*, incluyendo la corrección de cualquier deficiencia o problema;

(vii) el capital, interés u otro dinero pagado o debido como consecuencia de cualquier préstamo, arrendamiento o ampliación de crédito;

(viii) impuestos, multas, sanciones o recargos, salvo aquellos dispuestos bajo la cobertura 8. Procedimiento regulatorio, cobertura 9. Procedimiento del Reglamento general de protección de datos, y cobertura 10. Pagos PCI-DSS, o

(ix) *pérdidas propias.*

5.60 Pérdida de beneficios

Pérdida de beneficios significa:

(a) el beneficio neto, antes del impuesto de la renta y el impuesto de sociedades, que el ***asegurado*** hubiera dejado de ganar durante el *periodo de restablecimiento*, únicamente como consecuencia de una *interrupción del servicio*, y

(b) los gastos normales de explotación incurridos por el *asegurado*, pero únicamente en la medida en que dichos gastos de explotación deban continuar necesariamente durante el *periodo de restablecimiento* y hubieran sido incurridos de no haber existido una *interrupción del servicio*;

calculado según las disposiciones de la cláusula 9.6 Valoración de la pérdida de beneficios,

siempre y cuando dicha *pérdida de beneficios*, *pérdida de beneficios derivada de proveedores* sea calculada neta de cualquier ahorro atribuible al *asegurado* o créditos de servicio que el *asegurado* perciba como consecuencia de una *interrupción del servicio* y sin incluir:

(i) penalizaciones contractuales;

(ii) costes o gastos en los que se haya incurrido para corregir cualquier deficiencia o problema en relación con cualquier *sistema informático*, o para actualizar, restaurar, remplazar o mejorar un *sistema informático* a un nivel superior al existente inmediatamente antes de la *interrupción del servicio*, salvo en el caso de una *mejora*;

(iii) costes o gastos incurridos para identificar o corregir errores de *programas informáticos* o vulnerabilidades;

(iv) costes o gastos legales;

(v) pérdidas que resulten de cualquier responsabilidad frente a un *tercero*;

(vi) cualquier pérdida o daño consecuencial, o

(vii) un *incremento de gastos de operaciones.*

5.61 Pérdida de beneficios derivada de proveedores

Pérdida de beneficios derivada de proveedores significa la ***pérdida de beneficios*** (sin incluir cualquier responsabilidad frente al ***proveedor del servicio*** en sí) incurrida por el ***asegurado*** como consecuencia directa de una ***interrupción del servicio*** que afecte el ***sistema informático*** del ***proveedor del servicio***, siempre y cuando dicha *interrupción del servicio* hubiera quedado cubierta bajo esta póliza si el *proveedor del servicio* hubiese sido el *asegurado*.

5.62 Pérdidas propias

Pérdidas propias significa ***gastos de gestión de eventos***, ***pérdida de beneficios***, ***pérdida de beneficios derivada de proveedores***, ***incremento de gastos de operaciones***, ***gastos de reposición de activos digitales***, ***gastos por extorsión***, ***pagos por extorsión*** y ***pagos de recompensas***.

5.63 Periodo adicional de declaración

Periodo adicional de declaración significa el periodo inmediatamente posterior al ***periodo del seguro*** durante el cual el ***asegurado*** puede notificar al ***asegurador*** cualquier ***reclamación***, ***procedimiento regulatorio*** o ***procedimiento RGPD***, presentados o iniciados por primera vez durante dicho periodo y derivados de un ***acto incorrecto*** que haya tenido lugar en o con posterioridad a la ***fecha de retroactividad*** y antes del vencimiento del ***periodo del seguro***.

El ***periodo adicional de declaración*** está indicado como tal en las ***Condiciones Particulares.***

5.64 Periodo de espera

Periodo de espera significa el periodo de tiempo, si hubiera, transcurrido desde la fecha y la hora en que el ***sistema informático*** del ***asegurado*** sufre por primera vez una ***interrupción del servicio***, según se especifica en las ***Condiciones Particulares*** y termina una vez transcurrido el número de horas establecido en el resumen de coberturas, límites, sublímites y franquicias contratadas del apartado III. Condiciones particulares del seguro.

5.65 Periodo de restablecimiento

Periodo de restablecimiento significa el periodo comprendido entre la fecha y hora en que el ***sistema informático*** del ***asegurado*** hubiera sufrido por primera vez una ***interrupción del servicio*** hasta la fecha y hora en la que dicho ***sistema informático*** hubiera sido restaurado sustancialmente al nivel de operación existente antes de dicha ***interrupción del servicio***.

El *periodo de restablecimiento* comenzará tras el *periodo de espera* y en ningún caso podrá exceder el periodo indicado en las *Condiciones Particulares*.

5.66 Periodo del seguro

Periodo del seguro significa el periodo de tiempo especificado como tal en las ***Condiciones Particulares***.

5.67 Persona asegurada

Persona asegurada significa:

(a) cualquier persona física que es o haya sido director, socio o ***ejecutivo*** o que llegue a serlo durante el ***periodo del seguro*** de la póliza;

(b) cualquier ***empleado*** actual o anterior o cualquier persona que llegue a serlo durante el ***periodo del seguro*** de la póliza;

(c) los herederos, legatarios, albaceas o representantes legales en caso de muerte, incapacidad o insolvencia de las personas mencionadas en los puntos a) y b) anteriores;

(d) cualquier director, socio o ***ejecutivo*** retirado o jubilado, mientras continúe actuando como consultor del ***asegurado***;

(e) cualquier contratista independiente, distinto de un ***proveedor del servicio***, **pero únicamente con respecto a un *acto incorrecto* cometido dentro del alcance de los deberes que dicho contratista independiente lleva a cabo en nombre del *asegurado* bajo las instrucciones, dirección y supervisión directa de este y de conformidad con lo previsto en un contrato firmado con el *asegurado*.**

5.68 Prima

Prima significa el precio del seguro. El cálculo de la ***prima*** neta se hace teniendo en cuenta el conjunto de las coberturas contratadas en el apartado III. Condiciones particulares, incluyendo el ***límite de indemnización***, el ***límite agregado de indemnización***, la ***franquicia***, los ***periodos de espera***, condiciones de aseguramiento y demás condiciones pactadas que constan en la póliza, de forma que la variación en cualesquiera de estas condiciones determinará la correspondiente modificación de las primas. El recibo contendrá, además, los recargos y tributos que sean legalmente aplicables en cada momento

5.69 Procedimiento regulatorio

Procedimiento regulatorio significa:

(a) una investigación formal a un ***asegurado*** por parte de un organismo o autoridad administrativa o regulatoria, autoridad de control o un ente público similar en relación con un ***evento de privacidad***, o

(b) un procedimiento judicial administrativo instado contra un ***asegurado*** por un organismo administrativo o regulatorio, autoridad de control u organismo público similar debido a un ***acto incorrecto***, incluyendo cualquier posterior alegación o recurso en relación con dicho procedimiento interpuesto por el ***asegurado***, tras la recepción por parte del ***asegurado*** de cualquier reclamación, solicitud de investigación, apertura de procedimiento sancionador, notificación judicial, orden judicial, citación o documento similar.

Un ***Procedimiento regulatorio*** **no incluye un *procedimiento RGPD* o una *reclamación PCI-DSS*.**

5.70 Procedimiento RGPD

Procedimiento RGPD significa una investigación formal de un organismo administrativo o regulatorio u organismo gubernamental similar, en relación con una violación del ***RGPD*** o de otra ***normativa de protección de datos personales***, real o presunta, cometida por el ***asegurado***.

5.71 Programa informático

Programa informático significa cualquier operación o aplicación, código y programa a través del cual se recogen, transmiten, procesan, almacenan o reciben electrónicamente ***datos electrónicos***.

Bajo la definición de ***programa informático*** no se incluyen los ***datos electrónicos***.

5.72 Proveedor del servicio

Proveedor del servicio significa una entidad de la que el ***asegurado*** no es propietario, no opera ni controla y que el ***asegurado*** contrata, bajo un contrato escrito, para que le preste a este último:

(a) servicios de mantenimiento, gestión o control del ***sistema informático***, o

(b) servicios de ***hosting*** o facilitar cualquier sitio web de Internet de acceso público utilizado por el ***asegurado*** para su negocio o actividad, cuyo contenido esté bajo el control del ***asegurado***.

5.73 Publicación electrónica

Publicación electrónica significa la reproducción, publicación, diseminación, transmisión o divulgación de información incluyendo ***datos electrónicos***, archivos de imagen, archivos de audio o texto en cualquier página de Internet públicamente accesible que el ***asegurado*** utilice a los efectos de su negocio y cuyo contenido esté bajo su control, **siempre y cuando dicha información haya sido desarrollada por o para el *asegurado* o adquirida por el *asegurado* o para su uso.**

5.74 Radiación electromagnética

Radiación electromagnética significa cualquier sucesión de ondas electromagnéticas.

5.75 Reactor nuclear

Reactor nuclear significa cualquier planta, incluida cualquier maquinaria, equipo o aparato, fijada a la tierra o no, diseñada o adaptada para la producción de energía atómica mediante un proceso de fisión en el que se pueda mantener una reacción en cadena controlada sin una fuente adicional de neutrones.

5.76 Reclamación

Reclamación significa:

(a) una reclamación escrita contra cualquier ***asegurado*** imputándole cualquier presunta responsabilidad por daños y perjuicios.

(b) cualquier procedimiento judicial, administrativo o arbitral contra un ***asegurado***, o contra el ***asegurador*** en ejercicio de la acción directa, que pueda dar lugar a una resolución o sentencia en la que se pueda declarar una responsabilidad civil por daños o perjuicios, o

(c) únicamente con respecto a la cobertura 8. Procedimiento regulatorio, la cobertura 9. Procedimiento del Reglamento general de protección de datos y la cobertura 10. Pagos PCI-DSS, un ***procedimiento regulatorio***, un ***procedimiento RGPD*** o una ***reclamación PCI-DSS***.

5.77 Reclamación PCI-DSS

Reclamación PCI-DSS significa una demanda o reclamación escrita presentada bien por el Consejo de estándares de seguridad de la industria de tarjetas de pago, la ***Asociación de tarjetas***, el banco emisor o el banco adquiriente alegando el incumplimiento o la violación de:

(a) el Estándar de seguridad de la industria de tarjetas de pago, o

(b) un acuerdo de servicios comerciales en relación con el Estándar de seguridad de la industria de tarjetas de pago,

tras un ***evento de privacidad*** o un ***evento de seguridad***.

5.78 RGPD

RGPD significa el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos (Reglamento general de protección de datos).

