GOBIERNO DE MÉXICO | CONAHCYT CONSEJO NACIONAL DE HUMANIDADES CIENCIAS Y TECNOLOGÍAS | INFOTEC

BIBLIOTECA INFOTEC
VISTO BUENO DE TRABAJO TERMINAL

Maestría en Derecho de las Tecnologías de Información y Comunicación
(MDTIC)

Ciudad de México, a 13 de febrero de 2024

UNIDAD DE POSGRADOS
PRESENTE

Por medio de la presente se hace constar que el trabajo de titulación:

"Riesgo en la emisión de pólizas de fianzas electrónicas"

Desarrollado por el alumno: **Raúl Chávez Castañeda**, bajo la asesoría del **Mtro. Jorge Reyes Negrete,** cumple con el formato de Biblioteca, así mismo, se ha verificado la correcta citación para la prevención del plagio; por lo cual, se expide la presente autorización para entrega en digital del proyecto terminal al que se ha hecho mención. Se hace constar que el alumno no adeuda materiales de la biblioteca de INFOTEC.

No omito mencionar, que se deberá anexar la presente autorización al inicio de la versión digital del trabajo referido, con el fin de amparar la misma.

Sin más por el momento, aprovecho la ocasión para enviar un cordial saludo.

Mtro. Carlos Josué Lavandeira Portillo
Director Adjunto de Innovación y Conocimiento

jah CJLP/jah

C.c.p. Felipe Alfonso Delgado Castillo.- Gerente de Capital Humano.- Para su conocimiento.
Raúl Chávez Castañeda.- Alumno de la Maestría en Derecho de las Tecnologías de Información y Comunicación.- Para su conocimiento.

MDTIC

MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

“RIESGO EN LA EMISIÓN DE PÓLIZAS DE FIANZAS ELECTRÓNICAS”

REPORTE ANALÍTICO DE EXPERIENCIA LABORAL
Que para obtener el grado de MAESTRO EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presenta:

Raúl Chávez Castañeda

Asesor:

Mtro. Jorge Reyes Negrete

Ciudad de México, septiembre, 2020.

CONACYT

INFOTEC POSGRADOS

Agradecimientos

A mis padres con amor infinito.

Tabla de contenido

Introducción..... 1

Capítulo 1. Antecedentes de internet y de los actos de comercio electrónico. 5

1.1 Historia de internet. 5

1.2 Desarrollo de internet en México 6

1.3 Regulación de internet en México 7

1.4 Generalidades de las TIC en los actos jurídicos. 8

1.5 ¿Qué es el comercio electrónico? 9

1.6 Características del comercio electrónico. 10

1.7 ¿Quiénes participan en el comercio electrónico? 11

1.8 Desarrollo del comercio electrónico en México. 11

1.9 Legislación nacional aplicable a los actos electrónicos: 12

Capítulo 2. Riesgo cibernético y ciber seguridad en los actos de comercio electrónicos 18

2.1 Concepto de riesgo cibernético y ciber seguridad 18

2.2 Características del ciber ataque, clasificación y ciber atacantes. 19

2.3. Ciberseguridad en México. 22

2.4. Legislación Internacional aplicable a los actos de comercio electrónico. 23

2.4.1. Ley modelo de la Comisión de las Naciones Unidas para el desarrollo del derecho mercantil Internacional sobre comercio electrónico. 24

2.4.2. Ley modelo de la Comisión de las Naciones Unidas para el desarrollo del derecho mercantil internacional sobre firmas electrónicas. 25

2.4.3. Directiva 2000/31/ce del Parlamento Europeo y del Consejo de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior – Directiva sobre el comercio electrónico. 25

2.4.4. Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica. 26

2.4.5. Directiva 2002/58 de 12 de julio de 2002, sobre tratamiento de los datos personales y la protección de las intimidades en el sector de las comunicaciones electrónicas. 26
2.4.6. Directiva 95/46CE tratamiento de datos personales..... 27
2.4.7. Directiva 2000/46/CE del Parlamento Europeo y del Consejo de 18 de septiembre de 2000, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como la supervisión cautelar de dichas entidades. 28
2.4.8. Convenio de Roma de 1980 sobre la Ley aplicable a las obligaciones contractuales. 28
2.4.9. Tratado de Derecho Civil Internacional de Montevideo. 29
2.5 Datos personales en el entorno digital como finalidad de los ciber ataques. . 29
2.6. El derecho a la protección de datos personales. 30

Capítulo 3. La fianza electrónica y el dato financiero. 33
3.1 Orígenes de la fianza..... 33
3.2 Actividad afianzadora en México. 34
3.3 Fianza electrónica y el dato financiero. 37
3.3.1. El dato financiero. 40
3.3.2 Elementos personales de la fianza 44
3.3.3 Elementos materiales y formales..... 46
3.3.4 Elementos de existencia. 46
3.3.5 Elementos de validez. 47
3.3.6 Elementos reales. 47
3.3.7 Elementos de validez. 47
3.4 Manifestación del consentimiento para el perfeccionamiento de la fianza..... 48
3.5 Firma electrónica..... 51
3.6 Firma electrónica avanzada..... 52
3.7 Elementos de la Firma Electrónica. 54

Capítulo 4. Riesgo en la operación de las Instituciones de Fianzas a través de medios electrónicos. 57
4.1 ¿Cuándo es vinculante la póliza en la que se documenta una fianza? 57
4.2 Prueba pericial en informática forense. 59

4.2.1 La informática forense como herramienta para hacer frente a los riesgos operativos y de emisión de pólizas de fianzas: 59
4.3 Bases de coordinación en materia de seguridad de la información..... 62
4.4 Uso de medios electrónicos para la operación y contratación de fianzas..... 68
4.5 ¿Qué riesgos se actualizan por la emisión de fianzas electrónicas? 75
4.6 ¿Qué ilícitos se actualizan cuando alguien comercializa pólizas de fianzas electrónicas para aparentar el otorgamiento de fianzas? 76
4.7 Situaciones que favorecen la realización de estas conductas. 89
4.7.1 La falta de cultura de validación. 89
4.7.2 Falta de interés en los beneficiarios para denunciar estos hechos. 89
4.7.3 Poco riesgo de quebranto a la institución de fianzas. 90

Conclusiones 93

Bibliografía 95

Índice de figuras

Figura 1 Elementos personales de las relaciones contractuales vinculadas con la fianza. 45

Siglas y abreviaturas

AAGEDE	Asociación de Almacenes Generales de Depósito.
ARPA	Agencia de Proyectos de Investigación Avanzada
ARPANET	Red de la Agencia de Proyectos de Investigación Avanzada
ABM	Asociación de Bancos de México
AFICO	Asociación FinTech México, Asociación de Plataformas de Fondeo Colectivo
AMFORE	Asociación Mexicana de Afores
AMIB	Asociación Mexicana de Instituciones Bursátiles
AMIG	Asociación Mexicana de Instituciones de Garantías
AMIS	Asociación Mexicana de Instituciones de Seguros
AMSOFIPO	Asociación Mexicana de Sociedades Financieras Populares
ARPA	Agencia de proyectos de Investigación Avanzada
ASOFOM	Asociación de Sociedades Financieras de Objeto Múltiple
BANXICO	Banco de México
CERT-MX	Centro Nacional de Respuesta a Incidentes Cibernéticos
CNBV	Comisión Nacional Bancaria y de Valores
CNSF	Comisión Nacional de Seguros y Fianzas
CONCAMEX	Confederación de Cooperativas de Ahorro y Préstamo de México
CONACyT	Consejo Nacional de Ciencia y Tecnología
CONSAR	Comisión Nacional del Sistema de Ahorro para el Retiro
CUSF	Circular Única de Seguros y Fianzas
DOF	Diario Oficial de la Federación
DDOS	Ataque de denegación de servicio
FGR	Fiscalía General de la República
FINTECH	Instituciones de Tecnología Financiera
GRI	Grupo de Respuesta a Incidentes Sensibles de Seguridad de la Información
LFT	Ley Federal de Telecomunicaciones
LGPDPPSO	Ley General de Protección de Datos personales en Posesión de Sujetos Obligados
LISF	Ley de Instituciones de Seguros y Fianzas
LPDUSF	Ley de Protección y Defensa de los Usuarios de Servicios Financieros
LFPDPPP	Ley Federal de Protección de Datos personales en Posesión de Particulares
MITM	Ataque de intermediario
NSD	Servidor de Nombres
NIP	Número de identificación personal
OMC	Organización Mundial de Comercio
SHCP	Secretaría de Hacienda y Crédito Público
SQL	Lenguaje de consulta estructurada
TIC	Tecnologías de la Información y Comunicación
UCAR-NCAR	Centro Nacional de Investigación Atmosférica
UNAM	Universidad Nacional Autónoma de México

WWW	World Wide Web
XML	Lenguaje de Mercado Extensible

Introducción

El presente trabajo de investigación puede explicar su origen atendiendo la experiencia laboral dentro de la Comisión Nacional de Seguros y Fianzas, en el ejercicio del cargo de Jefe de Departamento de Ratificación y Certificación de Firmas en donde se realizan, entre otros, el registro de las firmas de los funcionarios facultados para suscribir fianzas y las ratificaciones de los contratos de afianzamiento múltiple, el análisis de las Disposiciones de Carácter General emanadas de la Ley de Instituciones de Seguros y Fianzas para el ejercicio de las facultades de Inspección y Vigilancia de dicha Comisión, situación que ha permitido una cercanía con el sector para conocer la problemática que se desarrollará en la presente investigación, considerando para estos efectos tres apartados importantes identificados como áreas de oportunidad, el primero refiere al crecimiento exponencial de las herramientas electrónicas susceptibles de ser utilizadas por las instituciones de garantías para emitir pólizas de fianzas electrónicas y en términos generales operar logrando con ello altos niveles de eficiencia en beneficio de sus clientes. El segundo apartado refiere a la identificación y análisis de los riesgos que dichas instituciones de garantías asumen y se enfrentan utilizando dichas herramientas electrónicas novedosas. Finalmente, el tercer apartado, no menos importante, atiende a la poca bibliografía que refiera a la operación de las instituciones en los medios digitales por tratarse de un sector financiero especializado y poco abordado por la academia, constituyendo con ello el marco de referencia del presente trabajo de investigación.

En este orden de ideas resulta trascendente analizar el contexto internacional, las practicas mercantiles en medios electrónicos para luego identificar las disposiciones normativas nacionales afines, hasta abordar directivas de coordinación implementadas por el Sector Financiero Mexicano, en conjunto con las Disposiciones de Carácter General emanadas de la Ley de Instituciones de Seguros y Fianzas.

El estudio de los riesgos ante los que se enfrentan las instituciones por el uso de medios electrónicos busca aportar elementos para que dichas Instituciones

implementen, con mayor seguridad y certeza jurídica, sistemas electrónicos que faciliten la operación y emisión de pólizas.

Importancia del tema.

En la actualidad existen 17 instituciones de garantías debidamente constituidas dentro del territorio nacional, autorizadas para emitir pólizas de fianzas, las cuales en menor o mayor medida han adoptado sistemas electrónicos para su operación, enfrentando los riesgos inherentes a la operación a través de medios electrónicos encargándose de garantizar el cumplimiento de obligaciones en todo el territorio nacional, resaltando el ramo de fianzas administrativas otorgadas a favor de la Federación para garantizar el cumplimiento, entre otros, de licitaciones públicas.

El objetivo general del presente trabajo se traduce en contribuir con el sano desarrollo del sistema financiero mexicano, brindando mayor protección y certeza jurídica a las mismas instituciones, a los clientes o usuario de dichos instrumentos de garantía con la identificación de los riesgos a los que se enfrentan el sector al operar y emitir pólizas de fianza a través de medios electrónicos.

En cuanto a los objetivos específicos no referimos a analizar cada uno de los riesgos referidos, aportar elementos con los cuales las instituciones puedan, en la práctica, hacerles frente y, en su caso, con los resultados obtenidos del análisis planteado, impulsar las modificaciones apropiadas y correspondientes a las Disposiciones de Carácter General emanadas de la Ley de Instituciones de Seguros y de Fianzas.

El capítulo primero refiere a los antecedentes y generalidades de internet, de las tecnologías de la información y comunicación, así como de los actos de comercio electrónico y la legislación nacional aplicable a fin de tener un mayor contexto del crecimiento exponencial de las nuevas tecnologías y su impacto en las relaciones mercantiles.

El segundo capítulo refiere a los riesgos cibernéticos, ciberseguridad y las generalidades de los ciberataques en un contexto nacional e internacional, abordando la tendencia actual de los datos personales como finalidad de los atacantes y su relación con el derecho de la protección de datos personales.

El tercer capítulo refiere a los orígenes y desarrollo de la fianza en México, su evolución hacia la fianza electrónica, su perfeccionamiento y uso de firma electrónica, firma electrónica avanzada y el dato financiero involucrado.

Por último, el cuarto capítulo aborda los riesgos asumidos por las Instituciones y usuarios, por la operación, emisión y contratación de la fianzas a través de medios electrónicos, la informática forense como herramienta indispensable para hacer frente a los mismos, los ilícitos que se actualizan con una fianza electrónica apócrifa, los delitos especiales previstos en la Ley de Instituciones de Seguros y Fianzas en congruencia con las disposiciones legales aplicables en materia de seguridad de la información.

Capítulo 1.

Antecedentes de internet y de los actos de comercio electrónico

Capítulo 1. Antecedentes de internet y de los actos de comercio electrónico

1.1 Historia de internet

Las distintas versiones del surgimiento de internet atienden a diferentes vertientes como ámbitos sociales, ciencia y/o comunicación, por lo que se plantean aproximaciones con el propósito de situar el acontecimiento y la evolución del mismo.

Es en la década de los 60's, el Departamento de Defensa de los Estados Unidos, a través de la Agencia de Proyectos de Investigación Avanzada (ARPA por sus siglas en inglés), financió un proyecto denominado ARPANET, que se constituye como el génisis de lo que conocemos como Internet evolucionando con posterioridad al world wide web.

Si bien es cierto que la finalidad del desarrollo de ARPANET como génesis del Internet, se vincula de manera directa con una finalidad militar o industria bélica, hay textos que difieren de dicha referencia, en este sentido el autor Manuel Castells manifiesta:

"ARPANET fue una red de investigación, no un sistema de control militar; no hay evidencia de que fuera mirado como un objeto milita, y lejos de ser secreto, los detalles técnicos de ARPANET fueron abiertamente publicados"[1]

También se puede referir a la evolución de ARPANET del sector militar al sector civil lo que trajo como resultado una privatización de la red siendo más accesible al público y constituyéndose como el nacimiento de Internet como lo conocemos hoy en día.

Las universidades jugaron un rol muy importante convirtiéndose en intermediarios, pues facilitaban el acceso mediante redes locales pequeñas.

Fue en 1990 donde se le asigna el nombre de world wide web o www, cuando con un navegador se permitía sacar e introducir información de cualquier ordenador conectado a la red.

[1] Castells Manuel, La Galaxia Internet, Madrid, Areté, 2001. P. 25

En este sentido la WWW puede explicarse como una red mundial que funciona sin un nodo central, poniendo al alcance de todos cualquier punto de la red con el uso de nuevos protocolos como el TCP/IP.

El Diccionario de la Real Academia de la Lengua Española define al internet como: "*Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.*"[2]

Por su parte el Dr. Alfredo Reyes Kraft lo define como "*un canal mundial de telecomunicaciones informáticas integrado por muchos canales que a su vez, están interconectadas entre si, lo cual convierte en el medio de comunicación más veloz en toda la historia de la humanidad.*"[3]

1.2 Desarrollo de internet en México

Rastrear la genealogía de internet en México nos remite al ámbito académico en dos instituciones de educación superior, la Universidad Nacional Autónoma de México y el Instituto Tecnológico de Estudios Superiores de Monterrey.

"El Tecnológico de Monterrey, Campus Monterrey, logró conectarse a la red BITNET (EDUCOM) por medio de una línea conmutada hacia la Universidad de Texas, en San Antonio. La velocidad del referido enlace era de 2,400 bps y los equipos interconectados eran maquinas IBM modelo 4381. Cabe destacar que se realizaban dos conexiones al día, cada una con un promedio de 30 minutos."[4]

Por otra parte, la Universidad Nacional Autónoma de México (UNAM) logró la conexión mediante su Instituto de Astronomía a través de un convenio de enlace con la red de la NSD en EUA, el cual se realizó utilizando el satélite mexicano Morelos II para conectar el Instituto de Astronomía de la UNAM con el UCAR-NCAR, con residencia en Boulder Colorado.

La primera conexión mexicana a internet tuvo al objetivo de hacer eficiente el intercambio de información de carácter científico y académico entre investigadores.

---

[2] Diccionario de la Real Academia de la Lengua Española portal electrónico. https://dle.rae.es/?w=internet consultado el 08-09-2019

[3] Reyes Kraft Alfredo Alejandro, La firma electrónica y las entidades de certificación. Editorial Porrúa, México, 2003, P. 27.

[4] Oscar Robles Garay, Evolución de Internet en México y en América Latina, ITESM/CECSA, México, 2000. P. 4

La condición de las universidades como intermediarias que facilitaban el acceso a la red, fue la condición que permitió a México conectarse mediante un acuerdo de la National Science Fundatión quien se constituyó como una entidad central encargada de unificar las redes ya existentes.

1.3 Regulación de internet en México

La adopción de internet por parte de la sociedad mexicana requiere necesariamente una regulación apropiada, actualizada, incluyente y congruente con el marco normativo estatal y federal, permitiendo con ello la adopción de servicios innovadores en beneficio del ciudadano.

"*La sociedad en su conjunto vive la ciencia y tecnología sobre todo como un fenómeno cultural propio de la civilización contemporánea de un modo que ninguna sociedad (del pasado) ha experimentado."*[5]

Bajo este contexto en 1995 surgió la primera disposición legal relativa al servicio de internet ofrecido mediante líneas telefónicas, la Ley Federal de Telecomunicaciones (LFT) publicada en el Diario Oficial de la Federación (D.O.F.) el 7 de junio de dicho año, que pretendía "*regular el uso, aprovechamiento y explotación del espectro radioeléctrico, de las redes de telecomunicaciones, y de la comunicación vía satélite".*[6]

La evolución y acelerado desarrollo puede ser atribuido a algunos factores como la utilidad de dichas tecnologías para la vida cotidiana, la competitividad en la industria por los mercados, el alta demanda de aplicaciones por parte de usuarios para el procesamiento de información, investigación de tecnologías por parte de universidades en relación con la demanda académica de conexión a la red, y globalización de los mercados atendiendo a las relaciones comerciales entre empresas internacionales y, por último, la sociedad demandante al reconocer los beneficios que internet ofrece como medio de comunicación en la vida diaria.

[5] Julio E. Rubio y Javier Ordoñez (Coordinadores), Ciencia, tecnología y sociedad en México, México, ITESM, Porrúa, 2008, P. 13.
[6] Ley Federal de Telecomunicaciones. Diario Oficial de la Federación de 7 de junio de 1995.

1.4 Generalidades de las TIC en los actos jurídicos

La finalidad de las tecnologías de la información y comunicación es optimizar el manejo de información y comunicación en diversos ámbitos como el gubernamental, académico, laboral y comercial entre muchos otros.

El intercambio de bienes y servicios se ha visto beneficiado con el desarrollo de estas tecnologías, permitiendo de manera ágil el establecimiento de acuerdos mercantiles sin la necesidad de la manifestación de la voluntad de manera presencial.

Para estos efectos es necesario plantear principios generales del derecho y contrastarlos con los aspectos electrónicos para con ello consolidar una idea congruente de acuerdo al entorno social y las practicas mercantiles.

Se define el acto jurídico como la "*manifestación de la voluntad hecho con el propósito de crear, modificar o extinguir derechos, y que produce efectos queridos por su autor o por las partes por que el derecho sanciona dicha manifestación de voluntad.* "[7]

Otra definición de la doctrina clásica refiere que "*el acto jurídico es el acto humano lícito con manifestación de voluntad destinado a crear, regular, modificar o extinguir relaciones jurídicas"*[8]

De lo anterior se puede advertir que la manifestación de la voluntad es uno de los elementos importantes y de existencia en un acto jurídico, la manifestación de la voluntad traduciéndose también en la manifestación del consentimiento para la celebración de un acto representan un pilar para el perfeccionamiento de los mismos.

En el ámbito electrónico la manifestación del consentimiento que no es más que el acuerdo de voluntades, puede ser mal interpretado en cuanto al momento de su perfeccionamiento.

La manifestación del consentimiento atiende a dos clases, la expresa o explicita y la tácita o implícita, independientemente de que dicha manifestación sea por escrito (en el caso de la expresa) o por medios electrónicos.

---

[7] Rojina Villegas Rafael, Compendio de Derecho Civil. Volumen I, Porrúa, México, 2006, P. 221.
[8] De Pina Vara Rafael, Diccionario de Derecho, Porrúa, México, 1995, P. 198.

Es importante aclarar que el documento electrónico se refiere a un medio a través del cual se manifiesta una idea por medios digitales, incluyendo también manifestaciones de la voluntad encaminadas a alcanzar acuerdos para crear, modificar o extinguir derechos u obligaciones.

El Dr. Julio Téllez concluye que documento electrónico "*es información producto de una interacción hombre -máquina, cuyo origen es el hombre, y que tienen valor de escrito ya que es un mensaje (texto alfanumérico o gráfico) en lenguaje convencional (bits) sobre un soporte material mueble (cintas o discos magnéticos, discos ópticos o memorias de circuitos"*[9]

Adicionalmente se puede inferir que documento electrónico es el medio soportado en un conjunto de bits que, sometidos a un adecuado proceso, permiten su representación visual, auditiva y hasta táctil con el propósito de transmitir una idea reconocible por el hombre, el documento electrónico original se encuentra de manera intangible siendo exteriorizado a través de los medios mencionados.

En el comercio electrónico la información y manifestación del consentimiento de las partes es procesada enviada y recibida de manera digital, a través de un documento electrónico, aspecto que difiere de la manifestación del consentimiento presencial o por escrito en medios físicos.

1.5 ¿Qué es el comercio electrónico?

