UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES
ESCUELA PROFESIONAL DE DERECHO

Fraude informático frente a la libertad de empresa como garantía constitucional, Lima, 2023

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Abogada

AUTORA:

Chumbe Huarhuachi, Briggit Bettsy (orcid.org/0000-0001-5233-5601)

ASESOR:

Dr. Santisteban Llontop, Pedro Pablo (orcid.org/0000-0003-0998-0538)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal, Procesal Penal, Sistema de Penas, Causas y Formas del Fenómeno Criminal

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2023

DEDICATORIA

A Dios todopoderoso que en su infinita misericordia me ha permitido concluir con el desarrollo de mi tesis, que será el inicio de muchas metas por cumplir, concediéndome la dicha de permitirme celebrar y gozar de cada esfuerzo y meta concluida, a mi amada madre Huarhuahi Sánchez Magdalena, mujer guerrera quien es mi inspiración, mi fortaleza y quien ha sacrificado todo para yo obtener este logro, la que ha sido testigo de mi esfuerzo y mi compañera en cada día para cumplir esta meta que es de las dos. A mi tía Huarhuachi Sánchez Lidia, por el apoyo incondicional que me da día a día.

AGRADECIMIENTO

Agradezco a Dios, a mi madre y a mi distinguido profesor Pedro Pablo Santisteban, por haberme guiado en este camino rumbo al éxito, por haberme exigido en mejorar en cada clase.

Sin la participación de estas personas no me hubiera sido posible concluir mi tesis, por ello les agradezco de todo corazón.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La investigación nace por el incremento de casos de fraudes informáticos llegando a niveles organizacionales, que generan impacto significativo en la libertad de empresa, generando diversas consecuencias negativas, trayendo consigo riesgos para la sociedad, empresas y gobierno; cuyo **objetivo** es analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional. Siendo ello un derecho fundamental de las personas y organizaciones a establecer, operar y desarrollar actividades económicas y comerciales.

En ese sentido, la **metodología** busca abordar un análisis cualitativo, básico, hermenéutico bajo la teoría fundamental, para su aplicación se recolectó información de bases de datos y hallazgos ya existentes de los libros, revista indexadas, leyes y resoluciones, las técnicas empleadas fueron la entrevista y el análisis de documento. **Resultado y conclusión,** los fraudes informáticos han llegado a niveles organizacionales, evidenciando que la mayoría de empresas no emplean medidas y estrategias de seguridad para prevenir o minimizar un posible fraude informático, se señala la importancia de salvaguardar la base de datos, para contrarrestar los fraudes informáticos,

Palabras clave: Fraude informático, libertad de empresa, derecho informático

ABSTRACT

The investigation was born due to the increase in cases of computer fraud reaching organizational levels, which generate a significant impact on business freedom, generating various negative consequences, bringing risks for society, companies and government; whose objective is to analyze how computer fraud affects business freedom as a constitutional guarantee. This being a fundamental right of people and organizations to establish, operate and develop economic and commercial activities.

In this sense, it seeks to address a qualitative, basic, hermeneutic analysis under the fundamental theory, for its application information was collected from existing databases and findings from books, indexed journals, laws and resolutions, the result indicates the importance of safeguarding. the database, to counteract computer fraud.

Keywords: IT fraud, business freedom, IT law

I. INTRODUCCIÓN. - Sobre la **aproximación temática**, se precisa aspectos esenciales **a nivel internacional**, en la era de la tecnología y de la industria 4.0, los delitos informáticos generaron impacto económico en las empresas mediante las nuevas modalidades de delinquir de los ciberdelincuentes; en varios países latinoamericanos han incrementado +25% en delitos informáticos (Campos, 2019, p. 101). Por ello, las empresas transnacionales cerraron brechas en su seguridad digital invirtiendo en especialistas de ciberseguridad, asimismo, utilizaron tecnologías emergentes como la inteligencia artificial para poder garantizar su libertad económica; claro ejemplo países como China, Canadá, Japón, Reino Unido regularon legalmente la inteligencia artificial para el desarrollo que Fomentar el uso de la inteligencia artificial y promover el desarrollo económico y social.

En comparación **a nivel nacional,** se vio que las empresas se enfrentan a una creciente amenaza de delitos informáticos que afectan su libertad de operación, seguridad, competitividad. Por ello, la creciente incidencia de fraudes informáticos y sus subtipos afecta a las empresas y su libertad para operar en entornos digitales; estos incidentes pueden causar graves daños económicos y reputacionales a las empresas, así como socavar la confianza del público. El Ministerio Público (2022) las fiscalías provinciales penales, especializadas y mixtas han registrado un incremento significativo, donde en el 2021 se registró 57.63% de delitos informáticos, mientras tanto en el 2022 incrementó en un 72.74 % de delitos registrados.

En concordancia con lo mencionado, la libertad de empresa como garantía constitucional se refiere al derecho fundamental de las personas y organizaciones a establecer, operar y desarrollar actividades económicas y comerciales sin interferencias indebidas del Estado u otros actores. Esta garantía está reconocida en numerosas constituciones y tratados internacionales como un componente esencial de derechos y/o económicos y sociales para que la nación se desarrolle; sobre todo luego de la crisis de los 90 que el Perú implementaron políticas de libre mercado.

Para evitar el fraude informático, se ha implementado métodos y técnicas de inteligencia artificial o IA propiamente en la mayoría de empresas de América Latina y del Perú, sobre todo en áreas como operaciones con tecnología de la información, ciberseguridad y automatización de los procedimientos de negocios ya que vuelve

complejo el vencer a la IA. Conforme al estudio del IBM (2022), el mayor porcentaje de uso de la IA en detección de amenazas y ciberseguridad, corresponden al 44% de su aplicación. El Diario “El Comercio” (2022) señaló que, en el 28% de empresas en el Perú, han logrado implementado la inteligencia artificial en sus operaciones comerciales, sin embargo, aún no contemplan su uso especializado para la prevención de la seguridad de información frente al delito informático, donde está el fraude.

La realidad problemática, es que los fraudes informáticos generan impacto significativo en la libertad de empresa, generando diversas consecuencias negativas como: la pérdida de recursos financieros generando inestabilidad financiera de la empresa, limitando su capacidad para invertir, crecer y competir en el mercado, genera el daño a la reputación y pérdida de confianza. Cuando una empresa se convierte en víctima de fraude informático, su reputación puede sufrir un daño significativo, los clientes, proveedores y socios comerciales pueden perder confianza en la empresa y dudar de su capacidad para proteger sus datos y garantizar transacciones seguras, asimismo, la pérdida de contratos comerciales y una imagen negativa en el mercado, restringiendo la libertad de la empresa para operar y crecer.

En este contexto, se formuló el siguiente **problema general** ¿De qué manera el fraude informático afecta la libertad de empresa como garantía constitucional?, a continuación, formulamos como **problema específico 1** ¿De qué manera la ciberseguridad garantiza la libertad de acceso de mercado como garantía constitucional?, y como **problema específico 2** ¿De qué manera el derecho a la protección de datos contribuye a la libertad de la organización empresarial como garantía constitucional? Derecho de protección de datos

En ese sentido, se establece el **objetivo general**: Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional. Asimismo, como **objetivo específico 1**, Analizar de qué manera la ciberseguridad garantiza la libertad de acceso de mercado como garantía constitucional; y como **objetivo específico 2**, Analizar de qué manera el derecho a la protección de datos contribuye a la libertad de la organización empresarial como garantía constitucional.

La investigación tuvo como **justificación teórica**, el analizar y evaluar el marco teórico existente, políticas, marcos legales y medidas de protección más sólidas y efectivas para preservar la libertad empresarial en la era digital existente, desde una perspectiva constitucional y legal; con el fin de generar conocimiento académico y científico en este campo, mientras que la **justificación práctica**, la investigación permitió contribuir a la identificación de vulnerabilidades y desafíos específicos que enfrentan las empresas en relación con la protección de su información, datos y operaciones en el entorno digital; además, la investigación proporcionó información relevante para la implementación de medidas preventivas y la adopción de estrategias de seguridad, por último la **justificación metodológica**, va de la mano con la gruía de entrevista y la ficha de análisis documental, para así rescatar la indagación comprendida por los expertos que consolidaron el presente trabajo.

En ese sentido, como **contribución** la creación de un organismo autónomo regulador, fiscalizador que supervise que tanto empresas públicas y privadas cumplan con las normas y políticas de seguridad de información, así mismo el establecer conductas infractoras en las materia administrativa y penal para aquellas personas que incumplimiento, y proponer lineamientos de uso de la inteligencia artificial en la seguridad de la información de las empresas conforme al derecho comparado y soporte jurídico internacional para garantizar la prevención de los delitos informáticos.

Aunado a ello, la **relevancia** de la presente investigación es poder garantizar la libertad de empresa, previniendo el fraude informático con el uso de las tecnologías emergentes de la actualidad como la inteligencia, las regulaciones de la inteligencia artificial, desafíos y oportunidades para el Perú; para así lograr un desarrollo económico libre de obstaculizaciones.

Finalmente, se consideró como **supuesto general**, el fraude informático afecta la libertad de empresa como garantía constitucional. Además, como **supuesto específico 1**, la ciberseguridad garantiza la libertad de acceso al mercado como garantía constitucional. Y finalmente, como **supuesto específico 2**, el derecho a la protección de los datos contribuye a la libertad de la organización empresarial como garantía constitucional.

II. MARCO TEÓRICO. - **E**ste capítulo de trabajo de investigación, desarrolló trabajos previos, investigaciones que fueron realizados con posterioridad, cuyos antecedentes tienen mayor relevancia para la investigación de la tesis con propuestas de nivel nacional e internacional, revistas indexadas, libros, con la finalidad de aportar y contribuir en las respuestas a los objetivos planteados.

En relación a los **antecedentes internacionales**, desde la posición de **Lux y Calderón** (2020) nos comenta que en Chile el **fraude informático** es una modalidad de delito informático, su interés jurídico común es una función informática, la cual se define como algo que permite a un sistema informático realizar operaciones de almacenamiento y procesamiento correctamente. Un conjunto de condiciones. y transferencia de datos en el marco de riesgos aceptables. Estas condiciones pueden ser violadas por interacciones que ocurren en el ciberespacio, similares a las que ocurren en el tráfico vehicular. (p. 155) Es por ello que el ilícitos de fraude informático es de carácter pluriofensivo, ya que trae como consecuencias lesiones relacionados con los datos como la funcionalidad informática y el bien patrimonial.

Por otro lado, en Brasil **Minahim y Spinola** (2017) menciona que, la influencia del comportamiento de las víctimas en el **fraude informático** conlleva a riesgos creados por la popularización de los dispositivos tecnológicos, las cuales son detectadas mediante técnicas para cometer fraude es en colaboración de la víctima, la que es una pieza fundamental para la consumación del delito. (p. 158) En ese sentido el uso de Internet debe ser realizando cautelosamente, de no ser observada por la víctima, puede reducir la pena para el ejecutor y, en casos extremos, la conducta del ejecutor no se considera delictiva.

Según **Lux** (2018) en Europa, precisa que, la doctrina coincide que la participación de la víctima juega un importante papel en la prevención de los **fraudes informáticos**, ya que los riesgos que son creados mediante el uso de internet pueden ser disminuidos, con la adopción de medidas de seguridad de autoprotección, ya que muchos delitos informáticos suceden por la vulnerabilidades de los sistemas informáticos, que suceden por diversas causas, como una programación deficiente, el cambio tecnológico o un uso de ventana que pueden haberse dejado abiertas. (p. 192) En ese sentido, la medida de autoprotección que puedan usar las víctimas disminuirá la vulnerabilidad de los sistemas informáticos,

se reducirán probabilidades de que terceros accedan a ellos y puedan cometer alguna ilícito.

De acuerdo con **Barceló** (2021) la **ciberseguridad** blockchain en España, como una base de datos mantenidas mediante distribución de ordenadores, las características esenciales serian su certeza, seguridad, inmutabilidad e irrefutabilidad; Así mismo la tecnología blockchain excluye cualquier intermediario como la cadena de bloques es un registro de transacciones; también es usada como plataforma que va permite dichas transacciones. Es decir, va actuar como registro compartido e identifica, inequívocamente, los datos anotados, ello da soporte a la Ley General de Defensa de los Consumidores y Usuarios entre otras leyes complementarias. (p. 39) En esa misma línea **Ablon** (2018) indica que se sigue evolucionando con la tecnología para los consumidores tradicionales, cualquier cosa nueva (dispositivos móviles, computación en la nube, plataformas de redes sociales) proporciona nuevos puntos de entrada para los ataques y, por lo tanto, conducirá a una explotación equitativa del mercado negro. (p. 9) Por lo tanto, es un registro permanente de la tecnología, que viene dando soporte legal a la información disponible para todos los asociados a la red.