5.79 Seguridad de la red

Seguridad de la red significa el empleo de equipos informáticos, ***programas informáticos***, *firmware* (*software* incluido en un dispositivo de *hardware* que proporciona instrucciones sobre cómo dicho dispositivo debe operar), así como las políticas y procedimientos de seguridad escritos por el ***asegurado*** o en su nombre para protegerse frente a un ***acceso no autorizado***, incluyendo el uso de un ***sistema informático*** en un ***ataque de denegación de servicio***.

5.80 Secretos comerciales

Secretos comerciales significa cualquier información que genera un valor económico independiente, real o potencial, por el simple hecho de no ser conocida públicamente, sin necesidad de comprobación a través de métodos adecuados por otras personas que puedan obtener una ventaja económica por su revelación o uso.

5.81 Servicio de respuesta a incidentes

Servicio de respuesta a incidentes significa los proveedores indicados como tal en las ***Condiciones Particulares***.

5.82 Servicios profesionales

Servicios profesionales significa los actos o servicios que requieren conocimientos especializados, habilidades o criterio profesional que el ***asegurado*** presta a otros en virtud de un contrato o acuerdo escrito; a cambio de la correspondiente remuneración, incluidos, pero no limitados al análisis financiero, la valoración de valores y previsiones, etc.

5.83 Sistema informático

Sistema informático significa equipos informáticos y ***programas informáticos***, así como los ***datos electrónicos*** almacenados en los mismos, incluidos los dispositivos asociados de entrada y salida, los dispositivos de almacenamiento de datos, el equipo de red, componentes, el *firmware*; así como los equipos de copias de seguridad, incluidos los sistemas disponibles a través de la Internet, las intranets, las extranets o las redes privadas virtuales.

Exclusivamente en relación con el ***sistema informático*** del ***asegurado***, se incluye el equipo informático y los ***programas informáticos***, así como los ***datos electrónicos*** almacenados en los mismos, que:

(a) el ***asegurado*** arrienda, posee u opera;

(b) el ***asegurado*** arrienda o posee, pero que son operados por un tercero en virtud de un contrato escrito con el ***asegurado***, o

(c) sean propiedad de los ***empleados*** del ***asegurado*** y operados por ellos en nombre del ***asegurado*** con el propósito de obtener el acceso remoto al ***sistema informático*** del ***asegurado***, o bien operados de otra manera de acuerdo con los términos de la política de "Traer Tu Propio Dispositivo" *(Bring Your Own Device)* del ***asegurado***,

para prestar servicios al ***asegurado***.

Sistema informático también significa cualesquiera de los anteriores que forman parte de un Sistema de control industrial.

5.84 Socio comercial

Socio comercial significa cualquier persona que haga negocios con el ***asegurado*** bajo los términos de un acuerdo de colaboración o asociación, con independencia de que tenga carácter expreso o implícito, según la legislación aplicable.

5.85 Subcontratista

Subcontratista significa cualquier consultor o subcontratista independiente, que no sea un ***empleado***, que presta servicios al ***asegurado*** conforme a un contrato por escrito.

5.86 Tercero

Tercero significa cualquier persona física o jurídica, entidad, individuo, sociedad, organización o corporación que no sea el ***asegurado*** ni cualquier ***entidad relacionada*** o cualquier otra persona física o jurídica que tenga un interés financiero o ejecutivo en las operaciones del ***asegurado***.

5.87 Tomador del seguro

Tomador del seguro significa la persona jurídica designada como tal en las ***Condiciones Particulares*** que, juntamente con el ***asegurador***, suscribe esta póliza, y a la que corresponden las obligaciones que de la misma deriven.

5.88 Valores

Valores significa cualquier bono, obligación, instrumento, acción, participación u otra acción o valor de deuda, e incluirá cualquier certificado de interés o participación en, recibo de, garantía de, u otro derecho de suscripción o de compra, certificado de derecho a voto en relación con, u otro interés en cualesquiera de los anteriores que representen dinero o bienes. **El concepto de *valores* no incluye *dinero* o *bienes*.**

VI. Exclusiones

Esta póliza no cubre ninguna *reclamación*, *pérdida*, *pérdida propia*, *gastos de defensa*, daño, daño consecuencial, responsabilidad legal, honorarios, costes, desembolsos, indemnizaciones u otros gastos de cualquier naturaleza, con independencia de que consten o no específicamente definidos en ella, y que, directa o indirectamente, sean consecuencia de, o atribuibles a, estén relacionados con, o basados en, o se deriven de:

6.1 Daños corporales y daños materiales

(a) **Fallecimiento, daños corporales, lesión mental, enfermedad, patología, angustia mental o un estado de shock sufrido por cualquier persona,** salvo que se trate de una angustia emocional a consecuencia de un ***evento de privacidad***, o

(b) **pérdida física, destrucción, deterioro o daño material a los *bienes*, incluida la pérdida de uso de los mismos.**

6.2 Reclamaciones por entidades relacionadas

Una *reclamación* presentada o una pérdida reclamada por cualquier *asegurado* o cualquier *entidad relacionada*.

No obstante, esta exclusión no será aplicable a aquella ***reclamación*** presentada por el ***asegurado*** en su condición de:

(i) ***cliente***, o

(ii) ***empleado***, en relación con un ***evento de privacidad*** relacionado con la divulgación no autorizada de la ***información personal*** de dicho ***empleado***.

6.3 Responsabilidad contractual

Cualquier garantía expresa, aval expreso u obligación contractual (salvo en relación con ***pagos PCI-DSS*** en el caso de que aplique esta cobertura) **en la medida en que dé lugar a una *reclamación* de la cual el *asegurado* no hubiera sido responsable de no existir la garantía expresa, aval expreso u obligación contractual.**

6.4 Actos delictivos o maliciosos

(a) **Cualquier acto u omisión doloso, delictivo, deshonesto, fraudulento o malicioso cometido o consentidos por cualquier *asegurado*;**

(b) **cualquier infracción de la ley intencional o deliberada cometida o consentida por cualquier *asegurado*, o**

(c) **cualquier obtención de ganancia, remuneración, ventaja, ya sea de carácter económico o no, por el *asegurado* a la que el *asegurado* legalmente no tenía derecho,**

no obstante, en los casos anteriores:

(i) el ***asegurador*** abonará los ***gastos de defensa*** y defenderá dicha ***reclamación*** hasta que exista una sentencia, laudo arbitral vinculante o determinación de hechos contra dicho ***asegurado*** o una admisión de responsabilidad bajo juramento o declaración de conformidad por parte de dicho ***asegurado*** que establezca la existencia del ***acto incorrecto*** penal, deshonesto, fraudulento o malicioso, de naturaleza intencional, la infracción de la ley o la obtención de una ganancia, remuneración o ventaja. **En estos casos, el *asegurado* reembolsará al *asegurador* cualquier *gasto de defensa* pagado por el *asegurador* en nombre de dicho *asegurado* como consecuencia de dicha *reclamación*, y**

(ii) ningún ***acto incorrecto*** cometido por o en conocimiento de una ***persona asegurada*** será imputado a cualquier otro ***asegurado***, excepto si el ***acto incorrecto*** fuese del conocimiento del consejero delegado, director financiero, director de recursos humanos, director de asesoría jurídica o gerente de riesgos del ***asegurado***, o cualquier otra ***persona asegurada*** en un puesto funcional equivalente.

6.5 Criptoactivos

Cualquier pérdida de, robo de, pérdida de acceso a, o caída de valor de cualquier criptoactivo incluido, pero no limitado a, cualquier criptodivisa y criptoactivos de naturaleza distinta a las divisas, como, por ejemplo, los tokens.

6.6 Campo electromagnético, radiación electromagnética o electromagnetismo

Cualquier *campo electromagnético*, *radiación electromagnética* o *electromagnetismo*.

6.7 Comunicaciones electrónicas

(a) **La Ley de protección al consumidor telefónico (EE. UU.) (*TCPA*);**

(b) **la Ley CAN-SPAM de 2003 (EE. UU.);**

(c) la Ley Legislativa Federal anti-correos basura (Canadá): una ley para promover la eficiencia y la adaptabilidad de la economía canadiense mediante la reglamentación de ciertas actividades que desalienten la dependencia de los medios electrónicos para llevar a cabo actividades comerciales, y para enmendar la Ley de la Comisión Canadiense de radiotelevisión y telecomunicaciones, la Ley de competencia, la Ley de protección de la información personal y los documentos electrónicos y la Ley de telecomunicaciones; e incluyendo, todas las normas y reglamentos promulgados en virtud de la misma, cualquier enmienda o adición a la misma y cualquier aspecto de otra ley, derecho o estatuto federal, provincial, territorial o municipal que enmiende;

(d) las directrices de la Comisión de Radiotelevisión y Telecomunicaciones de Canadá (CRTC)

(e) la lista "No llamar" de la Asociación Canadiense de Comercialización;

(f) la Fair Credit Reporting Act (EE. UU) (FACTA) y la Fair and Accurate Credit Transactions Act (EE. UU.) (FACTA);

(g) cualquier ley, ordenanza, reglamento o directriz federal, estatal, provincial, territorial o local distinta de las enumeradas en los puntos (a) a (f) anteriores, o cualquier otra responsabilidad jurídica, de derecho común o de otro tipo, que se refiera, prohíba o limite la impresión, la difusión, la eliminación, la vigilancia, la recopilación, el registro, el uso, el envío, la transmisión, la comunicación o la distribución de material o información, o

(h) cualquier enmienda, adición o sustitución de cualquier ley, ordenanza, reglamento, norma o directiva que figure en los puntos (a) a (g) anteriores,

Esta exclusión no será aplicable si la distribución no solicitada de faxes, correos electrónicos u otros tipos de comunicaciones dirigidos a múltiples *clientes* actuales o potenciales por parte del ***asegurado*** o cualquier otro ***tercero*** es causada por un ***evento de seguridad***.

6.8 Responsabilidad laboral

(a) Fallecimiento, lesiones corporales, lesiones mentales, enfermedad, patología, angustia mental o shock de cualquier *socio comercial*, director, *ejecutivo*, mandante o *empleado* durante el transcurso de su relación laboral con el *asegurado*;

(b) cualquier obligación que tiene el *asegurado* como empleador o empleador potencial con cualquier director o *empleado* o solicitante de empleo, o

(c) cualquier condición asumida expresa o implícita de un acuerdo de asociación, colaboración mercantil, joint venture o similares, o de un acuerdo de membresía,

si bien esta exclusión no se aplicará a ninguna ***reclamación*** por un ***empleado*** por un ***evento de privacidad*** relacionada con la divulgación no autorizada de la ***información personal*** de dicho ***empleado***.

6.9 Incautación gubernamental

Cualquier incautación, confiscación, expropiación, nacionalización o destrucción de un *sistema informático* por orden de cualquier autoridad administrativa competente, si bien esta exclusión no se aplicará a un *procedimiento regulatorio* o a un *procedimiento RGPD* tras un *evento de privacidad*.