La Organización Mundial de Comercio (OMC) define al comercio electrónico como "*La producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos*".[10]

La expresión comercio electrónico, para el Dr. Julio Téllez, "*se utiliza con frecuencia en los medios informativos en los negocios y en el lenguaje común para referirse a una amplia gama de actividades que normalmente se asocian al uso de computadoras, de internet para el comercio de bienes y servicios de una manera*

[9] Téllez Valdés Julio, Derecho Informático, 4ta Edición ; Mc Graw Hill, México, 2009, P. 300
[10] Organización Mundial del Comercio, Programa de trabajo sobre el comercio electrónico, S.L.I., 1998, portal electrónico https://www.wto.org/spanish/tratop_s/ecom_s/ecom_s.htm consultado el 09-09-19.

nueva, directa y electrónica"[11] en un sentido amplio lo define como "*cualquier forma de transacción o intercambio de información comercial basada en la transmisión de datos sobre redes de comunicación como internet"*[12]

Como se puede advertir, el comercio electrónico no es aquella actividad que se lleva a cabo solamente mediante internet, la cual es la primer vía conocida y con mayor relevancia ejemplificativa.

1.6 Características del comercio electrónico

En cuanto a características se refiere, se puede advertir la desaparición de los límites geográficos gracias a una conectividad global que no se circunscribe a países determinados, el perfeccionamiento de contratos o transacciones sin presencia física de las partes a través de transmisiones electrónicas de datos usando un medio o canal de comunicación y utilizando dispositivos digitales que procesan la información enviada y recibida, la nula restricción de horarios para efectuar cualquier tipo de transacción electrónica, la disminución de costos y un desarrollo paulatino de la confianza de los usuarios en su uso.

Atendiendo al medio tecnológico que utilicen se puede identificar un comercio electrónico abierto refiriéndose a aquel que utiliza redes que no cuentan con ningún tipo de bloqueo o se encuentran restringidas a determinados usuarios, mientras que el comercio electrónico cerrado es el que utilizan redes que requieren tanto configuración de hardware, software y credenciales especiales para su acceso.

Atendiendo a los bienes que ofrecen, bienes tangibles: ejemplo la compra de un producto, bien mueble o inmueble, así como la prestación de algún servicio que se materialice, en contraposición con los bienes Intangibles que son aquellos que se obtienen únicamente en medios electrónicos para su aprovechamiento.

[11] Tellez Valdés Julio, Derecho Informático, 4ta Edición ; Mc Graw Hill, México, 2009 P. 214.
[12] Ibidem P. 218.

1.7 ¿Quiénes participan en el comercio electrónico?

El proveedor: persona física o moral que en su calidad de comerciante brinda un servicio u ofrece un bien, en el tema que nos ocupa, mediante redes de comunicación y tecnologías de la información con fines de lucro.

El consumidor: persona física o moral que, como destinatario final es quien paga por la prestación de un servicio o adquisición de un producto.

El intermediario: toda persona que actuando por cuenta de otra en relación con un determinado mensaje de datos lo envía recibe o archiva, o bien preste algún servicio con respecto a dicho mensaje. En cuanto a este elemento, se puede advertir que una de las finalidades del comercio electrónico es disminuir en la medida de lo posible la intermediación logrando con ello abatir los costos de los productos o servicios, no obstante lo anterior, se observa en la actualidad que grandes empresas se ven favorecidas intermediando de manera electrónica como lo hace actualmente Amazon.

Instituciones de crédito: son aquellas sociedades mercantiles que la Ley de Instituciones de Crédito les da tal calidad entendiéndose como tal la banca múltiple y la banca de desarrollo. Dichas instituciones disponen de plataformas electrónicas que ofrecen la posibilidad de realizar transferencias o pagos casi de manera instantánea. Con el desarrollo de estos mecanismos las instituciones se erigen como actores importantes dentro del comercio electrónico.

1.8 Desarrollo del comercio electrónico en México

No existe un registro claro en fuentes físicas ni digitales, que indique de manera puntual el inicio del comercio electrónico en nuestro país.

Podemos considerar dos escenarios o sucesos importantes para la interpretación del desarrollo del comercio electrónico en México, uno es la entrada en vigor de la regulación legal y el segundo a partir de los modelos de negocio que se fueron implantando por medio de las tecnologías vigentes al momento de su implementación.

El primer escenario se refiere, entre otros, con la implementación del marco jurídico en el año 2000, otorgando un reconocimiento jurídico a los actos de

comercio que se generaban a través de medios no convencionales, así como los elementos o mecanismos probatorios al generarse alguna controversia.

Posteriormente en 2003 se reforzó la idea del fortalecimiento del comercio electrónico incluyendo la temática de la firma electrónica como un mecanismo de aseguramiento para la transacción comercial llevada a cabo por medios electrónicos.

El segundo escenario va de la mano con la evolución de programas, interfaces, software y hardware que constituyeron nuevos modelos para el desarrollo de las dinámicas de prestación de servicios u ofertas de productos, por señalar algunos ejemplos se puede referir a las plataformas que ofrecen el servicio de audio o video en streaming o plataformas como MercadoLibre y Amazon.

En cuanto a las formas o medios de pago actualmente coexisten muchas alternativas para las transacciones comerciales, ya sea mecanismos propios de instituciones de crédito, plataformas distribuidas en otros establecimientos mercantiles, servicios de pago implementado por las grandes empresas desarrolladoras de equipos de telefonía móvil (Samsung Pay y Apple Pay), criptomonedas, Paypal, etc.

Finalmente, la entrega de productos: generalmente son los servicios de mensajería quienes, cobrado gran importancia con el desarrollo del comercio electrónico, dichos servicios de mensajería y paquetería han perfeccionado con tal habilidad su servicio que actualmente son el mecanismo predilecto de los usuarios para recibir sus productos. Gracias a su servicio eficiente, bajo costo en relación con los volúmenes que manejan se consideran un pilar para el desarrollo del comercio electrónico.

1.9 Legislación nacional aplicable a los actos electrónicos

Actualmente no existe un cuerpo normativo que de manera especializada englobe esta temática, si no que se ha optado por hacer reformas menores y adecuaciones para con ello tener injerencia en el comercio electrónico. Disposiciones legales como Código de Comercio, Código Civil Federal, Código Federal de Procedimientos Civiles, Ley Federal de Protección al Consumidor, Ley Federal de Protección de

Datos Personales en Posesión de los Particulares (LFPDPPP) y Ley de Protección y Defensa de los Usuarios de Servicios Financieros (LPDUSF) son algunas disposiciones legales que han sido adecuadas para la persecución de estos fines.

En el artículo 73 de la Constitución Política de los Estados Unidos Mexicanos observamos la facultad del Congreso para legislar en materia mercantil. El artículo 5 de la misma refiere a la libertad de profesión, industria o comercio atendiendo siempre a su licitud.

En cuanto al Código Civil Federal, el articulo 1803 refiere la manifestación del consentimiento expreso manifestado, entre otros, por medios electrónicos, ópticos o por cualquier otra tecnología.

En este mismo sentido, dicho ordenamiento legal establece en su artículo 1834 bis lo relativo a la forma, refiriendo que cuando la forma escrita sea exigible como elemento de validez, se tendrán por cumplida cuando en medios electrónicos, ópticos o de cualquier otra tecnología la información generada o comunicada de forma íntegra, sea atribuible a las personas obligadas y accesibles para su ulterior consulta.

Por otra parte, el Código Federal de Procedimientos Civiles prevé en su artículo 210-A:

“ARTICULO 210-A.- Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.

Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.

Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento

en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta"[13]

Como ha sido mencionado dos reformas fueron importantes para el comercio electrónico, su inclusión en el Código de Comercio en el año 2000 y la firma electrónica en 2003 y 2016.

A grandes rasgos dicho ordenamiento prevé lo relacionado con los mensajes de datos, definiciones como: certificado, datos de creación de firma electrónica, destinatario, digitalización, emisor, firma electrónica, firma electrónica avanzada o fiable, firmante, intermediario, mensaje de datos, prestador de servicios de certificación, sello digital de tiempo, sistema de información y titular del certificado.

También advierte la validez de la información contenida en un mensaje de datos atribuyéndole el mismo valor probatorio que la documentación impresa.

Adicionalmente el artículo 93 refiere, de manera similar al Código Civil lo relativo a la forma, como se puede observar:

"Artículo 93.- Cuando la ley exija la forma escrita para los actos, convenios o contratos, este supuesto se tendrá por cumplido tratándose de Mensaje de Datos, siempre que la información en él contenida se mantenga íntegra y sea accesible para su ulterior consulta, sin importar el formato en el que se encuentre o represente.

Cuando adicionalmente la ley exija la firma de las partes, dicho requisito se tendrá por cumplido tratándose de Mensaje de Datos, siempre que éste sea atribuible a dichas partes.

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de Mensajes de Datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de

[13] Código Federal de Procedimientos Civiles. Diario Oficial de la Federación de 24 de febrero de 1943.

los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.[14]

Por último, es relevante expresar que algunos de los servicios financieros son actos de comercio pues se prestan dentro del ámbito mercantil, por la finalidad de lucro que persiguen algunas las instituciones financieras, entendiéndose como tales a cualquiera de las previstas en la fracción IV del artículo 2 de la LPDUSF

"Artículo 2o.- Para los efectos de esta Ley, se entiende por:

…

IV. Institución Financiera, en singular o plural, a las sociedades controladoras, instituciones de crédito, sociedades financieras de objeto múltiple, sociedades de información crediticia, casas de bolsa, especialistas bursátiles, fondos de inversión, almacenes generales de depósito, uniones de crédito, casas de cambio, instituciones de seguros, sociedades mutualistas de seguros, instituciones de fianzas, administradoras de fondos para el retiro, PENSIONISSSTE, empresas operadoras de la base de datos nacional del sistema de ahorro para el retiro, Instituto."[15]

También es importante referir el Reglamento del Código de Comercio en materia de prestadores de servicios de certificación, el cual dispone en su artículo primero su objeto:

"ARTÍCULO 1o.- El presente ordenamiento tiene por objeto establecer las normas reglamentarias a las que deben sujetarse los Prestadores de Servicios de Certificación en materia de firma electrónica y expedición de Certificados para actos de comercio.

En la aplicación de este Reglamento se estará a las definiciones a que se refiere el artículo 89 del Código de Comercio."[16]

Lo anterior en relación con las "Reglas generales a las que deberán sujetarse los prestadores de servicios de certificación" publicada en el Diario Oficial de la

[14] Código de Comercio. Diario Oficial de la Federación de 7 de octubre al 13 de diciembre de 1889.
[15] Ley de Protección y Defensa al Usuario de Servicios Financieros. Diario Oficial de la Federación de 18 de enero de 1999.
[16] Reglamento del Código de Comercio en materia de prestadores de servicios de certificación. Diario Oficial de la Federación de 19 de julio de 2004.

Federación el 14 de mayo de 2018, las cuales prevé la finalidad de las mismas en su disposición primera:

"1. El presente instrumento establece las Reglas que deberán cumplir los interesados en obtener la acreditación por parte de la Secretaría de Economía para poder ser Prestadores de Servicios de Certificación y ofrecer los servicios de emisión de Certificados Digitales, Sellos Digitales de Tiempo, Conservación de Mensajes de Datos, Digitalización de Documentos en Soporte Físico, así como para actuar como Tercero Legalmente Autorizado, de acuerdo con lo establecido en el artículo 100 del Código de Comercio y la NOM-151-SCFI-2016, publicada en el Diario Oficial de la Federación el 30 de marzo de 2017."[17]

[17] Reglas generales a las que deberán sujetarse los prestadores de servicios de certificación. Diario Oficial de la Federación de 14 de mayo de 2018.

Capítulo 2.

Riesgo cibernético y ciber seguridad en los actos de comercio electrónicos

Capítulo 2. Riesgo cibernético y ciber seguridad en los actos de comercio electrónicos

2.1 Concepto de riesgo cibernético y ciber seguridad

El diccionario de la Real Academia de la Lengua Española define al riesgo como "*Contingencia o proximidad de un daño" y a la cibernética como "creado y regulado mediante computadora*."[18]

En este sentido, podemos converger ambas definiciones para proponer que el riesgo cibernético puede ser definido como la probabilidad de un acontecimiento futuro que representa un daño o un menoscabo económico, derivado de la falla de sistemas tecnológicos u electrónicos.

El concepto de ciber seguridad puede en algunos casos ser muy genérico, el Diccionario de la Real Academia de la Lengua señala que el término "Ciber" refiere a un elemento compositivo que indica relación con las redes informáticas[19], del mismo modo define al término de "Seguridad" como cualidad de seguro.[20]

Por otra parte, la Organización Internacional de Estandarización, en la norma ISO/IEC 270323 define la ciber seguridad como la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciber espacio.[21]

En este sentido el término ciber amenaza se puede considerar como una circunstancia o evento que, aprovechándose de alguna vulnerabilidad tecnológica puede e impactar negativamente en las operaciones, activos o información.

"*La seguridad en el comercio electrónico es fundamental para su desarrollo. En una transacción en donde las partes no tienen contacto 'físico', ¿cómo pueden asegurarse de la identidad de aquel con quien están realizando una operación? e incluso, ¿cómo pueden tener la certeza de que la información intercambiada que en*

[18] Diccionario de la Real Academia de la Lengua Española, portal electrónico. https://dle.rae.es/?w=riesgo consultado el 10-10-2019.
[19] Definición de "Ciber" RAE: Recuperado de https://dle.rae.es/?w=ciber consultado el 01-10-2018.
[20] Definición de "Seguridad" RAE: Recuperado de https://dle.rae.es/?w=seguridad consultado el 01-10-2018.
[21] International Organization for Standardization (ISO), norma ISO/IEC 27032, disponible en https://www.iso27001security.com/html/27032.html consultado el 01-10-2018.

la mayoría de los casos constituyen datos personales. no ha sido robada alterada o conocida por personas ajenas?"[22]

Por lo que la ciber seguridad es importante referir tres aspectos importantes: prevención, detección y respuesta al ataque.

2.2 Características del ciber ataque, clasificación y ciber atacantes

Como características del ciber ataque se pueden identificar:

- La ejecución por parte de un atacante con conocimientos especializados.
- El grado de efectividad e impacto.
- Reducido riesgo para el atacante de ser identificado y juzgado.
- En algunos casos su bajo costo.

La facilidad para realizar un ciber ataque, en relación con el bajo riesgo para el que lo ejecuta, hace que cada vez se presenten de manera más frecuente y se intensifique la severidad del impacto.

Se puede inferir un ciber ataque "*corresponde a la materialización de una o varias ciber amenazas, de esta forma el ciber riesgo o riesgo cibernético, constituye la probabilidad de ocurrencia de un ciber ataque con la severidad o daño que dicho ciber ataque pueda ocasionar; o bien, dicho de otra forma, la pérdida potencial por la materialización de uno o varios ciber ataques.*

Los ciber ataques pueden ocasionar una multiplicidad de daños, esto es, podrían generar en su caso un efecto de contagio en cadena hacia distintas entidades o eslabones de la cadena productiva."[23]

Es importante referir que por el alto grado de especialización del agente que ejecute el ciber ataque, este puede o no ser descubierto o reconocido por la víctima, o incluso ser descubierto días después de haber sido objeto del ilícito, para con ello evaluar el nivel de efectividad o impacto.

En cuanto a su clasificación podemos referir:

[22] Reyes Kraft Alfredo Alejandro, La firma electrónica avanzada. P. 14.
[23] Perez Marquez Fernando, Riesgo Cibernético y Ciberseguridad, Documento de trabajo No. 181 Comisión Nacional de Seguros y Fianzas. P. 6.

*"**Malware**: es el término simplificado para denotar "malicious code" y consiste en aquel software destinado a realizar un proceso no autorizado que tendrá un impacto adverso en la confidencialidad, integridad o disponibilidad de un sistema de información. Dentro de esta categoría se encuentran principalmente los siguientes tipos:"*[24] virus, spyware y adware

- Virus: sector oculto de software informático con la capacidad de replicarse o propagar la infección, con la posibilidad de introducir parte de sí mismo en otro software y formar en parte de él.

- Spyware: aplicativo que de forma secreta se instala en un sistema para recabar información o datos personales sin consentimiento.

- Adware: aplicación que muestra automáticamente publicidad no deseada, sin permiso y de manera aleatoria en un equipo de cómputo después de instalar un software o durante el uso de cierta aplicación.

Rootkit: conjunto de herramientas para obtener acceso al nivel de raíz en un host con el propósito de ocultar actividades del agente atacante concediendo acceso de nivel de raíz "root" al host para controlar a distancia un dispositivo o aprovecharse de una red, entre los cuales podemos referir: trojan horse, worm, ramsomware keylogger y botnet.

- Trojan horse: Software con funciones ocultas y la finalidad de evadir las herramientas de seguridad.

- Worm: "write once, read many", aplicativo con la capacidad de ejecutarse de forma independiente, replicándose en versiones más complejas en otros host o redes, y con la característica de consumir los recursos del equipo.

- Ransomware: virus que impide el acceso a archivos o programas, requiriendo un pago para la recuperación de la información o retomar el control del equipo.

- Keylogger: software con la finalidad de guardar un registro de las teclas presionadas cuya preponderante finalidad es obtener contraseñas de acceso.

[24] Perez Marquez Fernando, Riesgo Cibernético y Ciberseguridad, Documento de trabajo No. 181 Comisión Nacional de Seguros y Fianzas. P. 10.

- Botnet: consiste en toda una Red de equipos infectados con algún software malicioso que facilita a los ejecutantes controlar una botnet sin el conocimiento del propietario.

Phishing: Técnica para adquirir datos confidenciales a través de solicitudes aparentemente legítimas en correos o sitios web.

Man-in-the-middle attack (MitM): es la intercepción de la comunicación entre dos personas, para suplantar la identidad de ambas partes con el propósito de accesar a datos personales, sin el conocimiento de las víctimas.

Distributed denial-of-service attack (DDoS): ataque de denegación de servicio que satura sistemas, servidores o redes para consumir recursos y ancho de banda. [25]

SQL injection: es la implantación de un código malicioso en un servidor que utiliza SQL (Structured Query Language) para permitir acceso o modificación de datos. [26]

Zero-day attack: ataque que explora las vulnerabilidades desconocidas de un sistema con la finalidad de hacerlas públicas de manera previa a sus actualizaciones.

Existe una gran variedad de ciber atacantes y ellos pueden clasificarse atendiendo a su capacidad, a la finalidad que persigan o daño que pretendan lograr o inclusive a su nivel de especialización.

De manera genérica se pueden advertir organizaciones criminales, ciber activistas, organizaciones privadas, ciber terroristas, ciber vándalos, agentes internos o hasta estados que pretendan entre otros, obtener una posición estratégica frente a otros estados.

Lo anterior generalmente atiende a la obtención de beneficios económicos, en algunos casos pueden atender a una motivación ideológica para inclusive influir en la toma de decisiones políticas.

[25] Ibidem P. 12.
[26] Ibidem P. 12.

2.3. Ciberseguridad en México

Toda vez que el término ciber seguridad es relativamente nuevo, es un reto importante concientizar los diversos sectores sociales, desde ámbitos como académico, empresarial o iniciativa privada, así como la Administración Pública Federal.

En virtud de que el Plan Nacional de Desarrollo 2019-2024 publicado en el D.O.F. refiere que, en cuanto a Ciencia y Tecnología se refiere, el Consejo Nacional de Ciencia y Tecnología CONACYT (sic) coordinará el Plan Nacional para la Innovación, mismo que a la fecha no ha sido publicado., es que se abordará lo referente a la Estrategia Nacional de Ciberseguridad, la cual permitiría dar a México un marco referencial para sus políticas cibernéticas nacionales.

En la Estrategia Nacional de Ciber Seguridad[27] se establece la visión del Estado Mexicano en materia de ciber seguridad. Hace un reconocimiento a la importancia de las tecnologías de la información y la comunicación como factor de desarrollo político, social y económico; los riesgos asociados al uso de las tecnologías, el creciente número de ciberdelitos y la necesidad de una cultura general de ciberseguridad.

También define objetivos y ejes transversales, plasma los principios rectores, identifica a los diferentes actores involucrados y da claridad sobre la articulación de esfuerzos entre individuos, sociedad civil, organizaciones privadas.

Durante 2017 se presentó un incremento de ataques cibernéticos a nivel mundial y que afectaron nuestro país de manera importante, como el caso del ransomware Wanna Cry.

El sector financiero fue uno de los más afectados atendiendo también al surgimiento de las Instituciones de Tecnología Financiera (FINTECH) como principal blanco de dichos ataques.

En este sentido el sector privado en el ámbito financiero ha logrado mayores niveles de protección, no obstante, el Estado puede verse superado por el desarrollo

[27] Estrategia Nacional de Ciber Seguridad https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf consultado el 07-09-2019.

de sistemas novedosos que superan la velocidad legislativa para hacer frente a los riesgos que dichos dispositivos o sistemas representan.

Actualmente existe la Policía Cibernética, la Policía Federal alberga al Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX) quien tiene la encomienda de vigilar la integridad de la infraestructura tecnológica del país manteniendo un monitoreo permanente de la red pública de internet, realizando acciones de prevención e investigación de conductas ilícitas en medios informáticos.[28]

Del mismo modo, la Fiscalía General de la República (FGR) cuenta con un departamento de informática forense que se encarga de proporcionar los fundamentos técnicos que sirvan como soporte en la investigación de posibles hechos delictivos concernientes a la modificación, destrucción, reproducción no autorizada de la información contenida en dispositivos electrónicos.

2.4. Legislación Internacional aplicable a los actos de comercio electrónico

Durante el estudio de las diversas legislaciones que rigen la forma de llevar a cabo las contrataciones electrónicas encontramos que, independientemente de que cada Estado tenga la autonomía de dictar sus leyes; han existido diversos esfuerzos para unificar las legislaciones con la finalidad de lograr una adecuada relación comercial, en donde, estar homologadas las legislaciones, las cuestiones jurisdiccionales resultarán de fácil observancia; sin tener que buscar los puntos de conexión entre las leyes de cada país.

En este orden de ideas, revisaremos las disposiciones normativas más importantes dentro del ámbito internacional.

[28]Portal del Centro Nacional de respuesta a incidentes Cibernéticos de la Policía Federal https://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es consultado el 10-10-2019.

2.4.1. Ley modelo de la Comisión de las Naciones Unidas para el desarrollo del derecho mercantil Internacional sobre comercio electrónico [29]

El propósito de dicha ley aprobada el 12 de junio de 1966, es impulsar el empleo de los medios de comunicación novedosos sin soporte de papel, fungiendo como guía para los Estados en cuanto a plantear directrices para la emisión de leyes sobre comercio electrónico.