Según **Mendoza** (2018) manifiesta que el **derecho de protección de datos**, en México si bien en cierto de la regulación en materia de protección de datos personales para empresas públicas y privadas garantiza un derecho humano, también es un beneficio económico a nivel internacional, la cual deben tener un alto nivel adecuado de protección de la información, ello para que el país se pueda declarar seguro en el intercambio comercial. (p.589) En ese sentido los derechos y privacidad de datos personales tienen un alto valor económico y social en su protección, ya que reside oportunidad para generar confianza entre los clientes y usuarios de servicios, para fortalecer el modelo de negocio.

Dentro del contexto de los trabajos previos **nacionales, Beaumont** (2023) menciona que **la libertad de empresa** en el ejercicio de estos derechos sin perjuicio de la moral, la salud o la seguridad pública; cooperación entre el Estado y empresas estatales o privadas, libertad de contratación, libre competencia, igualdad de condiciones para las inversiones nacionales y extranjeras, almacenamiento y disposición de divisas y adopción de normas dentro de la economía social de mercado, protección interna y protección del consumidor. (p.

16) Por tanto, la iniciativa privada es libre, lo es y seguirá siendo, porque el Estado es el escudo constitucional del sistema económico y debemos conservarlo, tratar de corregir su realización y todo lo que interfiera en la creación de la igualdad para todos sociedad y mejores oportunidades.

Carrasco (2018) Afirma que la **libertad de empresa** constituye estrictamente una clase de instrumentos que confiere importancia constitucional porque apoya y sirve a los derechos fundamentales, y su formulación e implementación jurídica está sujeta al contenido axiológico expresado de los derechos fundamentales. (p. 920) Teniendo en cuenta lo anterior, la libertad de negocios incluye el derecho de todas las personas naturales o jurídicas a participar en la vida económica del país, a producir y vender bienes y servicios, a organizar el capital y el trabajo.

Además, **Téllez et al.** (2022) Desarrollo que, La manera de abordar las cláusulas infractoras de la **libertad de empresa** es analizarlas no como infracciones puramente accidentales, incidentales, temporales o reales, sino como injusticias deliberadas, a menudo contra los empresarios. Las estrategias comerciales responden y, por lo tanto, influyen en una base universal y sistemática para una amplia gama de consumidores. (p. 94) Por lo tanto, es necesario desarrollar un marco teórico legal que defina la libertad empresarial de manera suficientemente científica para ver las condiciones bajo las cuales puede ocurrir el abuso.

A juicio de **Acosta et al.** (2020) expresa que **la libertad de organización de empresa** en Perú la prevención y sanciones contra quienes violan las normas, los organismos responsables de hacer cumplir esta ley se basan únicamente en programas cibernéticos que brindan recomendaciones para reducir los riesgos y demuestran que una de las mejores armas en este sentido es la prevención y la seguridad. (p. 15) En este sentido, el propósito de la ley es garantizar el derecho a la protección y confiabilidad de la información en línea y combatir a los autores que ataquen ilegalmente a los usuarios de dicha información.

A juicio de **Cabrera** (2017) en el Perú el **derecho de protección de datos** en las empresas debe tomar la iniciativa en la regulación del contenido que respalda y cumpla con los estándares para ejercer estos derechos en Internet. Un ejemplo sorprendente es el caso de Facebook, donde las normas comunitarias diseñadas

para controlar el abuso generalizado violan la ley y violan la privacidad en Internet, igualdad y otros derechos. (p. 219) En ese sentido la existencia de vacíos que existe en la Ley, se va generando a lo largo de la existencia por falta de expertos que puedan dar una efectiva regulación del derecho que se van perdiendo por medio de la tecnología y la adecuada tipificación que se deben aplicar a los que comente los ciberataques.

En el **Perú**, se regula la **protección de datos** mediante la Ley N.º 29733, donde establece el tratamiento responsable de los datos personales que su ámbito de aplicación es a todas la entidades públicas y privadas que traten datos personales de los conciudadanos peruanos, la Ley se aplica a todas las entidades públicas y privadas, contempla principios del tratamiento de datos personales, seguridad, entre otros, también establece obligaciones para quienes tratan la información, incluyendo la implementación de medidas de seguridad y la notificación de incidentes de seguridad, ahora bien, en cuanto a las fortalezas de la presente Ley, cuenta con principios claros, proporciona un marco ético de las prácticas de privacidad, asimismo, establece una autoridad supervisora para fortalecer la aplicación y el cumplimiento de la normativa (Congreso de la República, Ley N.º 29733, Ley de Protección de Datos Personales)

En relación a **fundamentación teórica** respecto a las categorías y subcategorías. En relación al **fraude informático**, **Brenner** (2016) menciona que es un concepto que sigue en evolución, por lo cual lo define como aquella acción de usos tecnológicos en línea, como uno en Internet, para robar acceder a información confidencial con fines ilícitos para interferir en el uso y disfrute de la propiedad de otra persona. (p. 819) En ese sentido el impacto legal de este tipo de fraude, el cual es considerado la necesidad de crear nuevas leyes aplicables que velen por la seguridad de los usuarios y sus propiedades informáticas en el contexto de la modernización tecnológica, donde la autora menciona diversos antecedentes que llevaron a la creación de estas leyes.

Acuario (2016) entiende que **el fraude informático** es toda acción que es cometido con dolo, con la finalidad de provocar un perjuicio a personas o entidades mediante dispositivos habitualmente informáticos; Es el acto de índole ilegal que se encuentra direccionado en contra de la confidencialidad, integridad y los recursos a nivel informático, redes y documentos informáticos, abusando

indiscriminadamente sobre dichos sistemas. (p 12) En razón a ello los agentes comete de manera dolosa y acto ilícito mediante la accesibilidad que tiene como trabajador, haciendo uso de su posición especial de acceso a la base de datos.

Kynigopoulo (2019) comenta que las consecuencias son a nivel de compañía, donde puede acceder a la información financiera como créditos y débitos; impactar en la disrupción tecnológica, donde la empresa tiene que invertir en nuevas tecnologías; dañar la reputación de la marca, entre otros. A nivel de usuario afecta en obtener información personal, reemplazar su identidad ante bancos, empresas, otros. (p. 3)

En cuanto a las **subcategorías** de la categoría de **fraude informático** se posee los siguientes:

En este aspecto, **Fernández y Vargas** (2018) comentan sobre ciberseguridad, el aumento de los delitos informáticos es uno de los problemas más graves y recientes en el Perú, y el fácil acceso del país a la tecnología y las condiciones socioeconómicas lo convierten en un lugar adecuado para los delitos cibernéticos. (p. 37) El personal involucrado en el procesamiento de estos delitos, como la policía, está en desventaja porque no cuenta con recursos adecuados para combatirlos; es relevante la capacidad de los empleados de las comisarías para utilizar las tecnologías de la información y las comunicaciones (TIC) como función de seguridad. **Zhang y Dong** (2023) sostienen que cada gobierno debe implementar capacidades disruptivas en gobernanza digital en la nueva era de la nube informática así las normativas y acciones sean trasversal para toda la nación y la respuesta sea rápida y segura. (p. 2)

Echevarría et al. (2020) infiere que la **ciberseguridad** es necesaria, ya que los bancos están empezando a introducir nuevas tecnologías en aplicaciones móviles que permitirán controlar servicios financieros, con la nueva convergencia de servicios financieros y aplicaciones móviles, es importante comprobar qué tan preparados esta la sociedad para evitar el acceso no autorizado a sus datos personales. (p. 75) Los ciberataques amenazan a todos y a las instituciones del Perú, afectando a las personas y si las personas están tomando las medidas adecuadas para proteger sus datos.

De la misma manera el **derecho de protección de datos** desde la posición de **Mendoza** (2021) es la forma que depende de cada individuo decidir cómo,

cuándo y en qué medida puede revelar su información personal a otros, intentar proteger la privacidad contra posibles ataques arbitrarios y establecer mecanismos legales para la protección general de la privacidad. (p. 189) En este sentido, el derecho a la protección de datos personales es proteger el derecho del titular de los datos personales a tomar decisiones, salvo excepciones legales, es deber del Estado proteger la privacidad de las personas (Malik y Choudhury, 2019, p. 75).

Así mismo **Veliz** (2022) menciona que el **derecho de protección de datos** es la privacidad de información, pero no es privada en su totalidad, ya que es expuesta, como también se expone información de los demás, por ello la privacidad no es exclusivamente un asunto personal, ya que también sería un asunto político; no solo es un derecho individual, es de responsabilidad social. (p. 282-283) En ese sentido nuestros datos personales contienen los datos de otros individuos, pero, y sobre la pérdida de la privacidad nos conlleva a consecuencias negativas a nivel público, es derecho a la privacidad es un bien público la cual debe ser defendida por los seres humanos como un deber público.

En cuanto a la **libertad de empresa** para **Torres** (2020) menciona que los derecho o facultades que poseen cada persona natural o jurídica tiene para la realización o conformación de empresas, y que esta misma acción se encuentra reconocida en el artículo 59 de nuestra carta magna, siendo esta facultad protegida y respaldada por la norma de carácter constitucional. (p. 2)

En concordancia con **Viera** (2016) destaca que este derecho, consagrado en las constituciones, busca no solo garantizar que las personas tengan voz en la construcción de su propio destino, sino también establecer el marco legal que proteja los bienes jurídicos de la sociedad. (p. 198) En ese sentido la libertad de empresa es una garantía constitucional, que va de la mano como un derecho es fundamental para empoderar a los individuos y asegurar un entorno legal seguro de la economía de las personas, ya sean naturales o jurídicas.

Desde la posición de **Rodríguez** (2016) Referido a la **libertad de acceso de mercado**, a través de la denominada libertad de creación de empresas, que protege el derecho a crear empresas y a operar en el mercado, de acuerdo con la denominada libertad de entrada en el mercado, cualquier persona con capacidad para producir bienes o prestar servicios deben tener acceso al mercado en condiciones autodeterminadas, es decir, sin que nadie pueda impedir o restringir

dicha participación, como tampoco el Estado ni agentes económicos. (p. 123) En ese sentido, la libertad de organización de la empresa, que se ofrece al empresario para que así obtenga la facultad de fijar sus propios objetivos para orientar y organizar sus diversas actividades (libertad de gestión de la empresa) con función de sus recursos y de las circunstancias del mercado. En otras palabras, permite estructurar la actividad empresarial mediante la adopción de un orden interno, también es crucial, ya que permite al empresario coordinar los numerosos factores que le permitirán alcanzar el éxito económico en la actividad elegida.

Como plantea **Aliaga** (2021) respecto a la **libertad de organización de empresa,** es el terreno donde la organización empresarial es un derecho realizado como el aporte más importante al desarrollo de la economía nacional, porque cada ordenamiento jurídico crea formas diferentes para el desarrollo más ordenado de las diversas manifestaciones del negocio o empresa a fundar, teniendo en cuenta la voluntad individual o colectiva de la sociedad; Se define de diferentes maneras, pero la atención se centra siempre en la situación económica. (p. 184) En este sentido, se puede entender empresa como cualquier unidad socioeconómica o unidad de producción organizada por una o más personas que buscan obtener intereses o ganancias mediante la gestión de factores de producción, capital y trabajo.

Finalmente, en relación con los **enfoques conceptuales**, es preciso indicar que el **delito informático** o también conocido como ciberdelito es cualquier acto ilícito, inmoral o no autorizadas, que son cometido en un entorno digital, espacio digital o en Internet, este con el objetivo de dañar bienes patrimoniales de terceras personas como también a las entidades públicas y privadas, propiedades legales y protegidas, así mismo el **bien jurídico protegido** son conceptualizados como derechos fundamentales tutelados por el estado para las personas en la sociedad, y su universalidad es reconocida en el ordenamiento jurídico y sujeta a la doble y mayor protección del derecho penal, también está en el centro de la visión y el contenido de la ley de sanciones de garantía aplicable; Así mismo la **garantía constitucional**, consiste en un conjunto de mecanismos instituida por la Constitución; con el objetivo de prevenir, disminuir o enmendar la violación de una garantía constitucional, un derecho reconocido por ella; como también el poder proteger a determinados principios constitucionales.

III. METODOLOGÍA. – El trabajo de investigación fue desarrollado mediante la metodología de investigación, la cual busca sustentar el desarrollo de la tesis, bajo parámetros que se exige cumplir**,** ya que busca datos que son comprendidos empíricamente, el cual produce conocimientos que puede ir cambiando.