6.10 Fallo de infraestructura

Cualquier fallo eléctrico o mecánico, interrupción o corte de suministros, incluyendo cualquier interrupción o sobrecarga del suministro eléctrico, apagón, corte, cortocircuito, sobrevoltaje, sobretensión o fluctuación del suministro, o interrupción de los servicios de gas, agua, teléfono, cable, satélite, telecomunicaciones, Internet, o cualquier componente de los mismos, incluyendo hardware o software o cualquier otra infraestructura.

No obstante, esta exclusión no se aplicará a ningún fallo, interrupción o corte de teléfono, cable o telecomunicaciones bajo el control directo del ***asegurado*** que constituya un ***fallo del sistema*** o que surja de un ***acto incorrecto*** o un ***ataque de denegación de servicio*** contra los ***sistemas informáticos*** del ***asegurado***.

6.11 Insolvencia

La insolvencia, la liquidación, el embargo de cualquier activo, o la declaración de concurso del *asegurado* o de cualquier *proveedor del servicio* o *subcontratista* del *asegurado*.

6.12 Riesgos nucleares

(a) Radiaciones ionizantes o la contaminación por radiactividad de cualquier combustible nuclear o de cualquier desecho nuclear o de la combustión de combustible nuclear;

(b) las propiedades radiactivas, tóxicas, explosivas u otras propiedades peligrosas o contaminantes de cualquier *instalación nuclear*, reactor nuclear u otro conjunto nuclear o componente nuclear del mismo, o

(c) cualquier arma que emplee la fisión y/o fusión atómica o nuclear u otra reacción similar o fuerza o materia radiactiva.

6.13 Patentes

Cualquier apropiación indebida, infracción o violación, real o supuesta, de cualquier patente o *secretos comerciales*, la pérdida de derechos de un *tercero* para garantizar el registro previo de patentes o su concesión, el incumplimiento de cualquier licencia sobre patentes o la apropiación indebida de *secretos comerciales*,

si bien esta exclusión no será aplicable en la medida en que cualquier *reclamación* tenga su origen en una divulgación involuntaria de *secretos comerciales* derivada de un *evento de privacidad*.

6.14 Eventos físicos y riesgos naturales

Cualquier incendio, humo, explosión, relámpago, viento, inundación, terremoto, erupción volcánica, tormenta, hundimiento, maremoto, deslizamiento de tierra, disturbio, granizo, incendio subterráneo o un acto de fuerza mayor o cualquier otro suceso material, sea cual fuere la causa.

6.15 Contaminación

(a) La descarga, liberación, escape, filtración, migración o eliminación, real, presunta o en grado de amenaza de *contaminantes* en o sobre bienes muebles o inmuebles, en el agua o la atmósfera, o

(b) cualquier orden o solicitud que reciba cualquier *asegurado* para que realice pruebas, controle, monitorice, limpie, elimine, contenga, trate, desintoxique o neutralice los *contaminantes*, o cualquier decisión voluntaria del *asegurado* de hacerlo;

(c) el coste de la retirada, limpieza o neutralización de sustancias *contaminantes*, filtración o derrame.

6.16 Reclamaciones y circunstancias anteriores

(a) Cualquier acto, error u omisión o *acto incorrecto* o *circunstancia*:

  (i) que haya ocurrido o sido descubierto con anterioridad a la fecha de inicio del *periodo del seguro* o de la *fecha de retroactividad* recogida en las *Condiciones Particulares*, y que el *grupo de control* conocía o debería razonablemente haber conocido antes de la entrada en vigor de esta póliza, y que puedan dar lugar a una *reclamación* contra el *asegurado*;

  (ii) que haya sido notificado por el *asegurado* a cualquier otra póliza de seguro con carácter previo a la entrada en vigor de esta póliza; o

  (iii) que haya sido comunicado (o debería haber sido comunicado) en el cuestionario-declaración del riesgo y demás información facilitada por el *asegurado* al *asegurador* para la emisión y contratación de esta póliza;

(b) cualquier *reclamación* derivada de los mismos *actos incorrectos interrelacionados* o los mismos *eventos interrelacionados* a la presentada contra cualquier *asegurado* con carácter previo a la entrada en vigor de esta póliza; o

(c) basado en, derivado de, o atribuible a, directa o indirectamente, cualquier fallo en la *seguridad de la red* del *asegurado* o de un incidente susceptible de causar un *evento* del que cualquier persona del *grupo de control* era conocedora o debería haber sido conocedora antes de la ocurrencia de un *evento de privacidad*, un *evento de seguridad* o un *fallo del sistema*.

6.17 Productos y servicios profesionales

Cualquier real o presunto:

(a) fallo de los productos del *asegurado*, incluyendo los *programas informáticos*, para realizar la función o servir el propósito previsto por cualquier *tercero* o cualquier *asegurado*, o

(b) la prestación negligente o la falta negligente de prestación de *servicios profesionales* por parte del *asegurado*.

Sin embargo, lo previsto en esta exclusión no se aplica a cualquier *acto incorrecto de privacidad*.

6.18 Infracción de la Racketeer Influenced and Corrupt Organization Act (RICO)

Cualquier incumplimiento, real o presunto, de cualquier responsabilidad, obligación o deber impuesto por la Racketeer Influenced and Corrupt Organization Act (Ley de chantaje civil, influencia y organizaciones corruptas) de EE. UU. y sus posteriores modificaciones, y disposiciones normativas o de otro orden de similar naturaleza, que sean aplicables tanto en dicho país como en otros territorios o jurisdicciones.

6.19 Infracción de normativa de planes de pensiones, publicidad, competencia, consumo y mercado de valores

Cualquier real o presunto:

(a) violación por parte del *asegurado* de la Employee Retirement Income Security Act de 1974 (EE. UU.) (ERISA), la Canadian Pension Benefits Standards Act, la Ontario Pension Benefits Act, 1990, o cualquier otra ley federal, estatal, provincial, territorial o municipal similar;

(b) violación por parte del *asegurado* de la Securities Act de 1933 (EE. UU.), la Securities Exchange Act de 1934 (EE. UU.), la Investment Company Act de 1940 (EE. UU.), la Investment Advisors Act (EE. UU.), la Canadian Securities Act (Ontario), o cualquier otra ley de valores extranjera, federal, estatal, provincial, territorial o local;

(c) violación por parte del *asegurado* de cualquier norma o reglamento promulgado en virtud de los estatutos enumerados en los párrafos (a) y (b) anteriores, o de cualquier otra ley extranjera, federal, estatal, provincial, territorial o de derecho consuetudinario similar a los mismos;

(d) prácticas comerciales engañosas o desleales, el fraude al consumidor, la publicidad falsa o engañosa, o la tergiversación;

(e) competencia desleal, la fijación de precios, la restricción del comercio, la monopolización, el fraude al consumidor u otra violación de la Federal Trade Commission Act (EE.UU.), la Sherman Anti-Trust Act (EE.UU.), la Clayton Act (EE.UU.), la Competition Act (Canadá), o cualquier otra ley o reglamento federal, estatal, provincial, territorial, local o de derecho consuetudinario que se refiera a la defensa de la competencia, el monopolio, la fijación de precios, la discriminación de precios, la fijación de precios predatorios o la restricción del comercio, o que proteja la competencia de alguna otra manera;

(f) cualquier enmienda, adición o sustitución de cualquier ley, ordenanza, reglamento, norma o directiva que figure en los puntos (a) a (e) anteriores, o

(g) cualquier ley o derecho consuetudinario equivalente en cualquier otro territorio o jurisdicción fuera de EE. UU. de América o Canadá.

Esta exclusión no será de aplicación a:

i) un *procedimiento regulatorio* o un *procedimiento RGPD* que pudiera constituir una infracción de normativas que prohíben prácticas comerciales indebidas o desleales, incluido un *fondo de compensación del consumidor* establecido para resolver tal *procedimiento regulatorio* o *procedimiento RGPD*, o

ii) una *reclamación* o *gastos de gestión de eventos* que habrían estado por otra parte cubiertos.

6.20 Pérdida de valor monetario

El valor monetario de cualquier transacción o cambio de valor de cualquier cuenta, incluyendo, pero no limitado a transferencias electrónicas, pérdidas en una operación bursátil o responsabilidad derivada de una operación bursátil, pérdidas comerciales, deudas comerciales, premios, puntos, cupones, descuentos de precios o cualquier otra propiedad intangible.

6.21 Programas informáticos sin licencia

El uso consciente por parte de cualquier *asegurado* de programas ilegales o sin licencia que infrinjan los derechos de autor o que de alguna otra manera violen las leyes de protección de *programas informáticos*.

6.22 Guerra o conflicto civil

(a) guerra, ya sea declarada oficialmente o no, o guerra civil,
(b) terrorismo o acción de una fuerza militar, incluida la acción para obstaculizar o defenderse contra un ataque real o esperado, por parte de cualquier gobierno, soberano u otra autoridad que utilice personal militar u otros agentes; o
(c) insurrección, rebelión, revolución, motín, usurpación del poder o acción de la autoridad gubernamental para obstaculizar o defenderse de cualquiera de ellos.

Esta exclusión no será de aplicación al *ciberterrorismo*.

b. Blanqueo de capitales

Cualquier acto real o supuesto de blanqueo de capitales o cualquier acto real o supuesto que suponga el quebrantamiento de cualquier normativa, disposición, norma o reglamento creados por cualquier organismo regulatorio o autoridad al respecto, en particular de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, así como de cualquier otra legislación aplicable y sus posteriores modificaciones.

c. Pérdida, robo y transferencias

a) La pérdida, robo de *dinero* o *valores* de un *asegurado*, o

b) cualquier transferencia, robo o pérdida de *dinero* o *valores*, desde o a las cuentas del *asegurado*, o cuentas de otras personas que se encuentren bajo el cuidado, custodia y control del *asegurado*.

d. Responsabilidad de administradores y directivos

Cualquier responsabilidad en la que incurra un *asegurado* o cualquier *ejecutivo* en el desempeño de su cargo de administrador o directivo del *asegurado*, o como miembro de la comisión de control de un plan de pensiones o cualquier otro plan de beneficios de empleados.

VII. Disposiciones especiales

7.1 Límite de indemnización

El *límite de indemnización* fijado en las *Condiciones Particulares* constituye el importe máximo que el *asegurador* estará obligado a pagar bajo todas las coberturas contempladas bajo esta póliza.

(a) Todas las *reclamaciones* y *circunstancias* derivadas del mismo *acto incorrecto* y todos los *actos incorrectos interrelacionados* serán considerados una única *reclamación*, y dicha *reclamación* será considerada como presentada por primera vez en la fecha en la que la primera *reclamación* sea presentada, o bien cuando la *circunstancia* sea notificada por primera vez al *asegurador*.

(b) Todas las *pérdidas propias* derivadas del mismo *evento* y todos los *eventos interrelacionados*, serán consideradas como una única *pérdida propia*, y se entenderá que dicha *pérdida propia* ha sido descubierta por primera vez en la fecha en la que fue descubierto el primer *evento*.