Se divide en parte general y una parte específica sobre comercio electrónico en materia de transporte, la primera parte señala aspectos relacionados con el cumplimiento de los contratos electrónicos, su interpretación, existencia en el mundo digital, estándares y técnicas para la adopción de la firma digital, así como el perfeccionamiento de los mismos para disponerlos como medios de prueba.

Refiere que los derechos del consumidor tienen prioridad sobre esas normas y su aplicación se presupone a operaciones comerciales de suministro o intercambio de bienes o servicios, acuerdos de distribución, operaciones de representación o mandato comercial, factoraje arrendamiento de bienes de equipo con opción de compra; construcción de obras, consultoría, ingeniería, concesión de licencias, inversión, financiamiento, banca, seguros, concesión o explotación de un servicio público, empresa conjunta y otras formas de cooperación industrial o comercial, transporte de mercancías o de pasajeros por vía aérea y marítima o por ferrocarril y carretera. [30]

Dispone que las partes tendrán la libertad, de modificar las condiciones de contratación y facultándolos para establecer diferentes con apego a los derechos fundamentales.

[29]Delgado Flores Gaudencio y Téllez Valdés Julio, Temas de Derecho Informático, Orden Jurídico Nacional, Secretaría de Gobernación. P. 142.

[30] Ley Modelos sobre comercio electrónico, texto adoptado por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional en su 29ª periodo de sesiones, 28 de mayo a 14 de junio de 1996. Nueva York https://uncitral.un.org/es/about consultado el 10-10-19.

2.4.2. Ley modelo de la Comisión de las Naciones Unidas para el desarrollo del derecho mercantil internacional sobre firmas electrónicas[31]

Ley que será aplicable a todas las contrataciones donde se utilice la firma electrónica, pretende servir como ejemplo o punto de partida para los países que requieran la implementación de normativa interna.

2.4.3. Directiva 2000/31/ce del Parlamento Europeo y del Consejo de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior – Directiva sobre el comercio electrónico [32]

Reforzar la seguridad jurídica del comercio electrónico y aumentar la confianza de los usuarios son los principales objetivos de la presente Ley, siendo aplicable inclusive a servicios suministrados de manera gratuita entre empresas y consumidores.

Exceptuando los servicios o contratos que requieran de la presencia de las autoridades públicas; contratos de caución, garantía o crédito y los relativos a derechos de familia.

Dispone de la norma aplicable, de acuerdo al domicilio o ubicación de la sociedad prestadora de servicios, esto es donde esté establecida, basándose en el país de origen, entendiéndose como tal al sitio donde un operador ejerce de manera efectiva su actividad económica de manera estable y por un tiempo indeterminado.

Dispone que las asociaciones de consumidores participen en la elaboración y puesta en práctica de códigos de conducta para que la directiva sea aplicada de manera correcta.

---

[31] Ley modelo sobre comercio electrónico, texto adoptado por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional en su 85 periodo de sesiones. 12 de diciembre de 2001, Nueva York http://www.uncitral.org/uncitral/es/about_us.html consultado el 10-10-2019.

[32] Directiva 200/31/ce del parlamento europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), publicada en el Diario Oficial dL 178 de 17 de julio de 2000, disponible en https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1571100685430&uri=CELEX:32000L0031 consultado el 10-10-2019.

Entre las excepciones de aplicación o con limitaciones, se encuentran las actividades de notaría, defensa jurídica, derechos de autor, obligaciones de los contratos de consumidores y su protección, protección de menores y salud.

2.4.4. Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.[33]

Directiva referente al marco legal europeo de la firma electrónica y servicios de certificación para la implementación legal en los Estados miembros.

Determina obligaciones comunes para proveedores de servicios de certificación a fin de garantizar el reconocimiento transfronterizo de las firmas certificadas en la comunidad europea; establece disposiciones comunes en materia de responsabilidad a fin de dar confianza a los consumidores y a la utilización de mecanismos de cooperación para facilitar el reconocimiento transfronterizo de las firmas y certificados con terceros países. [34]

Hace referencia a la no restricción por parte de los estados miembros en cuanto a la prestación de servicios de certificación.

2.4.5. Directiva 2002/58 de 12 de julio de 2002, sobre tratamiento de los datos personales y la protección de las intimidades en el sector de las comunicaciones electrónicas[35]

Esta directiva justifica el derecho de los estados miembros de interceptar las comunicaciones electrónicas con la justificación de la protección de derechos y

---

[33] Directiva 199/93/CE del parlamento europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, publicada en el diario oficial L013 de 19 de enero de 2000, disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML consultado el 10-10-2019.

[34] Directiva 199/93/CE del parlamento europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, publicada en el diario oficial L013 de 19 de enero de 2000, disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML consultado el 10-10-2019.

[35] Directiva 2002/58 de 12 de julio de 2002, sobre tratamiento de datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas, publicada en el Diario Oficial L201 de 31 de julio de 2002, http://eur-

libertades propias del derecho comunitario, así como aspectos referentes a la seguridad pública, nacional o defensa.

También pretende uniformar las disposiciones legales de los estados miembros para proteger la intimidad y libre circulación de datos entre otros derechos fundamentales.

El ámbito específico de aplicación está señalado en el artículo 3 cuando determina que esta directiva será aplicable "*al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Comunidad*".

2.4.6. Directiva 95/46CE tratamiento de datos personales[36]

En el supuesto de que la directiva 2002/58/CE sea omisa en la regulación será aplicable la presente directiva y su objetivo es, de acuerdo a su artículo 1ero, proteger las libertades y los derechos fundamentales de las personas físicas, principalmente los de intimidad. Prohíbe a los estados miembros la restricción a la libre circulación de datos entre este grupo.

La directiva se aplicará, de acuerdo con el artículo 3, al tratamiento automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Deja fuera de esta regulación a los datos relativos a la seguridad pública, defensa, seguridad del Estado y materia penal.

lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=32002L0058&model=guichett&lg=en consultado el 10-10-2019.

[36] Directiva 95/46CE tratamiento de datos personales, publicada en el Diario oficial L 281 de 23 de noviembre de 1995, disponible en http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett consultado el 10-10-2019.

2.4.7. Directiva 2000/46/CE del Parlamento Europeo y del Consejo de 18 de septiembre de 2000, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como la supervisión cautelar de dichas entidades [37]

La principal finalidad es la regulación del dinero electrónico de acuerdo a su artículo 1°, aplicación de directivas bancarias, reembolsos, inversiones, entre otros.

Así mismo se deja fuera de la observancia de esta norma a los casos enunciados en el apartado 3 del artículo 2 de la directiva 2000/12/CE, relativos a instituciones de crédito de diversos países.

2.4.8. Convenio de Roma de 1980 sobre la Ley aplicable a las obligaciones contractuales[38]

Las disposiciones de este convenio serán ejercidas en el ámbito de los contratos de bienes muebles corporales o de servicios, así como el financiamiento de estos cuando el consumidor haga un uso diferente al profesional. Se exceptúan las obligaciones contractuales relativas a los testamentos y sucesiones, regímenes matrimoniales; derechos y deberes de las relaciones de familia, de parentesco, matrimonio o afinidad, incluidas las obligaciones alimenticias respecto a los hijos; letras de cambio, cheques, pagarés, cuestiones relativas a sociedades y personas jurídicas; a los servicios de transporte regulados por los artículos 01,4, 5 de este convenio.

Dentro del artículo 30 se establece una vigencia de 10 años la cuál puede ser renovada cada 5 años; este mismo regirá la interpretación, ejecución de obligaciones, extinción, prescripción, caducidad y nulidad del contrato lo anterior definido bajo el artículo 10.

---

[37] Directiva 2000/46/CE del parlamento Europeo y del Consejo de 18 de septiembre de 2000, sobre el acceso a la actividad de las etindades de dinero electrónic y su ejercicio así como la supervisión cautelar de dichas entidades, publicada en el Diario Oficial L 178 de 17 de julio de 2000, disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:ES:HTML consultada el 10-10-2019.

[38] Convenio de roma de 1980 sobre la ley aplicable a las obligaciones Contractuales, publicada en el diario Oficial C 027 de 26 de enero de 1998, disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:41998A0126(02):ES:HTML consultada el 10-10-2019.

El artículo 3, establece que las partes podrán determinar o no la ley aplicable al contrato total o parcial, en caso de no ser así la ley aplicable será la del país dónde preste sus servicios o si es una persona jurídica dónde radique su administración central.

2.4.9. Tratado de Derecho Civil Internacional de Montevideo.[39]

El objetivo de este es promover el desarrollo económico con la creación de un mercado único regulado de manera mutua para incentivar la cooperación recíproca

2.5 Datos personales en el entorno digital como finalidad de los ciber ataques

El uso de las tecnologías de la información y comunicación constituyen elementos que han explotado los Estados para propiciar el crecimiento de su economía.

El crecimiento relacionado con la explotación de las bondades que ofrece internet es resultado de la infinidad de datos que generamos al efectuar cualquier transacción o simple actividad en línea, dato que se constituye como insumo esencial para aquellas empresas que los recogen, procesan o tratan, transformándolos en información útil para mejorar productos o servicios y hasta redireccionar estrategias de negocio.

La generación de datos va desde el ingreso a un sitio web o plataforma, al comprar un producto en línea, manifestar alguna idea en redes sociales, el uso de apps en dispositivos móviles, o simplemente el uso de relojes y bandas deportivas inteligentes.

"Por la importancia que han adquirido en el mundo económico, se utiliza el término de economía de datos para referirse a esta nueva forma de obtener beneficios a partir de los datos que cada empresa posee."[40]

---

[39] Tratado de Derecho Civil Internacional de Montevideo., 1940, suscrito el 19 de maro de 1940, publicado por Decreto 7771/56 de 27 de abril de 1957, disponible en http://www.consulex.com.ar/Legislacion/Leyes/Tratado%20derecho%20procesal%20internacional%20Montevideo%201940.htm.

[40] Lopez Sabater Verónica y Ontiveros, Emilio, Economía de los datos. Riqueza 4.0, Madrid, Editorial Ariel, 2017, P. 11.

Este insumo sobre el que se edifica la nueva economía digital conlleva consecuencias que afectan el derecho a la protección de datos personales. La recolección o minería de datos puede resultar una actividad intrusiva en nuestra vida privada.

La recolección de datos en medios electrónicos con tecnologías disruptivas puede constituirse como una actividad ilícita, una actividad intrusiva en la vida privada que debe, necesariamente, contar con el consentimiento de su titular para su tratamiento.

En cuanto a tecnologías disruptivas se refiere, "*son aquellas que tienen como base la innovación (big data, virtualización, cloud, ciberseguridad inteligencia artificial, etc.) y tienen como denominador común su capacidad de evolucionar rápidamente y adaptarse a diferentes sectores generando nuevos modelos de negocio.*" [41]

La utilización de dichas tecnologías disruptivas constituye una actividad cotidiana en el sector tecnológico digital, acentuándose en aquellas que por su presencia internacional poseen gran cantidad de información.

El tratamiento de estos datos puede traer consigo riesgos para el titular al ser procesados, puesto que se existe la posibilidad de perder el control desconociendo la finalidad o uso de los mismos.

En este orden de ideas, obtener dicho insumo constituye actualmente uno de los principales motivos para vulnerar sistemas electrónicos, en este sentido las empresas pueden ser blanco de los ciber ataques en cualquiera de la clasificación referida en párrafos anteriores.

2.6. El derecho a la protección de datos personales

Por lo que hace a la privacidad, se puede afirmar que es ese núcleo reducido donde ubicamos nuestra información personal y que a su vez decidimos con quien compartir cierta información, sin que la misma deba ser revelada a nivel público.

[41] Sánchez del Campo Alejandro, "Reflexiones de una replicante legal: los retos jurídicos de la robótica y las tecnologías disruptivas Revista de tecnología y sociedad, España, 2016, Núm. 16 P 153.

En este contexto con el derecho de protección de datos personales podemos proteger o en su caso nos otorga esa facultad o poder, para decidir sobre nuestra información y todo aquel dato derivado de nuestra persona.

"Este poder de control ha de ponerse en íntima relación con el consentimiento, que ha de ser el título esencial que justifique injerencias en nuestra privacidad.

De hecho, la violación del derecho de una persona a controlar su esfera privada sea esta física o informativa, constituye el factor más importante para que se sienta invadida la privacidad. No es para ello necesario que la información sea más o menos importante o sensible,

Una persona puede hacer pública información que le afecte sin que por ello considere violada su privacidad. Pero si se pierde el control sobre ella, si alguien se la apropia, entonces pensará que su intimidad ha sido violada. Quien en alguna ocasión ha facilitado o ha permitido el acceso a su propia información no por ello renuncia a su privacidad"[42]

Con lo anterior nos referimos no solo a los datos propios de la vida privada e intimidad, sino a todos aquellos datos que dan individualidad y que, de ser expuestos, tendría repercusión en el desarrollo del ciudadano, en virtud de que los datos por si mismos o asociándolos con otros, forman parte de nuestra identidad, logrando de manera conjunta nuestra identificación.

Por otra parte, encontramos datos personales asociados a nuestro patrimonio, a nuestra economía e incluso, en muchos casos, a nuestro nivel adquisitivo, en este apartado se erige el dato financiero, también amparado por el Derecho a la Protección de Datos Personales.

Con lo referido destacamos que cada persona tiene el derecho a controlar la dispersión o flujo de su información dentro de la sociedad, ya sea información privada, sensible, comercial y/o financiera o de cualquier otro carácter, para en su interacción o asociación con otros, e inclusive, hasta de elegir la manifestación de los mismos y su finalidad.

[42] López Sabater Verónica y Ontiveros Emilio, Economía de los datos. Riqueza 4.0, Madrid España, Editorial Ariel, 2017. P. 155.

Capítulo 3.

La fianza electrónica y el dato financiero

Capítulo 3. La fianza electrónica y el dato financiero

3.1 Orígenes de la fianza

La fianza entendiéndose en términos más amplios como la herramienta de garantía para el cumplimiento de obligaciones, tiene sus inicios en el Código de Hammurabi elaborado por el Rey de Babilonia. En Egipto en el año 128 A.C. se encontraron tratados para garantizar obligaciones entre particulares, posteriormente en Roma, la fianza se advierte de los contratos más trascendentales de la época, denominado "stipulatio" en el año 212 D.C., posteriormente un Código llamado "De las siete partidas" promulgado en 1348 en el Reino de Castilla, se considera a la fianza ya como un contrato accesorio.

Por otra parte, en la época prehispánica dicho instrumento de garantía era conocido y operada por los aztecas como una forma de garantizar el pago de una deuda personal, la cual era hereditaria y se tenía que pagar en vida con servicios como ser esclavo del acreedor. [43]

En Nueva España hay vestigios de dicho contrato en el derecho precortesiano, donde los reyes españoles dieron forma legal a lo que los indios tenían y practicaban; así aparece la fianza en el derecho procesal indiano.

En México se registró en el Código Civil en 1870 que la fianza tenía carácter de contrato y podía otorgarse a título oneroso.

El 19 de julio de 1895 se firmó el primer contrato de concesión entre el Gobierno Federal y los señores Guillermo Obregón y Zan L. Tidball para establecer la primera compañía de Fianzas como sucursal de "American Surety Company of New York." [44]

El 24 de mayo de 1910 se expidió la Ley Sobre las Compañías de Fianza; a pesar que la fianza ha estado presente desde hace bastante tiempo, su uso no se popularizó hasta hace un par de décadas, culturalmente las empresas buscan

[43] Aguilar Beltrán Pedro y Gudiño Antillón Juliana, Fundamentos Actuariales de Primas y Reservas de Fianzas, Los procedimientos técnicos de la regulación mexicana, Fundación Mapfre, 2007. P. 4.
[44] Manuel Molina Bello, La fianza garantía por excelencia en México, Tirant Lo Blanch, 2015. P. 35.

garantizar los incumplimientos a través de penalizaciones explicitas en los contratos o seguros; la primera aunque efectiva, implicaba un proceso legal en los juicios de reclamación, la segunda cumplía el resarcimiento parcial y en ocasiones no era aplicable a situaciones particulares de algunos servicios al no considerarse de riesgo; así poco a poco fue haciendo más versátil la fianza para cubrir esas necesidades.

Fue al término de la revolución mexicana cuando se introdujeron varias modificaciones al contrato de fianza, a través del Código Civil del Distrito Federal en materia común para toda la república en materia federal, expedido el 30 de agosto de 1928. [45]

3.2 Actividad afianzadora en México

En cuanto a la actividad afianzadora en nuestro país, podemos referir que el Código Civil de 1870, propone la siguiente declaración ""*Es la obligación que una persona contrae de pagar o cumplir por otra, si ésta no lo hace" además de admitir de forma expresa que la misma puede ser a título gratuito pero también puede pactarse con retribución.*" [46]

El autor Efrén Cervantes Altamirano, refiere que en dicho código no se exigieron formalidades para el perfeccionamiento del contrato, ya que bastaba el consentimiento expreso de las partes, para que tuviera validez, así mismo, se continuaron transmitiendo los derechos y las obligaciones derivados del contrato a los herederos, además de que el fiador al ser demandado de la obligación garantizada, podía oponer todas las excepciones inherentes a la deuda con excepción de las personales del deudor, del mismo modo, el citado Código contemplaba los beneficios de orden, excusión y división, siempre y cuando el fiador no hubiere renunciado a ellos y los hubiere hechos valer al momento de exigirse cumplimiento de la obligación. Existía la figura de los fiadores solidarios, en la cual

[45] Aguilar Beltrán Pedro y Gudiño Antillón Juliana, Fundamentos Actuariales de Primas y Reservas de Fianzas, Los procedimientos técnicos de la regulación mexicana, Fundación Mapfre, 2007. P. 4.
[46] Cervantes Altamirano Efrén, Fianza de Empresa Antecedentes Históricos y Naturaleza Jurídica, Publicaciones del Semanario de Derecho Mercantil y Bancario. Universidad Nacional Autónoma de México, Escuela Nacional de Jurisprudencia, México, 1950. P. 14.

el fiador que hubiere pagado la deuda podría reclamar de los otros la parte proporcional de la deuda que les correspondía, cuando el fiador hubiera pagado la obligación garantizada, tenía que notificar tal circunstancia al deudor, para que éste no le opusiera las excepciones que tuviera contra el acreedor. Las formas de extinguir la fianza en el referido Código de mérito eran la que extinguía la fianza como obligación principal e indirecta o por vía de consecuencia.

Otro aspecto importante era que reglamentaba las fianzas legales y judiciales, en los que destaca el hecho de que los fiadores no podrían pedir la excusión del deudor principal, y en caso de que no se les hallara, en vez de fianza tenían que otorgar prenda o hipoteca para responder de la obligación.

Posteriormente en el Código Civil de 1928 se introduce la definición actual del contrato de fianza.

"*Artículo 2794. La fianza es un contrato por el cual una persona se compromete con el acreedor a pagar por el deudor, si éste no lo hace.*"

También es importante referir que dicho código acepta la posibilidad de afianzar deudas futuras, en las cuales la obligación del fiador lo es hasta que lo sea la deuda primigenia. La obligación del fiador nunca puede exceder a la obligación principal, aunque pueda afianzarse en parte. Los herederos del fiador responden en forma proporcional según la cuota que les corresponda del haber hereditario de las obligaciones del fiador.

En relación a las formalidades para la celebración del contrato, no requería formulas especiales, bastaba la simple manifestación del consentimiento en forma expresa para que el mismo tuviera plena validez.

En relación a la fianza mercantil el Código de Comercio de 1854, disponía que las fianzas eran mercantiles cuando tenían por objeto asegura el cumplimiento de contratos de comercio.

Hacia 1910 se expidió la Ley sobre Compañías de Fianzas, de la que se destaca que:

1. No se especificó el tipo de sociedad en que tenían que organizarse las instituciones de fianzas

2. La Secretaria de Hacienda era la competente, para autorizar el funcionamiento de las instituciones afianzadoras, fijar los requisitos de admisibilidad de las fianzas y cancelar las autorizaciones para funcionar como afianzadora

3. Las fianzas se encontraban clasificadas en: fidelidad, garantía de pago de impuestos, rentas y multas, y de garantías de cumplimiento de obligaciones de contratos a favor del estado.

4. Se consideraban a las instituciones de fianza de acreditada solvencia y tenían derecho de prelación sobre los bienes del fiado.

Con posterioridad, se expidieron las 32 bases reglamentarias sobre las cuales debían otorgarse las fianzas a favor de la Hacienda Pública, en las que destaca:

- Las fianzas se tenían que otorgar en forma de póliza.
- Se limitó la responsabilidad de la afianzadora a lo convenido en la póliza;
- La vigencia de la fianza era de un año, la cual era prorrogable.
- El plazo de prescripción de las pólizas de fianza era de tres años, a partir de su vencimiento o de su exigibilidad; y
- En caso de que las afianzadora se inconformaran con la resolución administrativa que decretaba el pago de la obligación caucionada, podía acudir a los tribunales comunes para dirimir dicha controversia.

Posteriormente en 1925 se expidió una nueva Ley sobre Compañías de Fianzas, en donde se destaca:

- Se facultó a las instituciones afianzadoras para otorgar fianzas a favor de particulares.
- Se consideraba a las afianzadoras como instituciones de crédito, por lo que quedaron sujetas a la normatividad aplicable.
- Se exigía que éstas se constituyeran bajo el régimen de sociedad anónima.
- Existían una serie de prohibiciones para evitar que desvirtuaran su objeto y

- Se les prohibió a los particulares expedir fianzas en forma sistemática ya que constituía un delito.

En 1942 se reglamentaron los procedimiento que debían seguirse en el caso de reclamaciones contra las instituciones de fianzas, además de establecer el procedimiento de conciliación, el cual, estaban obligados ha agotar, previamente los beneficiarios de las fianzas ante la Secretaría de Hacienda, pues debían tramitar su reclamación en la Comisión Consultiva de Fianzas de dicha Secretaría, y si ésta consideraba que la afianzadora estaba obligada a pagar, le ordenaba constituir una reserva para obligaciones pendientes de cumplir.