Es ese sentido el trabajo es de **enfoque cualitativo**, este método describirá la naturaleza del problema a resolver y analizar, por lo que en este estudio realizo un estudio analítico para poder explorar y comprender fenómenos sociales y humanos complejos como experiencias, comportamientos y emociones, ante ello, **Rosales** (2023) se basa en el análisis interpretativo y parte de cada investigador individual, complementado con diferentes métodos de análisis y recolección de datos no estructurados, por ejemplo, entrevistar a los participantes. (s.p.) así mismo **Iño** (2018) menciona que en este enfoque tiene mayor facilidad de acceso en la contribución a la humanidad social, con la finalidad de poder aclarar la interacción con la persona que investiga. (pp. 105-106).

3.1. Tipo y diseño de investigación

Esta tesis es de **tipo básico**, ya que este tipo investigación debe aspirar a convertirse en la base o pilar de futuras investigaciones, contiene información que contribuye a su desarrollo y especialización, lo cual es claro que en su aplicación misma generará nuevo conocimiento que contribuirá a este trabajo futuro, y donde se evidencia un estudio directo del fenómeno a analizar, en su implementación se utilizará el método científico para determinarlo; en esa línea **Esteban** (2018) resalta que la investigación es el soporte a aquellos fundamentos de investigación. (p. 1)

En esa misma línea **Ñaupas et al.** (2018) infiere que en el tipo básico se recogerá distintos conceptos de los encuestados que interactúan con el fenómeno estudiado para luego analizarlo, teniendo en cuenta el aporte del marco teórico, para obtener resultados de investigación que nos permitan contribuir al estudio de la investigación. (p. 133)

Respecto a las características que tiene el enfoque cualitativo, la tesis desarrollo el **nivel descriptivo** porque nos permite la descripción de la problemática dentro de su propio contexto, logrando así verificarse sobre la comisión de los delitos informáticos y su incidencia dentro de la libertad de empresa dentro de nuestro sistema jurisdiccional, y la cual se encuentra amparada por nuestra constitución de forma adecuada y asertiva. **Gallardo** (2018) es el acto de describir

nuestro problema sobre la base de su propia realidad, y su contexto claramente ancla actores que contribuirán a la investigación dentro de su desarrollo. También destaca el carácter funcional que ofrece este nivel dentro de la funcionalidad central del tema y su diferenciación en contextos sociales, legales y empresariales. (p. 17)

Esta tesis tuvo como diseño la **teoría fundamental**, porque se relaciona con la naturaleza de la investigación, pero es una teoría estable, fortalecida en el proceso de trabajo, y sus características metodológicas radican principalmente en el estudio teórico de las siguientes cuestiones: el objeto de estudio , uno de sus elementos, o cómo su decisión la fuente del factor sería la misma experiencia al respecto **Ibarra et al**. (2018) mencionaron que cada fuente empírica se refleja en la definición de hallazgos, los cuales deben estar sustentados en la información y teoría recolectada y vinculados a la pregunta de investigación.

Pertenece al paradigma hermenéutico, ya que permite obtener un conocimiento más profundo o integral de los primeros conocimientos adquiridos, lo que permitirá comprender lo que sucede en el objeto estudiado y brindar una explicación esquemática de lo aprendido. **Quintana y Hermida** (2019) dicen: “Se busca una conclusión pedagógica porque explica el papel de la educación en el desarrollo humano, mientras que el método apunta a procedimientos para una interpretación más profunda de las prácticas culturales en la actividad educativa”. (p. 75).

3.2. Categorías, Subcategorías y matriz de categorización.

Es necesario indicar que en este punto de la investigación se destacó aquel valor que poseen las categorías y subcategorías, partiendo del estudio cualitativo, que se examinó las ideas principales de la temática; en ese sentido, se precisó un concepto amplio con relación al análisis de lo destacado en la conceptualización, ello nos llevó a los planteamientos de los problemas generales y específicos.

En ese sentido, se expuso las categorías y subcategorías de la siguiente manera: Como **categoría 1** se desarrolló el **fraude informático**, que es una de las modalidades del delito cibernético que se encuentra en la Ley N°30096 específicamente en el artículo ocho, Según **Brenner** (2016) es la manifestación de hacer uso del servicio informático en línea, como es el Internet, para robar la propiedad de otra persona o para interferir en el uso y disfrute de la propiedad de otra persona. (p. 817).

Por ello, surgió la **subcategoría 1**, que es la **ciberseguridad,** se refiere a las implicaciones legales y jurídicas que surgen como resultado del avance y la adopción de nuevas tecnologías en la sociedad. Estos impactos legales pueden afectar diversos aspectos de la vida, los negocios y la regulación gubernamental, y como **subcategoría 2**, el **derecho de protección de datos** son las facultades inherentes a las personas para proteger su dignidad y su libertad, mientras que la privacidad se refiere a los derechos de todas las personas a controlar su información personal y mantenerla protegida de accesos no autorizados. La privacidad es un componente importante de varios derechos, como el derecho a la intimidad y el derecho a la libertad de expresión.

Como **categoría 2,** se abordó la **libertad de empresa**, la cual es un derecho constitucional que es primordial para la economía intervenida en nuestra población, mediante ello las personas deben hacer uso del derecho constitucional, por el cual el estado otorga a los empresarios realizar negocios sin trabas del gobierno. A razón de ello se estudió dos subcategorías, la **subcategoría 1,** se estableció la **libertad de acceso de mercado**, referido a operar en el mercado, de acuerdo con la denominada libertad de entrada en el mercado. Cualquier persona con capacidad para producir un bien o prestar un servicio debe tener acceso al mercado en condiciones autodeterminadas y la **subcategoría 2,** se desarrolló la **libertad de organización de empresa,** es la facultad que tiene el empresario para determinar su objetivo, posibilidades de objeto, nombre, domicilio, tipo de negocio o tipo de sociedad mercantil, poderes administrativos, fijación de precios, políticas de crédito y seguros, contratación de personal, política publicitaria, etc.

3.3. Escenario de estudio

El escenario de estudió se desarrolló en el distrito de Cercado de Lima, ubicado en la parte central de Lima Metropolitana, provincia y región de Lima - Perú, con una superficie de 21,98 km2 y 271 mil residentes. Tenemos al centro histórico como parte de este distrito, que fue declarado patrimonio cultural por el órgano del gobierno de las áreas protegidas, el año 1991, Considerado también la ciudad de los reyes durante la conquista

El distrito de Lima o Cercado es uno de los distritos más antiguos del Perú. La esperanza de vida es de más de 195 años. Su encanto radica sobre todo en su ubicación, actividad comercial y lugares históricos protegidos.

Figura 1

Mapa del Cercado de Lima

Nota. Mapa del Cercado de Lima. Tomado de *Libertad para caminar en el Centro de Lima* [Fotografía] La República, 2022, https://larepublica.pe/

3.4. Participantes

La tesis contó con nueve especialistas, a las que se realizaron por conveniencia la aplicación de la guía de entrevista, quienes son representantes del sistema de justicia del Cercado de Lima, especialistas en derecho penal, derecho informático, Dirección de Investigación Criminal (DEPINCRI), fiscales provinciales. Profesionales que cuentan con formación jurídica, con un amplio conocimiento en derecho penal, policías instituidos en el ámbito jurídico, que por su experiencia laboral fueron de gran aporte para ampliar los conocimientos.

Tabla 1

Cuadro de participantes del estudio

N°	ESPECIALISTA	PROFESIÓN	EXPERIENCIA LABORAL

1	Marquera Platero, Lester Manahen	Abogado Mg. En Derecho Penal	Fiscal adjunto provincial, de la Fiscalía Especializada de delitos de ciberdelincuencia, con más de 13 años de experticia.
2	Araujo Chávez, Alan Roldan	Abogado Mg. En Derecho Penal	Fiscal adjunto provincial, de la Fiscalía Especializada de delitos de ciberdelincuencia, con más de 10 años de experticia.
3	Pomacanchari Torres, Jorge	Abogada Mg. En Derecho Penal	Fiscal adjunto provincial del Ministerio Público, con más de 10 años de experiencia.
4	Quispe Quispe, Juan Pablo	Ciberpolicía- Efectivo Policial de la DIVINDAT	Trabaja en la división de investigación de delitos de alta tecnología - DIVINDAT con más de 2 años de experiencia.
5	Medina Arce, Antony Kevin	Ingeniero de sistemas	Responsable del campus virtual de la Dirección de Salud Virgen de Cocharcas, con más de 6 años de experiencia.
6	Marín Valderrama, David	Abogado con maestría en Derecho Penal	Asistente en función fiscal en el Ministerio Público con más de 8 años de experiencia.
7	Gutiérrez Palomino, Yanira Teresa	Abogado con maestría en Derecho Penal	Encargada del área penal en el estudio jurídico “González & León Asociados” con más de 4 años ejerciendo el derecho.
8	Huacre Méndez, Miguel	Abogado especialista en Derecho Penal.	Alcalde Municipal Distrital de Ancó Huallo, con más de 10 años de experiencia.
9	Mamani Peralta, Nilton	Ingeniero de sistemas, bachiller en derecho, especialista en derecho informático,	Jefe de tecnologías de la información de Universitario de Deportes, con más de 5 años de experiencia.

	maestrando en gestión pública en la UNMSM

Nota: Elaboración propia, 2023

3.5. Técnicas e instrumentos de recolección de datos

En este capítulo de la tesis, se explicó las técnicas e instrumentos que fueron desarrollados con el fin de lograr una adecuada recolección de datos, así mismo, los resultados obtenidos fueron de gran soporte a los problemas planteadas, la entrevista como también el análisis de fuente de documentos, y se tuvo como instrumento la guía de entrevista de la mano del análisis de fuente de documentos, en relación a ello, **Fernandes** (2023) menciona que los métodos de investigación son las herramientas que son utilizadas por los investigadores para la recopilar y análisis de los datos que son relevantes para su estudio de investigación, que incluyen muestras, cuestionarios, entrevistas, estudios de casos, métodos experimentales, ensayos y grupos de enfoque, para llegar a la selección del método, para su investigación va a depender del problema que se quiera resolver y de los datos a obtener. (s.p.)

Como técnica fue empleado **la entrevista** y a su vez el análisis de fuente de documentos, como instrumento tuvimos la guía de entrevista de la mano del análisis de fuente de documentos, en esa línea **Sordini** (2019) menciona que l**a entrevista** es la técnica que será utilizada para recopilar datos cualitativos, para lograr información completa, detallada y sustancial, la aplicabilidad de las técnicas de entrevista en la investigación depende directamente de la naturaleza y las características específicas en el enfoque. (p. 76) En otras palabras, las técnicas de entrevista presuponen un diálogo favorable para lograr establecer una conversación abierta, fluida y flexible en la que afloren las características personales e identitarias. La entrevista, será utilizada para la recolección de datos de nuestros participantes, que servirán para manejar la interpretación general del estudio; así mismo **Heinemann** (2019) indica que las preguntas que se formulan logran conseguir el objetivo que se busca estudiar, y permite atrae nuevos conocimientos relevantes a la respuesta del problema general de la investigación. (s.p.)

Guía de Entrevista, Sordini (2019) es un documento escrito por un entrevistador para guiar la entrevista y garantizar que se cubran todos los temas y preguntas relevantes, contiene una lista de preguntas, temas o tareas que el entrevistador desea abordar durante la entrevista, como también pueden ser estructuradas o no estructuradas y se pueden personalizar según el tipo. (p. 77) en esa misma secuencia, **Páramo** (2018) agrega que, los encargados de investigar unas técnicas que persiguen obtener la claridad para sus respuestas de su objetivo en la materia. (s.p.) la entrevista que fue la herramienta de agrupación de datos, la que consistió en 9 preguntas que fueron las respuestas a los objetivos planteados.

Tabla *2*

Tabla de validación de instrumento de la guía de entrevista

Especialistas	Cargo que desempeña	Resultado
Marchinare Ramos, Lidia Lucrecia	Docente de la UCV	Aceptable
Vilela Apón, Rolando Javier	Docente de la UCV	Aceptable
La Torre Guerrero, Ángel Fernando	Docente de la UCV	Aceptable

Nota: Elaboración propia, 2023.

Análisis de fuente de documentos, fue utilizado para obtener informaciones relevantes de jurisprudencias, doctrinas, que vayan referidas al planteamiento de esta investigación. **Peña** (2022) y **Menéndez** (2018) indican que se empleará como instrumento a la guía de análisis de documentos, la cual incluirá el diseño a desarrollar: los datos de las fuentes, como el título del documento, la fecha y lugar de su publicación, el contenido de la fuente para lograr extraer información relevante para la investigación en desarrollo del análisis y un adecuado planteamiento de conclusiones (p. 2).