(c) En los casos anteriores, y por considerarse como única *reclamación* o única *pérdida propia* cubierta bajo esta póliza, al *asegurado* solo le será aplicable una *franquicia*.

(d) Los *límites de indemnización* indicados en el apartado III. Condiciones Particulares son los importes máximos que el *asegurador* está obligado a pagar en relación con cada cobertura de la póliza, salvo cuando sea aplicable algún sublímite según se especifica en dicho apartado III. Dichos límites y sublímites de indemnización forman parte de y no operan en exceso del *límite agregado de indemnización*.

(e) El *límite agregado de indemnización* indicado en el apartado III. Condiciones Particulares constituye el importe máximo que el *asegurador* estará obligado a pagar bajo todas las coberturas contempladas bajo esta póliza y, salvo que se indique lo contrario, cualquier extensión o endoso.

(f) En el caso de que cualquier única *reclamación* o única *pérdida propia* estuviera cubierta bajo más de una cobertura:

(i) solo se aplicará una *franquicia* a dicha única *reclamación* o única *pérdida propia*, en concreto la *franquicia* más alta de las coberturas aplicables, y

(ii) sujeto a los apartados (d) y (e), solo se aplicará un *límite de indemnización* a dicha única *reclamación* o única *pérdida propia* y aplicará el *límite de indemnización*, siendo el más alto de las coberturas aplicables.

(g) En caso de un *evento ransomware*, la responsabilidad del *asegurador* no excederá el *límite de indemnización* por un *evento ransomware* indicado en el apartado III. Condiciones Particulares para las *reclamaciones* y *pérdidas* de cada una de las coberturas que se activen y que surjan de, en conexión con, atribuibles a, resultantes de, ya sea directa o indirectamente de un *evento ransomware*.

El *límite de indemnización* por un *evento ransomware* forma parte del *límite agregado de indemnización* indicado en el apartado III. Condiciones Particulares y no en adición a éste.

7.2 Periodo adicional de declaración

(a) En el supuesto de que esta póliza no sea objeto de renovación o sea reemplaza por otra distinta, el *tomador del seguro* tendrá derecho a un *periodo adicional de declaración*:

(i) automático y por un periodo de treinta (30) días sin prima adicional alguna, o

(ii) para el periodo de tiempo indicado en las *Condiciones Particulares*, siempre que el *tomador del seguro* hubiera solicitado por escrito la aplicación de dicho *periodo adicional de declaración* dentro de los treinta (30) días siguientes al vencimiento del *periodo del seguro* y hubiera abonado la correspondiente prima adicional aplicable.

(b) El *periodo adicional de declaración* solo se aplicará en relación con cualquier *acto incorrecto* cometido en o después de la *fecha de retroactividad* indicada en las *Condiciones Particulares* y antes de la fecha de vencimiento del *periodo del seguro*.

Asimismo, se hace constar que:

(i) cualquier *reclamación* presentada por primera vez durante el *periodo adicional de declaración* será considerada como presentada durante el *periodo del seguro*;

(ii) el *periodo adicional de declaración* no sustituye, reemplaza ni aumenta el *límite de indemnización*, ni extiende el *periodo del seguro* previsto en la póliza;

(iii) en el supuesto de un *cambio de control*, el *periodo adicional de declaración* no será aplicable y quedará automáticamente sin efecto, y

(iv) la prima adicional para cualquier *periodo adicional de declaración* se considerará completamente devengada a la fecha de inicio del *periodo adicional de declaración*.

(c) **El *periodo adicional de declaración* terminará inmediatamente en la fecha en que se produzca cualesquiera de las siguientes circunstancias:**

(i) **la renovación de esta póliza por el *asegurador*; o**

(ii) **la contratación de cualquier contrato de seguro de ciberriesgos emitido por otro asegurador que reemplace o renueve efectivamente la cobertura otorgada por esta póliza, ya sea en su totalidad o en parte y aunque la cobertura otorgada bajo la nueva póliza fuera más restrictiva.**

7.3 Defensa y fianzas

(a) Defensa

En cualquier procedimiento judicial que se derive de una ***reclamación*** amparada por la póliza, el ***asegurador*** asumirá, a costa suya, la dirección jurídica frente a la ***reclamación***, designando los letrados y procuradores que defenderán y representarán al ***asegurado*** en las actuaciones judiciales que se le siguiesen en la ***reclamación*** de responsabilidades civiles o penales cubiertas por esta póliza, y eso aunque dichas ***reclamaciones*** fuesen infundadas.

El ***asegurado*** deberá prestar la colaboración necesaria a dicha defensa, comprometiéndose a otorgar los poderes y la asistencia personal que fuesen necesarios, y a facilitar cuanta información y documentación se le requiera por parte del ***asegurador***.

Sea cual sea la resolución o resultado del procedimiento judicial, el ***asegurador*** se reserva la decisión de ejercer los recursos legales que procedan contra dicha resolución o conformarse con la misma.

Si el ***asegurador*** estima improcedente el recurso, lo comunicará al ***asegurado***, quedando este en libertad para interponerlo por su exclusiva cuenta y aquel obligado a reembolsarle los gastos judiciales y los de abogado y procurador, en caso de que dicho recurso prosperase. La comunicación de la improcedencia del recurso nunca podrá causar indefensión al ***asegurado***.

Si se produjese algún conflicto de intereses entre el ***asegurado*** y el ***asegurador***, motivado por tener que sustentar este en la ***reclamación*** intereses contrarios a la defensa del ***asegurado***, el ***asegurador*** lo pondrá en conocimiento del ***asegurado***, sin perjuicio de realizar aquellas diligencias que, por su carácter urgente, sean necesarias para la defensa. En este caso, el ***asegurado*** podrá optar entre el mantenimiento de la dirección jurídica por el ***asegurador*** o confiar su propia defensa a otra persona.

El *asegurado* no podrá incurrir en ningún honorario, coste, cargo o gasto, ni establecer ningún acuerdo, defensa, ajuste, liquidación o asumir responsabilidades u obligación alguna en una *reclamación* hecha o presentada contra cualquier *asegurado* sin el consentimiento previo por escrito del *asegurador*, el cual no será denegado ni retrasado injustificadamente. En caso contrario, el ***asegurador*** no será responsable de efectuar pago alguno.

El ***asegurador*** podrá ejercer cualquier investigación necesaria con respecto a una ***reclamación*** y establecer acuerdos o ajustes que considere convenientes con el consentimiento del ***asegurado***, el cual no será denegado ni retrasado injustificadamente. **La obligación y el derecho de defensa del *asegurador* terminarán en el momento en que el *límite de indemnización* que aplique se agote debido a los pagos realizados.**

Si el ***asegurador*** recomienda establecer un acuerdo o ajuste y el ***asegurado*** rehúsa dar su consentimiento a dicho acuerdo, sujeto al límite o sublímite de la garantía afectada, el ***asegurador*** será responsable solamente hasta el importe por el que el ***asegurador*** hubiera aceptado el acuerdo junto con los ***gastos de defensa*** incurridos hasta la fecha en la que el ***asegurado*** rehusó dar su consentimiento a dicho acuerdo.

Esta cobertura no se aplicará cuando el importe de la *reclamación* que se formule contra el *tomador del seguro* o el *asegurado* sea inferior al importe de la *franquicia* establecida para la garantía afectada.

(b) Prestación de fianzas judiciales

El ***asegurador*** garantiza igualmente los gastos incurridos por el ***asegurado*** para la constitución y mantenimiento de cualquier fianza judicial o aval que se requiera como parte de un procedimiento judicial derivado de una ***reclamación*** interpuesta contra el ***asegurado***. **Estos gastos no incluirán ni implicarán para el *asegurador* obligación alguna de obtener o tramitar la fianza o el aval ni de otorgar garantía alguna para su expedición.**

Dicho afianzamiento tendrá la consideración de pago a cuenta de la eventual indemnización y tendrá como límite máximo el límite máximo de indemnización para la cobertura de responsabilidad civil afectada. **No se incluye en esta cobertura la prestación de fianzas para el pago de sanciones personales, como multas o costas.**

En caso de pérdida de la fianza depositada para responder de la comparecencia del ***asegurado***, debido a su incomparecencia, el ***asegurador*** tendrá derecho a exigir al ***asegurado*** el reembolso de los gastos incurridos por el ***asegurado*** para la constitución y mantenimiento de cualquier fianza judicial o aval.

Los *gastos de defensa* no se aplicarán cuando el importe de la *reclamación* que se formule contra el *asegurado* sea inferior al importe de la *franquicia* establecida para la cobertura afectada.

7.4 Reembolso de pagos

El *tomador del seguro* o el *asegurado* reembolsarán íntegramente al *asegurador* cualquier pago realizado por el *asegurador* que se determine que no está sujeto a cobertura bajo esta póliza.

7.5 Cambio de control

En caso de un *cambio de control* durante el *periodo del seguro*, **la cobertura otorgada bajo esta póliza solo se aplicará en relación con cualquier *acto incorrecto* o cualquier *evento* que ocurra antes de la fecha efectiva de dicho *cambio de control*.**

El *asegurado* deberá notificar por escrito el *cambio de control* al *asegurador* tan pronto como sea razonablemente posible.

7.6 Adquisición y constitución de nuevas filiales

Si durante el *periodo del seguro* el *asegurado* adquiere o crea una *empresa filial*, esta póliza será automáticamente aplicable a dicha *empresa filial* y a las *personas aseguradas* de esta, desde la fecha de dicha adquisición o creación,

siempre y cuando:

(a) **dicha *empresa filial* esté domiciliada en el Espacio Económico Europeo, incluyendo el Reino Unido;**

(b) **no tenga una facturación que exceda el 15% de la facturación total consolidada del *tomador del seguro*, según lo indicado en los últimos estados financieros publicados;**

(c) **la *empresa filial* no haya sufrido, en los 3 años anteriores, reclamaciones o pérdidas similares a las que son objeto de cobertura por esta póliza (hayan estado aseguradas o no), que fuesen mayores que el importe de la *franquicia*, ni haya tenido conocimiento de *circunstancias* que pudieran dar lugar a una *pérdida* o *reclamación*; y**

(d) **el *asegurado* haya notificado por escrito al *asegurador* la adquisición o la creación de dicha *empresa filial* dentro de los 90 días siguientes a su acaecimiento.**

Con respecto a las *empresas filiales* recientemente adquiridas, que no cumplan las condiciones descritas en los párrafos (a) a (c) anteriores, el *asegurador* podrá, a su entera discreción, extender la cobertura a dicha *empresa filial* y a cualquier *persona asegurada* de la misma, si el *tomador del seguro*:

(i) notifica por escrito la adquisición de dicha empresa al *asegurador*;

(ii) proporciona al *asegurador* toda la información de suscripción que el *asegurador* pueda solicitar, y

(iii) acepta cualquier prima adicional o modificación de las disposiciones de esta póliza que requiera el *asegurador* en relación con dicha *empresa filial*.