Como preámbulo a la Ley Federal de Instituciones de Fianzas, es conveniente señalar algunos aspectos sobre la trascendencia del marco jurídico mexicano de dicha normatividad, al respecto el autor Guillermo Sánchez Flores expone:

"*La Ley Federal de Instituciones de Fianzas del 26 de diciembre de 1950, fue considerada como la disposición en materia de fianzas hasta entonces, que recogió todos los antecedentes legislativos del pasado. A partir de esta época la fianza de empresa, otorgada por las compañías afianzadoras autorizadas para operar en todo el país, sostuvo un crecimiento sostenido, al incorporar en la Ley de Obras Públicas la necesidad de obtener una garantía para contratos con el Gobierno Federal. Por ello, la fianza de empresa, constituyó un instrumento de uso generalizado y de utilidad evidente, debido a que dio la seguridad y firmeza a todo género de relaciones contractuales."*[47]

3.3 Fianza electrónica y el dato financiero

La Ley de Instituciones de Seguros y Fianzas (LISF) en su artículo 214 dispone lo siguiente:

"ARTÍCULO 214.- La celebración de las operaciones y la prestación de servicios de las Instituciones, se podrán pactar mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o

[47] Sánchez Flores Octavio Guillermo de Jesús. El contrato de Fianza. Porrúa, México, 2001. P 452.

públicos, estableciendo en los contratos respectivos las bases para determinar lo siguiente:

I. Las operaciones y servicios cuya prestación se pacte;

II. Los medios de identificación del usuario, así como las responsabilidades correspondientes a su uso, tanto para las Instituciones como para los usuarios;

III. Los medios por los que se hagan constar la creación, transmisión, modificaciones o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate, incluyendo los métodos de autenticación tales como contraseñas o claves de acceso, y

IV. Los mecanismos de confirmación de la realización de las operaciones celebradas a través de cualquier medio electrónico.

El uso de los medios de identificación que se establezcan conforme a lo previsto por este artículo, en sustitución de la firma autógrafa, producirá los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio.

La instalación y el uso de los equipos y medios señalados en el primer párrafo de este artículo se sujetarán a las disposiciones de carácter general que, en su caso, emita la Comisión." [48]

Como se observa el articulo 214 da pauta a que las Instituciones tanto de seguros como de fianzas aprovechen las bondades ofrecidas por las tecnologías de la Información y comunicación para la celebración de sus operaciones y prestación de sus servicios.

En este sentido las Instituciones ofrecen la posibilidad de emitir pólizas electrónicas mediante internet, con el propósito de expresar el acuerdo de voluntades para garantizar, (en el caso de fianzas) una obligación frente a un tercero.

Previo a la emisión de pólizas se requiere analizar tanto la manifestación de la voluntad como el consentimiento de ambas partes para perfeccionar dicho

[48] Ley de Instituciones de Seguros y Fianzas, Diario Oficial de la Federación de 22 de junio de 2018.

contrato de garantía, perfeccionamiento que puede verse distorsionada por el uso de sistemas informáticos.

Por otra parte, el Código Civil Federal establece en su artículo 2749 la definición legal de Fianza:

"*Artículo 2794.- La fianza es un contrato por el cual una persona se compromete con el acreedor a pagar por el deudor, si éste no lo hace."*[49]

El maestro Miguel Ángel Zamora y Valencia, en su libro titulado los Contratos Civiles señala:

"*El contrato de fianza es aquel por virtud del cual una de las personas llamada fiador se obliga ante la otra llamada acreedor, al cumplimiento de una prestación determinada, para el caso de que un tercero, deudor de éste último no cumpla su obligación".* [50]

El autor Bernardo Pérez Fernández del Castillo define a la fianza como:

"*Contrato de garantía en virtud del cual una persona llamada fiador, se obliga a pagar al acreedor si el deudor de la obligación garantizada no lo hace. Se celebra entre el acreedor y un tercero, independientemente de que el deudor esté o no de acuerdo*."[51]

Ahora bien, la referencia "electrónica" advierte únicamente el medio a través del cual se perfecciona el contrato.

En este sentido resulta importante reiterar lo relativo a comercio electrónico.

"*Se entiende por comercio electrónico al conjunto de transacciones comerciales y financieras realizadas por medios electrónicos, incluyendo texto, sonido e imagen. Es un sistema global que utilizando redes informáticas y en particular Internet, permite crear un mercado electrónico (operado por computadora y a distancia) de todo tipo de productos, servicios, tecnologías y bienes e incluye todas las operaciones necesarias para concretar operaciones de compra y venta, matching, negociación, información de referencia comercial. Intercambio de documentos, acceso a la información de servicios de apoyo (aranceles, seguros,*

[49] Código Civil Federal, Diario Oficial de la Federación, 26 de mayo, 14 de julio, 3 y 31 de agosto de 1928.
[50] Zamora y Valencia Miguel Ángel, Contratos Civiles, Editorial Porrúa, México, 2007, P. 405.
[51] Pérez Fernández del Castillo, Bernardo, Contratos Civiles, Editorial Porrúa, México, 2017, P.343.

transportes, etc.) y banking de apoyo, todo ellos en condiciones de seguridad y confidencialidad razonables."[52]

En cuanto a contrato electrónico el Jurista Julio Téllez refiere que "*Contrato informático en sentido estricto o contrato electrónico es la transacción de bienes y servicios que se hace a través de la tecnología informática*."[53]

Otra definición es propuesta por el Autor Davara Rodríguez:

"*Es aquel en el que una empresa ofrece sus servicios por internet y el usuario los adquiere por vía electrónica a través de la red; es decir, aquel contrato en el cual ambas partes manifiestan su deseo de contratar por medios electrónicos*"[54]

En este orden de ideas es conveniente considerar a la fianza electrónica como el contrato electrónico de garantía (concebido a través de medios electrónicos) por el cual una persona se compromete con el acreedor a pagar por el deudor, si éste no lo hace.

Uno de los mecanismos probatorios de la contratación de la fianza es la póliza, la cual podemos definir equiparándola con la definición legal aplicable al seguro, lo anterior atendiendo a lo dispuesto por el Capítulo II La Póliza, de la Ley Sobre el Contrato de Seguro, el cual establece lo siguiente:

"*Artículo 19.- Para fines de prueba, el contrato de seguro, así como sus adiciones y reformas, se harán constar por escrito. Ninguna otra prueba, salvo la confesional, será admisible para probar su existencia, así como la del hecho del conocimiento de la aceptación, a que se refiere la primera parte de la fracción I del artículo 21*."[55]

3.3.1. El dato financiero

"Financiero, ra. (Del fr. financier).

1. adj. Perteneciente o relativo a la Hacienda pública, a las cuestiones bancarias y bursátiles o a los grandes negocios mercantiles.

---

[52] Piaggi, Ana I., El comercio electrónico y el nuevo escenario de los negocios, Revista de la Asociación de Magistrados y Funcionarios de la Justicia Nacional, Buenos Aires No. 23, 1999, p. 77.

[53] Téllez Valdés Julio, Derecho Informático, 4ta Edición; Mc Graw Hill, México, 2000, P. 115 y 123

[54] Davara Rodriguez Miguel Ángel, Manual de Derecho Informático, 4ta Edición Editorial Aranzadi, España. 2001, P. 156.

[55] Ley Sobre el Contrato de Seguro, Diario Oficial de la Federación de 31 de agosto de 1935.

2. 2. m. y f. Persona versada en asuntos financieros."[56]

Es necesario referir la definición de institución financiera prevista en la LPDUSF que advierte en su artículo 2° lo siguiente:

"Artículo 2o.- Para los efectos de esta Ley, se entiende por:

…

***IV.** Institución Financiera, en singular o plural, a las sociedades controladoras, instituciones de crédito, sociedades financieras de objeto múltiple, sociedades de información crediticia, casas de bolsa, especialistas bursátiles, fondos de inversión, almacenes generales de depósito, uniones de crédito, casas de cambio, instituciones de seguros, sociedades mutualistas de seguros, instituciones de fianzas, administradoras de fondos para el retiro, PENSIONISSSTE, empresas operadoras de la base de datos nacional del sistema de ahorro para el retiro, Instituto del Fondo Nacional para el Consumo de los Trabajadores, sociedades cooperativas de ahorro y préstamo, sociedades financieras populares, sociedades financieras comunitarias, y cualquiera otra sociedad que requiera de la autorización de la Secretaría de Hacienda y Crédito Público o de cualesquiera de las Comisiones Nacionales para constituirse y funcionar como tales y ofrecer un producto o servicio financiero a los Usuarios.*

…"[57]

Como se puede observar las Instituciones de Fianzas se consideran por disposición legal como institución financiera en consecuencia los servicios que prestan se reputan como financieros.

De ambas fuentes podemos inferir que un dato financiero es aquel dato relacionado con la Hacienda Pública, bancaria o bursátil o, en su caso, relacionada a grandes negocios mercantiles, como lo es la fianza.

En ese orden de ideas es importante verificar en que esfera se encuentra el dato financiero, dentro de las tres clasificaciones de datos personales a saber: Información íntima, información privada o información pública.

---

[56] Diccionario de la Real Academia de la Lengua Española, portal electrónico. https://dle.rae.es/financiero consultado el 11-09-2019.

[57] Ley de protección y defensa de los usuarios de servicios financieros, Diario Oficial de la Federación de 10-01-2014.

Antes de continuar, es importante identificar que existen dos o vertientes que reflejan datos financieros, no obstante, la que se plantea en el presente trabajo de investigación es solo una de ellas:

1.- Vertiente de Derecho Administrativo: Relación jurídica entre los prestadores de servicios financieros y los organismos de gobierno que los regulan (comisiones nacionales), la cual no es objeto del presente trabajo de investigación pero que se considera importante diferenciar de la que sí.

2.- Vertiente de Derecho Mercantil: Relación jurídica entre usuarios y prestadores de servicios financieros. Ejemplo cuentahabiente y una institución de crédito o usuario de un servicio prestado por una institución afianzadora.

En este sentido los datos financieros los podemos definir como aquella información con la que podemos saber el estado del patrimonio económico de una persona, su variación o composición a una fecha determinada o en un periodo de tiempo.

En consecuencia, la información que es tratada por las instituciones afianzadoras es considerada como dato financiero, dato que por sí mismos pueden o no identificar a un usuario o ciudadano pero que en sí, refiere un contenido patrimonial.

Analizado lo antes expuesto es conveniente referir que cualquier elemento, información, dato personal, contenido o vinculado a la emisión de una póliza de fianza por una institución afianzadora debidamente constituida, se reputa como dato financiero, por lo que, en ese orden de ideas, y se encuentra inmerso dentro de la esfera de la información privada.

Atento a lo anterior, resulta trascendental analizar la obligación de las instituciones afianzadoras en su carácter de sujetos responsables y, en su caso, del encargado, respecto a la implementación de las medidas de seguridad técnicas que refiere la LGPDPPSO.

“Artículo 3. Para los efectos de la presente Ley se entenderá por:

…

XX. Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;

XXI. Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;

XXII. Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

XXIII. Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;

…"[58]

En este contexto se advierte que las instituciones afianzadoras como sujetos obligados, se encuentran constreñidas a implementar todas las medidas de seguridad en cualquiera de las acepciones referidas en el citado artículo 3 de la LGPDPPSO (administrativas, técnicas y físicas), para garantizar la debida protección de los datos financieros de sus clientes, obligados solidarios, fiados y beneficiarios, sujetos a la relación contractual de la fianza.

3.3.2 Elementos personales de la fianza

El fiador, esto es, la institución afianzadora, la cual solo puede ser una sociedad anónima que cuente con la autorización de, anteriormente la SHCP, actualmente la CNSF, su principal función es expedir fianzas, mediante el pago de una prima. Son instituciones que se encuentran estrictamente reguladas en su constitución, funcionamiento y vigilancia por la Comisión referida, lo anterior con el din ultimo de procurar el sano desarrollo del sistema afianzador mexicano.

Entre las principales obligaciones se encuentran el expedir las pólizas de fianza y el pago de suma afianzada, la cual debe realizarse en el momento de hacerse exigible la obligación garantizada, en contraposición, las mismas tienen el derecho a cobrar una prima y se constituye un derecho de regreso, esto es todo lo que pague la institución a nombre del fiado deberá serle restituido.

El solicitante o fiado, que puede ser cualquier persona física o moral, y es quien contrata generalmente la fianza y de manera general quien paga la prima para que se garantice la obligación que asumirá.

El beneficiario, es cualquier persona física o moral acreedora de la obligación garantizada mediante la fianza, es a quien se le garantiza el cumplimiento de la obligación del fiado.

[58] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Diario Oficial de la Federación de 26 de enero de 2017.

Puede existir un elemento personal adicional, consistente en el obligado solidario, toda vez que la normativa obliga a las instituciones afianzadoras a constituir las garantías suficientes de recuperación en atención al derecho de regreso de la institución afianzadora. El obligado solidario aporta parte de su patrimonio para ayudar al fiado en el caso de incumplimiento y pago de la institución afianzadora.

Existe un elemento personal externo, esto es que no juega un papel directo en la relación contractual, se trata del agente de fianzas, el cual es la persona que cuenta con los conocimientos técnicos y debidamente autorizado para intermediar fianzas.

Con la siguiente figura se ilustra el papel que desempeñan los elementos personales, advirtiendo una dualidad contractual.

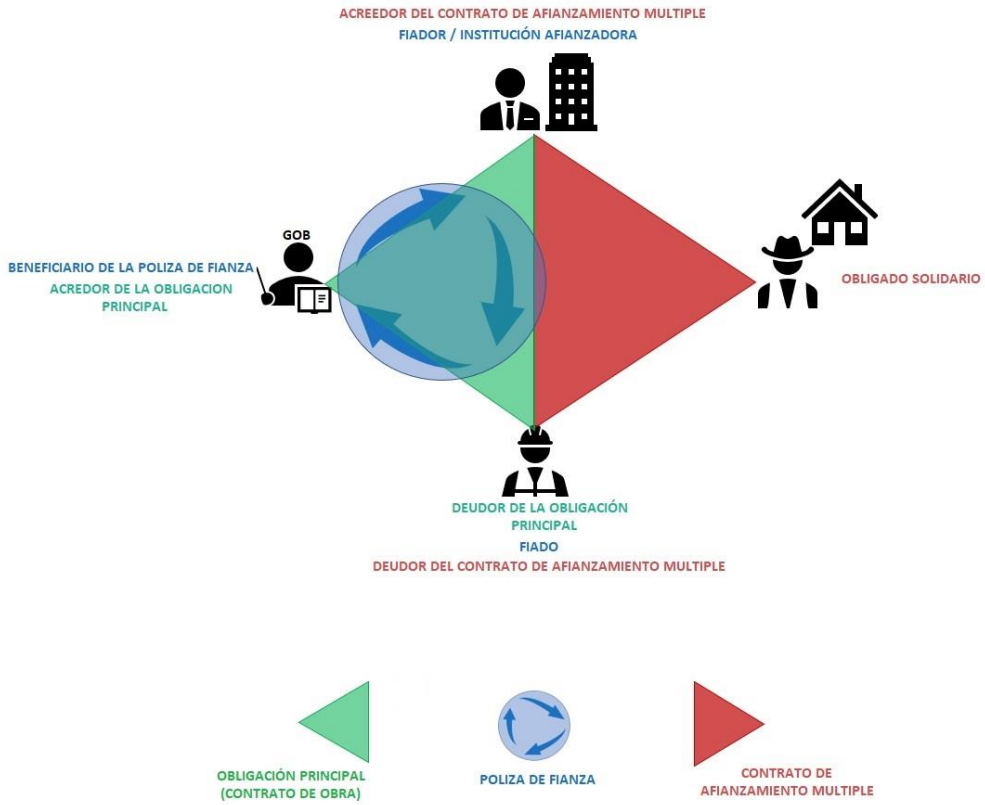

Figura 1 *Elementos personales de las relaciones contractuales vinculadas con la fianza.* FUENTE: Elaboración propia.

3.3.3 Elementos materiales y formales

Continuando con el análisis de la póliza de fianza, el Maestro Octavio Guillermo Sánchez Flores señala que en términos generales las pólizas de fianzas deben contener:

- *"Denominación y domicilio de la Institución*
- *Número de orden*
- *Importe de la prima y pago de derechos*
- *Plazo de vigencia*
- *Descripción de la obligación garantizada*
- *Nombre del beneficiario o acreedor*
- *Nombre del fiador*
- *Fecha en que se expide y*
- *Firma del presentante legal de la Institución"*[59]

El último aspecto referido cobra relevante importancia atendiendo a que, si la celebración del contrato se realiza a través de medios electrónicos, en consecuencia, deberá contener una firma electrónica, la cual será analizada más adelante.

A fin de que una fianza exista en el mundo jurídico produzca plenos efectos legales deberá atender a los siguientes elementos de existencia y validez.

3.3.4 Elementos de existencia

Los elementos de existencia, como en cualquier contrato son consentimiento y objeto.

Consentimiento: consiste en el acuerdo de voluntades entre la institución afianzadora y el solicitante o contratante o fiado, independientemente del pago de la prima.

Dicho consentimiento manifestado mediante sistemas, plataformas o equipos informáticos resulta imprescindible para el perfeccionamiento del contrato, por lo que deberá atenderse a las disposiciones legales nacionales propias de los medios

[59] Sánchez Flores Octavio Guillermo de Jesús, Ob. Cit. P.527.

electrónicos y en su caso a las disposiciones que en materia de comercio internacional lo prevean.

Objeto: El objeto en la fianza será la conducta del fiador manifestada como una prestación de dar o hacer a nombre del fiado, propiamente es garantizar el cumplimiento de una obligación.

La existencia de la obligación principal constituye un pilar importante para la vida de la fianza, toda vez que al ser un contrato accesorio siempre seguirá la suerte del principal.

3.3.5 Elementos de validez

Sobre los elementos de validez de la fianza electrónica podemos referir a la capacidad entendida como tal a la aptitud de las personas para ser titulares de derechos y sujetos de obligaciones. La ausencia de vicios del consentimiento, que refiere a que el mismo debe estar libre de aquellas circunstancias que sin suprimirlo lo afectan y son: el error, la falsa apreciación de la realidad el dolo, la mala fe, violencia y la lesión, la licitud en el objeto, motivo o fin del contrato, puesto que debe ser lícito y además de posible. Al respecto es importante referir que dicha aptitud o capacidad debe ser obtenida mediante autorización otorgada por la CNSF para constituirse y operar como Institución Afianzadora.

3.3.6 Elementos reales

Obligación garantizada, la cual consistente en que pueden garantizarse toda clase obligaciones, es propiamente el compromiso de pagar una suma de dinero, independientemente de que, como ya se explicó, tratándose de obligaciones de hacer, las instituciones de fianzas pueden sustituir al deudor principal en el cumplimiento de dicha obligación por si o inclusive hasta constituyendo un fideicomiso.

3.3.7 Elementos de validez

De lo antes señalado merece especial atención la capacidad de la parte fiadora, toda vez que requiere capacidad especial, consistente en la autorización de la

Comisión Nacional de Seguros y Fianzas (CNSF) para operar como institución afianzadora como lo prevé el artículo 11 de la LISF.

3.4 Manifestación del consentimiento para el perfeccionamiento de la fianza

La Circular Única de Seguros y Fianzas (CUSF), en su Capítulo 4.12. "Del registro de firmas de representantes de las instituciones para suscribir fianzas.", refiere que las Instituciones tienen la obligación de registrar a sus funcionarios que cuenten con facultades para suscribir dichas fianzas, ya sea con firma autógrafa o electrónica, con lo cual se manifiesta el consentimiento de la institución para asumir y garantizar una obligación.

Este apartado lo debemos iniciar analizando lo dispuesto en artículo 1803 del Código Civil Federal.

"Artículo 1803.- El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente:

I.- Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y

II.- El tácito resultará de hechos o de actos que lo presupongan o que autoricen a presumirlo, excepto en los casos en que por ley o por convenio la voluntad deba manifestarse expresamente."[60]

Derivado de lo anterior se desprende que la manifestación del consentimiento se tiene como legalmente manifestado cuando se expresa mediante medios electrónicos, y dentro de dicho ámbito encontramos a la firma electrónica como herramienta o medio que, por excelencia, permite estos efectos.

La Real Academia de la Lengua define la firma como: : *"Nombre y apellidos escritos por una persona de su propia mano en un documento, con o sin rúbrica, para darle autenticidad o mostrar la aprobación de su contenido."* [61]

[60] Código Civil Federal. Diario Oficial de la Federación 26 de mayo, 14 de julio, 3 y 31 de agosto de 1928.
[61] Diccionario de la Real Academia de la Lengua Española portal electrónico. https://dle.rae.es/?w=internet consultado el 10-10-2019.

Otra acepción refiere al rasgo o conjunto de rasgos, realizados siempre de la misma manera, que identifican a una persona y sustituyen a su nombre y apellidos para aprobar o dar autenticidad a un documento. [62]

El vocablo de firma proviene del latín "Firmare" que significa afirmar, dar fuerza y el vocablo "autógrafa" significar grabar o escribir por sí mismo y se aplica al escrito de mano de su propio autor en el entendido que los signos o trazos han de ser hechos por la mano del autor sin que la impresión se realice por medios mecánicos. [63]

Otra acepción sobre la misma refiere que "*es el conjunto de letras y signos entrelazados que identifican a la persona que la estampa, con un documento o texto*"[64]

"La firma consiste en asentar al pie de un acto jurídico escrito, el nombre y apellido de la persona que los expide, en forma, en que acostumbra hacerlo, con el propósito de dar autenticidad y firmeza al acto de que se trate." [65]

El jurista Reyes Kraft refiere que "*en su aspecto jurídico la firma autógrafa implica el hecho de tratarse de una inscripción manuscrita, realizada de una manera particular, hecha con el ánimo de obligarse al reconocimiento del escrito en que se estampe."* [66]

La finalidad de la firma es proporcionar seguridad jurídica a los particulares, de que el firmante ha aceptado expresamente el contenido del documento y que es responsable del contenido del mismo.