Ficha de análisis de documentos: es una herramienta donde se tomaron en cuenta resoluciones y leyes para analizar nuestra categoría y subcategorías en

un entorno de la realidad que se vive. Asimismo, ayudará a entender el impacto de las categorías.

Tabla 3

Tabla de validación de instrumento de la guía de Análisis de documentos.

Validación De Instrumento – Ficha De Análisis De Documento	**Datos Generales**	**Dr. Santisteban Llontop, Pedro Pablo**
	Cargo	Docente Metodólogo de Investigación UCV
	Porcentaje	
Promedio		95%

*Nota***:** Elaboración propia (2023)

3.6. Procedimiento

Para el desarrollo de la tesis, se determinó la aplicación de la técnica de entrevista y análisis documental para una óptima recolección de datos, así mismo el instrumento de guía de entrevista de la mano de la guía de análisis documental. **Moreno** (2021) hace referencia a la fuente, a la combinación de constructos teóricos y diferentes investigadores se le llama triangulación, y su reconocimiento fue en base a diferentes resultados que fueron obtenidos bajo diferentes elementos, esta triangulación se realiza tanto en métodos cualitativos como cuantitativos. Desde este punto de vista, se sabe que los académicos podrán verificar la información recopilada a través de la tecnología desarrollada para cumplir con los objetivos definidos, como categorías y subcategorías. (p. 78)

En cuanto al procedimiento recolección de datos con la ayudan de la guía de entrevista, primero, se formulará 03 preguntas por cada objetivo, después, fueron validadas con rigor científico por 03 metodólogos, segundo, fueron firmados el consentimiento informado a los especialistas, luego, se aplicó la guía entrevista a los 06 especialistas en la materia de investigación de manera presencial, asimismo, por los canales de videoconferencia Zoom, Google Meet, y vía telefónica.

En cuanto al procedimiento de recolección de datos con la guía de análisis documental, se realizó una revisión sistemática de las investigaciones

internacionales y nacionales que guarden relación con la investigación planteada de fuentes confiables y prestigiosas de la comunidad científica; en base a ello, se propuso 02 análisis documental por cada objetivo.

Finalmente, se aplicó el método de triangulación de datos con la información recabada de todos los instrumentos de recolección de datos para responder a los objetivos planteados en la presente tesis, que corresponde a:

Tabla *4*

Cuadro de categorización

Categorías	Definición conceptual	Subcategorías
Fraudes informáticos Brenner (2016)	Son aquellas acciones gracias a la transformación digital que permite cambiar la naturaleza de los delitos, tales como eludir los sistemas de dispositivos de seguridad, piratear sistemas, extraer información de sistema de datos de una organización entre otras que rompen la legalidad (Brenner, 2016)	Ciberseguridad
		Derecho de protección de datos
Libertad de empresa Rodríguez (2021)	Se define como la garantía de iniciar y mantener actividad empresarial con condiciones de libertad por una persona o asociación a su vez el derecho de una persona a elegir libremente (Rodríguez, 2021).	Libertad de acceso de mercado
		Libertad de organización de empresarial

Nota: Elaboración propia, 2023.

3.7. Rigor científico

Según **Vasconcelos et al.** (2021) El rigor científico es un medio para lograr dar confianza a las conclusiones de un estudio de investigación, esto permite a los investigadores lograr una coherencia metodológica a lo largo del tiempo. Además, representa fielmente a la población, objeto de estudio. (s.p.)

En relación con la **dependencia**, se estableció un diseño de investigación adecuada que permitió poder controlar categorías relevantes, se utilizó muestras representativas y se empleó métodos de recopilación de datos apropiados, también, se recopilo datos de manera precisa y confiable. Esto implica que se utilizó instrumentos de medición válidos y confiables, asegurar la calidad de los datos mediante técnicas de muestreo adecuadas y se aplicó protocolos rigurosos en la recopilación y registro de la información. Asimismo, será importante que la investigación sea revisada por otros expertos en el campo y que los resultados puedan ser replicados por otros investigadores. Esto va a contribuir a la validación y confiabilidad de los hallazgos, en el cual se tuvo que verificar los datos obtenidos para lograr sintetizar la información y lograr estructurar nuestras propias conclusiones en base al criterio de interpretación.

Por consiguiente, se cumplió de manera rigurosa con el **criterio de credibilidad** se centró en la validación y triangulación de datos, la reflexividad del investigador, el muestreo adecuado, el análisis riguroso de los datos y la transferibilidad contextualizada de los hallazgos. Estos aspectos contribuirán a la confianza y validez de los resultados a obtenidos en la investigación cualitativa.

Como también, se cumplió con el **criterio de transferibilidad**, se centró en la capacidad de los resultados para ser transferidos y aplicados a otros contextos similares. Para lograrlo, fue necesario proporcionar una descripción detallada del contexto, caracterizar a los participantes, documentar los procesos de investigación, comparar casos, y ser reflexivo/a y transparente en la presentación de los hallazgos. Asimismo, los resultados obtenidos fueron para futuros investigadores.

Por último, se cumplirá con el **criterio de conformidad** buscando la confirmación y corroboración de los hallazgos a través de la triangulación de datos, el análisis riguroso y transparente, la reflexividad del investigador, sin parcialidad.

Finalmente, el instrumento de recolección de datos “guía de análisis documental”, fueron validados por juicio de expertos.

3.8. Método de análisis de datos

Se utilizaron tres métodos de análisis de datos, que fueron el enfoque **descriptivo** para poder limpiar y organizar sistemáticamente la información agrupada, también se utilizó el enfoque **hermenéutico** para llevar a cabo un

análisis exhaustivo de toda la documentación que se investigó. Tercero fue el **inductivo**, logrando obtener conclusiones generales, por último, se utilizó un enfoque **interpretativo,** que busco deducir representaciones reflexivas a partir de los resultados obtenidos.

Se organizo y clasifico de información que se logró obtener para identificar las categorías y subcategorías que indican los especialistas y sus relaciones, se ha realizado un análisis cualitativo de los datos obtenidos, recolectando información, la cual se realizó con la ayuda de una guía de entrevista, verificando la información y preparando la información para la análisis de la identificación de nuevas categorías emergentes, la generación de explicación y teorías resultantes, y se realizó el rigor del estudio cualitativo.

3.9. Aspectos éticos

Para **Ferrero** (2018) dice que los aspectos ética siempre deben ir más allá de sus conceptos y se refiere a la protección de derechos a quienes emplean participar en la investigación y a la importancia de la actividad evidente de buscar respuestas a las preguntas formuladas. (p. 383)

La tesis tuvo como referencia a la Resolución Vicerrectorado de Investigación N°062-2023-VI-UCV 16 de marzo 2023 de la Universidad César Vallejo que regula el código de ética, en ella, señala criterios que un tesista debe cumplir para el desarrollo de la investigación. En ese sentido, se cumplió con las normas de ética porque la información consignada en la presente investigación se basó en el respeto, honestidad, objetividad e integridad. Además, se reunió los criterios, requisitos de originalidad de la investigación planteadas en las categorías y subcategorías. Por otro lado, se utilizó el formato APA de la séptima edición. Finalmente, se contempló el artículo 7 del código de ética del Colegio de Abogados del Perú.

IV. RESULTADOS Y DISCUSIÓN. – Con referencia al fraude informático frente a la libertad de empresa como garantía constitucional, Lima 2023, se hace un abordaje minucioso y significativo de toda la información que fue recopilada por medio de la implementación de los diversos instrumentos de recolección de datos que se emplearon a cada uno de los expertos participantes en la investigación, por lo cual se hace a continuación una simplificación de todo lo que se pudo recolectar durante la aplicación del instrumento, que en este caso concreto fue una guía de entrevista.

Del mismo modo, resulta relevante exponer que no existe un orden puntual de cada uno de los diversos planteamientos que generan las diversas respuestas de los diversos expertos que colaboraron en dar respuesta a cada una de las interrogantes de las guías de las entrevistas, llevándose a cabo por medio del criterio propio de la investigadora para lograr de este modo un análisis claro de las respuestas emitidas por los mismos en base a cada una de las interrogantes de cada guía de entrevista.

Infiriendo en el **Objetivo General**, el cual es: "Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional"

Resultados obtenidos por parte de nuestros expertos entrevistados

Con relación a la **primera** pregunta planteada dentro de la guía de entrevista se tiene: ¿cómo afecta el fraude informático al desarrollo de la libertad de empresa como garantía constitucional?

Se logró la emisión de las respuestas generadas por Quispe (2023), Pomacanchari Torre (2023), Medina (2023), Huacre (2023) y Marín (2023), quienes coinciden en señalar que este tipo de fraude informativo afecta de forma directa a las empresas, debido a que nadie está exento de ser víctima de este tipo de delito el cual genera una significativa afectación a la economía financiera de la empresa, asimismo se señala que este tipo de fraude puede considerarse una modalidad de delito informático, que lamentablemente a estas alturas dentro de la Ley 30096 no dispone de una tipificación real de manera escrita de los diversos procesos, procedimientos y las pautas necesarias que permitan que se combatan de forma oportuna los ciberdelitos, generándose de este modo que el Ministerio Público no se encuentra especializado en este tipo de delitos puntuales.

En tal sentido Medina (2023), expone que según su punto de vista esta figura de fraude informático genera una verdadera afectación a lo que se conoce como la libertad de empresa, debido a que esto genera que se suscite un compromiso ineludible de la propiedad intelectual y de los secretos comerciales, generándose además pérdidas financieras, daños a la reputación de la organización y en muchos casos menoscabo de innovación en el ámbito empresarial, minando al mismo tiempo la confianza de los clientes reduciendo la capacidad de competencia de la empresa en la era digital, por lo cual se puede señalar que tanto la protección de los datos comerciales y la propiedad intelectual son claves para que se logre una verdadera garantía de la libertad de empresas como una verdadera garantía constitucional de las mismas.

Huacre (2023) y Marín (2023), exponen que el fraude informático puede traducirse en un delito real cometido por aquellos que manipulan los sistemas informáticos de determinada empresa, donde la libertad de empresa se traduce en una garantía constitucional, debidamente amparada en la Constitución Política del Perú, al ser esta una víctima del fraude informático que vulnera la estabilidad de redes de internet, la cual puede generar ciertas consecuencias de carácter legal así como pérdidas de tipo económico.

Finalmente, Maquera Platero (2023), con relación a la pregunta 1 refiere que el delito de fraude informático afecta al desarrollo de la libertad de empresa como garantía constitucional, haciéndolo por una parte respecto a la persona (natural o jurídica) titular del sistema informático afectado; así como, por otro lado, respecto a la persona (natural o jurídica) usuaria de dicho sistema informático. Mientras que, Araujo (2023) señaló que la comisión de los diversos delitos que han incidido de forma negativa en lo que se refiere al goce de los derechos, al encontrarse las mismas proclives a un determinado ataque a datos informáticos de la empresa que inciden en su patrimonio.

Es importante considerar a Brenner (2016), quien menciona que el fraude informático es una acción de usos tecnológicos en línea, como uno en Internet, para robar acceder a información confidencial con fines ilícitos para interferir en el uso y disfrute de la propiedad de otra persona. (p. 819). De allí que, el impacto legal de este tipo de fraude, el cual es considerado la necesidad de crear nuevas leyes aplicables que velen por la seguridad de los usuarios y sus propiedades

informáticas en el contexto de la modernización tecnológica, donde la autora menciona diversos antecedentes que llevaron a la creación de estas leyes.

Con relación a la **segunda** pregunta: En su máxima experiencia, ¿qué medidas y estrategias utilizan las empresas para prevenir y mitigar los efectos del avance tecnológico en el fraude informático para sí mismo?

De los participantes entrevistados, Quispe (2023), Pomacanchari Torre (2023), Medina (2023), Huacre (2023) y Marín (2023), expusieron que muchas organizaciones hoy en día no disponen de medidas de protección que sean de calidad, es necesario que estas empresas ejecuten lo más pronto posible medidas de ciberseguridad, así como capacitación al personal, siendo otra alternativa también disponer de un equipo especializado que sea capaz de lograr la detección oportuna de posibles vulnerabilidades del sistema informático que eviten además la puesta en marcha en muchos casos de operaciones bancarias que sean fraudulentas. Asimismo, las empresas deben disponer de reglamentos internos que le permitan cumplir la salvaguardia de la empresa.

De este modo, se puede decir además que, a pesar de lo referido anteriormente algunas empresas emplean un grupo de medidas y de estrategias que tratan de lograr prevenir o minimizar un posible fraude informático, entre las que se destacan el desarrollo de políticas de seguridad, la formación de empleados, la correcta protección de datos, el empleo de firewalls, los procesos de actualización, monitoreo, así como la gestión de acceso, la correcta evaluación de posibles proveedores, el empleo de la seguridad en la nube, el correcto uso de auditorías de seguridad cibernética.