Cualquier cobertura proporcionada para cualquier *empresa filial* creada o adquirida durante el *periodo del seguro* y sus *personas aseguradas*, **solo se aplicará a *actos incorrectos*, *evento* o *reclamaciones* que ocurran después de la adquisición o creación de dicha *empresa filial* por parte del *asegurado*, y estará condicionada a que el *tomador del seguro* pague, cuando corresponda y si es aplicable, cualquier prima adicional requerida por el *asegurador* para dicha *empresa filial*.**

7.7 Cese de empresas filiales

Si durante el *periodo del seguro* una *empresa filial* deja de ser una *empresa filial*, no se proporcionará cobertura alguna con respecto a dicha *empresa filial* y sus *personas aseguradas* por ningún *acto incorrecto*, *evento* o *reclamación* que involucre a dicha empresa o personas o por cualquier otra *pérdida* o *reclamación* después de la fecha en que dicha empresa dejó de ser una *empresa filial*.

7.8 Modificaciones y cesiones

Ningún cambio o modificación de esta póliza tendrá validez a menos que haya sido solicitado expresamente por el *asegurado* y cuente con el previo consentimiento por escrito y en forma de endoso del *asegurador*, que pasará a formar parte de esta póliza.

7.9 Reclamaciones y franquicias

Esta póliza se contrata con las *franquicias* y *periodos de espera* especificados en las *Condiciones Particulares*. En consecuencia, el *asegurador* será responsable de las cantidades a las que tenga derecho el *asegurado* únicamente cuando las *pérdidas*, *gastos de defensa*, *pérdidas propias* o *reclamaciones* excedan el importe de la *franquicia* o del *periodo de espera*. El *asegurado* asume por su propia cuenta las *pérdidas*, *gastos de defensa*, *pérdidas propias* o *reclamaciones* inferiores a la suma fijada como *franquicia* o las horas establecidas como *periodos de espera*, los cuales no forman parte del *límite de indemnización* y no son asegurables.

No obstante, el *asegurador* podrá asumir parte o la totalidad de la *franquicia* a los efectos de alcanzar un acuerdo en cualquier cobertura contratada bajo esta póliza y poniéndolo en conocimiento, estando el *asegurado* obligado a reembolsar sin demora la *franquicia* que hubiera sido asumida por el *asegurador*.

Cuando existan *eventos interrelacionados*, tendrán la consideración de un solo *evento*, y se considerará que ha ocurrido por primera vez en el momento en que tuviera lugar el primer *evento*. En el caso de que algún *evento* active más de una cobertura, se aplicará la mayor de las ***franquicias*** de entre dichas coberturas y el ***límite de indemnización*** o sublímite asociado a dicha ***franquicia*** que fuere aplicable.

Cuando existan varias ***reclamaciones*** procedentes de un mismo ***acto incorrecto*** o ***actos incorrectos interrelacionados***, tendrán la consideración de una única ***reclamación***, independientemente del número de ***reclamaciones*** que hayan sido presentadas, y dicha ***reclamación*** será atribuida solamente al ***periodo del seguro*** o ***periodo adicional de declaración***, si fuera aplicable, durante el cual la primera ***reclamación*** haya sido presentada por primera vez, y estarán sujetas a una sola ***franquicia***, al ***límite de indemnización*** aplicable por ***reclamación*** y al ***límite agregado de indemnización*** a cargo del ***asegurador***.

7.10 Confidencialidad

La existencia y los términos de esta póliza tendrán carácter confidencial entre el ***asegurado*** y el ***asegurador***, y no serán objeto de publicación, revelación, difusión o comunicación en forma alguna, excepto en los casos en que:

(a) la ley requiera que sean revelados o mostrados en los estados financieros o en los informes anuales de los pagos de las primas que realizara el ***tomador del seguro***, o bien

(b) el ***asegurador*** diera su consentimiento por escrito a la revelación de la existencia o los términos de esta póliza

7.11 Cooperación

El ***asegurado*** acepta proporcionar al ***asegurador*** toda la información, asistencia y cooperación que el ***asegurador*** pueda razonablemente requerir con respecto a cualquier ***reclamación***, ***circunstancia***, ***evento de privacidad***, ***evento de seguridad*** o ***evento de publicación electrónica***, incluyendo la asistencia a audiencias y comparecencias judiciales, así como la ayuda para asegurar y suministrar la documentación y evidencia necesarias, y obtener la asistencia y la declaración de testigos. El ***asegurado*** acepta no hacer cosa alguna que pudiera perjudicar al ***asegurador***.

Tan pronto como fuere posible, una vez que el ***asegurado*** haya dado notificación al ***asegurador*** de cualquier ***reclamación***, ***circunstancia***, ***evento de privacidad***, ***evento de seguridad*** o ***evento de publicación electrónica***, o de cualquier otra cantidad que fuere objeto de ***reclamación*** bajo esta póliza, el ***asegurado*** también deberá proporcionar al ***asegurador*** las correspondientes copias de informes, fotografías, investigaciones realizadas, alegatos presentados y todos los demás papeles y documentos relacionados con la situación.

7.12 Justa representación del riesgo

(a) En el momento de entrada en vigor y renovación de esta póliza, así como cada vez que se realicen cambios a la misma bajo petición del ***asegurado***, el ***asegurado*** deberá:

  (i) informar al ***asegurador*** acerca de todos los hechos materiales de manera clara y comprensible, y

  (ii) evitar tergiversar cualquier hecho material.

(b) En el supuesto de que el ***asegurado*** incumpla la cláusula (a) de esta disposición, el ***asegurador*** podrá:

  (i) resolver esta póliza, lo que significa que el ***asegurador*** le dará un trato como si jamás hubiese llegado a existir y denegará todas las ***reclamaciones*** en las que cualquier falta o falsedad de información por parte de ***asegurado*** quede probado por el ***asegurador*** como intencional o imprudente. En tal caso, el ***asegurador*** no devolverá la prima abonada por el ***asegurado***; y

  (ii) recobrar del ***asegurado*** cualquier importe que el ***asegurador*** haya desembolsado en concepto de cualquier ***reclamación***, incluyendo aquellos gastos o costes incurridos por el ***asegurador***.

(c) Si el ***asegurado*** no cumple con la cláusula (a) de esta disposición y la falta o falsedad de información no es deliberada o imprudente, esta póliza puede verse afectada en una o más de las siguientes formas, dependiendo de lo que el ***asegurador*** habría hecho si hubiera tenido conocimiento de los hechos que el ***asegurado*** no reveló o tergiversó:

  (i) si el ***asegurador*** no habría prestado cobertura alguna al ***asegurado***, el ***asegurador*** tendrá la opción de:

    1. resolver la póliza, lo que significa que el ***asegurador*** le dará un trato como si nunca hubiera existido y devolverá la prima pagada, y

    2. recuperar del ***asegurado*** cualquier importe que el ***asegurador*** hubiera pagado por cualquier ***reclamación***, incluyendo los costes y gastos incurridos por el ***asegurador***;

  (ii) si el ***asegurador*** habría aplicado términos diferentes a la cobertura, el ***asegurador*** tendrá la opción de tratar esta póliza como si esos términos diferentes aplicaran. El ***asegurador*** podrá recuperar cualquier pago efectuado por el ***asegurador*** por ***reclamaciones*** que ya hayan sido pagadas, en la medida en que dichas ***reclamaciones*** no habrían sido pagadas si se hubieran aplicado dichos términos adicionales, o

  (iii) si el ***asegurador*** habría cobrado al ***asegurado*** una ***prima*** superior por proporcionar la cobertura, el ***asegurador*** cobrará al ***asegurado*** la ***prima*** adicional que proceda.

7.13 Reclamaciones fraudulentas

Si el ***asegurado*** o cualquiera que actúe en nombre del ***asegurado***:

(a) presenta una ***reclamación*** fraudulenta o exagerada bajo esta póliza;

(b) emplea medios o dispositivos fraudulentos, incluyendo la presentación de documentos falsos o falsificados como soporte de una ***reclamación***, con independencia de que la ***reclamación*** en sí sea verdadera;

(c) comete un falso testimonio en defensa de una ***reclamación***, con independencia de que la ***reclamación*** en sí sea verdadera;

(d) presenta una ***reclamación*** bajo esta póliza por una pérdida o daños que el ***asegurado*** o cualquiera que actúe en nombre del ***asegurado*** o en connivencia con el ***asegurado*** provocó deliberadamente;

(e) se da cuenta, tras presentar lo que a su juicio era una verdadera ***reclamación*** conforme a esta póliza y no informa al ***asegurador*** de que el ***asegurado*** no ha sufrido ninguna pérdida o daño, u

(f) oculta información que el ***asegurado*** sabe que, de lo contrario, permitiría al ***asegurador*** denegar el pago de una ***reclamación*** conforme a esta póliza,

el ***asegurador*** estará autorizado a denegar el pago total de la ***reclamación*** y a recuperar cualquier cantidad que haya abonado ya en relación con la ***reclamación.***

El ***asegurador*** podrá también notificar al ***asegurado*** que el ***asegurador*** tratará esta póliza como terminada con efecto desde la fecha de cualesquiera de los actos u omisiones indicadas en las cláusulas a) a f) de esta disposición.

Si el ***asegurador*** resuelve esta póliza bajo esta condición, el ***asegurado*** no tendrá cobertura alguna bajo esta póliza desde la fecha de la resolución y no tendrá derecho a ningún reembolso de prima.

Si cualquier fraude es perpetrado por o en nombre de la ***persona asegurada*** y no en nombre del ***asegurado***, esta condición debe leerse como si se aplicara solo a la ***reclamación*** de dicha ***persona asegurada***, y las referencias a esta póliza deben leerse como si fueran referencias a la cobertura disponible solo para esa persona y no a la póliza en su totalidad.

7.14 No acumulación de límites con otros seguros del Grupo Zurich

Si cualquier siniestro quedara cubierto, total o parcialmente, por esta y cualesquiera otras pólizas de otros ramos emitidas por Zurich Insurance plc, Sucursal en España, o por cualquier otra entidad del Grupo Zurich, para el ***tomador del seguro*** o los ***asegurados*** en cualquier lugar del mundo, el límite de indemnización para tal siniestro y por el conjunto de pólizas afectadas:

(a) no excederá nunca el límite más alto de dichas pólizas;

(b) consecuentemente, los límites de dichas pólizas no se consideran en adición, sino que se aplica el más alto de ellos para el conjunto de las mismas.

7.15 Consentimiento

Cuando se requiera el consentimiento del ***asegurador*** en virtud de esta póliza (incluso para incurrir en cualquier honorario, coste o gasto razonable y necesario), dicho consentimiento no será denegado o retrasado injustificadamente.