"Según el criterio de la Suprema Corte de Justicia menciona que la firma puede estar constituida por los caracteres, signos o nombre que use o estampe determinada persona, en un documento para obligarse a responder del contenido de ese documento, o para hacer constar que ha recibido alguna cosa." [67]

---

[62] Ibidem
[63] Enciclopedia Jurídica Omeba, Tomo XII, Editorial Bibliográfica Argentina, pp. 290-293
[64] Acosta Romero Miguel, Nuevo Derecho Mercantil. Ed. Porrúa. 1era. Edición, México, 2000, P. 537.
[65] Díaz González Luis, Documentación y Firma electrónica, Revista Nuevo Consultorio Fiscal, No. 344. 2003 México.
[66] Reyes Kraft Alfredo Alejandro, La firma electrónica y las entidades de certificación. Tesis de Doctorado, 2002, P. 135.
[67] Ibidem P. 49

Como se aprecia la firma es un "*signo escrito que una persona anota de su puño y letra en cierto documento y que, al hacerlo así, acepta el contenido del mismo. El asentamiento antes señalado le otorga autenticidad al documento, máxime si proviene de un servidor público en ejercicio de sus funciones*." [68]

Existen diversas clases de firmas: autógrafa, en facsímil, mecánica, de la persona física, de la persona jurídica colectiva, con lápiz o con tinta, con otros instrumentos de escritura, y electrónica, entre otras.

"*En algunas ocasiones la firma constituye el nombre y los apellidos o alguno de éstos, manuscritos de manera particular, o bien, de una o dos iniciales más un apellido, así como rasgos diversos."* [69]

"La firma acredita la autoría del documento suscrito normalmente al pie del mismo y representa la formalización del consentimiento y la aceptación de lo expuesto, y es por tanto origen de derechos y obligaciones. La firma será válida siempre que no sea falsificada o se haya obtenido con engaño, coacciones o de cualquier otro ilícito proceder." [70]

Características de la firma.

De acuerdo al Dr. Reyes Kraft se pueden identificar tres características de la firma: Identificativa, declarativa y probatoria. La primera con la *finalidad de identificar quien es el autor del documento, la Declarativa refiere a hacer propio o asumir el contenido de un documento, constituyéndose como el signo principal que representa la voluntad de obligarse*, y por último la *Probatoria que permite identificar si el autor de la firma es efectivamente aquel que ha sido identificado como tal en el acto de la propia firma*.[71]

Elementos de la Firma:

En cuanto a los elementos de la firma podemos referir a los elementos formales y funcionales.

---

[68] Diaz Gonzalez, Luis Raúl, Diccionario Jurídico para Contadores y Administradores. 5ta Edición, Editorial Gasca, 2012.
[69] Ibidem P. 135
[70] Cuervo Alvarez José, Las Instrucciones de la Agencia y las Entidades de Crédito. Las Instrucciones de la Agencia y las Entidades de Crédito - Informática Jurídica (informatica-juridica.com) consultado el 07-09-2019.
[71] Reyes Kraft Alfredo Alejandro, La firma electrónica avanzada. P. 11.

Los elementos formales se relacionan con el ánimo signandi o ánimo de asumir el contenido de un documento y en consecuencia obligarse y la firma como signo personal referente a un distintivo propio.

Los elementos funcionales se relacionan con una función indicadora y una función de autenticación:

La función indicadora se refiere al enlace que se plantea entre el acto de firmar y la persona que ha firmado.

En relación con la función de autenticación, esta refiere a que el firmante manifiesta su consentimiento asumiendo el contenido y haciéndolo propio.

Atendiendo a lo anterior, el Dr. Reyes Kraft dispone que "*La función primordial de la firma no es la identificación del firmante, si no la de ser instrumento de su declaración de voluntad, que exige esa actuación personal del firmante en la que declara que aquello es un documento y no un proyecto o un borrador, que el documento está terminado y declara que el firmante asume como propias las manifestaciones, declaraciones o acuerdos que contiene.*"[72]

3.5 Firma electrónica

El Fiador u oferente del servicio de garantía, es quien genera un mensaje de datos que es representado a través de la figura de la póliza. Dicho mensaje de datos deberá contener indudablemente la manifestación del consentimiento del representante de la Institución afianzadora, esto es, una firma electrónica.

"La firma electrónica surgió debido a la necesidad de un mundo globalizado en donde las transacciones y la interacción entre individuos son impersonales y sin vínculos físicos, haciendo de la identificación un problema y requerimiento de primera necesidad." [73]

"*La firma electrónica técnicamente, es un conjunto o bloque de caracteres que viajan a un documento, fichero o mensaje y que puede acreditar cuál es el autor*

[72] Ibidem P. 12.
[73] Reyes Kraft Alfredo Alejandro, La firma electrónica y las entidades de certificación. Tesis de Doctorado, 2002, P. 164.

o emisor del mismo (lo que se denomina autenticación) y que nadie ha manipulado o modificado el mensaje en el transcurso de la comunicación (o integridad)". [74]

Para el autor Del Peso Navarro:

"*Es una señal digital representada por una cadena de bits que se caracteriza por ser secreta, fácil de reproducir y de reconocer, difícil de falsificar y cambiante en función del mensaje y en función del tiempo, cuya utilización obliga a la aparición de lo que denomina fedatario electrónico o telemático que será capaz de verificar la autenticidad de los documentos que circulan a través de las líneas de comunicación, al tener no solamente una formación informática, si no también jurídica."*[75]

Así pues, "*es el conjunto de datos en forma electrónica, ajenos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge"* [76]

3.6 Firma electrónica avanzada

Para poder hablar de este tema, debemos hacer un pequeño análisis de la manera en que se genera este tipo de firma.

Todo parte del hecho de que "*las firmas electrónicas consisten básicamente en la aplicación de algoritmos de encriptación a los datos, de esta forma, solo serán reconocibles por el destinatario, el cual además podrá comprobar la identidad del remitente, la integridad del documento, la autoría y la autentificación, preservando al mismo tiempo la confidencialidad"*[77], todo esto mediante lo que se ha denominado como clave pública y clave privada.

---

[74] Ibidem P. 244.
[75] Del Peso Navarro Emilio. Resolución de conflictos en el intercambio electrónico de documentos. Cuadernos de Derecho Judicial. Escuela Judicial / Consejo General del Poder Judicial, Madrid, 1996, P. 191.
[76] Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica. Portal electrónico REAL DECRETO-LEY 14/1999, de 17 de septiembre, sobre firma electrónica. - BOE. Boletín Oficial del Estado - Legislación - VLEX 15036082. Consultado el 10-10-2019.
[77] Cuervo Alvarez, José, La Firma Digital y Entidades de Certificación. Portal electrónico La Firma Digital y Entidades de Certificación - Informática Jurídica (informatica-juridica.com). Consultado el 10-10-2019.

"Las claves no son otra cosa que una combinación de letras y números, es decir un conjunto de bits, que a su vez constituyen un conjunto de ceros y unos"[78].

Para que la firma se considere avanzada esa debe de ir avalada por un certificado.

La firma electrónica avanzada posee además cuatro cualidades que garantizan su seguridad: Integridad, no repudio, autenticidad y confidencialidad.

Por integridad nos referimos a que el mensaje original no puede ser modificado por un tercero; no repudio refiere que el autor del mensaje no puede decir que no lo hizo; autenticidad refiere a que el emisor del mensaje queda acreditado y su firma electrónica avanzada tiene la misma validez que una firma autógrafa y por último, confidencialidad la cual refiere que la información contenida en el mensaje se encuentra en código, por lo que solo el receptor designado puede descifrar el mensaje.

Otra definición general de firma electrónica avanzada que podemos referir es la siguiente:

"La firma electrónica avanzada son aquellos datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, utilizados para identificar al firmante en relación con el mensaje de datos, siempre que cuenten con un certificado expedido por el Servicio de Administración Tributaria o, en su caso, por un prestador de servicios de certificación autorizado por el banco de México.[79]

De las definiciones anteriores se observa un elemento importante al que se hace referencia, se trata del "*documento electrónico o informático, se concibe como un medio de expresión de voluntad con efectos de creación, modificación o extinción de derechos y obligaciones por medio de la electrónica".* [80]

De esta manera analizando las definiciones se puede establecer en términos generales *que "una firma electrónica sería cualquier método o símbolo basado en*

---

[78]Mauricio Devoto, Comercio Electrónico y Firma Digital, Buenos Aires, Editorial La Ley S.A. 2001, P. 205

[79] Firma electrónica Avanzada, Portal https://www.sat.gob.mx/ Preguntas frecuentes. Consultado el 10-10-2019.

[80] Barriuso Ruiz, Carlos, La contratación electrónica. Editorial Dykinson, S.L., Tercera Edición, España, 2006, P. 367.

medios electrónicos" [81] utilizados para autenticar un documento, que además cumple algunas funciones de la firma manuscrita.

La firma electrónica permite a los autores "*el servicio de autentificación (verificación de la autoridad del firmante para estar seguro de que fue él y no otro el autor del documento) y no de repudio (seguridad de que el autor del documento no puede retractarse en el futuro de las opiniones o acciones asignadas en el).*

Quizás la parte que más interesa a los usuario es la garantía de detección de cualquier modificación de los datos firmados, proporcionando una integridad total ante alteraciones fortuitas o deliberadas durante la transmisión telemática del documento firmado. El hecho de la firma sea creada por el usuario mediante medios que mantienen bajo su propio control (clave privada protegida, la contraseña, tarjeta, chip, etc.) asegura la imposibilidad de efectuar de lo que se conoce como suplantación de personalidad." [82]

Por tanto, la firma electrónica garantiza, así a cualquiera que reciba el documento y sea capaz de descifrarlo con la clave pública del firmante, la identidad del emisor y que el contenido del documento no ha sido alterado durante la transmisión, así como la fecha y hora en que ha tenido lugar.

De esta manera la firma electrónica consigue, iguales e incluso superiores efectos que la tradicional firma manuscrita, pues da integridad, autenticidad y evita el problema del rechazo o negación.

3.7 Elementos de la Firma Electrónica

Básicamente son los mismos elementos que componen el concepto de la firma manuscrita, aunque de este tipo de firma resaltan los siguientes:

La autenticidad

La integridad

La fecha

La hora y

[81] Cuervo, José, La Firma Digital y Entidades de Certificación. Portal José Cuervo Alvarez, Autor en Informática Jurídica (informatica-juridica.com). Consultado el 10-10-2019.
[82] Reyes Kraft Alfredo Alejandro, La firma electrónica. 2002, P. 14.

La recepción

De lo anterior se desprenden otros elementos, así como su concepto que son de gran ayuda para establecer los siguientes parámetros:

- Inalterabilidad: significa que la información no se puede alterar cuando la misma es almacenada. La firma digital no impide que la información se altere, si no que detecta si esta ha sido alterada.

- Perdurabilidad: significa que la información perdure en el tiempo y es una cualidad del medio de almacenamiento. La información que perdura en el tiempo debe ser archivada en un medio perdurable. [83]

Con estos parámetros se observa que los riesgos más importantes del uso de sistemas electrónicos y telemáticos pueden ser resumidos en cuatro:

1.- Que el autor del mensaje haya sido suplantado.

2.- Que el mensaje sea alterado.

3.- Que el emisor del mensaje niegue haberlo transmitido o el destinatario recibido no rechazado al igual que ocurre con las notificaciones escritas.

4.- Que el contenido del mensaje es elegido por una persona no autorizada a continuación se muestra un cuadro que resulta útil para establecer la distinción entre la firma autógrafa electrónica.

La firma electrónica permite tener la certeza absoluta de que la persona que envía el documento electrónico es quien dice ser. Por tal motivo se observa que la firma electrónica consiste en cifrar un resumen del contenido del documento, extraído mediante un algoritmo que asegura la unicidad del resumen con la clave privada del firmante que incluyen la fecha y hora.

[83] Arce Alfonso José, Diaz Lannes Federico Santiago, Revista Ponencia, Portal SAIJ - La firma digital. Aspectos jurídicos. Su aplicación a las comunicaciones previstas por la ley 22.172 Consultado el 10-10-2019.

Capítulo 4.

Riesgo en la operación de las Instituciones de Fianzas a través de medios electrónicos

Capítulo 4. Riesgo en la operación de las Instituciones de Fianzas a través de medios electrónicos

4.1 ¿Cuándo es vinculante la póliza en la que se documenta una fianza?

El cuestionamiento planteado parece fácil de resolver, ya que los elementos que formalmente deben agotarse para identificar cuando una póliza es o no vinculante deben constreñirse teóricamente a la manifestación del consentimiento para asumir una obligación.

Dicha manifestación del consentimiento vía electrónica refiere el punto álgido y objeto del presente trabajo de investigación, por la posibilidad de verse falseada con el uso de herramientas tecnológicas novedosas.

No es suficiente para abordar esta problemática, el referirnos únicamente a los ilícitos que se actualizarían con la realización de una conducta, es importante abordar los temas relacionados con las partes que se ven involucradas y afectadas por esta conducta y las situaciones que favorecen dicha situación.

¿Cómo se demuestra que una póliza es atribuible a una Institución? En este punto habrá que diferenciar los procesos de expedición que se basan en una constancia escrita y los procesos que se basan en la generación de archivos y registros digitales (póliza electrónica) en donde la informática forense juega un importante papel.

Para que una póliza sea considerada auténtica, deberá atenderse a que la misma, haya cumplido con los requisitos legales, y adicionalmente con los establecidos por la institución.

En la práctica, los procesos de expedición digital, con independencia del medio de reproducción, deben ser congruentes con los registros en los sistemas administrativos y contables, para la consecuente expedición por parte de la Institución.

¿Por qué en los procesos digitales no se menciona la idea de la originalidad del formato de impresión?

Tratándose de nuevas tecnologías, la voluntad del fiador consta en el archivo o registro digital, por ello es intrascendente que la póliza apócrifa se maquile en “papel original”. Este papel, es un mero formato de impresión para “reproducir” el archivo digital o póliza digital.

Las pólizas electrónicas no serán auténticas y en consecuencia vinculantes, por el simple hecho de estar impresas en papel oficial. Serán auténticas en tanto obre un archivo digital con los datos específicos de la fianza, congruentes con los sistemas electrónicos institucionales para su emisión.

En atención a lo planteado, se puede discernir que nos encontramos ante un panorama dividido, por una parte, los usuarios de fianzas pretenden comprobar la validez de la garantía con la exhibición de una póliza de fianza, como cuando se pretende comprobar la propiedad de un bien, exhibiendo la factura.

Por otra parte, las instituciones refieren que una fianza electrónica será válida si existen registros contables y administrativos de la emisión de la misma, esto quiere decir, que las instituciones se pronunciarán sobre que póliza es válida y vigente y cual no.

La implementación de las tecnologías de la Información u comunicación, además de ofrecer múltiples beneficios en las operaciones de las instituciones afianzadoras, también presuponen riesgos, entre los cuales podemos advertir: el acceso no autorizado a sistemas informáticos exponiendo con ello los datos financieros, intervención en líneas de comunicación, sustracción o copiado de información privada o confidencial, aprovechamiento indebido o violación de códigos para acceso a sistemas, desviación de dinero hacia cuentas bancarias, daño en el funcionamiento de los sistemas, destrucción de información o daño en programas o memoria de computadoras y por último, en el caso que nos ocupa: la falsificación de documentos vía computarizada.

Es materia del presente capitulo analizar algunos apartados relevantes en cuanto al uso de las TIC por parte de Instituciones y las herramientas tecnológicas idóneas para hacer frente a los riesgos antes descritos.

4.2 Prueba pericial en informática forense

Es trascendental acreditar que la póliza electrónica vincula o no a la institución afianzadora de que se trate, para estos efectos se prevé como medio de prueba pericial la relativa a informática forense, medio de prueba por excelencia para determinar la emisión y, en su caso manipulación de la póliza de fianza electrónica.

4.2.1 La informática forense como herramienta para hacer frente a los riesgos operativos y de emisión de pólizas de fianzas

La informática forense se erige como una disciplina auxiliar para la impartición de la justicia moderna, su efectividad depende del entendimiento de nosotros, los usuarios de los sistemas electrónicos, respecto de lo que puede y no puede lograr, en este orden de ideas si desconocemos las bondades de la misma, difícilmente alcanzaremos nuestros objetivos legales en un procedimiento judicial, por lo que resulta imprescindible la formación técnico legal de un abogado.

"Según el FBI, la informática forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional."[84]

La informática forense forma parte de la seguridad en cómputo que se integra de procesos y técnicas para brindar integridad en los sistemas informáticos, buscando prevenir ataques de manera proactiva y reactiva. La primera refiere a componentes físicos o lógicos como firewalls, detectores de intrusos y controles de acceso. En cuanto a la segunda se refiere a planes de contingencia, respaldos.

Como última finalidad, se puede mencionar que lo es la obtención de evidencia para fincar responsabilidad judicial al autor de un delito informático como la falsificación y/o fraude.

Como se ha referido la informática forense persigue la identificación, preservación, extracción, análisis, interpretación documentación y presentación de las pruebas o evidencia recabadas en un contexto tecnológico.

[84] Portal electrónico https://www.ecured.cu/Inform%C3%A1tica_Forense Consultado el 15 de septiembre de 2019.

En relación con la evidencia digital la podemos interpretar como cualquier dato o registro con características como volátil, anónimo, duplicable, alterable o eliminable y que es creado y almacenado en un sistema de cómputo, que se requiere para ser aportado dentro de un procedimiento judicial, y que, como característica puede ser volátil, anónima, duplicable, alterable y eliminable.

Así pues, la informática forense podrá dividirse en computación forense, forensia de redes y la forensia digital.

En cuanto a computación forense se refiere, se puede intuir que es la disciplina especializada atendiendo a elementos propios de equipos de cómputo, para el análisis e interpretación de la información contenida en el mismo.

En cuanto a la forensia de redes, se puede precisar que refiere a la actividad desarrollada por el profesional en relación a las operaciones de redes de computadores para la persecución o rastreo de movimientos y acciones desplegadas para la comisión de un ilícito.

En cuanto a la forensia digital, la misma se asemeja a la computación forense, pues tiene la finalidad de apoyar en la administración de justicia en relación con eventos que podrían calificarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a acciones internas de las organizaciones para la implementación de protocolos de seguridad informática.

De la informática forense podemos distinguir que persigue 3 objetivos: la compensación del daño ocasionado por la comisión de un delito cometido vía electrónica, la persecución y en su caso procesamiento del delincuente y por último establecer medidas o mecanismos preventivos o de seguridad.

Lo anterior con el propósito de preservar los datos, instrumentos o dispositivos electrónicos a través de los cuales se cometió el ilícito, o en su defecto recuperar información que aporte indicios para establecer la responsabilidad o autoría de un ilícito.

Se pretende analizar los sistemas que han recibido algún tipo de daño, su reparación, recolección y análisis de la evidencia digital y consecuente persecución y procesamiento judicial.

Para los fines que persigue la informática forense existen diversas herramientas tecnológicas, como lo es el análisis del sistema o plataforma operativa (sistema operativo), búsqueda de datos manteniendo integridad de los mismos, programas de recuperación de datos previamente borrados en medios magnéticos, reparación y visualización de ficheros y directorios dañados, rastreo de direcciones IP, URLs e inclusive correos electrónicos, análisis de la actividad de navegadores de internet, análisis de puestos del equipo de cómputo, etc.

Sobre dichas herramientas podemos mencionar “Encase”, “Handy Recovery”, “Aida32”, “Visual Route”, entre otros.

Como ejemplo podemos mencionar “Encase” el cual usa el algoritmo HASH MD5 (Message Digest 5) para hacer una comparación de ficheros y comprobar la integridad de los mismos. Con este algoritmo podemos tener la certeza de que la información que estamos manejando es exactamente igual a la original y que los ficheros no han sido modificados ni corrompidos en ningún momento.

No debemos olvidar que debemos identificar y tratar por separado dos aspectos importantes. En cuanto a la materia mercantil: el perito en informática forense podrá pronunciarse respecto a la autenticidad de un archivo .xml y su representación gráfica .pdf. En cuanto a la a materia penal: el informático forense deberá establecer la cadena de custodia e investigar para atribuir la comisión del delito de falsificación de un documento privado.

Adicionalmente debemos referir lo relativo a las cadenas de custodia, para lo cual se deberá observar el “Acuerdo A/009/15 por el que se establecen las directrices que deberán observar los servidores públicos que intervengan en materia de cadena de custodia.” Publicado en el Diario Oficial de la Federación el 12 de febrero de 2015, el cual abroga el “El Acuerdo número A/002/10 mediante el cual se establecen los lineamientos que deberán observar todos los servidores públicos para la debida preservación y procesamiento del lugar de los hechos o del hallazgo y de los indicios, huellas o vestigios del hecho delictuoso, así como de los instrumentos, objetos o productos del delito.” publicado el 3 de febrero de 2010.

Por último, no se omite referir que la prueba pericial en materia de informática forense y el informe emitido por peritos expertos en sistemas, deberá describir y

explicar el proceso que lleva a cabo la institución de fianzas para la creación del archivo digital.

Dicha relación será trascendental para los resultados que se persiguen (acreditar que la póliza es apócrifa), validando con ello las medidas de seguridad de los sistemas informáticos empleados para la emisión de pólizas, con la finalidad de que el personal a cargo de la investigación por parte de la autoridad ministerial determine si la póliza tachada de apócrifa tiene algún registro de emisión en el sistema de la institución.

Por otra parte, es importante abordar las medidas adoptadas tanto por la Administración Pública como por las entidades que integran el Sistema Financiero Mexicano para hacer frente a los riesgos de operación a través de medios electrónicos.

4.3 Bases de coordinación en materia de seguridad de la información

Las bases de coordinación en materia de seguridad de la información[85] emitidas el 24 de mayo de 2018, "*son el instrumento de colaboración entre las instancias públicas, las asociaciones gremiales y las entidades pertenecientes al sistema financiero mexicano.*

En dicho documento se acordó, entre otras cosas:

Las autoridades financieras mantendrán una coordinación efectiva entre ellas, así como implementar mediante la regulación correspondiente los principios básicos en materia de seguridad de la información, tomando en cuenta las mejores prácticas internacionales.

Asimismo, las autoridades financieras acordaron la creación del Grupo de Respuesta a Incidentes Sensibles de Seguridad de la Información (GRI), el cual tiene por objeto coordinar las acciones para dar respuesta a incidentes sensibles de seguridad, así como el intercambio de información entre las partes." [86]

[85] Bases de Coordinación en Materia de Seguridad de la Información, Portal electrónico https://www.gob.mx/cms/uploads/attachment/file/332698/Ciberseguridad-Bases_Coordinacion.pdf consultado el 07-09-2019.
[86] Ibidem.

Por su parte las entidades acordaron la creación de un equipo interno de identificación y respuesta a incidentes sensibles de seguridad de la información, estableciendo una estrategia de comunicación para proveer información clara, oportuna y relevante a los clientes.