En este sentido, Huacre (2023) señaló con relación a ello, que cada organización se encuentra obligada a lograr que se puedan establecer diversos mecanismos que permitan tanto resguardar como proteger todas las piezas de información.

Por su parte, Marín (2023), con relación a esta interrogante sostiene que existen estrategias que se implementan en ciertas empresas, como los antivirus, siendo los mismos una herramienta que puede considerarse como ineficiente para que se empleen como protección ante una base de datos grande y confidencial.

Finalmente, Maquera (2023) señaló que cada una de las diversas medidas y estrategias que emplean las organizaciones para tratar de lograr la prevención y mitigación de los diversos efectos del avance tecnológico en el fraude informático son múltiples, desde la implementación de mecanismos de ciberseguridad como la aplicación de la ISO 27001, a la contratación de personal altamente capacitado, coordinación con instituciones estatales que colaboren en la prevención, detección y sanción de la ciberdelincuencia. Asimismo, Araujo (2023) coincide en que es necesaria la aplicación de técnicas de ciberseguridad en la organización las cuales van a permitir disminuir intromisiones de ciberdelincuentes.

En general las empresas no están usando un mecanismo real y eficiente que logre que se genere una verdadera prevención y mitigación de los diversos efectos que se han logrado alcanzar en base a los avances tecnológicos que han venido en aumento en los últimos años en materia de fraude informático.

Con relación a la pregunta **tres**: En ese escenario, ¿cómo la creación de un organismo supervisor de seguridad digital garantizaría la libertad de empresa en la prevención de los fraudes informáticos?

Para Quispe (2023), un organismo supervisor de seguridad digital no ha de ser garante de que la organización no se convierta en víctima de fraudes de tipo informáticos, esto se debe principalmente a que los mismos no disponen de una verdadera frontera, ya que los mismos pueden cometerse desde cualquier ámbito de la geografía mundial y de crearse un organismo posiblemente este no sería capaz de lograr una verdadera solución de la problemática.

Del mismo modo, coincide Maquera (2023), quien considera que la creación de un organismo supervisor de seguridad digital no es garante según su punto de vista de lo que es la libertad de empresa en lo referente a prevención de fraudes informáticos; en base a experiencia propia el expone que en la comisión del citado delito en la mayoría de casos es producto de negligencias previas en las que ha venido incurriendo el usuario y de allí en muchos casos los ciberdelincuentes logran apoderarse de información sensible de cada una de sus posibles víctimas realizando seguidamente un fraude informático en contra de estos.

Mientras que, Pomacanchari Torre (2023), Medina (2023), Huacre (2023) y Marín (2023), refirieron que resulta en primer lugar imprescindible la implementación y sensibilización de lo que es la Ley 30096 frente a la sociedad, logrando de este modo con esto contar con un organismo supervisor de seguridad digital que logre el control del empleo de la cibernética como una verdadera herramienta que alcance el desarrollo de la libertad de las empresas, además de la existencia de un seguro cibernético que ayude a la disminución de las cifras de delitos informáticos y que garantice la prevención de fraudes informáticos estableciendo además estándares, supervisando el cumplimiento de las normas y proporcionando además educación y formación, fomentando la colaboración, supervisando el cumplimiento, impulsando investigaciones, coordinando respuestas a posibles incidentes y promoviendo un entorno empresarial que sea regulado en términos de seguridad cibernética.

Por su parte, Araujo (2023) con relación a esta interrogante señaló que actualmente se encuentran diversos organismos que tienen la tarea de combatir este tipo de delitos, argumentando además que fue aprobada una Ley de Gobierno Digital que ha permitido la dotación de funciones que se relacionan de manera directa con la seguridad digital a la Secretaria de Gobierno Digital.

Además de lo anterior es necesario que se logre llevar a cabo una verdadera reformulación de los diversos organismos de carácter autónomos junto con el Ministerio Público, así como también el Poder Judicial, logrando que la administración de justicia respete cada uno de los cánones jurídico- normativos y legales, confinando de manera definitiva y puntual el flagelo de la corrupción que es responsable directa del debilitamiento de dichas entidades responsables de tutelar la justicia.

Análisis e interpretación de las categorías apriorísticas y emergentes

Respecto al objetivo general:

Analizar: de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional

La tesis conto con las **categorías emergentes**, las cuales no se mencionan en el desarrollo de la investigación, pero fueron extraídas del conocimiento amplio de los especialistas entrevistados, las cuales fueron nuevas categorías dando soporte y nutriendo a la tesis, por ello, en cuanto al objetivo general, ciertamente la existencia de **plataforma digitales** para la prevención de fraudes informáticos y modalidades de delitos informáticos, la ISO es una plataforma que varios países ya lo implementan con obligatoriedad las empresas públicas y privadas para la protección de la base de dato, en general serian de gran soporte en la protección de la **propiedad intelectual** que es la protección de los bienes económicos, productos tangibles las cuales deben ser protegidas por el estado, así mismo el incluir un **seguro cibernético** en las empresas para la protección de gastos a causa de un fraude informáticos, como el robo, eliminación, copia y agregados tendría un gasto económico en la defensa legal que tendría que afrontar al ser víctima de ello, pera para poder lograr un seguro es obligatorio primero incluir medidas de protección seguras.

Resultados obtenidos de las fuentes de documentos

En lo relacionado con el **objetivo general** se presentó dos fuentes documéntale que fueron de soporte a la tesis; las cuales son:

En primer lugar, la **Ley N° 30096 –** sobre delitos informáticos en su **artículo primero,** la cual hace mención a la prevención y sanciones de aquellas conductas ilícitas que atentan contra los sistemas y datos informáticos que son bienes jurídicos protegidos, estos ilícitos con cometidos mediante la utilización de tecnologías para invadir el ciber espacio de la información, como también de la comunicación, esta Ley tiene como finalidad garantizar la lucha eficaz contra los ciberataques. En la cual se puede evidenciar que las empresas están siendo atacadas mediante una modalidad que se encuentra en el **artículo 8 fraude informático,** el cual impide la libertad de empresa como garantía constitucional.

Debe señalarse que la Sentencia del Tribunal Constitucional del expediente N.º 0011-2013-PI/TC - Lima, en el apartado B consideraciones del TC en el **numeral treinta** conformes a **la libertad de empresa** es la representación de la libertad individual, que es consustancial en el aparo de esta garantía, para proteger la libertad de empresa, el Estado deberá permitir la existencia, actividad y

permanencia de las empresas, es por ello que la intervención del Estado debe garantizar la libertad de trabajo y la libertad de empresa sin límites, como se encuentra amparada en el en nuestra Constitución Política del Perú.

Los criterios mencionados son de documentos jurídicos relevantes en el derecho como son leyes y sentencias constitucionales.

Por otro lado, respecto **al Objetivo Especifico 1**, “Analizar de qué manera la ciberseguridad garantiza la libertad de acceso de mercado como garantía constitucional”.

Resultado en base a los expertos entrevistados

Al respecto, la pregunta **cuatro**: ¿de qué manera mantener un marco legal en la tecnología aportaría a la libertad de acceso de mercado de la empresa?

De los participantes entrevistados, Quispe (2023), Pomacanchari Torre (2023), Medina (2023), Huacre (2023) y Marín (2023), coinciden que disponer de un marco legal en tecnología que ampare y proteja la seguridad informática, mediante legisladores capacitados y expertos en la materia de tecnología y el ciberespacio, seria coparticipe de la libertad de empresas, permitiendo acceso por internet a cada uno de los servicios o productos ofertados por las empresas, disminuyendo delitos informáticos, al mismo tiempo que se trata de contribuir además a una posible libertad que permita acceso al mercado de las diversas empresas u organizaciones al lograr el fomento de la innovación, lograr alcanzar la protección de la propiedad intelectual, asegurando al mismo tiempo una verdadera competencia justa, abordando además ciertas preocupaciones tanto relacionadas con la seguridad como también con la privacidad, promoviendo al mismo tiempo el cumplimiento de ciertos estándares de tipo global, al mismo tiempo que se alcancen y se faciliten las diversas resoluciones de disputas.

Por su parte, Maquera (2023) y Araujo (2023) con relación a esta interrogante señalaron que resulta ampliamente positiva implementar un marco legal que logre promover la utilización de la tecnología en diversos ámbitos y especialmente en la libertad de acceso de mercado de la empresa.

En efecto, considera que este uso va a permitir no solo una reducción de costos de personal, materiales y tiempo, sino además la puesta en marcha de un

mejor producto o un mejor servicio, para lograr de este modo que aquellos individuos que deseen acceso al mercado puedan hacerlo de manera más fácil y brindando un producto o servicio competitivo.

Acotando Araujo (2023) que es necesario que se actualice y se consolide un marco normativo que se relacione a las tecnologías digitales, debido a que estas son cambiantes y con el correr de los años presentan nuevos avances y la aparición de nuevos delitos, por lo cual disponer de un marco legal actualizado de manera constante va a permitir brindar seguridad jurídica en relación a la satisfacción de este derecho antes expuesto.

Todo lo anterior va a permitir que se suscite o formule la creación de un ambiente favorable para que todas las empresas logren no sólo ingresar sino además operar en diversos mercados competitivos y que en muchos casos sean tecnológicamente avanzados y al mismo tiempo lograr que se le brinde una más rápida y mayor seguridad informática posible a cada uno de los posibles clientes y/o usuarios.

En lo referente a la pregunta **quinta**, desde su perspectiva, ¿cómo se han desarrollado las políticas de ciberseguridad para promover o inhibir la entrada de nuevas empresas en el mercado?

Para Quispe (2023), no existe un verdadero desarrollo de las políticas de ciberseguridad, debido a que durante los últimos tiempos y por diversas problemáticas que ha enfrentado el país ha privado la puesta en marcha de empresas nuevas, por lo cual es necesario que se incremente de forma eficiente tales políticas de seguridad.

Por su parte, Pomacanchari Torre (2023), sostiene que la política de ciberseguridad resulta muy diversa y es necesario que se incluyan tanto agentes estatales, económicos como sociales, esclareciendo al mismo tiempo la ponderación directa de objetivos e identificando el papel cumplido por el Estado en cada uno de sus múltiples fines, argumentando además que Perú dispone de políticas de ciberseguridad, aunque no son ejecutadas y no hay un apropiado rastreo.

Asimismo, Medina (2023), expone que, las políticas de ciberseguridad promueven e inhiben una entrada de nuevas empresas dentro del mercado. Para

lograr que se promuevan políticas de ciberseguridad ofreciendo un entorno confiable que logre el fomento de la inversión tecnológica e innovación. A pesar de ello, se puede decir que, en muchos casos, políticas ampliamente restrictivas y costosas actúan como barreras de entrada y desincentivar nuevas empresas como consecuencia de altos costos de cumplimiento.

Mientras, Huacre (2023) señala que las instituciones que se encargan de la prevención de delitos informáticos ponen en acción capacitaciones transversales especialidad y por niveles tanto para fiscales, como a peritos de especialidad, realizándose ciertos esfuerzos que permitan la sensibilización del público, para alcanzar la prevención del ciberdelito.

Marín (2023), hizo referencia a la relevancia de la estrategia Nacional de Ciberseguridad Española en el contexto de la Estrategia de Seguridad Nacional se traduce en un resultado de un gran esfuerzo de la administración para enfrentarse de modo más seguro y con más amplias garantías de retos como país, dentro del contexto internacional dominado por uso exponencialmente creciente de la tecnología.

Maquera (2023) argumenta que las organizaciones no solo por normativa deben implementar mecanismos de ciberseguridad, sino que están en la necesidad de hacerlo; caso contrario, estarían prácticamente condenas a dejar de existir tarde o temprano. Sea para promover o inhibir la entrada de nuevas empresas al mercado, por lo general, el gobierno responde tarde en la regulación; al contrario, son las mismas empresas quienes implementan mecanismos de seguridad, unos mejores que otros, claro está; sea para ingresar, sea para permanecer en el mercado.

Finalmente, Araujo (2023) señala que conforme van apareciendo nuevas modalidades de atentados contra las empresas, se ha visto la imperiosa necesidad de que se implementen políticas de ciberseguridad por parte del gobierno y de particulares, sea ello desde un ámbito preventivo o desde una verdadera actuación insitu.

Con referencia a la pregunta **sexta**: En Perú, ¿cómo se han adaptado las regulaciones internacionales sobre tecnología para equilibrar la libertad de acceso de mercado?