VIII. Condiciones generales del seguro

8.1 Declaraciones sobre el riesgo

8.1.1 Al contratar el seguro y durante su vigencia

Al otorgar la cobertura de esta póliza, el ***asegurador*** se ha basado en la solicitud de seguro, la cual forma la base de la cobertura y queda incorporada a esta póliza, pasando a formar parte de la misma.

La póliza ha sido concertada sobre la base de las declaraciones formuladas por el ***tomador del seguro*** en el cuestionario-declaración del riesgo que han motivado la aceptación del riesgo por el ***asegurador***, la asunción por su parte de las obligaciones para él derivadas del contrato y la fijación de la ***prima***.

En relación con lo anterior, el ***tomador del seguro*** tiene el deber, antes de la contratación y conclusión del contrato, de declarar al ***asegurador***, de acuerdo con la solicitud de seguro/cuestionario-declaración del riesgo a que este le someta, todos los hechos o las circunstancias por él conocidas que puedan influir en la valoración del riesgo.

Asimismo, si el contenido de la póliza difiere de la solicitud/proposición de seguro y de las cláusulas acordadas, el ***tomador del seguro*** podrá reclamar al ***asegurador***, en el plazo de un mes, a contar desde la entrega de la póliza, para que subsane la divergencia existente.

Si transcurrido dicho plazo no se ha efectuado la reclamación, se aplicará lo dispuesto en la póliza.

8.1.2 Consecuencias de la reserva o inexactitud de las declaraciones

El ***asegurador*** podrá rescindir el contrato mediante declaración dirigida al ***tomador del seguro*** en el plazo de un mes, a contar desde el día en que tuvo conocimiento de la reserva o inexactitud de la declaración del ***tomador del seguro***.

Si el siniestro sobreviene antes de que el ***asegurador*** haga la declaración a la que se refiere el párrafo anterior, la prestación de esta se reducirá proporcionalmente a la diferencia entre la ***prima*** convenida y la que se habría aplicado de haberse conocido la verdadera entidad del riesgo.

Si medió dolo o culpa grave del ***tomador del seguro***, el ***asegurador*** quedará liberada del pago de la prestación.

8.1.3 En caso de agravación del riesgo

El ***tomador del seguro*** o el ***asegurado*** deberán, durante el curso del contrato, comunicar al ***asegurador***, tan pronto como le sea posible, las circunstancias declaradas o traídas del cuestionario previo, o recogidas en las ***Condiciones Particulares*** y especiales que agraven el riesgo, así como el acaecimiento de cualquier hecho, conocido por aquellos que pueda agravarlo, y sean de tal naturaleza que, si hubieran sido conocidas por el ***asegurador*** en el momento de la perfección del contrato, no lo habría celebrado o lo habría concluido en condiciones más gravosas.

8.1.4 Facultades del asegurador en caso de agravación del riesgo

En el caso de que durante el ***periodo del seguro*** se le comunique al ***asegurador*** una agravación del riesgo, esta puede proponer una modificación de las condiciones del contrato en un plazo de dos (2) meses, a contar desde el día en que la agravación le ha sido declarada.

En este caso, el ***tomador del seguro*** dispone de quince (15) días, a contar desde la recepción de esta proposición, para aceptarla o rechazarla.

En caso de rechazo o de silencio, el ***asegurador*** puede, transcurrido dicho plazo, rescindir el contrato previa advertencia al ***tomador del seguro***, dándole un nuevo plazo de quince (15) días para que conteste. Transcurridos estos quince (15) días, y dentro de los ocho (8) días siguientes, comunicará al ***tomador del seguro*** la rescisión definitiva.

El ***asegurador*** podrá, igualmente, rescindir el contrato comunicándolo por escrito al ***asegurado*** dentro del plazo de un (1) mes, a partir del día en que tuvo conocimiento de la agravación del riesgo.

8.1.5 Consecuencias de no comunicar la agravación del riesgo

Si sobreviene un siniestro sin haber hecho declaración de agravación del riesgo, el ***asegurado*** queda liberado de su prestación si el ***tomador del seguro*** o el ***asegurado*** han actuado con mala fe. En otro caso, la prestación del ***asegurador*** se reducirá proporcionalmente a la diferencia entre la ***prima*** convenida y la que se habría aplicado si se hubiera conocido la verdadera entidad del riesgo.

8.1.6 En caso de transmisión

En caso de transmisión del objeto asegurado, el adquirente se subroga en el momento de la enajenación, en los derechos y obligaciones que correspondían en la póliza al anterior titular.

El ***asegurado*** está obligado a comunicar por escrito al adquirente la existencia de la póliza sobre la cosa transmitida. Una vez verificada la transmisión, también deberá comunicarla por escrito al ***asegurador*** o a sus representantes en el plazo de quince (15) días.

El adquirente y el anterior titular son solidariamente responsables del pago de las ***primas*** vencidas en el momento de la transmisión.

El ***asegurador*** puede rescindir el contrato dentro de los quince (15) días siguientes desde que tiene conocimiento de la transmisión verificada. Una vez ejercitado su derecho y notificado por escrito al adquirente, el ***asegurador*** queda obligado durante el plazo de un (1) mes, a partir de la notificación. El ***asegurador*** deberá restituir la parte de ***prima*** que corresponda al periodo de seguro por el que, como consecuencia de la rescisión, no haya soportado el riesgo.

El adquirente de la cosa asegurada también puede rescindir el contrato si lo comunica por escrito al ***asegurador*** en el plazo de quince (15) días, contados desde que conoció la existencia del seguro. En este caso, el ***asegurador*** adquiere el derecho a la ***prima*** correspondiente al periodo que hubiera comenzado a correr cuando se produce la rescisión.

Las normas anteriores rigen para los casos de muerte, suspensión de pagos, quita y espera, quiebra o concurso del ***tomador del seguro*** o del ***asegurado***.

8.1.7 En caso de concurrencia de seguros

Cuando en dos o más contratos estipulados por el *tomador del seguro* con distintos aseguradores se cubran los efectos que un mismo riesgo puede producir sobre el mismo interés y durante idéntico periodo de tiempo, el *tomador del seguro* o el *asegurado* deben, salvo pacto contrario, comunicar a cada *asegurador* los demás seguros que estipule.

Si por dolo se omite esta comunicación y se produce el siniestro en situación de sobreseguro, los *aseguradores* no están obligados a pagar la indemnización

Si una *reclamación* estuviera asegurada en virtud de cualquier otra póliza de indemnización válida y cobrable, distinta a esta póliza, esta póliza actuará en exceso de dicha otra póliza.

8.2 Duración del contrato

Esta póliza terminará en la fecha de vencimiento indicado en las *Condiciones Particulares* de esta póliza. Esta póliza no es de renovación automática.

8.3 Pago de la *prima*

El ***tomador del seguro*** está obligado al pago de la ***prima*** en el momento de la formalización del contrato de acuerdo con las condiciones estipuladas en las ***Condiciones Particulares*** de la póliza.

8.4 Fraccionamiento del pago de la *prima*

Si entre ambas partes se pacta expresamente el pago fraccionado de las ***primas*** del seguro, esta facilidad no se aplicará a las ***primas*** devengadas por regularización de capitales flotantes, cambios en sumas aseguradas o cambios en la naturaleza del riesgo, que se pagarán de forma inmediata a la presentación de las mismas al ***asegurado*** por parte del ***asegurador***, salvo pacto expreso en contrario.

La concesión del pago fraccionado no merma en ningún caso el derecho del ***asegurador*** al cobro de la prima total, aun en el supuesto de ocurrir un siniestro que destruyera las propiedades aseguradas.

El ***asegurador*** se reserva el derecho de resarcirse de posibles fraccionamientos de prima pendientes, deduciendo el importe de estos de cualquier indemnización a que hubiere lugar.

Se declara expresamente que el pago fraccionado es una facilidad para el ***tomador del seguro*** o el ***asegurado*** de la cual no puede prevalerse ni puede ir en perjuicio de quien concede tal facultad.

8.5 Comunicaciones

Las comunicaciones al ***asegurador*** por parte del ***tomador del seguro***, del ***asegurado*** o del beneficiario se harán en el domicilio social del ***asegurador***, señalado en la póliza.

8.6 Formalización del contrato

El contrato se perfecciona por el consentimiento, manifestado por la suscripción de la póliza y mediante el cobro de la ***prima***.

IX. Gestión del siniestro

9.1 Tramitación

El ***tomador del seguro*** o el ***asegurado*** deben comunicar al ***asegurador*** el acaecimiento del siniestro dentro del plazo máximo de siete (7) días, contados a partir de la fecha en que fue conocido, salvo que se pacte un plazo más amplio en la póliza.

El ***asegurador*** podrá reclamar los daños y perjuicios causados por la falta de esta declaración. Este efecto no se producirá si se prueba que la compañía ha tenido conocimiento del siniestro por otro medio.

El ***tomador del seguro*** y el ***asegurado*** deben dar al ***asegurador*** toda clase de informaciones sobre las circunstancias y consecuencias del siniestro. En caso de violación de este deber, en el supuesto de que hubiese concurrido dolo o culpa grave, el ***asegurador*** puede reclamar los daños y perjuicios que le cause esta falta de información.

En caso de que existan contratos estipulados por el ***tomador del seguro*** con distintos aseguradores, la comunicación del siniestro debe hacerse a cada uno de ellos, con indicación del nombre de los demás.

9.2 Subrogación y repetición

(a) Subrogación

El ***asegurador***, una vez pagada la indemnización y hasta el límite de la misma, se subroga en todos los derechos y acciones que correspondan al ***asegurado*** contra terceros responsables, quedando desligado proporcionalmente de sus obligaciones en cuanto el ***asegurado*** hubiera renunciado a tales derechos, especialmente frente a sus propios ***proveedores del servicio***.

Sin el consentimiento del *asegurador*, el *asegurado* no puede renunciar a hacer valer cualquier cláusula contractual que limite o excluya su propia responsabilidad frente a terceros, pues ello supondría la pérdida de sus derechos en caso de siniestro.

El ***asegurado*** deberá cooperar con el ***asegurador*** en el ejercicio de su derecho de subrogación, y el ***asegurador*** no realizará ningún acto u omisión en perjuicio de dicho derecho. En este sentido, el ***asegurado*** será responsable de los perjuicios que, con sus actos u omisiones, pueda causar al ***asegurador*** en su derecho a subrogarse.

Cualquier cantidad recobrada, en exceso del importe indemnizado por el ***asegurador***, será devuelta al ***asegurado*** una vez deducido el coste incurrido por el ***asegurador*** en dicha recuperación.

Si el daño fue indemnizado solo en parte, el ***asegurado*** y el ***asegurador*** concurrirán a hacer valer sus derechos en la proporción correspondiente.