Las bases de coordinación fueron firmadas por parte de las autoridades financieras por la Secretaría de Hacienda y Crédito Público (SHCP), Banco de México (BANXICO), (Comisión Nacional Bancaria y de Valores (CNBV), Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), Comisión Nacional del Sistema de Ahorro para el Retiro (CONSAR), CNSF y Procuraduría General de la República (PGR), ahora Fiscalía General de la República (FGR). Por parte de las asociaciones gremiales, la Asociación de Bancos de México (ABM), Asociación Mexicana de Instituciones Bursátiles (AMIB), Asociación Mexicana de Instituciones de Seguros (AMIS), Asociación Mexicana de Instituciones de Garantías (AMIG), Asociación Mexicana de Afores (AMFORE), Asociación Mexicana de Sociedades Financieras Populares (AMSOFIPO), Asociación de Almacenes Generales de Depósito (AAGEDE), Asociación de Sociedades Financieras de Objeto Múltiple (ASOFOM), Asociación FinTech México, Asociación de Plataformas de Fondeo Colectivo (AFICO) y la Confederación de Cooperativas de Ahorro y Préstamo de México (CONCAMEX). [87]

Las autoridades que integran el Sistema Financiero Mexicano junto con las entidades que lo integran, impulsan el desarrollo de herramientas y prácticas para enfrentar los riesgos cibernéticos, en este sentido y en común acuerdo, dentro del primero foro sobre seguridad denominado “Fortaleciendo la ciberseguridad para la estabilidad del Sistema Financiero Mexicano” celebrado el 23 de octubre de 2017, firmaron los “Principios para el fortalecimiento de la ciber seguridad para la estabilidad del Sistema Financiero Mexicano” [88] donde tanto sector público como privado establecieron los siguientes principios:

[87] Perez Márquez Fernando, Riesgo Cibernético y Ciberseguridad, Documento de Trabajo No. 181, SHCP, CNSF, 2019 Portal electrónico https://www.gob.mx/cms/uploads/attachment/file/478193/181._Riesgo_Cibern_tico_y_Ciberseguridad_2019.pdf, consultado el 07-09-2019.
[88] Ibidem.

"1. Adoptar y mantener actualizadas las políticas, métodos y controles para identificar, evaluar, prevenir y mitigar los riesgos de ciber seguridad que se autoricen por los órganos de gobierno de mayor decisión y permeen todos los niveles de organización.

2. Establecer mecanismos seguros para el intercambio de información entre los integrantes del sistema financiero y las autoridades sobre ataques ocurridos en tiempo real y su modo de operación, estrategias de respuesta, nuevas amenazas, así como del resultado de investigaciones y estudios que permitan a las entidades anticipar acciones para mitigar los riesgos de ciberataques: lo anterior, protegiendo la confidencialidad de la información.

3. Impulsar iniciativas para actualizar los marcos regulatorios y legales que den soporte y hagan converger acciones y esfuerzos de las partes considerando las mejores prácticas y acuerdos internacionales.

4. Colaborar en proyectos para fortalecer los controles de seguridad de los distintos componentes de las infraestructuras y plataformas operativas que soportan los servicios financieros del país, promoviendo el aprovechamiento de las tecnologías de información para prevenir, identificar reaccionar, comunicar, tipificar, y hacer un frente común ante las amenazas presentes y futuras.

5. Fomentar la educación y cultura de ciberseguridad entre los usuarios finales, y el personal de las propias instituciones que, a través de una capacitación continua, redunde en una participación activa para mitigar los riesgos actuales de ciberataques."[89]

De igual manera se establecieron los siguientes elementos que, de acuerdo a dichas bases, fueron emitidos en octubre de 2016 por los ministros de finanzas y gobernadores de los bancos centrales de los países que integran el G7:

"*Elemento 1. Estrategia y Marco de Ciberseguridad*

Establecer y mantener una estrategia y marco de seguridad cibernética ajustados a los riesgos informáticos específicos, así como mantenerse informados

[89] Bases de Coordinación en Materia de Seguridad de la Información, Portal electrónico https://www.gob.mx/cms/uploads/attachment/file/332698/Ciberseguridad-Bases_Coordinacion.pdf consultado el 07-09-2019.

adecuadamente de los estándares y guías nacionales e internacionales y de los sectores correspondientes.

Elemento 2 Gobernanza

Definir y facilitar el desempeño de funciones y responsabilidades para el personal a cargo de implementar, administrar y vigilar la efectividad de la estrategia y marco de ciberseguridad para asegurar la rendición de cuentas, así como proveer recursos adecuados, facultades y apropiadas y acceso a la autoridad de gobierno (E.g., consejo de administración o funcionarios de alto nivel en las autoridades públicas).

Elemento 3 Evaluación de Riesgos y Control

Identificar funciones, actividades productos y servicios – incluyendo interconexiones, dependencias y terceros- priorizar su importancia y evaluar sus riesgos informáticos. Identificar e implementar controles – incluyendo sistemas, políticas, procedimientos y capacitación- para protegerse contra esos riesgos y administrarlos dentro del margen de tolerancia establecido por la autoridad de gobierno.

Elemento 4. Monitoreo

Establecer procesos sistemáticos de monitorio para detectar rápidamente incidentes informáticos y evaluar periódicamente la efectividad de los controles, incluyendo el monitoreo de redes, pruebas, auditorias y ejercicios.

Elemento 5 Respuesta

Llevar a cabo las siguientes acciones de manera oportuna: (a) evaluar la naturaleza, alcance e impacto de un incidente informático. (b) contener el incidente y mitigar su impacto. (c) notificar a las partes relevantes internas y externas (tales como procuradurías de justicia, autoridades financieras y otras autoridades, proveedores de servicios externos y clientes, según sea adecuado y (d) coordinar actividades de respuestas conjuntas, según sea necesario.

Elemento 6 Recuperación

Recuperar debidamente las operaciones al tiempo de permitir una enmienda continua, incluyendo las siguientes acciones: a) eliminar remanentes dañinos del incidente, b) restaurar a la normalidad los sistemas y datos y confirmar el estado

normal, c) identificar y mitigar todas las vulnerabilidades que hubieran sido explotadas, d) remediar las vulnerabilidades para prevenir incidentes similares y e) comunicar interna y externamente, de manera apropiada.

Elemento 7. Intercambio de Información

Comprometerse a intercambiar de manera oportuna entre las partes relevantes internas y externas (incluyendo entidades y autoridades públicas dentro y fuera del sector financiero) información sobre seguridad cibernética confiable y útil sobre amenazas, vulnerabilidades, incidentes y respuestas para fortalecer defensas, limitar daños, incrementar la alerta de las situaciones y ampliar el conocimiento.

Elemento 8 Aprendizaje continuo.

Revisar regularmente la estrategia y marco de seguridad cibernética y cuando los eventos lo ameriten -incluir los componentes de su gobernanza, evaluación de riesgos y controles, monitoreo, respuestas, recuperación, así como del intercambio de información- para enfrentar los cambios en los riesgos informáticos, distribuir recursos, identificar y remediar brechas e incluir lecciones aprendidas."[90]

Finalmente, de dichas bases de coordinación, se desprende que la CNSF buscará estar coordinada con las demás autoridades financieras con el propósito de mantener homologada la normativa aplicable y con ello continuar replanteando los principios que en materia de seguridad de la información se han señalado.

La CNSF tendrá el deber de considerar los lineamientos desarrollados en el ámbito internacional aplicables en la materia, en relación con las mejores prácticas, pudiendo suscribir convenios para que, en el ámbito de la supervisión encomendada a cada una de ellas, se vea reflejada sobre sistemas y equipos de tecnologías de la información y comunicación.

En cuanto a la creación de un Grupo de Respuesta de Incidentes Sensibles de Seguridad de la Información (GRI), deberá estar integrado por los representantes que cada autoridad financiera, las cuales a su vez contaran con personal adscrito a las áreas de sistemas, comunicación y jurídica.

[90] Ibidem.

Tratándose de la CNSF entre otros, el representante deberá ser el titular de la unidad administrativa encargada de dar respuesta a incidentes sensibles de seguridad de la Información. A este grupo podrán ser invitados los representantes de las asociaciones gremiales y de las entidades.

Es importante referir que dichas bases también definen el incidente sensible de seguridad de la información considerándolo como:

"*Evento evaluado que efectiva o potencialmente pone en peligro la confidencialidad, integridad o disponibilidad de un componente o la totalidad de la infraestructura tecnológica o de la información que se procesa, almacena o transmite; que puede representar una pérdida, alteración o extravío de información; o bien que constituye una violación o una amenaza inminente de violación de las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable; que puede derivar en interrupción del servicio o bien en daño o perdida para los clientes en la Entidad afectada, para el público en general, para sus contrapartes o para la Entidad misma siempre y cuando dicho evento:*

i.- Pudiera representar una afectación a:

- Más de una entidad.

- Los clientes de las entidades

- La estabilidad del sistema financiero o de pagos, o bien

- A los sistemas centrales de pagos, cámaras de compensación o a los depositarios centrales de valores, u

ii. Observe las siguientes características:

-Genere pérdida económica, de información o interrupción de los servicios de la entidad de que se trate;

- Su modo de operación se pueda replicar a otras instituciones

- pueda representar un alto riesgo reputacional para las entidades u otros participantes del sistema financiero, o bien,

- Pueda generar desconfianza al público."[91]

Por otra parte, la base quinta refiere que las entidades tendrán la obligación de crear un grupo interno de identificación y respuesta a incidentes sensibles de

[91] Ibidem.

seguridad de la información, también conformado por personal de sistemas, comunicación y jurídico, quienes deberán informar a la autoridad financiera, sobre incidentes que comprometan lo siguiente:

"*- Los servicios que hayan sido interrumpidos, así como el tiempo estimado para recuperar la operación.*

- Las operaciones no reconocidas y la pérdida económica con el monto estimado

- El tipo de recursos o información alterada, robada o perdida-

- Las situaciones que pongan en riesgo la seguridad de los clientes, empleados o las instalaciones

- La clasificación del impacto del cliente con base en la información que la propia entidad tenga disponible.[92]

Después de haber analizado la estrategia implementada por la administración pública y las entidades que integran el Sistema Financiero Mexicano es apropiado abordar el riesgo operativo propio de las Instituciones Afianzadoras en relación con la emisión de pólizas de fianzas.

4.4 Uso de medios electrónicos para la operación y contratación de fianzas

Con apego a lo previsto en el artículo 214 de la LISF, las Instituciones podrán operar y prestar sus servicios pactando mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología o sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, estableciendo en los contratos los siguientes aspectos:

"Artículo 214…

I. Las operaciones y servicios cuya prestación se pacte;

II. Los medios de identificación del usuario, así como las responsabilidades correspondientes a su uso, tanto para las Instituciones como para los usuarios;

[92] Ibidem.

III. Los medios por los que se hagan constar la creación, transmisión, modificaciones o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate, incluyendo los métodos de autenticación tales como contraseñas o claves de acceso, y

IV. Los mecanismos de confirmación de la realización de las operaciones celebradas a través de cualquier medio electrónico.

El uso de los medios de identificación que se establezcan conforme a lo previsto por este artículo, en sustitución de la firma autógrafa, producirá los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio."[93]

Este artículo da la pauta para que las Instituciones del país puedan operar mediante medios electrónicos con mayor seguridad y certeza jurídica.

Las disposiciones de carácter general que emanan de dicha Ley (CUSF), establecen en el Capítulo 4.10 las condiciones que deben cumplir dichas Instituciones para poder operar y prestar servicios a través de estos medios.

En términos generales, la CUSF dispone que, en virtud de que las Instituciones pueden pactar la celebración de sus operaciones y la prestación de sus servicios a través de operaciones electrónicas, las mismas deben establecer o cubrir aspectos como los que se mencionan a continuación:

- Hacer del conocimiento al usuario condiciones de uso de medios electrónicos.

- Informar los términos y condiciones

- Poner a disposición del usuario el clausulado y la documentación contractual respecto a la posibilidad de efectuar operaciones de manera electrónica.

- Informen los riesgos derivados de las operaciones electrónicas.

- Las condicionantes para llevar a cabo operaciones electrónicas y la necesidad de la obtención del consentimiento expreso para contratación de servicios adicionales.

[93] Ley de Instituciones de Seguros y de Fianzas, Diario Oficial de la Federación de 4 de abril de 2013.

- Requerimientos para inicio de sesión en medios electrónicos donde presten el servicio.

- Factores de autenticación tanto para la institución afianzadora como para el usuario.

- Supuestos en donde aplica los distintos tipos de autenticación.

- Generación de comprobantes electrónicos

- Envío de estados de cuenta cifrados.

- Supuestos para el envío de notificaciones por medios electrónicos.

- Acciones para evitar el uso por terceros de sesiones abiertas.

- Supuestos para el bloqueo automático de contraseñas o factores de autenticación

- Restricciones para las instituciones afianzadoras para el manejo y manipulación de contraseñas.

- Obligación de las instituciones de implementar mecanismos de seguridad cuando ofrezcan operaciones o servicios a través de centro de atención telefónica.

- Acciones a implementar para transmitir, almacenar y procesar la información (cifrado).

- Control de acceso a la base de datos a los empleados de las instituciones afianzadoras.

- Acciones a implementar en el caso de acceso modificación o extracción de información sensible,

- Obligación de las instituciones de llevar un registro de incidencias o fallas en operaciones electrónicas.

- Registro y evidencia de las operaciones en medios electrónicos.

- Acciones en caso de robo o extravío de dispositivos de acceso o medios de autenticación.

- Periodicidad en la revisión de seguridad informática.

- Obligación de tener herramientas electrónicas para detectar eventos que afecten la confidencialidad de la información bajo su resguardo

- Acciones correctivas observadas por la CUSF.

Es importante destacar que las instituciones, en cuanto al registro de sus operaciones electrónicas y/o vía telefónica, deberán poder proporcionar a los usuarios que así lo requieran expresamente y mediante sus canales de atención al cliente, copia de dicho registro, en un plazo que no exceda de diez días hábiles, siempre y cuando que se traten de operaciones realizadas durante los ciento ochenta días naturales previos al requerimiento de la grabación o información.

De manera adicional, es importante mencionar los medios de autenticación que se encuentran obligadas a implementar las instituciones para con ello, realizar las operaciones electrónicas y reforzar la manifestación del consentimiento para la celebración de las mismas.

Dichos medios de autenticación y su clasificación se encuentran contenidos en la Disposición 4.10.5. de la CUSF, Disposición que se reproduce a continuación

"4.10.5. Las Instituciones y Sociedades Mutualistas deberán utilizar Factores de Autenticación para verificar la identidad de sus Usuarios y la facultad de estos para realizar Operaciones Electrónicas. Dichos Factores de Autenticación, dependiendo del Medio Electrónico de que se trate y de lo establecido en el presente Capítulo, deberán ser de cualquiera de las categorías siguientes:

I. Factor de Autenticación Categoría 1: Se compone de información obtenida mediante la aplicación de cuestionarios al Usuario, por parte de operadores telefónicos, en los cuales se requieran datos que el Usuario conozca. En ningún caso los Factores de Autenticación de esta categoría podrán componerse únicamente de datos que hayan sido incluidos en comunicaciones impresas o electrónicas enviadas por las Instituciones y Sociedades Mutualistas a sus clientes.

Las Instituciones y Sociedades Mutualistas, en la utilización de los Factores de Autenticación de esta categoría, para verificar la identidad de sus Usuarios, deberán observar lo siguiente:

a) Definir previamente los cuestionarios que serán practicados por los operadores telefónicos, impidiendo que sean utilizados de forma discrecional, y

b) Validar al menos una de las respuestas proporcionadas por sus Usuarios, a través de herramientas informáticas, sin que el operador pueda consultar o conocer anticipadamente los datos de Autenticación de los Usuarios.

II. Factor de Autenticación Categoría 2: Se compone de información que sólo el Usuario conozca e ingrese a través de un Dispositivo de Acceso, tales como Contraseñas y Números de Identificación Personal (NIP), y deberán cumplir con las características siguientes:

a) En ningún caso se podrá utilizar como tales, la información siguiente:

1) El Identificador de Usuario;

2) El nombre de la Institución o Sociedad Mutualista;

3) Más de dos caracteres idénticos en forma consecutiva, o

4) Más de dos caracteres consecutivos numéricos o alfabéticos.

No resultará aplicable lo previsto en el presente inciso para el caso de las Operaciones Electrónicas Móviles, siempre que las Instituciones y Sociedades Mutualistas informen al Usuario al momento de la contratación, de la importancia de la composición de las Contraseñas para estos servicios;

b) Su longitud deberá ser de al menos seis caracteres, salvo en el caso de Operaciones Electrónicas por Internet en el que deberá ser de ocho caracteres, y

c) La composición de estos Factores de Autenticación deberá incluir caracteres alfabéticos y numéricos, cuando el Dispositivo de Acceso lo permita.

Las Instituciones y Sociedades Mutualistas deberán permitir al Usuario cambiar sus Contraseñas, Números de Identificación Personal (NIP) y otra información de Autenticación estática, cuando este último así lo requiera, utilizando los servicios de las Operaciones Electrónicas.

Tratándose de Contraseñas o Números de Identificación Personal (NIP) definidos o generados por las Instituciones y Sociedades Mutualistas durante la contratación de un servicio de Operaciones Electrónicas o durante el restablecimiento de dichas contraseñas, las propias Instituciones y Sociedades Mutualistas deberán prever mecanismos y procedimientos por medio de los cuales el Usuario deba modificarlos inmediatamente después de iniciar la Sesión correspondiente. Las Instituciones y Sociedades Mutualistas deberán contar con controles que les permitan validar que las nuevas Contraseñas o Números de Identificación Personal (NIP) utilizadas por sus Usuarios, sean diferentes a los definidos o generados por las propias Instituciones y Sociedades Mutualistas.

Las Instituciones y Sociedades Mutualistas deberán recomendar a sus Usuarios en el proceso de contratación de Operaciones Electrónicas, que mantengan Contraseñas seguras;

III. Factor de Autenticación Categoría 3: Se compone de información contenida o generada por medios o dispositivos electrónicos, así como la obtenida por dispositivos generadores de Contraseñas dinámicas de un solo uso. Dichos medios o dispositivos deberán ser proporcionados por las Instituciones y Sociedades Mutualistas a sus Usuarios y la información contenida o generada por ellos, deberá cumplir con las características siguientes:

a) Contar con propiedades que impidan su duplicación o alteración;

b) Ser información dinámica que no podrá ser utilizada en más de una ocasión;

c) Tener una vigencia que no podrá exceder de dos minutos, y

d) No ser conocida con anterioridad a su generación y a su uso por los funcionarios, empleados, representantes o comisionistas de la Institución o Sociedad Mutualista, o por terceros.

Las Instituciones y Sociedades Mutualistas podrán proporcionar a sus Usuarios medios o dispositivos que generen Contraseñas dinámicas de un solo uso, las cuales utilicen la información relacionada con el tipo de operación o servicio de que se trate, de manera que dicha Contraseña únicamente pueda ser utilizada para la operación solicitada. En estos casos, no será aplicable lo dispuesto en el inciso c) de la presente fracción.

Asimismo, las Instituciones y Sociedades Mutualistas podrán considerar dentro de esta categoría a la información contenida en el circuito o chip de Tarjetas con Circuito Integrado, siempre y cuando dichas tarjetas se utilicen únicamente para operaciones que se realicen en Terminales Punto de Venta y tales Dispositivos de Acceso obtengan la información de la tarjeta a través del dicho circuito o chip.

Las Instituciones y Sociedades Mutualistas que aprueben la celebración de operaciones mediante el uso de tarjetas sin circuito integrado en Terminales Punto de Venta, deberán pactar con sus Usuarios que dichas Instituciones y Sociedades

Mutualistas asumirán los riesgos y por lo tanto los costos de las operaciones que no sean reconocidas por los Usuarios en el uso de dichas tarjetas.

Tratándose de Operaciones "Host to Host", las Instituciones y Sociedades Mutualistas podrán utilizar como Factor de Autenticación de esta categoría, cualquier mecanismo que les permita verificar que los equipos de cómputo o dispositivos utilizados por los Usuarios para establecer la comunicación son los que la propia Institución o Sociedad Mutualista autorizó.

Las Instituciones y Sociedades Mutualistas podrán utilizar tablas aleatorias de Contraseñas como Factor de Autenticación de esta categoría, siempre y cuando dichas tablas cumplan con las características listadas en los incisos a), b) y d) de la presente fracción. Para el caso del inciso a), las Instituciones y Sociedades Mutualistas deberán asegurarse que las propiedades que impidan la duplicación o alteración se cumplan hasta el momento de la entrega al Usuario, y

IV. Factor de Autenticación Categoría 4: Se compone de información del Usuario derivada de sus propias características físicas, tales como huellas dactilares, geometría de la mano o patrones en iris o retina, entre otras.

Las Instituciones y Sociedades Mutualistas que utilicen los Factores de Autenticación de esta categoría, deberán aplicar a la información de Autenticación obtenida por dispositivos biométricos, elementos que aseguren que dicha información sea distinta cada vez que sea generada, a fin de constituir Contraseñas de un solo uso, que en ningún caso puedan utilizarse nuevamente o duplicarse con la de otro Usuario."[94]

Como puede observarse, los medios de autenticación referidos han sido clasificados en 4 categorías, las cuales establecen mecánicas cada vez más complejas para la autenticación, que van desde cuestionarios vía telefónica, hasta la implementación de contraseñas generadas a partir de datos biométricos, mecánica que se estima idónea y proporcional a los fines que persigue, la prestación de un servicio financiero.

[94] Circular Única de Seguros y Fianzas. Diario Oficial de la Federación de 19 de diciembre de 2014.

4.5 ¿Qué riesgos se actualizan por la emisión de fianzas electrónicas?

Las instituciones afianzadoras emiten fianzas electrónicas en formato .XML y su representación gráfica. La modificación de dichos archivos puede ser analizada gracias a la Informática forense que se constituye como un pilar para solventar dudas y, en su caso determinar la responsabilidad u obligación de una institución o deslindarla de la obligación que se pretendía garantizar.

En cuanto a los riesgos por la emisión de pólizas de fianzas electrónicas se pueden referir atendiendo a las partes que participan en la relación contractual.