Los entrevistados Quispe (2023), Pomacanchari Torre (2023), Medina (2023), Huacre (2023) y Marín (2023), refieren que, existe una complicada realidad económica en Perú, la cual es consecuencia de una ausencia tanto de productos como de servicios competitivos dentro del mercado globalizado; por ausencia de conocimientos tanto científicos como tecnológicos, ya que no existe promoción de investigación con presupuestos que se ajusten.

Finalmente, Maquera (2023) argumenta que él no dispone de amplio conocimiento sobre el tema comercial, pero señala que la implementación de mecanismos de ciberseguridad tales como ISO 27001, ISO 27032 o, mejor aún, NIST SP 800-53, vienen a constituir estándares internacionales que le otorgan mayor confiabilidad y, por tanto, competitividad a las empresas para con sus clientes. Siendo que dichos mecanismos de seguridad son, pues, en su gran mayoría implementados por las grandes empresas en el país.

De este modo también Araujo (2023) señala que respecto a la normativa internacional y con referencia al tema comercial posee desconocimiento al igual que Maquera, pero es de conocimiento público que existe a nivel nacional recomendaciones con relación a que se implementen políticas de ciberseguridad en cada una de las empresas para lograr de este modo confiabilidad de todos sus actores.

Asimismo, este país ha logrado un valioso acceso en la figura del convenio de Budapest, que dispone de un marco legal internacional que permite el salvaguardo de la seguridad informática, la cual no ha sido explotada para el empleo de la legislación peruana.

Es por ello que en Perú se han venido adaptando regulaciones internacionales sobre tecnología que equilibren la libertad de acceso al mercado mediante la armonización normativa, participación en tratados internacionales, promoción de innovación, creación de agencias reguladoras especializadas y fomento de inversión extranjera dentro del sector tecnológico, con tales medidas se trata de lograr la promoción de un ambiente empresarial competitivo facilitando acceso al mercado para organizaciones tecnológicas.

Por todo lo anterior, se puede decir que los avances tecnológicos que manejen las empresas para la protección de la información podrían significar una real ventaja competitiva ante otras empresas.

Por lo que la regulación internacional sobre la tecnología avanza y se actualiza de manera constante para tratar de proteger la correcta implementación de normas ISO.

Análisis e interpretación de las categorías apriorísticas y emergentes

Respecto al objetivo específico 1:

Analizar de qué manera la ciberseguridad garantiza la libertad de acceso al mercado como garantía constitucional

En este objetivo específico 1; nuestros especialistas indican que todos los atentados que tuvieron en estos años tanto empresas públicas como privadas son por la falta de **base legal de la tecnología**, la cual debería exigir el estado para una protección adecuada de la economía y privacidad de datos de los clientes y asociados, la cual debería ir de la mano con las **políticas de ciberseguridad** que deben ser incluidas en las normas de confiabilidad de los personales de las empresas, para así lograr la disminución de fraudes informáticos.

Resultados obtenidos de las fuentes de documentos

Como fuente de documento relevante para este objetivo específico primero se tuvo a bien indicar que, en la **Resolución Presidencial N.º 097-2020-CONCYTEC-P** en el **numeral 3** de la Ley Marco de Ciencia, Tecnología e Innovación Tecnológica refiere sobre la **ciberseguridad,** ya que esta tiene la finalidad de diseñar el marco legal e institucional, sobre todo el de la administración de justicia, para el beneficio de la economía social y el amparo de la protección de datos que atraigan cada empresa de sus clientes, dentro del cual, tanto las personas naturales como las empresas productivas, deban disponer de un orden jurídico, para así lograr dar estabilidad y no incertidumbre en la disposición y ejercicio de sus derechos adquiridos bajo ley.

En relación con este tema la Sentencia del Tribunal Constitucional del EXP. N.º 01405-2010-PA/TC – Callao, Consideraciones del Tribunal Constitucional, en el **apartado 15** conforme a la **libertad de acceso de mercado,** que en el Perú se encuentra regulado en la carta magna, en el art. 59, la cual indica que es una garantía constitucional, la libertad de acceso al mercado, así mismo garantiza a todas las personas una libertad de decisión que es la libertad de fundación de una

empresa, también para actuar en el mercado, el cual es la libertad de acceso al mercado, y el poder establecer los propios objetivos de la empresa, a que viene hacer la libertad de organización del empresario, a su vez dirigir y poder planificar su actividad, que la libertad de dirección de la empresa, en atención a sus recursos y a las condiciones del propio mercado, así como la libertad de cesación o de salida del mercado

En cuanto al **objetivo específico 2**, que busca “analizar de qué manera el derecho de protección de datos contribuye a la libertad de la organización empresarial como garantía constitucional”.

Resultados obtenidos por parte de nuestros expertos entrevistados

De los participantes entrevistados en virtud de la pregunta **siete**: En su opinión, ¿cómo pueden apoyar o perjudicar los derechos y privacidad de información en la libertad de la organización como garantía constitucional?

Se tiene que los participantes Quispe (2023), Pomacanchari Torre (2023), Medina (2023), Huacre (2023) y Marín (2023), coinciden en sus respuestas al señalar que si puede dar apoyo a la privacidad de la información debido a que es imprescindible ejercer el derecho de la libertad de expresión, evitando de este modo violación de un derecho reconocido por esta, por lo que tal derecho a la privacidad de información trata de garantizar el derecho fundamental a la protección de datos personales, por medio de un idóneo tratamiento, dentro del respeto a los derechos que en ella se reconocen, tratando lograr de esta manera un acertado equilibrio entre derechos y privacidad de información así como la libertad de organización, la cual puede ser de beneficio al garantizar protección de datos y confianza dentro del mercado, pero además puede perjudicar si las regulaciones son excesivas y dificultan el proceso operativo de las empresas, limitando la recopilación de datos o un adecuado equilibrio con las necesidades de ciberseguridad.

Maquera (2023) expone que la privacidad de los datos personales de los usuarios en nada perjudica a la libertad de la organización de empresa. Por el contrario, el respeto al derecho inicialmente citado generaría una confianza de los usuarios que más adelante podrían generar mayores ingresos a la empresa y Araujo (2023) coincide que coadyuva el respeto de este derecho por parte de las empresas, a la mayor confiabilidad de los particulares en los servicios que los mismos ofrecen a las organizaciones.

Asimismo, no hay menoscabo de por medio a la libertad de organización, cuando una empresa obtiene información privada de determinado cliente, la misma recibe la responsabilidad de otorgarle un adecuado procedente a esta información, la cual quedará obligada a lograr la salvaguarda de toda la información que se le brinde.

En cuanto a la pregunta **ocho**: ¿Qué consecuencias legales y reputacionales pueden enfrentar las empresas por la falta de medidas preventivas en las regulaciones sobre privacidad de información?

Los participantes entrevistados, Quispe (2023), Pomacanchari Torre (2023), Medina (2023), Huacre (2023) y Marín (2023), coinciden que muchas empresas que son víctimas de delitos informáticos se han enfrentado al robo de datos tanto informáticos como personales, accesos no autorizados a sistemas informáticos, daños informáticos en sistemas, así como pérdidas económicas. Puede decirse además que la ausencia de medidas preventivas en las regulaciones relacionadas con la privacidad de información induce a consecuencias legales, tales como sanciones y demandas, así como a graves repercusiones en la reputación de la empresa, incluyendo también pérdida de confianza de clientes, de negocios y de daños financieros. Siendo imprescindible que las empresas implementen ciertas medidas que sean sólidas de privacidad de datos para evitar de este modo consecuencias.

Maquera (2023) y Araujo (2023) coinciden en que son varias las consecuencias legales y reputacionales que pueden enfrentar las empresas por falta de medidas preventivas en las regulaciones sobre privacidad de la información, así como sanciones administrativas. Argumentando el primero que, si una empresa incumple la correspondiente normativa, las sanciones podrían ir desde una simple multa hasta la disolución de la empresa (sin mencionar, eventualmente, las implicancias jurídico-penales para con sus representantes, si fuera el caso). Por otro lado (y tal vez de mayor trascendencia para con los intereses económicos de la empresa), en el aspecto reputacional, los clientes al advertir que una determina empresa no cumplen con las regulaciones debidas, pues, sencillamente elegirá a una empresa que sí las cumpla.

Estos consideran además que las principales consecuencias legales vienen a ser: empresas que pueden ser demandas por clientes, socios comerciales así como otras partes afectadas por delito informático, que puede resultar en multas y en daños económicos, además de enfrentar sanciones regulatorias por tener incumplimiento de leyes de protección de datos, generándose de este modo finalmente pérdidas económicas producto de los ciberataques, crisis de seguridad en posición de sanciones, daño de reputación y finalmente pérdida de clientes.

Con relación a la pregunta **nueve**: Bajo un marco legal, ¿en qué medidas una libre organización de empresa garantizaría el uso de la información personal y sensible de los clientes y empleados?, los entrevistados Quispe (2023), Pomacanchari Torre (2023), Medina (2023), Huacre (2023) y Marín (2023), señalan que es posible garantizar por medio de copias de seguridad o de respaldos, empleando antivirus en el sistema informático, controlando el acceso a la información que comparte con sus usuarios, fomentando una cultura de contraseñas seguras entre otras. De este modo sostienen que, las empresas víctimas de delitos informáticos se enfrentan al robo de datos informáticos y personales, accesos no autorizados a sistemas informáticos.

Asimismo, la Constitución Política del Perú ampara la libre organización de las empresas, con el fin de lograr para sí mismo una posición en el mercado laboral y ganancias económicas, pero ello también implica cumplir con parámetros establecidos por los legisladores, como es el proteger y salvaguardad la información personal y cesible que puedan llegar a obtener dependiendo en el área que se desempeñan, existiendo la ley de protección de datos personales, las empresas deben operar en entorna a esta ley.

Huacre (2023), expone además que un marco legal puntual es crucial que exista un marco legal claro y actualizado que defina los delitos informáticos, que establezcan las penas correspondientes, mientras que la cooperación internacional, dado que los delitos informáticos transcienden las fronteras nacionales, la cooperación internación es necesaria para prevenir los delitos.

Finalmente, Maquera (2023) sostiene que, cumpliendo con los estándares internacionales sobre ciberseguridad y demás normativa correspondiente; estando siempre a la vanguardia al respecto, es decir cumpliendo la normativa nacional tal como lo señala Araujo (2023), además de tomar en cuenta las pertinentes y

efectivas recomendaciones sobre ciberseguridad lograran las empresas estar a la vanguardia de la protección de la información.

Análisis e interpretación de las categorías apriorísticas y emergentes

Respecto al objetivo específico 2:

Analizar de qué manera el derecho de protección de datos contribuye a la libertad de la organización empresarial como garantía constitucional.

En nuestra última categoría los especialistas entrevistados hiciera mención de nuevas categorías emergente que contribuyeron a la tesis, en ese sentido la navegación en el ciberespacio mediante el internet ha ido en aumento cada año más, convirtiéndose un lugar de trabajo como también de entretenimiento por la mayor parte de la población, en la cual se puede visualizar y publicar contenido referidas de diversos indoles en la cual se puede evidenciar la **libertad de expresión** mediante la red se puede existen varios opciones para hacer público todo lo que pensamos, esa se considera la vía de expresión predominante, sin embargo, es importante mencionar que existen límites, ya en ocasiones afectan a otras personas.

Resultados obtenidos de las fuentes de documentos

La **Resolución N. ° 071-2022-2023-OM-CR**, en el **apartado 2** que nos habla de la protección de datos personales – **Ley N.º 29733,** con relación a **derecho de protección de datos,** el uso de los datos personales y/o sensibles se maneja con sumo cuidado puesto que el gobierno peruano debe velar que no haya un perjuicio al usuario con fines públicos o privados, Brindar medidas de óptimas para la seguridad de los titulares de los datos personales, con el fin de garantizar la atención de derechos de acceso, rectificación, cancelación y oposición, asimismo, asegurar la atención de las solicitudes o requerimientos formulados por la Autoridad Nacional de Protección de Datos Personales.

Finalizando, es conveniente acotar que la **Resolución Ministerial N.º 129-2012-PCM,** en el **numeral 8** que nos comenta sobre técnicas peruanas “NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información, con relación a la **libertad de organización de empresa** establece un Plan de Seguridad de la Información

bajo normas Técnicas, esta se establece en la Agenda Digital Peruana 2.0, donde establece la necesidad de contar estrategias de ciberseguridad para evitar incidentes en recursos de información, las bases se encuentran en Códigos de buenas prácticas para la gestión de seguridad de la información.

DISCUSIÓN. – Bajo el análisis de la información obtenidas de los instrumentos de recolección de datos, instrumentos recopilados mediante la aplicación de las entrevistas, tablas y marcos de análisis de documentos, a nivel nacional e internacional.