(b) Repetición

El ***asegurador*** podrá repetir contra el ***asegurado*** por el importe de las indemnizaciones que haya debido satisfacer como consecuencia del ejercicio de la acción directa por el perjudicado o sus derechohabientes, cuando las ***pérdidas*** causadas a ***terceros*** sean debidas a conducta dolosa del ***asegurado***.

El ***asegurador*** podrá igualmente reclamar al ***asegurado***, para exigirle el reintegro de las indemnizaciones que hubiese tenido que satisfacer a ***terceros*** perjudicados por siniestros no amparados por la póliza o de las ***franquicias*** establecidas en las ***Condiciones Particulares***.

9.3 Prescripción

Las acciones que se derivan del contrato de seguro prescriben en el término de dos años.

9.4 Procedimiento de reclamaciones

(a) Responsabilidades del ***asegurado***.

Se acuerda que:

(i) en caso de recibir una ***reclamación***, el ***asegurado*** deberá:

1. notificar al ***asegurador*** por escrito la ***reclamación*** recibida tan pronto como sea razonablemente posible, y en cualquier caso dentro del plazo máximo de siete (7) días desde la fecha en la que tuvo conocimiento de la misma. En caso de incumplimiento, el ***asegurador*** podrá reclamar los daños y perjuicios causados por la falta de declaración;

2. dentro de dicho plazo, reenviar al ***asegurador*** cualquier ***reclamación***, orden judicial o citación emitida contra cualquier ***asegurado***;

3. a expensas del ***asegurado***, y tan pronto como sea razonablemente posible, suministrar por escrito al ***asegurador*** todos los detalles de la ***reclamación*** junto con cualquier evidencia e información que pueda ser razonablemente requerida por el ***asegurador*** con el propósito de investigar o verificar la ***reclamación*** y mantener al ***asegurador*** informado de cualquier evidencia e información futura recibida por el ***asegurado*** o razonablemente requerida por el ***asegurador***, y

4. en caso de tener conocimiento de una ***circunstancia***, deberá notificarla lo antes posible y facilitar detalles completos, incluyendo todos los hechos materiales, fechas y personas involucradas y las razones por las que anticipa, por definición, que se trata de una ***circunstancia***.

(ii) Ante el descubrimiento de un ***evento de privacidad***, deberá notificarlo al ***asegurador*** tan pronto como sea razonablemente posible, y en cualquier caso dentro del plazo máximo de siete (7) días desde la fecha en la que se produjo dicho descubrimiento. En caso de incumplimiento, el ***asegurador*** podrá reclamar los daños y perjuicios causados por la falta de declaración. Asimismo, el ***asegurado*** deberá:

1. tan pronto como sea razonablemente posible, notificar al ***asegurador***, a través del número de emergencia del ***Servicio de respuesta a incidentes***, y en cualquier caso no más de setenta y dos (72) horas después de que el ***asegurado*** tenga conocimiento por primera vez del ***evento de privacidad***, proporcionar al ***asegurador*** una notificación escrita durante el ***periodo del seguro***;

2. tomar todas las medidas razonables para proteger los ***sistemas informáticos***, ***información personal***, ***activos digitales*** o ***información corporativa*** frente a una mayor pérdida o daño, y tomar todas las medidas y pasos razonables para limitar o mitigar la ***pérdida de beneficios***;

3. colaborar con el ***asegurador*** en su investigación y con cualquier perito u otro asesor o profesional que designe el ***asegurador*** por sí mismo o por cuenta del ***asegurado***, y

4. a expensas del ***asegurado*** y tan pronto como sea razonablemente posible, suministrar detalles completos de cualquier prueba e información que el ***asegurador*** pueda requerir de manera razonable a los efectos de investigar o comprobar el ***evento de privacidad***.

(iii) Ante el descubrimiento de un ***evento de seguridad***, ***error administrativo*** o ***fallo del sistema***, el ***asegurado*** deberá:

1. notificar al ***asegurador*** por escrito o utilizando el número de emergencia del ***Servicio de respuesta a incidentes***, tan pronto como sea razonablemente posible, pero siempre dentro de los siete (7) días posteriores al momento en que el ***asegurado*** tenga conocimiento por primera vez del ***evento de seguridad***, ***error administrativo*** o ***fallo del sistema***, y en ningún caso después de los sesenta (60) días posteriores a la fecha de vencimiento del ***periodo del seguro*** de la póliza. En caso de incumplimiento, el ***asegurador*** podrá reclamar los daños y perjuicios causados por la falta de declaración;

2. tomar todas las medidas y pasos necesarios para limitar o mitigar la ***pérdida de beneficios*** y ***pérdida de beneficios derivada de proveedores***, y

3. facilitar al ***asegurador*** la prueba por escrito de las pérdidas y con todos los detalles del caso, dentro de los seis (6) meses contados a partir del descubrimiento de dicho ***evento de seguridad***, ***error administrativo*** o ***fallo del sistema*** bajo esta póliza o, con el previo consentimiento por escrito del ***asegurador***, dentro del periodo adicional que el ***asegurado*** pueda requerir,

siempre y cuando no se pueda interponer acciones legales para el recobro de cualquier cantidad antes de sesenta (60) días tras la remisión por parte del ***asegurado*** de la prueba original de la pérdida al ***asegurador***, o más de doce (12) meses después del descubrimiento del ***evento de seguridad***, ***error administrativo*** o ***fallo del sistema***.

(iv) Ante el caso que se produjera una ***amenaza de extorsión cibernética***, el ***asegurado*** deberá notificar al ***asegurador***, a través del teléfono de emergencia del ***Servicio de respuesta a incidentes***, y facilitar al ***asegurador*** con una notificación escrita tan pronto como sea razonablemente posible, pero en ningún caso más tarde de sesenta (60) días después del final del ***periodo del seguro***, y

(v) **El *asegurado* no realizará ninguna liquidación, admisión de responsabilidad, pago o promesa de pago a un *tercero* sin el consentimiento por escrito del *asegurador*.**

(b) Derechos del ***asegurador***.

El ***asegurador*** tendrá:

(i) derecho a dirigir la defensa o la liquidación de cualquier ***reclamación*** presentada contra cualquier ***asegurado***, y el ***asegurado*** proporcionará toda la asistencia que pueda requerir el ***asegurador***, y

(ii) derecho a designar el asesoramiento jurídico;

(iii) derecho a, pero no la obligación de, defender cualquier ***procedimiento regulatorio*** y ***procedimiento RGPD***. **El *asegurado* no incurrirá en *gastos de defensa* en ningún *procedimiento regulatorio* sin el previo consentimiento por escrito del *asegurador*.**

(c) Notificación presunta.

Cualquier ***reclamación*** que posteriormente se presenta contra un ***asegurado*** y se notifica al ***asegurador*** que alegue, surja de, esté basada en o sea atribuible a una ***circunstancia*** notificada durante el ***periodo del seguro***, o que alegue cualquier ***acto incorrecto*** que sea igual o esté relacionado con cualquier ***acto incorrecto*** anticipado en la ***circunstancia*** notificada, **se considerará hecha en el momento en que dicha notificación de *circunstancia* fue recibida por primera vez por el *asegurador*.**

(d) Disposiciones generales sobre las notificaciones.

Salvo lo dispuesto en sentido contrario en esta póliza, todos los avisos o notificaciones contemplados bajo cualquier disposición de esta póliza deberán entregarse por escrito mediante mensajería expresa con franqueo previamente pagado, o por correo certificado, correo electrónico o fax correctamente dirigido a la parte que corresponda. Las notificaciones al ***asegurado*** podrán dirigirse al ***tomador del seguro*** a la dirección que aparece en las ***Condiciones Particulares*** de esta póliza. Las notificaciones dirigidas al ***asegurador*** deberán enviarse a la dirección respectiva que se indica en las ***Condiciones Particulares*** de esta póliza. Las notificaciones que fuesen entregadas de la manera descrita se considerarán recibidas y en vigor a partir del momento en que fueran efectivamente recibidas por el destinatario o un día después de la fecha de envío de las mismas, lo que suceda primero, siempre que exista prueba de su envío.

9.5 Valoración de los gastos de reposición de activos digitales

En caso de que el ***asegurado*** no pueda restaurar o reconstituir los ***activos digitales***, entonces los ***gastos de reposición de activos digitales*** **quedarán limitados al gasto real incurrido por el *asegurado* de modo necesario y razonable para poder determinar que no pueden restaurar ni reconstituir dichos *activos digitales*.**

9.6 Valoración de la pérdida de beneficios

Se acuerda que las ***pérdidas de beneficios*** y las ***pérdidas de beneficios derivada de proveedores*** se calcularán sobre una base horaria en función de la pérdida real en la que incurra el ***asegurado*** durante el ***periodo de restablecimiento***, según sea el caso.

Para determinar el importe de la pérdida a pagar, el ***asegurador*** considerará los beneficios netos y gastos del ***asegurado*** antes del momento en que ocurrió la ***interrupción del servicio*** y los beneficios netos y gastos probables del ***asegurado*** de no haber ocurrido la ***interrupción del servicio***. **No obstante, estos cálculos referentes al beneficio neto y gastos no incluirán, y esta póliza no cubrirá, cualquier estimación o proyección sobre los ingresos netos que el *asegurado* probablemente hubiera obtenido como consecuencia de un incremento del volumen de su negocio debido a unas condiciones favorables del negocio experimentadas por competidores u otros negocios comparables.**

El *asegurado* proporcionará al *asegurador* acceso a todas las fuentes de información relevantes, incluyendo, pero no limitado a:

(a) los registros financieros, las declaraciones de impuestos, los procedimientos contables del *asegurado*;

(b) recibos, facturas y otros comprobantes, y

(c) escrituras, gravámenes y contratos.

X. Regulación legal

Quejas y reclamaciones

Las quejas y reclamaciones pueden dirigirse al Servicio de Defensa del Cliente de la compañía, conforme al procedimiento que establece el Reglamento para la defensa del cliente dispuesto por la compañía y que se encuentra disponible en nuestra página web www.zurich.es/defensacliente. Este reglamento se ajusta a los requerimientos de la Orden Ministerial ECO 734/2004 y a aquellas normas que la sustituyan o modifiquen.

El Servicio para la Defensa del Cliente regulado en dicho reglamento dictará resolución dentro del plazo máximo señalado en este último, a partir de la presentación de la queja o reclamación. El reclamante puede, a partir de la finalización de dicho plazo, acudir al Servicio de reclamaciones de la Dirección General de Seguros y Fondos de Pensiones, en su caso.

Protección de datos personales

Responsable del tratamiento de los datos: Zurich Insurance plc, Sucursal en España ("la compañía o aseguradora")

Finalidades y destinatarios del tratamiento de los datos:

1. En la póliza:

Para la ejecución del contrato de seguro, la aseguradora se encuentra sujeta a la normativa propia de seguro y, en tal condición, actúa como responsable del tratamiento. Asimismo, el tomador, en lo que respecta a su propia actividad, puede actuar también como responsable de tratamiento.