Para el beneficiario: El riesgo consiste en la recepción de una póliza de fianza electrónica que manipulada electrónicamente sea apócrifa y en consecuencia no se esté garantizando la obligación que requiere el beneficiario y acreedor de la obligación principal.

Para el fiador: Que se emita una póliza de fianza electrónica a su nombre, pero sin su consentimiento, pretendiendo garantizar una obligación principal en una relación contractual donde no manifestó su consentimiento para ser parte y obligarse.

Para el fiado: El riesgo consiste en pretender garantizar una obligación con o sin conocimiento de la autenticidad de la póliza de fianza electrónica.

Adicionalmente, se puede identificar otro riesgo consistente en la puesta en peligro del sano desarrollo del sistema financiero mexicano, en el supuesto de que una persona se dedique a emitir pólizas de fianzas electrónicas sin tener la autorización correspondiente por parte de la CNSF, configurándose la comisión de un delito especial previsto en la LISF a saber:

"ARTÍCULO 496.- Serán sancionadas las violaciones a lo dispuesto en los artículos 33 y 35, de esta Ley, conforme a lo siguiente:

I. Con prisión de tres a quince años y multa de 5,000 a 20,000 Días de Salario, a quienes, en contravención a lo dispuesto por los artículos 33 y 35 de este ordenamiento, otorguen habitualmente fianzas a título oneroso o a quienes actúen como intermediarios en las operaciones que dichas personas realicen, y

II. Con prisión de dos a diez años y multa de 2,500 a 10,000 Días de Salario, a quienes, en contravención a lo dispuesto por el artículo 35 de esta Ley, ofrezcan directamente o como intermediarios en el territorio nacional por cualquier medio, público o privado, la contratación de las operaciones a que se refiere el artículo 34, primer párrafo, de este ordenamiento.

Se consideran comprendidos dentro de los supuestos señalados en las dos fracciones anteriores y, consecuentemente, sujetos a las mismas sanciones, a los directores, gerentes, administradores, miembros del consejo de administración, funcionarios, empleados y los representantes y agentes en general de personas morales que practiquen habitualmente las operaciones ilícitas a que aluden los artículos 33 y 35 de esta Ley.

Cuando quede firme la resolución judicial correspondiente que confirme que la empresa o negociación efectuaba la operación u operaciones que prohíbe el artículo 33 de esta Ley, la Comisión podrá intervenir administrativamente a la empresa o negociación o establecimiento de la persona física o moral de que se trate. La intervención que realice la Comisión tendrá como único propósito llevar a cabo la corrección de las operaciones ilícitas."[95]

Así pues, tenemos que para poder otorgar fianzas de manera habitual y a título oneroso, es necesario que la CNSF lo autorice y solo estas personas autorizadas, podrán ejercer dicha actividad que se ejerce al amparo de lo previsto por la LISF, la que refiere en su artículo 166 que las instituciones de fianzas asumirán obligaciones mediante el otorgamiento de pólizas enumeradas y documentos adicionales.

En este sentido se puede identificar que, en términos generales el riesgo propiamente dicho, es la falsificación o emisión de una póliza de fianza apócrifa en detrimento, entre otros, del sano desarrollo del sistema financiero mexicano.

4.6 ¿Qué ilícitos se actualizan cuando alguien comercializa pólizas de fianzas electrónicas para aparentar el otorgamiento de fianzas?

[95] Ley de Instituciones de Seguros y de Fianzas, Diario Oficial de la Federación de 4 de abril de 2013.

Sobre este apartado el trabajo presentado por los Licenciados Huberto Goycoolea Heredia y el Lic. Francisco José López Álvarez refieren "A efecto de poder identificar plenamente los distintos ilícitos que se actualizan con esta conducta, es necesario en primer término, definir claramente cada uno de los elementos de los que se compone la acción.

Es necesario referir en primer término que, dado que la fianza es un instrumento que busca asegurar el cumplimiento de una obligación contraída, asegurando así los intereses de ciertas operaciones, el Estado ponga especial cuidado en que las personas que garantizan dichas operaciones cuenten con la capacidad u solvencia suficiente para responder de las mismas, aun que obtienen un lucro por ello, en este sentido el primero ilícito a referir es el previsto en la LISF." [96]

Por otra parte, se puede inferir que los ilícitos que se actualizan al emitir una póliza de fianzas electrónica apócrifa sin contar con la autorización por parte de la CNSF, con independencia del delito especial previsto en la LISF, son la falsificación y el fraude mediante medios electrónicos.

En este orden de ideas podemos referir que este tipo de delitos se incrementan en gran media en virtud de la facilidad para que cualquier individuo pueda adquirir un equipo de cómputo, que cada vez es más barato, con mayor rendimiento y capacidades. Actualmente los criminales informáticos no requieren de tantos conocimientos especializados, es suficiente contar con habilidades técnicas para alterar la información.

Delitos especiales

En cuanto a los delitos especiales podemos referir que los mismos y su reglamentación surgen con problemas correspondientes a áreas ajenas Leyes u Códigos de carácter penal, así pues, las leyes administrativas contienen capítulos bajo el nombre de delitos o infracciones y sanciones, que contienen la descripción de figuras penales.

[96] Goycoolea Heredia, Humberto, López Álvarez, Francisco. Los diversos ilícitos que se producen, cuando se crean pólizas de fianzas apócrifas. XV Premio de Investigación sobre Seguros y Fianzas, 2008. Tercer Lugar Categoría de Fianzas.

La LISF dispone que solamente las instituciones aseguradoras y afianzadoras del país que se encuentren debidamente constituidas y debidamente autorizada por la SHCP y la CNSF podrán emitir pólizas de fianzas a título oneroso.

En este sentido el artículo 11 de dicha Ley refiere a la autorización que otorga la CNSF para constituirse como institución aseguradora o afianzadora.

"ARTÍCULO 11.- Para organizarse y operar como Institución o Sociedad Mutualista se requiere autorización del Gobierno Federal, que compete otorgar discrecionalmente a la Comisión, previo acuerdo de su Junta de Gobierno. Por su naturaleza, estas autorizaciones serán intransmisibles.

…"[97]

El artículo 33 de la LISF dispone la prohibición a toda persona física y moral distintas de las instituciones autorizadas para otorgar fianzas a título oneroso.

"ARTÍCULO 33.- Se prohíbe a toda persona física o moral distinta a las Instituciones autorizadas en los términos de esta Ley, otorgar habitualmente fianzas a título oneroso.

Salvo prueba en contrario se presume la infracción de este precepto, cuando el otorgamiento de fianzas se ofrezca al público por cualquier medio de publicidad, o se expidan pólizas, o se utilicen agentes." [98]

En concordancia con el artículo anterior, el artículo 496 de la referida ley dispone las sanciones a la violación de dicho precepto.

"ARTÍCULO 496.- Serán sancionadas las violaciones a lo dispuesto en los artículos 33 y 35, de esta Ley, conforme a lo siguiente:

I. Con prisión de tres a quince años y multa de 5,000 a 20,000 Días de Salario, a quienes, en contravención a lo dispuesto por los artículos 33 y 35 de este ordenamiento, otorguen habitualmente fianzas a título oneroso o a quienes actúen como intermediarios en las operaciones que dichas personas realicen, y

II. Con prisión de dos a diez años y multa de 2,500 a 10,000 Días de Salario, a quienes, en contravención a lo dispuesto por el artículo 35 de esta Ley, ofrezcan directamente o como intermediarios en el territorio nacional por cualquier medio,

[97] Ley de Instituciones de Seguros y de Fianzas, Diario Oficial de la Federación de 4 de abril de 2013.
[98] Ibidem.

público o privado, la contratación de las operaciones a que se refiere el artículo 34, primer párrafo, de este ordenamiento.

Se consideran comprendidos dentro de los supuestos señalados en las dos fracciones anteriores y, consecuentemente, sujetos a las mismas sanciones, a los directores, gerentes, administradores, miembros del consejo de administración, funcionarios, empleados y los representantes y agentes en general de personas morales que practiquen habitualmente las operaciones ilícitas a que aluden los artículos 33 y 35 de esta Ley.

Cuando quede firme la resolución judicial correspondiente que confirme que la empresa o negociación efectuaba la operación u operaciones que prohíbe el artículo 33 de esta Ley, la Comisión podrá intervenir administrativamente a la empresa o negociación o establecimiento de la persona física o moral de que se trate. La intervención que realice la Comisión tendrá como único propósito llevar a cabo la corrección de las operaciones ilícitas."[99]

A fin de contrastar lo antes referido la fracción V del artículo 506 dispone la sanción correspondiente a quien falsifique pólizas a saber:

"ARTÍCULO 506.- Se impondrá pena de prisión de uno a doce años y multa de 500 a 5,000 Días de Salario a:

I. Las personas que con el propósito de obtener la expedición de una póliza de seguro de caución o una póliza de fianza, para sí o para otra persona, proporcionen a una Institución datos falsos sobre el monto de activos o pasivos de una entidad o persona física o moral, si como consecuencia de ello resulta quebranto o perjuicio patrimonial para la Institución;

II. Los agentes de seguros o los médicos que dolosamente o con ánimo de lucrar, oculten a una Institución de Seguros la existencia de hechos cuyo conocimiento habría impedido la celebración de un contrato de seguro;

III. Las personas que para obtener la expedición de una póliza de fianza presenten avalúos que no correspondan a la realidad, de manera que el valor real de los bienes que ofrece en garantía sea inferior al importe de la fianza, y

[99] Ibidem.

IV. Las personas que falsifiquen pólizas o certificados de seguros, o pólizas de fianzas, así como a las personas que las ofrezcan o actúen como intermediarios.

En los casos previstos en este artículo se procederá a petición de parte agraviada."

En este sentido la indagatoria que se siga en contra de los actos ilícitos deberá identificar el supuesto legal aplicable.

La falsificación usando herramientas electrónicas.

De acuerdo a lo manifestado por *los Licenciados Huberto Goycoolea Heredia y el Lic. Francisco José López Álvarez, "la falsificación es como comúnmente identificamos a la conducta en estudio. Sin embargo, es incorrecto hablar de falsificación de pólizas de fianza, ya que lo que en verdad ocurre, es que se crea un documento en forma de póliza, en la que se aparente documentar una fianza*." [100]

En este sentido proponen una definición de falsificación:

"*Definición de falsificación: Es el proceso por el cual se realizan una serie de maniobras sobre un documento, para hacerlo pasar como si fuera auténtico en el caso de que no lo sea, o para alterar su contenido original*." [101]

El delito de falsificación se encuentra regulado en el Código Penal Federal y en cada uno de los Códigos Penales de las Entidades Federativas, así como en la LISF. "*Es un delito que pude cometerse en el orden federal y en el orden local. La diferencia de orden corresponde al pasivo del ilícito. Las Instituciones de Fianzas, aún y cuando son reguladas por una Ley Federal, son consideradas sujetos al orden local. en cuanto a su competencia, ésta dependerá del lugar en donde se pretenda usar el documento falsificado".* [102]

El artículo 506 de la LISF dispone lo siguiente:

"ARTÍCULO 506.- Se impondrá pena de prisión de uno a doce años y multa de 500 a 5,000 Días de Salario a:

[100] Goycoolea Heredia, Humberto, López Álvarez, Francisco. Los diversos ilícitos que se producen, cuando se crean pólizas de fianzas apócrifas. XV Premio de Investigación sobre Seguros y Fianzas, 2008. Tercer Lugar Categoría de Fianzas.
[101] Ibidem.
[102] Ibidem.

I. Las personas que con el propósito de obtener la expedición de una póliza de seguro de caución o una póliza de fianza, para sí o para otra persona, proporcionen a una Institución datos falsos sobre el monto de activos o pasivos de una entidad o persona física o moral, si como consecuencia de ello resulta quebranto o perjuicio patrimonial para la Institución;

II. Los agentes de seguros o los médicos que dolosamente o con ánimo de lucrar, oculten a una Institución de Seguros la existencia de hechos cuyo conocimiento habría impedido la celebración de un contrato de seguro;

III. Las personas que para obtener la expedición de una póliza de fianza presenten avalúos que no correspondan a la realidad, de manera que el valor real de los bienes que ofrece en garantía sea inferior al importe de la fianza, y

IV. Las personas que falsifiquen pólizas o certificados de seguros, o pólizas de fianzas, así como a las personas que las ofrezcan o actúen como intermediarios."

Así mismo, la conducta descrita se encuentra prevista en el artículo 244 del Código Penal Federal:

"Artículo 244.- El delito de falsificación de documentos se comete por alguno de los medios siguientes:

I.- Poniendo una firma o rúbrica falsa, aunque sea imaginaria, o alterando una verdadera;

II.- Aprovechando indebidamente una firma o rúbrica en blanco ajena, extendiendo una obligación, liberación o cualquier otro documento que pueda comprometer los bienes, la honra, la persona o la reputación de otro, o causar un perjuicio a la sociedad, al Estado o a un tercero;

III.- Alterando el contexto de un documento verdadero, después de concluido y firmado, si esto cambiare su sentido sobre alguna circunstancia o punto substancial, ya se haga añadiendo, enmendando o borrando, en todo o en parte, una o más palabras o cláusulas, o ya variando la puntuación;

IV.- Variando la fecha o cualquiera otra circunstancia relativa al tiempo de la ejecución del acto que se exprese en el documento;

V.- Atribuyéndose el que extiende el documento, o atribuyendo a la persona en cuyo nombre lo hace: un nombre o una investidura, calidad o circunstancia que no tenga y que sea necesaria para la validez

del acto;

VI.- Redactando un documento en términos que cambien la convención celebrada en otra diversa en que varíen la declaración o disposición del otorgante, las obligaciones que se propuso contraer, o los derechos que debió adquirir;

VII.- Añadiendo o alterando cláusulas o declaraciones, o asentando como ciertos hechos falsos, o como confesados los que no lo están, si el documento en que se asientan, se extendiere para hacerlos constar y como prueba de ellos;

VIII.- Expidiendo un testimonio supuesto de documentos que no existen; dándolo de otro existente que carece de los requisitos legales, suponiendo falsamente que los tiene; o de otro que no carece de ellos, pero agregando o suprimiendo en la copia algo que importe una variación substancia, y

IX.- Alterando un perito traductor o paleógrafo el contenido de un documento, al traducirlo o descifrarlo.

X.- Elaborando placas, gafetes, distintivos, documentos o cualquier otra identificación oficial, sin contar con la autorización de la autoridad correspondiente."[103]

Tipicidad: La actualización del tipo requiere se reúnan los elementos o condiciones referidas en el artículo 245 del Código Penal Federal:

"Artículo 245.- Para que el delito de falsificación de documentos sea sancionable como tal, se necesita que concurran los requisitos siguientes:

I.- Que el falsario se proponga sacar algún provecho para sí o para otro, o causar perjuicio a la sociedad, al Estado o a un tercero;

II.- Que resulte o pueda resultar perjuicio a la sociedad, al Estado o a un particular, ya sea en los bienes de éste o ya en su persona, en su honra o en su reputación, y

[103] Código Penal Federal, Diario Oficial de la Federación de 14 de agosto de 1931.

III.- Que el falsario haga la falsificación sin consentimiento de la persona a quien resulte o pueda resultar perjuicio o sin el de aquella en cuyo nombre se hizo el documento." [104]

El Juzgador deberá realizar el ejercicio de valoración de los elementos de carácter objetivos a través de la voluntad, el nexo causal y normativos, a través de valoraciones culturales y jurídicas, y subjetivo como el dolo y la culpa de manera genérica o algún elemento especifico, lo anterior a fin de adecuar la conducta al tipo penal.

Resulta de mayor importancia el análisis de los elementos subjetivos específicos como la finalidad o intención de manera dolosa o culposa.

Antijuricidad: Entendida como tal a la conducta ilícita en razón de esar contenida y prohibida en un ordenamiento jurídico, como lo acontece en el supuesto que nos ocupa, al verse contemplada en el Código Penal Federal, en su Libro Segundo, Título Décimo Tercero, Capítulo IV.

Culpabilidad: Entendida como tal el reproche de la conducta ilícita desplegada por su autor, la cual en algunos casos podrá ser dolosa , por tener la intención de exhibir un documento apócrifo y en otros casos podrá ser culposa, al exhibir un documento que desconoce es apócrifo.

En ambas situaciones el documento apócrifo carece de un carácter vinculante que obligue a la Institución.

Punibilidad: contenida en el artículo 243 del Código Penal, el cual establece la sanción por la realización de la conducta.

"ARTÍCULO 243.- El delito de falsificación se castigará, tratándose de documentos públicos, con prisión de cuatro a ocho años y de doscientos a trescientos días multa. En el caso de documentos privados, con prisión de seis meses a cinco años y de ciento ochenta a trescientos días multa." [105]

Es importante referir que para el supuesto de falsificación de documentos privados referido en el artículo antes invocado, se considera un delito no grave que se persigue de oficio

[104] Ibidem.
[105] Ibidem.

Bien jurídico tutelado.

El bien jurídico tutelado lo constituye el bien que es lesionado por el sujeto activo en la comisión del delito, es decir, el bien jurídico protegido por la norma y, en el caso concreto, el bien jurídico tutelado es la Fe Pública.

El bien jurídico tutelado en este delito es la fe pública.

El concepto de fé pública no debe confundirse con la atribución o función notarial o atribución conferida a algunos funcionarios públicos, si no como un valor abstracto de confianza social o colectiva sobre la veracidad de un documento al cual el Estado y la sociedad le atribuyen un valor probatorio pleno.

En este sentido, todo acto encaminado a falsificar un documento de carácter público o privado ofende la confianza que la sociedad y, en su caso, el Estado, le atribuyen, por tratar de hacer parecer como verdadero o autentico algo que no lo es.

Es importante referir le la falsificación se puede dividir en falsificación formal y falsificación material por lo que resulta necesario aclarar las diferencias entre ambas.

- La falsificación material: Dicha falsificación puede explicarse a través de tres supuestos.

i) La creación de un documento falso (en su totalidad o una parte)

ii) Modificar o adulterar un documento verdadero

iii) Suprimir de manera parcial o total un documento verdadero con la finalidad de ocultar la verdad y ocasionar un daño u obtener un beneficio.

- Falsificación ideológica.

Dicha falsificación se materializa cuando en un documento verdadero o genuino se consigna información falsa.

En el caso que nos ocupa, la falsificación de pólizas a través de medios electrónicos podría encontrarse en cualquiera de los dos supuestos referidos, falsificación material como falsificación ideológica.

Como ejemplo podemos invocar la manipulación de un documento en papelería oficial o con firma autógrafa o electrónica, haciendo variaciones en el

contenido, suplantando por ejemplo los nombres, montos a garantizar, fecha de emisión, etc, con ello invocamos ambos tipos de falsificación.

Así mismo, un falsificador podría crear un documento que simule haber sido generado a través de un archivo digital o procesos electrónicos propios de una institución financiera, sin que acontezca dicha situación y solo constituya la impresión de un formato o plantilla manipulada o creada con herramientas de edición digital.

Por otra parte, la descripción del tipo penal no incluye elementos como la habitualidad ni la onerosidad.

En virtud de que el tipo penal no considera elementos como la onerosidad y la habitualidad, se infiere que la creación de un documento en forma de póliza, tanto en medios físicos (papel) como en medios electrónicos, constituye el ilícito planteado, aún siendo por única ocasión y sin la percepción de una retribución o beneficio económico.

Este tipo de conductas suelen se observadas por parte del fiado quien requiere cumplir con el requisito de exhibir una póliza de fianza para garantizar el cumplimiento de sus obligaciones, o en su caso, por un tercero que, por instrucción del fiado, realiza la falsificación.

Uso de documento falso.

La fracción VIII del artículo 246 del Código Penal refiere el aspecto conductual relativo al uso de documento falso, en el caso que nos ocupa, ya sea por parte del fiado como por parte del beneficiario, descansando sobre el supuesto de tener conocimiento de tratarse de un documento apócrifo y usarlo para obtener un beneficio para si mismo o un tercero.

La conducta es realizada por el fiado al usar un documento apócrifo con la finalidad de cumplir el requisito de exhibición de una garantía para respaldar el cumplimiento de sus obligaciones.

La conducta es realizada por un beneficiario cuando a sabiendas de que se trata de un documento apócrifo, se requiere formalmente a la institución para que se haga efectiva la póliza de fianza.

En virtud de lo antes expuesto, se pueden advertir dos variantes de actos tendientes a la falsificación de documentos en el entorno digital.

La primera variante corresponde a la falsificación material:

La creación de una póliza, desde cero, copiando imágenes y diseño de una póliza autentica emitida por la Institución Afianzadora.

El uso de formatos oficiales para, a través de medios electrónicos, incrustar la imagen o texto que contiene, entre otros, la obligación a garantizar. Esto quiere decir, que en formatos oficiales, a través de herramientas digitales, se hace constar información falsa para ser exhibida ante el beneficiario de la supuesta póliza.

La segunda variante corresponde a la falsificación ideológica

La modificación de una póliza autentica para hacer constar obligaciones garantizadas o montos distintos, a través de herramientas electrónicas.

No se omite hacer mención que, no obstante, las referidas modalidades tendientes a crear un documento apócrifo o falsificar alguno ya existente, se requiere de un archivo electrónico que necesariamente le debe corresponder una representación digital, misma que, a criterio de la institución, contendrá la firma electrónica avanzada del funcionario que la suscribe, para que la misma pueda considerarse auténtica.

En este sentido el archivo electrónico debe estar vinculado de manera directa con su representación documental, en donde, en el mejor de los casos se hará constar la firma electrónica avanzada, o algún facsímil del funcionario que la emite.

El presente supuesto, presupone que los creadores de un documento o archivo en forma de póliza pretenden duplicar una o algunas que si tuvieron un proceso de emisión en una institución debidamente autorizada, por lo que no se logra falsificar los registros de emisión pues no hay acceso a los sistemas de la Institución, solo generan un archivo, imagen o documento sin valor alguno en donde se contienen imágenes entre las que se encuentra la firma facsimilar, la cual no expresa la voluntad de asumir obligaciones de garantizar un contrato u obligación principal.

El fraude

En virtud de que se trata de un ilícito que pretende alcanzar un lucro indebido, es que se le tiene clasificado como delito de naturaleza patrimonial,

Tipo penal federal y los elementos del ilícito.

Conducta: El artículo 386 del Código Penal Federal contiene el tipo penal aplicable al Fraude.