La investigación de tesis fue un trabajo hacha con base sólida de teorías, la información anterior debe vincularse entre sí para ejecutar comandos de acuerdo a lo escrito para cada propósito, pues es necesario unificar cada herramienta según su propósito para poder responder a lo que se le pide, en el marco de acentuar esta etapa de la discusión, se debe recordar lo anterior y poder averiguar si lo planteado en la hipótesis coincide con lo obtenido en el instrumento redactado en las líneas anteriores.

Esto debería resolverse utilizando la siguiente solución.

Tabla 5

Tabla de la discusión de objetivo general

Objetivo General	Supuesto General
Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional	El fraude informático afecta la libertad de empresa, los efectos que deja los fraudes informáticos a las empresas son pérdidas significativas de su economía, pérdida de clientes y socios, los atentados traer perdías de recursos financieros girando inestabilidad financiera de la empresa, pérdida de confianza y calidad de dicha empresa, trayendo quiebras e incluso en cierre de las empresas.

Nota: Elaboración Propia

En ese sentido, sobre la recolección de hallazgos e información por parte de los especialistas se realizó la rememoración de tolo lo hallado; en nuestro objetivo general es necesario el concepto del fraude informático, **Lux y Calderón** (2020) nos comenta que en Chile el **fraude informático** es una forma de delito informático. En rigor, se realizan a través de Internet. Su interés jurídico común es una función informática. Una función informática se define como aquella que permite a un sistema informático realizar correctamente operaciones de almacenamiento, procesamiento y un conjunto de condiciones operativas. Transferencia de datos.

Asimismo, **Carrasco** (2018) menciona que la **libertad la libertad de empresa** es solo una categoría instrumental que le da relevancia a la constitución porque sustenta y sirve a los derechos fundamentales, y su configuración jurídica e implementación está sujeta a los valores que expresan los derechos fundamentales en su contenido. (p. 920)**.**

Por su parte, Acuario (2016) entiende que **el fraude informático** es toda acción que es cometido con dolo, con la finalidad de provocar un perjuicio a personas o entidades mediante dispositivos habitualmente informáticos; Es el acto de índole ilegal que se encuentra direccionado en contra de la confidencialidad, integridad y los recursos a nivel informático, redes y documentos informáticos, abusando indiscriminadamente sobre dichos sistemas. (p 12) En razón a ello los agentes cometen de manera dolosa e acto ilícito mediante la accesibilidad que tiene como trabajador, haciendo uso de su posición especial de acceso a la base de datos

Las posiciones que dieron nuestro especialista en base a la **primera** pregunta, por el cual Quispe (2023), Pomacanchari Torre (2023), Medina (2023), Huacre (2023) y Marín (2023), quienes coinciden en señalar que este tipo de fraude informativo afecta de forma directa a las empresas, debido a que nadie está exento de ser víctima de este tipo de delito el cual genera una significativa afectación a la economía financiera de la empresa, asimismo se señala que este tipo de fraude puede considerarse una modalidad de delito informático, que lamentablemente a estas alturas dentro de la Ley 30096 no dispone de una tipificación real de manera escrita de los diversos procesos, procedimientos y las pautas necesarias que permitan que se combatan de forma oportuna los

ciberdelitos, generándose de este modo que el Ministerio Público no se encuentra especializado en este tipo de delitos puntuales.

No obstante Medina (2023), expone que según su punto de vista esta figura de fraude informático genera una verdadera afectación a lo que se conoce como la libertad de empresa, debido a que esto genera que se suscite un compromiso ineludible de la propiedad intelectual y de los secretos comerciales, generándose además pérdidas financieras, daños a la reputación de la organización y en muchos casos menoscabo de innovación en el ámbito empresarial, minando al mismo tiempo la confianza de los clientes reduciendo la capacidad de competencia de la empresa en la era digital, por lo cual se puede señalar que tanto la protección de los datos comerciales y la propiedad intelectual son claves para que se logre una verdadera garantía de la libertad de empresas como una verdadera garantía constitucional de las mismas.

Así mismo, Huacre (2023), Marín (2023), Maquera (2023) y Araujo (2023), exponen que el fraude informático puede traducirse en un delito real cometido por aquellos que manipulan los sistemas informáticos de determinada empresa, donde la libertad de empresa se traduce en una garantía constitucional, debidamente amparada en la Constitución Política del Perú, al ser esta una víctima del fraude informático que vulnera la estabilidad de redes de internet, la cual puede generar ciertas consecuencias de carácter legal así como pérdidas de tipo económico.

Con relación a la **segunda** pregunta, Quispe (2023), Pomacanchari Torre (2023), Medina (2023), Huacre (2023) y Marín (2023), expusieron que muchas organizaciones hoy en día no disponen de medidas de protección que sean de calidad, es necesario que estas empresas ejecuten lo más pronto posible medidas de ciberseguridad, así como capacitación al personal, siendo otra alternativa también disponer de un equipo especializado que sea capaz de lograr la detección oportuna de posibles vulnerabilidades del sistema informático que eviten además la puesta en marcha en muchos casos de operaciones bancarias que sean fraudulentas. Asimismo, las empresas deben disponer de reglamentos internos que le permitan cumplir la salvaguardia de la empresa.

En este sentido, Huacre (2023) señaló con relación a ello, que cada organización se encuentra obligada a lograr que se puedan establecer diversos

mecanismos que permitan tanto resguardar como proteger todas las piezas de información.

Por su parte, Marín (2023), con relación a esta interrogante sostiene que existen estrategias que se implementan en ciertas empresas, como los antivirus, siendo los mismos una herramienta que puede considerarse como ineficiente para que se empleen como protección ante una base de datos grande y confidencial.

En general las empresas no están usando un mecanismo real y eficiente que logre que se genere una verdadera prevención y mitigación de los diversos efectos que se han logrado alcanzar en base a los avances tecnológicos que han venido en aumento en los últimos años en materia de fraude informático; En relación a la **tercera** para Quispe (2023), un organismo supervisor de seguridad digital no ha de ser garante de que la organización no se convierta en víctima de fraudes de tipo informáticos, esto se debe principalmente a que los mismos no disponen de una verdadera frontera, ya que los mismos pueden cometerse desde cualquier ámbito de la geografía mundial y de crearse un organismo posiblemente este no sería capaz de lograr una verdadera solución de la problemática.

Mientras que, Pomacanchari Torre (2023), Medina (2023), Huacre (2023) Marín (2023), Maquera (2023) y Araujo (2023), refirieron que resulta en primer lugar imprescindible la implementación y sensibilización de lo que es la Ley 30096 frente a la sociedad, logrando de este modo con esto contar con un organismo supervisor de seguridad digital que logre el control del empleo de la cibernética como una verdadera herramienta que alcance el desarrollo de la libertad de las empresas, además de la existencia de un seguro cibernético que ayude a la disminución de las cifras de delitos informáticos y que garantice la prevención de fraudes informáticos estableciendo además estándares, supervisando el cumplimiento de las normas y proporcionando además educación y formación, fomentando la colaboración, supervisando el cumplimiento, impulsando investigaciones, coordinando respuestas a posibles incidentes y promoviendo un entorno empresarial que sea regulado en términos de seguridad cibernética.

Además de lo anterior es necesario que se logre llevar a cabo una verdadera reformulación de los diversos organismos de carácter autónomos junto con el Ministerio Público, así como también el Poder Judicial, logrando que la

administración de justicia respete cada uno de los cánones jurídico- normativos y legales, confinando de manera definitiva y puntual el flagelo de la corrupción que es responsable directa del debilitamiento de dichas entidades responsables de tutelar la justicia. En ese mismo sentido las **fichas de análisis de documentos**, en lo relacionado con el **objetivo general**, el fraude informático es una de las modalidades más empleados para atentar contra la libertad de empresa la cual es mencionada por la **Ley N.º 30096 –** que hace mención a los **delitos informáticos** en el **artículo uno** la cual tiene por objetivo prevenir y a la vez sancionar aquellas conductas ilícitas que afectan los sistemas y datos informáticos y bienes jurídicos protegidos, las cuales son cometidas mediante el uso de tecnologías en el ciberespacio así mismo de las comunicación, esta Ley debe garantizar la lucha eficaz contra los ciberataques. Se puede evidenciar que las empresas están siendo atacadas mediante una modalidad que se encuentra en el **artículo 8 fraude informático,** el cual impide la libertad de empresa como garantía constitucional. En relación a la idea anterior la Sentencia del Tribunal Constitucional del expediente N.º 0011-2013-PI/TC - Lima, en el apartado B consideraciones del Tribunal Constitucional en el **apartado treinta** conformes a **la libertad de empresa** indican que, es la manifestación individual de la libertad, por lo que al ser consustancial con la libertad, el Estado debe permitir la existencia, actividad y permanencia de la empresa, es por ello que la intervención del Estado debe garantizar la libertad de trabajo y la libertad de empresa sin límites, como se encuentra amparada en el Constitución art. 59.

En concordancia con lo mencionado líneas arriba **Lux y Calderón** (2020) nos comenta que en Chile El fraude informático es una forma de delito informático. En rigor, se realizan a través de Internet. Su interés jurídico común es una función informática. Una función informática se define como aquella que permite a un sistema informático realizar correctamente operaciones de almacenamiento, procesamiento y un conjunto de condiciones operativas. Transfiera datos dentro de un riesgo aceptable. Estas condiciones pueden ser violadas por interacciones que ocurren en el ciberespacio, similares a las que ocurren en el tráfico vehicular. (p. 155), e **Minahim y Spinola** (2017) menciona que, la influencia del comportamiento de las víctimas en el fraude informático conlleva a riesgos creados por la popularización de los dispositivos tecnológicos, las cuales son detectadas mediante técnicas para cometer fraude es en colaboración de la víctima, la que es una pieza

fundamental para la consumación del delito. (p. 158) además **Lux** (2018) en Europa, precisa que, la doctrina coincide que la participación de la víctima juega un importante papel en la prevención de los fraudes informáticos, ya que los riesgos que son creados mediante el uso de internet pueden ser disminuidos, con la adopción de medidas de seguridad de autoprotección, ya que muchos delitos informáticos suceden por la vulnerabilidades de los sistemas informáticos, que suceden por diversas causas, como una programación deficiente, el cambio tecnológico o un uso de ventana que pueden haberse dejado abiertas. (p. 192)

Se llegó al ponderado de la guía de entrevista, de las fichas de análisis de documento y hallazgos del marco teórico, en base al **objetivo general** de la presente tesis, llegando a la conclusión que, si bien es cierto el Perú cuenta con, el Ley 30096 la cual implica la protección y prevención de los delitos informáticos fraude informático ha venido desarrollándose y avanzando al mismo ritmo de la tecnología, evidenciando con ello que los delitos cometidos mediante la tecnología son pluriofensivos, es así que los fraudes informáticos ah llegando a niveles organizacionales, evidenciando que la mayoría de empresas no emplean medidas y estrategias de seguridad para prevenir o minimizar un posible fraude informático, entre las que se destacan el desarrollo de políticas de seguridad, la formación de empleados, la correcta protección de datos, el empleo de firewalls, los procesos de actualización, monitoreo, así como la gestión de acceso, la correcta evaluación de posibles proveedores, el empleo de la seguridad en la nube, el correcto uso de auditorías de seguridad cibernética. Por ello, la creación de un organismo autónomo regulador, fiscalizador que supervise que las empresas cumplan con las normas y políticas de seguridad de información para garantizar la prevención de los fraudes informáticos; Así mismo establecer conductas infractoras en materia de responsabilidad administrativa y penal para los casos de incumplimiento y exigir que las empresas hagan uso de medidas y estrategias para prevenir y mitigar los efectos del avance tecnológico en el fraude informático.

Siendo las cosas así, se determinó el **supuesto general** propuesto, donde se analizó que el fraude informático afecta la libertad de empresa; los efectos que deja los fraudes informáticos a las empresas son pérdidas significativas de su economía, pérdida de clientes y socios, los atentados traer perdías de recursos financieros girando inestabilidad financiera de la empresa, pérdida de confianza y

calidad de dicha empresa, trayendo quiebras e incluso en cierre de las empresas. Cabe mencionar que la libertad de empresa es una garantía constitucional, el cual debe ser garantizado por el estado peruano para la estimulación de la creación de riquezas para la economía social del estado.