Finalidades del tratamiento de los datos personales en la póliza:

Para gestionar el contrato: los datos de carácter personal se incluirán en ficheros de Zurich Insurance plc, Sucursal en Espa ña, y de su matriz Zurich Insurance plc, con la finalidad de celebrar el contrato, la perfección, mantenimiento y control del contrato de seguro, así como para estudios estadísticos, de calidad o análisis técnicos, la gestión del coaseguro, reaseguro, en su caso, y, por parte de la matriz, para tratamientos relativos a la prevención del blanqueo de capitales y la financiación del terrorismo.

Legitimación: la ejecución del contrato y de la normativa propia del seguro, principalmente la Ley de contrato de seguro o la Ley de ordenación y supervisión y solvencia de las entidades aseguradoras y reaseguradoras, y de la normativa de prevención de blanqueo de capitales y financiación del terrorismo.

2. Datos personales del representante (persona física) de la persona jurídica

El representante (persona física) de cada una de las partes queda informado por esta cláusula de que sus datos personales facilitados para ejecutar este contrato de seguro serán tratados por la otra con la finalidad de gestionar la relación contractual.

En su caso, el tomador garantiza a la aseguradora, con respecto a cualquier otro dato personal que haya podido comunicarle en ejecución del contrato de seguro, que ha informado al interesado (ya sea asegurado, beneficiario o cualquier otra figura), con carácter previo a dicha comunicación, del tratamiento de sus datos en los términos previstos en esta cláusula, y que ha cumplido cualquier otro requisito que sea necesario para posibilitar la legítima comunicación de sus datos personales a la aseguradora conforme a la normativa aplicable.

La base legal para los citados tratamientos es la ejecución del contrato y de la normativa propia del seguro, principalmente, la Ley de contrato de seguro o la Ley de ordenación y supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

Los datos personales no se comunicarán a terceros, salvo, en su caso, para el cumplimiento de las obligaciones contenidas en la normativa aplicable.

3. Datos de terceros (colectivos o cuando se incluyan listados con datos personales de personas físicas)

En aquellos casos en los que la póliza la formalice el tomador en beneficio de un tercero, el tratamiento de los datos de los asegurados/beneficiarios, incluidos los de salud, si los hay, están legitimados por la existencia de una relación contractual que los hace necesarios para la formalización del contrato.

En este caso, el tomador/asegurado, asume contractualmente la obligación de informar a dichos terceros sobre el tratamiento de sus datos personales que hace la aseguradora y, en su caso, debe facilitar a la aseguradora el boletín de adhesión debidamente firmado; todo ello siguiendo el mismo procedimiento que se establece en el Real Decreto 1060/2015 de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras en lo relativo a la información previa de seguros. Para más información, consulten el apartado Información adicional.

Derechos e Información adicional

Derechos: el titular de los datos personales (en caso de que sea persona física) y el interesado y el representante (en caso de que sea persona jurídica) tienen derecho a acceder, rectificar, oponerse y suprimir los datos personales, así como otros derechos, tal y como se explica en la Información adicional.

Nombre Asegurado, S.L.
Póliza xxxxxxxxx

Información adicional: puede consultar la información adicional en www.zurich.es/rgpd.

Especialidades en quejas y reclamaciones por comunidades autónomas

Zurich, además de las oficinas abiertas en las distintas comunidades autónomas, dispone de una dirección física para todos los consumidores y usuarios, situada en Paseo de la Castellana, 81, de Madrid, donde pueden ser atendidos sobre cualquier queja o reclamación que planteen sobre sus seguros. También dispone del servicio telefónico gratuito de atención de quejas y reclamaciones 900 110 770, para los consumidores y usuarios.

Aplicación de orden público internacional

Sin perjuicio de las condiciones de este acuerdo, no puede considerarse que el asegurador de cobertura haga pagos o preste algún servicio o beneficio a favor de cualquier asegurado o tercero mientras esa cobertura, pago, servicio o beneficio y/o cualquier otro negocio o actividad del asegurado pueda contravenir legislaciones o regulaciones comerciales, de embargo comercial o de sanciones económicas afectadas por un orden público internacional.

Asimismo, en el eventual caso de que la aseguradora, con ocasión del cumplimiento de las formalidades previstas en dichas regulaciones, sobrepase el plazo máximo previsto para el cumplimiento de determinadas obligaciones, estas no devengarán intereses de demora.

Sin perjuicio de las condiciones de este acuerdo, no puede considerarse que el asegurador de cobertura haga pagos o preste algún servicio o beneficio a favor de cualquier asegurado o tercero mientras esa cobertura, pago, servicio o beneficio tenga relación con un "negocio en Irán".

El término "negocio en Irán" incluye, pero no está limitado a, cualquier actividad, transacción, operación, subsidiaria, sucursal, producto, bien, persona física o jurídica, directa o indirectamente relacionada con Irán, o trasladándose a, desde o por el territorio de Irán, o por cualquier persona residente en Irán o por una entidad sujeta a la legislación Iraní, o cualquier entidad controlada o que sea propiedad de alguno de los anteriores.

Normativa SEPA (Single European Payment Area)

El tomador/asegurado, al facilitar los datos bancarios para el pago de la prima del seguro o, en su caso, para el recobro de franquicias, consiente y autoriza que su importe sea cargado en la cuenta que se facilita y se recoge en este documento o en aquel que se comunique a la entidad aseguradora con tal finalidad y durante la vida del contrato.

En el supuesto de que el tomador/asegurado no sea el titular de la cuenta facilitada, este asegura que ha obtenido la autorización del titular a tales efectos.

XI. Cláusula final: aceptación íntegra del contrato

Las partes reconocen que las condiciones económicas de esta póliza se han establecido teniendo en cuenta los términos y limitaciones convenidos, particularmente en lo que se refiere al objeto de cobertura del seguro, ámbito temporal de cobertura, límites de indemnización y franquicias, así como exclusiones y otras estipulaciones. Si se hubiera pretendido extender las coberturas a otros ámbitos, bien el contrato de seguro no se habría suscrito, o bien tanto las condiciones del riesgo a cubrir como las primas asignadas habrían alcanzado un nivel más gravoso. Por ello, mediante el abono de la prima convenida, el tomador del seguro presta su consentimiento al contrato de seguro y reconoce que ha examinado la totalidad de las cláusulas contenidas en esta póliza y que está plenamente conforme con cada una de las mismas.

Localidad, a 00/00/0000

El tomador del seguro [redacted]

Póliza de Seguridad y Responsabilidad de Privacidad

ENDOSO N.º 1

SERVICIO DE REPUESTA ANTE INCIDENTES

Este endoso forma parte integrante de la póliza. Como contraprestación a la ***prima*** cobrada, mediante el presente se hace constar y se acuerda que la póliza se modifica de la siguiente manera:

En el ámbito de las coberturas de la póliza, el ***asegurador***, tiene acuerdos con las siguientes empresas para la asistencia y gestión de siniestros. El ***asegurado*** podrá contactar con ellas sin el previo consentimiento por escrito del ***asegurador*** en caso de ocurrencia de un ***evento de seguridad***, un ***evento de privacidad***, un ***evento de publicación electrónica*** o una ***interrupción del servicio*** y que sean incurridos en un periodo de 72 horas, a contar desde que se notifica por primera vez el incidente al proveedor de ***servicio de respuesta ante incidentes*** contactando al número de emergencia especificado a continuación:

Cómo contactar con los proveedores aprobados para Primera respuesta

Servicio de respuesta ante incidentes: **Lazarus**
Llamando a este teléfono: **931 845 872**

¿Qué información debe facilitar?:

- Nombre del asegurado (persona jurídica) y número de póliza.
- Datos de contacto del asegurado (persona física) para futuras comunicaciones.
- Breve descripción del incidente.

Proceso para Notificar un Siniestro

De acuerdo con lo establecido en el apartado IX. Gestión del siniestro de la póliza, y más concretamente, punto 9.4 Procedimiento de reclamaciones. El ***asegurado*** en caso de recibir una ***reclamación*** o, de la ocurrencia de un ***evento de privacidad***, un ***evento de seguridad***, un ***error administrativo*** o un ***fallo del sistema,*** deberá comunicarlo al ***asegurador*** a la dirección de e-mail indicada a continuación:

Cómo declarar el siniestro al asegurador

Enviando un e-mail

Exención de Responsabilidad
Los servicios que presten cualquiera de las empresas recogidas en este documento en relación con las coberturas y extensiones de esta póliza le son directamente prestados al ***asegurado*** en du condición de cliente de dichas empresas sin la supervisión o control por parte deXXX. En virtud de lo anterior, XXXXX no puede garantizar la prestación de tales servicios y no asume ninguna responsabilidad o ninguna otra consecuencia que se derive de la prestación de o falta de prestación de servicios por parte de estos proveedores.

EL RESTO DE LOS TÉRMINOS, CONDICIONES Y LIMITACIONES DE ESTA PÓLIZA NO SE MODIFICAN.

Tomador del seguro

Nombre Asegurado, S.L.
Póliza XXXXXXXX

Póliza de Seguridad y Responsabilidad de Privacidad

ENDOSO N.º 2

Renovación Tácita

Este endoso forma parte integrante de la póliza, mediante el presente se hace constar y se acuerda que la póliza se modifica de la siguiente manera:

Sujeto a todos los términos, condiciones y limitaciones de esta póliza, se acuerda que al vencimiento del ***periodo de seguro*** estipulado en las ***Condiciones Particulares***, el contrato quedará tácitamente prorrogado por un año desde la fecha de vencimiento de la póliza y así en lo sucesivo, salvo que o bien el ***asegurador*** se opusiera a su prorroga mediante notificación escrita a la otra parte con dos meses, por lo menos, de antelación a la conclusión del ***periodo de seguro*** en curso o bien el ***asegurado*** se opusiera a su prórroga mediante notificación escrita a la otra parte con un mes, por lo menos, de antelación a la conclusión del ***periodo de seguro*** en curso.

Esta cláusula de renovación tácita queda sujeta a que no se haya producido un *cambio de control*.

En caso de que no se cumplan las condiciones arriba detalladas al vencimiento del *periodo del seguro*, la póliza se dará por extinguida y será necesario que el *tomador del seguro* remita una nueva solicitud de seguro al *asegurador*, con el fin de que este proponga condiciones de renovación.

Tomador del seguro

XXXXXXXXXX, Sucursal en España

XXXXXXXXXXXXXXX
Director General
ZXXXXXXXXXXXXXXXXXXXXXXXXXXX
Sucursal en España

Fuente: Elaborado por una empresa de seguros que vende seguros en Latinoamérica que desea mantenerse en anonimato (Enero, 2023)