"Artículo 386.- Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido.

El delito de fraude se castigará con las penas siguientes:

I.- Con prisión de 3 días a 6 meses o de 30 a 180 días multa, cuando el valor de lo defraudado no exceda de diez veces el salario;

II.- Con prisión de 6 meses a 3 años y multa de 10 a 100 veces el salario, cuando el valor de lo defraudado excediera de 10, pero no de 500 veces el salario;

III.- Con prisión de tres a doce años y multa hasta de ciento veinte veces el salario, si el valor de lo defraudado fuere mayor de quinientas veces el salario." [106]

Por su parte, el artículo 387 del propio Código Penal Federal, enumera las conductas que se equiparan al fraude.

"Artículo 387.- Las mismas penas señaladas en el artículo anterior, se impondrán:

…

X.- Al que simulare un contrato, un acto o escrito judicial, con perjuicio de otro o para obtener cualquier beneficio indebido.

…"[107]

Tipicidad Habrá que analizar a la luz de los elementos que componen a la tipicidad, sí esta efectivamente se actualiza con la realización de la conducta.

Elemento objetivo. – El aspecto externo de la conducta, perceptible con los sentidos y en el caso que nos ocupa, la póliza apócrifa y su mecanismo de expedición.

[106] Ibidem.
[107] Ibidem.

-Elemento Subjetivo. - Relacionado con la voluntad dirigida al resultado, esto es la verificación si el activo se aprovechó de un error o engaño al activo.

-Elemento Normativo. - – Relacionado con la valoración del interprete o juez sobre el lucro indebido.

Antijuridicidad. - Es la contradicción de una norma jurídica con una acción reprochada por el derecho, por lo que en nuestro caso se refiere a la disposición legal prevista en el Libro Segundo, Titulo Vigésimo Segundo, Capítulo III del Código Penal Federal.

Culpabilidad. El reproche que se realiza contra el sujeto activo del delito, en virtud de desplegar una conducta dolosa, cuya realización es necesariamente intencional.

La creación de un documento en forma de póliza presupone la intencionalidad de aparentar la emisión y otorgamiento de una fianza, que finge el respaldo de una institución debidamente autorizada para respaldar una operación, haciendo creer que la misma se encuentra debidamente garantizada

Así pues, se deberá obtener un lucro indebido por la supuesta expedición y subsecuente exhibición del documento haciéndolo pasar por autentico

Punibilidad. - **-** El artículo 386 del Código Penal Federal señala la sanción por realizar esta conducta, la cual, atendiendo al perjuicio patrimonial ocasionado, será calificado como como delito grave o no grave.

Es importante referir que el presente delito, para su persecución, en se requiere la presentación de la querella del ofendido.

Bien jurídico tutelado en el delito de fraude.

El patrimonio de las personas es el bien jurídico tutelado. En las operaciones de afianzamiento, la obligación principal constituye el objeto que se pretende garantizar, por lo que, en caso de incumplimiento, al no existir el compromiso de una institución afianzadora debidamente autorizada, el acreedor del contrato y supuesto beneficiario de la póliza tendría un perjuicio en su patrimonio.

Supuestos de fraude

Fraude del creador de la póliza en perjuicio del fiado. - El fraude en este supuesto se concreta cuando el fiado paga una prima por la emisión de una póliza

de fianza, la cual, normalmente para el caso que nos ocupa, es creada por el agente de fianzas. El quebrando patrimonial acontece al cobrar la prima indebidamente

Fraude del fiado creador de la póliza en perjuicio del beneficiario. – Cuando el propio fiado a través del engaño, otorga al beneficiario un documento con forma de fianza, manipulada a través de medios electrónicos, para supuestamente, garantizar su obligación.

Como puede observarse, el fraude y la falsificación se encuentran vinculados en las hipotesis planteadas.

4.7 Situaciones que favorecen la realización de estas conductas

4.7.1 La falta de cultura de validación

Los beneficiarios de las pólizas de fianzas, quienes ostentan el carácter de principales interesados en la autenticidad del documento, adolecen de una cultura de validación.

Por otra parte, las instituciones afianzadoras dentro de su operación deberían considerar la publicidad de dicha práctica. Al día de hoy ninguna Institución afianzadora da publicidad en redes sociales o medios masivos de comunicación.

Adicionalmente el órgano regulador debería promover que dicho mecanismo de validación sea agregado a los textos que deben contener las pólizas

Finalmente, se estima que la CONDUSEF, podría publicar en el DOF “Disposiciones de carácter general en materia de sanas prácticas, transparencia y publicidad aplicables a las instituciones de fianzas” así como “Disposiciones de carácter general para el registro de contratos de adhesión de fianzas” en ejercicio de las facultades que el artículo 197 de la Ley de Instituciones de Seguros y Fianzas otorga a dicha Comisión.

4.7.2 Falta de interés en los beneficiarios para denunciar estos hechos

Siendo el Gobierno Federal uno de los principales consumidores beneficiarios de fianzas, la “Ley de adquisiciones, arrendamientos y servicios del sector público” no establece la obligación de validar las pólizas de fianzas otorgadas a favor de la federación para verificar la autenticidad del documento y con ellos verificar que el servicio financiero efectivamente se encuentre respaldando la operación.

Un aspecto importante a considerar es que, los responsables de la verificación del cumplimiento de los requisitos en licitaciones públicas y cualquier otro mecanismo de adquisición de bienes o servicios garantizados a través de la fianza, se preocupan en evitar las responsabilidades administrativas por recibir pólizas apócrifas que en realizar la denuncia correspondiente.

Por otra parte, en cuanto a la iniciativa privada se refiere, los interesados ejercitan acción legal a fin de forzar el cumplimiento de la fianza, logrando en muchos casos que a través de una orden judicial, las instituciones afianzadoras se vean obligadas a dar cumplimiento con la obligación garantizada de una póliza electrónica no emitida por ellos. La acción de carácter penal representa el último recurso del beneficiario de la póliza de fianza electrónica, ya que el interés supremo es el cumplimiento de la obligación que se asumía garantizada y no la persecución del delito.

La principal razón de la falta de la cultura de validación se encuentra relacionada con el supuesto hipotético del “migrante digital”, quien a diferencia del “nativo digital” carece del interés o habilidad inherente para el uso de los mecanismos electrónicos de validación como, por ejemplo, la simple lectura de los códigos QR (Quick Response) que permiten la inmediata verificación electrónica.

Tampoco se practica la validación de pólizas de fianzas emitidas de manera electrónica, teniendo como consecuencia los mismos efectos, valoración negativa de este tipo de herramientas de garantía, daños patrimoniales cuando se presentan reclamaciones por incumplimiento de obligaciones garantizadas en una póliza de fianzas electrónica apócrifa y en el mejor de los casos, cuando no existe reclamación, indiferencia hacia el documento apócrifo al no haber incumplimiento alguno de obligaciones.

4.7.3 Poco riesgo de quebranto a la institución de fianzas

El uso de pólizas digitales apócrifas no pretende generar un daño directo a las Instituciones de fianzas, pretende cubrir el requisito que el beneficiario impone para garantizar el cumplimiento de una obligación, sin embargo, el riesgo de una afectación patrimonial a dichas instituciones se encuentra presente.

El porcentaje de reclamaciones con este tipo de pólizas apócrifas es pequeño, sin embargo, representa la punta del iceberg del porcentaje real de documentos apócrifos en el mercado. El reconocimiento de dicho porcentaje se advierte gracias a solicitudes de cancelación de pólizas, solicitudes de endosos o en su caso, renovaciones que son ingresadas a las Instituciones.

En el caso del beneficiario, quien se convierte en el sujeto pasivo de estas conductas, no cuenta con una garantía real de cumplimiento. No existe afectación en el contrato u obligación principal sin embargo no cuenta con la garantía que respalde dicha obligación. Normalmente el beneficiario intenta hacer exigible el documento apócrifo vía jurisdiccional.

En el caso del fiado, puede asumir dos calidades, la primera donde, a través una prima recibe un documento apócrifo, el cual, es generado por el agente de fianzas u otro tercero, y la segunda, ser el autor de la falsificación del documento evitando así pagar la prima y ser sujeto de una nueva relación contractual accesoria donde, normalmente le es exigida una contragarantía de recuperación.

En ambos supuestos, la policía cibernética jugará un papel importante para la determinación del responsable a través de investigaciones sobre este tipo de incidentes en medios electrónicos

Finalmente, es importante reflexionar que ante el supuesto donde no existe un quebranto patrimonial (delito material), si se materializa una amenaza (delito de peligro), toda vez que, a pesar de no concretarse un daño palpable, la amenaza al bien jurídico tutelado, que en el caso que nos ocupa es la confianza y el sano desarrollo del sistema financiero mexicano, si aconteció.

Dentro del sector financiero existen estrechas interconexiones que facilitarían la dispersión de ataques en los sistemas, provocando la perdida de la confianza, daños patrimoniales y trastornos operativos, por lo que las Instituciones de fianzas deberán desarrollar estrategias de seguridad con higiene cibernética, el diseño de sistemas seguros con estrategias para una pronta recuperación, en tanto que el regulador financiero, en adición a su preocupación por la implementación de normativa que considere resiliencia, deberán considerar mecanismos que permitan continuidad de los servicios críticos.

En ese contexto, la comunidad internacional deberá priorizar los mecanismos para reportar incidentes permitiendo la retroalimentación entre autoridades nacionales y extranjeras, observando en todo momento los principios que rigen la protección de datos personales, y lograr administrar eficazmente cualquier incidente,

Conclusiones

Conclusiones

Los riesgos a los que se enfrentan las Instituciones de garantías al emitir fianzas y operar en medios electrónicos son variados, ello en virtud de los nuevos modelos de negocio o mecanismos y herramientas con los que la sociedad celebra actos de comercio electrónico.

Con el paso del tiempo y gracias a las innovaciones tecnológicas, las TIC han transformado en mayor o menor medida la forma en que celebramos los contratos, dando como resultado situaciones antes no consideradas.

Cada contrato refiere situaciones especiales, cada contrato muestras aristas antes no previstas. Así pues, la figura de la fianza, contrato accesorio y por excelencia de garantía, ha mostrado aspectos legales no considerados al trasladarse al mundo digital.

El perfeccionamiento del contrato en el mundo digital es el más claro ejemplo, esto es, la manifestación del consentimiento para establecer la relación vinculante entre las partes.

La operación de las Instituciones afianzadoras en medios electrónicos para la consecuente emisión de pólizas electrónicas ha traído como consecuencia riesgos poco estudiados.

Es por esto, que la CNSF como autoridad reguladora, continúa trabajando en el desarrollo de normativa en materia de seguros y fianzas relativa, entre otros, a la seguridad de la información de las Instituciones, para poder hacer frente a riesgos consecuencia de falsificación, fraude o ataques informáticos que pudieran afectar sus operaciones y estabilidad del Sistema Financiero Mexicano y en perjuicio de los fiados o beneficiarios.

Riesgos como la recepción de una póliza digital apócrifa manipulada con herramientas electrónicas (falsificación de documentos), el uso de esa póliza electrónica con el conocimiento de ser un documento apócrifo (fraude), o la simple emisión de pólizas electrónicas de manera habitual y con fines de lucro sin contar con la autorización por parte del Gobierno Federal (delito especial previsto en la LISF), agregando el riesgo que enfrentan las Instituciones al operar en estos medios

haciendo frente a los Ciber ataques a sus sistemas informáticos, fueron los principales apartados analizados en la presente investigación.

Conocer los alcances de la Informática forense, como herramienta idónea para obtener evidencia en la comisión de un ilícito dentro del ámbito electrónico y con la que se logra la identificación, preservación, análisis e interpretación de evidencia digital para fincar, en su caso, responsabilidad, debe constituir uno de los principales objetivos de las instituciones y, en su caso, del equipo legal con el que cuente dicha sociedad.

Con base a lo planteado se pueden identificar que los riesgos que las instituciones asumen por la operación y emisión de pólizas de fianzas electrónicas se pueden abordar desde tres vertientes distintas:

- Las vertientes del ámbito del derecho mercantil y el derecho penal; puesto que se atenta contra el patrimonio de los usuarios de servicios financieros y en el caso concreto en los integrantes de la relación contractual de la fianza.

- Las vertientes del ámbito mercantil y penal que atenta contra el patrimonio de la institución ya sea por ataques a sus sistemas informáticos o por la comisión del delito de fraude derivado de pólizas apócrifas.

- Las vertientes dentro del ámbito de la Administración Pública, que atenta contra el sano desarrollo del Sistema Financiero Mexicano.

Finalmente, en lo que refiere a las situaciones que favorecen la realización de estas conductas, encontramos la nula cultura de validación de las pólizas con las propias Instituciones, acto que diezmaría la comisión de los ilícitos como falsificación y el fraude. Es necesario que la Administración Pública, quien se constituye como el principal consumidor y solicitante de esta garantía, impulse el uso de este mecanismo validador, implementando normativa que disponga llevar a cabo este ejercicio en todos los instrumentos contractuales garantizados por una fianza.

Bibliografía

- Acosta Romero, Miguel (2000). Nuevo Derecho Mercantil. México: Porrúa.
- Castells, Manuel (2001). La Galaxia Internet. Madrid: Areté.
- Cervantes Altamirano, Efrén (1950). Fianza de Empresa Antecedentes Históricos y Naturaleza Jurídica. Publicaciones del Semanario de Derecho Mercantil y Bancario. UNAM Escuela nacional de Jurisprudencia. México.
- Davara Rodriguez, Miguel Ángel (2001). Manual de Derecho Informático (4ta Edición). España: Aranzadi.
- Del Peso Navarro, Emilio (1996). Resolución de conflictos en el intercambio electrónico de documentos. Cuadernos de Derecho Judicial. Escuela Judicial Consejo General del Poder Judicial. Madrid.
- De Pina Vara, Rafael (1995). Diccionario de Derecho. México: Porrúa.
- Díaz González, Luis (2003) Documentación y Firma electrónica. Revista Nuevo Consultorio Fiscal, México: No. 344.
- López Sabater, Verónica y Ontiveros, Emilio (2017). Economía de los datos. Riqueza 4.0. Madrid: Ariel.
- Molina Bello, Manuel (2015). La fianza garantía por excelencia en México. México: Tirant Lo Blanch.
- Pérez Fernández del Castillo, Bernardo (2017). Contratos Civiles. México: Porrúa.
- Piaggi, Ana I. (1999). El comercio electrónico y el nuevo escenario de los negocios. Revista de la Asociación de Magistrados y Funcionarios de la Justicia Nacional. Buenos Aires: No. 23
- Reyes Kraft, Alfredo Alejandro (2003). La firma electrónica y las entidades de certificación. México: Porrúa.
- Robles Garay, Oscar (2000). Evolución de Internet en México y en América Latina. México: ITESM/CECSA.

- Rojina Villegas, Rafael (2006). Compendio de Derecho Civil. Volumen I. México: Porrúa.
- Rubio, Julio E. y Ordoñez, Javier (Coordinadores) (2008). Ciencia, tecnología y Sociedad en México. México: ITESM / Porrúa.
- Sánchez del Campo, Alejandro (2016). Reflexiones de una replicante legal: los retos jurídicos de la robótica y las tecnologías disruptivas. Revista de tecnología y sociedad. España: No. 16
- Sánchez Flores, Octavio Guillermo de Jesús (2001). El contrato de Fianza. México: Porrúa
- Téllez Valdés, Julio (2009). Derecho Informático (4ta Edición). México: Mc Graw Hill.
- Zamora y Valencia, Miguel Ángel (2007). Contratos Civiles. México: Porrúa.

Fuentes de consulta en internet.

- Centro Nacional de Respuesta a Incidentes Cibernéticos de la Policía Federal (2018). Blog de la Policía Federal. Recuperado de https://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es
- ECURED. Enciclopedia colaborativa en la red cubana. Informática Forense. Recuperado de https://www.ecured.cu/Inform%C3%A1tica_Forense
- International Organization for Standardization (ISO) (2012). Norma ISO/IEC 27032. Recuperado de https://www.iso27001security.com/html/27032.html
- Organización Mundial del Comercio (1998). Programa de trabajo sobre el comercio electrónico. S.L.I., Recuperado de https://www.wto.org/spanish/tratop_s/ecom_s/ecom_s.htm
- Portal Servicio de Administración Tributaria. Preguntas Frecuentes. Firma Electrónica Avanzada. Recuperado de https://www.sat.gob.mx/personas/ayuda
- Portal electrónico Diccionario de la Real Academia de la Lengua Española https://www.rae.es/

- Reyes Kraft, Alfredo Alejandro, La firma electrónica avanzada. Razón y Palabra Primera revista digital en Iberoamérica especializada en comunicología. Recuperado de http://www.razonypalabra.org.mx/libros/libros/firma.pdf

Cuerpos normativos.

- Bases de Coordinación en Materia de Seguridad de la Información, emitidas el 4 de mayo de 2018. Link de consulta: https://www.gob.mx/cms/uploads/attachment/file/332698/Ciberseguridad-Bases_Coordinacion.pdf
- Circular Única de Seguros y Fianzas, publicada en el Diario Oficial de la Federación el 19 de diciembre de 2014, última reforma publicada en el Diario Oficial de la Federación el 8 de enero de 2024. Link de consulta: https://www.gob.mx/cms/uploads/attachment/file/882077/Circular__nica_de_Seguros_y_Fianzas_compulsada_sin_Anexos___actualizada_08-01-2024_.pdf
- Código Penal Federal, publicado en el Diario Oficial de la Federación el 14 de agosto de 1931, última reforma publicada en el Diario Oficial de la Federación el 18 de octubre de 2023. Link de consulta: https://www.diputados.gob.mx/LeyesBiblio/ref/cpf.htm
- Código de Comercio, publicado en el Diario Oficial de la Federación el 13 de diciembre de 1889, última reforma publicada en el Diario Oficial de la Federación el 28 de diciembre de 2023. Link de consulta: https://www.diputados.gob.mx/LeyesBiblio/ref/ccom.htm
- Código Federal de Procedimientos Civiles, publicado en el Diario Oficial de la Federación el 24 de febrero de 1943, última reforma publicada en el Diario Oficial de la Federación el 7 de junio de 2021. Link de consulta: https://www.diputados.gob.mx/LeyesBiblio/ref/cfpc.htm
- Código Civil Federal, publicado en el Diario Oficial de la Federación el 26 de mayo, el14 de julio, el 3 y 31 de agosto de 1928, última reforma publicada en

el Diario Oficial de la Federación el 11 de enero de 2021. Link de consulta: https://www.diputados.gob.mx/LeyesBiblio/ref/ccf.htm

- Convenio de roma de 1980 sobre la ley aplicable a las obligaciones Contractuales, publicado en el Diario Oficial de las Comunidades Europeas el 26 de enero de 1998. Link de consulta: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:41998A0126(02)&from=LT
- Directiva 199/93/CE del parlamento europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, publicado en el Diario Oficial de las Comunidades Europeas el 19 de enero de 2000. Link de consulta: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31999L0093&from=ES
- Directiva 2002/58 de 12 de julio de 2002, sobre tratamiento de datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas, publicado en el Diario Oficial de las Comunidades Europeas el 31 de julio de 2002, última reforma publicada en el Diario Oficial de las Comunidades Europeas el 30 de julio de 2021. Link de consulta: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32002L0058
- Directiva 2000/46/CE del parlamento europeo y del Consejo de 18 de septiembre de 2000, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como la supervisión cautelar de dichas entidades, publicada en el Diario Oficial de las Comunidades Europeas el 27 de octubre de 2000, última reforma publicada en el Diario Oficial de las Comunidades Europeas el 10 de octubre de 2009. Link de consulta: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32000L0046
- Directiva 2000/31/ce del parlamento europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), publicada en el Diario Oficial de las Comunidades Europeas el 17 de julio de 2000, última reforma publicada en el Diario Oficial de las Comunidades Europeas el 27 de

octubre de 2022. Link de consulta: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32000L0031

- Directiva 95/46 CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, publicada en el Diario Oficial de las Comunidades Europeas el 23 de noviembre de 1995, última reforma publicada en el Diario Oficial de las Comunidades Europeas el 31 de octubre de 2003. Link de consulta: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046
- Estrategia Nacional de Ciber Seguridad 2017. Link de consulta https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf
- Ley Federal de Telecomunicaciones, publicada en el Diario Oficial de la Federación el 14 de julio de 2014, última reforma publicada en el Diario Oficial de la Federación el 20 de mayo de 2021. Link de consulta: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017. Link de consulta: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf
- Ley de Instituciones de Seguros y de Fianzas, publicada en el Diario Oficial de la Federación el 4 de abril del 2013, última reforma publicada en el Diario Oficial de la Federación el 11 de mayo de 2022. Link de consulta: https://www.diputados.gob.mx/LeyesBiblio/pdf/LISF.pdf
- Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Comercio Electrónico, 85 sesión plenaria el 16 de diciembre de 1996. Link de consulta: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453_s_ebook.pdf
- Ley de Protección y Defensa de los Usuario de Servicios Financieros, publicada en el Diario Oficial de la Federación el 18 de enero de 1999, última reforma publicada en el Diario Oficial de la Federación el 9 de marzo de 2018.

Link de consulta: https://www.diputados.gob.mx/LeyesBiblio/pdf/64_090318.pdf

- Ley Sobre el Contrato de Seguro, publicada en el Diario Oficial de la Federación el 31 de agosto de 1935, última reforma publicada en el Diario Oficial de la Federación el 4 de abril de 2013. Link de consulta: https://www.diputados.gob.mx/LeyesBiblio/pdf/211.pdf
- Reglamento del Código de Comercio en materia de prestadores de servicios de certificación, publicada en el Diario Oficial de la Federación el 19 de julio de 2004. Link de consulta: https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_CComer_MPSC.pdf
- Reglas generales a las que deberán sujetarse los prestadores de servicios de certificación, publicadas en el Diario Oficial de la Federación el 14 de mayo de 2018. Link de consulta: https://www.dof.gob.mx/nota_detalle.php?codigo=5522462&fecha=14/05/2018#gsc.tab=0
- Tratado de Derecho Civil Internacional de Montevideo de 1940, suscrito el 19 de maro de 1940, publicado por Decreto 7771/56 de 27 de abril de 1957. Link de consulta: http://www.consulex.com.ar/Legislacion/Leyes/Tratado%20derecho%20procesal%20internacional%20Montevideo%201940.htm