Continuando correlativamente con el Objetivo Específico 1, en la cual se evidencia la tabla a fin de continuar lo enmarcado por la tesis:

Tabla 6

Tabla de discusión del objetivo específico 1

Objetivo Específico 1	Supuesto Específico 1
Analizar de qué manera la ciberseguridad garantiza la libertad de acceso de mercado como garantía constitucional.	la ciberseguridad garantiza la libertad de acceso al mercado como garantía constitucional, porque, a libertad de acceso al mercado se considera un derecho económico fundamental y está respaldada por la legislación constitucional o por leyes específicas de comercio. La ciberseguridad puede desempeñar un papel crucial en la protección de este derecho.

Nota: Elaboración Propia

Por consiguiente, se desarrollaron los objetivos específicos, se comenzó con el objetivo específico 1, en el cual **Fernández y Vargas** (2018) comentan sobre la ciberseguridad, la aparición de los delitos informáticos es una de la problemática más grave y que va creciendo con el avance de la tecnología; en el Perú es muy fácil el acceso a la tecnología y las condiciones socioeconómicas de nuestro país ha ocasionado que se convierta en un lugar adecuado para cometer ciberdelitos. (p. 37) en consecuencia a ello **Aliaga** (2021) respecto a la libertad de organización de empresa, es el terreno donde la organización empresarial es un derecho realizado como el aporte más significativo al desarrollo de la economía nacional, porque cada ordenamiento jurídico crea formas diferentes para el desarrollo más

ordenado de las diversas manifestaciones del negocio o empresa a fundar, teniendo en cuenta la voluntad individual o colectiva de la sociedad; Se define de diferentes maneras, pero la atención se centra siempre en la situación económica. (p. 184)

Dentro de este orden, la **cuarta pregunta cuatro** Quispe (2023), Pomacanchari Torre (2023), Medina (2023), Huacre (2023), Marín (2023), Maquera (2023) y Araujo (2023), coinciden que disponer de un marco legal en tecnología que ampare y proteja la seguridad informática, mediante legisladores capacitados y expertos en la materia de tecnología y el ciberespacio, seria coparticipe de la libertad de empresas, permitiendo acceso por internet a cada uno de los servicios o productos ofertados por las empresas, disminuyendo delitos informáticos, al mismo tiempo que se trata de contribuir además a una posible libertad que permita acceso al mercado de las diversas empresas u organizaciones al lograr el fomento de la innovación, lograr alcanzar la protección de la propiedad intelectual, asegurando al mismo tiempo una verdadera competencia justa, abordando además ciertas preocupaciones tanto relacionadas con la seguridad como también con la privacidad, promoviendo al mismo tiempo el cumplimiento de ciertos estándares de tipo global, al mismo tiempo que se alcancen y se faciliten las diversas resoluciones de disputas.

Todo lo anterior va a permitir que se suscite o formule la creación de un ambiente favorable para que todas las empresas logren no sólo ingresar sino además operar en diversos mercados competitivos y que en muchos casos sean tecnológicamente avanzados y al mismo tiempo lograr que se le brinde una más rápida y mayor seguridad informática posible a cada uno de los posibles clientes y/o usuarios.

Así mismo la **quinta pregunta** para Quispe (2023), no existe un verdadero desarrollo de las políticas de ciberseguridad, debido a que durante los últimos tiempos y por diversas problemáticas que ha enfrentado el país ha privado la puesta en marcha de empresas nuevas, por lo cual es necesario que se incremente de forma eficiente tales políticas de seguridad.

Por su parte, Pomacanchari Torre (2023), sostiene que la política de ciberseguridad resulta muy diversa y es necesario que se incluyan tanto agentes estatales, económicos como sociales, esclareciendo al mismo tiempo la

ponderación directa de objetivos e identificando el papel cumplido por el Estado en cada uno de sus múltiples fines, argumentando además que Perú dispone de políticas de ciberseguridad, aunque no son ejecutadas y no hay un apropiado rastreo.

Mamani (2023) sostiene que la ciberseguridad juega un papel crucial en la prevención y mitigación del fraude informático porque el fraude informático abarca una amplia gama de actividades delictivas que se llevan a cabo a través de medios electrónicos, como el robo de información personal, fraudes financieros, ataques de phishing, y otros tipos de estafas en línea. Los sistemas de ciberseguridad están diseñados para detectar y prevenir amenazas cibernéticas, incluyendo aquellas relacionadas con el fraude. Esto se logra mediante el uso de herramientas como firewalls, sistemas de detección de intrusiones, y software antivirus que identifican patrones de comportamiento sospechosos o firmas de malware conocidas. Por otro lado, manifiesta que la libertad de acceso al mercado es un derecho económico fundamental y está respaldada por la legislación constitucional y por leyes específicas. En ese sentido, la ciberseguridad puede desempeñar un papel crucial en la protección de este derecho, un entorno cibernético seguro ayuda a prevenir fraudes y manipulación del mercado

Asimismo, Medina (2023), Maquera (2023) y Araujo (2023), exponen que, las políticas de ciberseguridad promueven e inhiben una entrada de nuevas empresas dentro del mercado. Para lograr que se promuevan políticas de ciberseguridad ofreciendo un entorno confiable que logre el fomento de la inversión tecnológica e innovación. A pesar de ello, se puede decir que, en muchos casos, políticas ampliamente restrictivas y costosas actúan como barreras de entrada y desincentivar nuevas empresas como consecuencia de altos costos de cumplimiento.

Mientras, Huacre (2023) señala que las instituciones que se encargan de la prevención de delitos informáticos ponen en acción capacitaciones transversales especialidad y por niveles tanto para fiscales, como a peritos de especialidad, realizándose ciertos esfuerzos que permitan la sensibilización del público, para alcanzar la prevención del ciberdelito.

Continuando con la **sexta pregunta** Quispe (2023), Pomacanchari Torre (2023), Medina (2023), Huacre (2023), Marín (2023), Maquera (2023) y Araujo

(2023) refieren que, existe una complicada realidad económica en Perú, la cual es consecuencia de una ausencia tanto de productos como de servicios competitivos dentro del mercado globalizado; por ausencia de conocimientos tanto científicos como tecnológicos, ya que no existe promoción de investigación con presupuestos que se ajusten.

Finalmente, Marín (2023), hizo referencia a la relevancia de la estrategia Nacional de Ciberseguridad Española en el contexto de la Estrategia de Seguridad Nacional se traduce en un resultado de un gran esfuerzo de la administración para enfrentarse de modo más seguro y con más amplias garantías de retos como país, dentro del contexto internacional dominado por uso exponencialmente creciente de la tecnología.

Aunado a ello el impacto leal de la tecnología aporta al acceso de mercado, referente a ello la **Resolución Presidencial N.º 097-2020-CONCYTEC-P** en el **numeral 3** de la Ley Marco de Ciencia, Tecnología e Innovación Tecnológica refiere que la ciberseguridad**,** tiene la finalidad el diseñar del marco legal e institucional, el cual también incluye la administración de justicia, dentro del cual, las personas naturales como las empresas productivas, dispongan de un orden jurídico que les dé estabilidad y no incertidumbre en la disposición y ejercicio de sus derechos adquiridos bajo Ley. Así mismo la Sentencia del Tribunal Constitucional del EXP. N.º 01405-2010-PA/TC – Callao, Consideraciones del Tribunal Constitucional, en el **apartado 15** conforme a la **libertad de acceso de mercado,** es una garantía de toda persona jurídica o natural la cual tiene libertad y decisión de crear empresas - libertad de fundación de una empresa, para actuar en el mercado - libertad de acceso al mercado, y poder establecer sus propios objetivos en su creación de empresa - libertad de organización del empresario, por ultimo dirigir y planificar su actividad - libertad de dirección de la empresa, bajo sus recursos condiciones, como también tienen la libertad de cesación y/o de salida del mercado cuando la persona lo vea conveniente.

El marco teórico, precisa, **Fernández y Vargas** (2018) comentan sobre la **ciberseguridad**, el aumento de los delitos informáticos es uno de los problemas más graves y recientes en el Perú, y el fácil acceso del país a la tecnología y las condiciones socioeconómicas lo convierten en un lugar adecuado para los delitos cibernéticos. (p. 37) Asimismo, **Rodríguez** (2016) se refiere al libre acceso al

mercado utilizando la llamada libertad de creación de empresas, que protege no solo el derecho a constituir una empresa, sino también el derecho a operar en el mercado, según la llamada libre acceso al mercado. Cualquiera que tenga la capacidad de producir bienes o prestar servicios debe ingresar al mercado a su discreción, es decir. nadie (ni el Estado ni otras entidades económicas) puede impedir o limitar dicha participación. (p. 123).

En cuanto al objetivo **específico 1,** se refiere a que el país ha logrado un valioso acceso en la figura del convenio de Budapest, que dispone de un marco legal internacional que permite el salvaguardo de la seguridad informática, la cual no ha sido explotada para el empleo de la legislación peruana. Es por ello que en Perú se han venido adaptando regulaciones internacionales sobre tecnología que equilibren la libertad de acceso al mercado mediante la armonización normativa, participación en tratados internacionales, promoción de innovación, creación de agencias reguladoras especializadas y fomento de inversión extranjera dentro del sector tecnológico, con tales medidas se trata de lograr la promoción de un ambiente empresarial competitivo facilitando acceso al mercado para organizaciones tecnológicas, los avances tecnológicos que manejen las empresas para la protección de la información podrían significar una real ventaja competitiva ante otras empresas. Por lo que la regulación internacional sobre la tecnología avanza y se actualiza de manera constante para tratar de proteger la correcta implementación de normas ISO.

Se llego a **supuesto especifico 1**, por lo que se infiere, que la ciberseguridad se relaciona con la garantía a la continuidad de las operaciones comerciales por que los ataques cibernéticos pueden interrumpir las actividades comerciales, afectando directamente la libertad de acceso al mercado de los actores económicos. En ese sentido, un entorno cibernético seguro fomenta la confianza entre los participantes del mercado. La confianza es fundamental para el buen funcionamiento de las transacciones comerciales y, por ende, para la libertad de acceso al mercado. En relación con ello, la ciberseguridad debe de estar respaldada por regulaciones que busquen proteger los intereses económicos y la libertad de acceso al mercado. En ese sentido, la ciberseguridad se centra en proteger la integridad, confidencialidad y disponibilidad de la información. Por ello, la implementación de medidas como la encriptación de datos, el control de acceso y las políticas de gestión de la información contribuye a prevenir el acceso no

autorizado y el robo de datos, elementos clave en muchos fraudes informáticos. También, es fundamental la colaboración entre entidades, organizaciones y gobiernos para compartir información sobre amenazas y técnicas de fraude es esencial. La ciberseguridad se ve reforzada cuando hay una red sólida que permite una respuesta coordinada frente a amenazas y ataques.

Finalmente, en el orden que corresponde el objetivo específico 2, se mostró la siguiente tabla.

Tabla 7

Tabla de discusión del objetivo específico 2

Objetivo Específico 2	Supuesto Específico 2
Analizar de qué manera el derecho protección de datos contribuye a la libertad de la organización de empresa como garantía constitucional	El derecho a la protección de los datos contribuye a la libertad de la organización empresarial como garantía constitucional, ya que el derecho a la protección de datos desempeña un papel fundamental en la prevención y gestión del fraude informático, asimismo, coadyuva el respeto de este derecho por parte de las empresas a generar mayor confianza a los usuarios, logrando obtener una posición en el mercado mediante la reputación y generar mayores ingresos a las empresas.

Nota: Elaboración Propia

Es de resaltar que, Mendoza (2018) manifiesta que el derecho y privacidad, en México si bien en cierto de la regulación en materia de protección de datos personales para empresas públicas y privadas garantiza un derecho humano, también es un beneficio económico a nivel internacional, la cual deben tener un alto

nivel adecuado de protección de la información, ello para que el país se pueda declarar seguro en el intercambio comercial. (p. 589)

Continuando con la pregunta **siete** Quispe (2023), Pomacanchari Torre (2023), Medina (2023), Huacre (2023), Marín (2023), Maquera (2023) y Araujo (2023), coinciden en sus respuestas al señalar que si puede dar apoyo a la privacidad de la información debido a que es imprescindible ejercer el derecho de la libertad de expresión, evitando de este modo violación de un derecho reconocido por esta, por lo que tal derecho a la privacidad de información trata de garantizar el derecho fundamental a la protección de datos personales, por medio de un idóneo tratamiento, dentro del respeto a los derechos que en ella se reconocen, tratando lograr de esta manera un acertado equilibrio entre derechos y privacidad de información así como la libertad de organización, la cual puede ser de beneficio al garantizar protección de datos y confianza dentro del mercado, pero además puede perjudicar si las regulaciones son excesivas y dificultan el proceso operativo de las empresas, limitando la recopilación de datos o un adecuado equilibrio con las necesidades de ciberseguridad.

Sobre ello, Beaumont (2023) menciona que la libertad de empresa en el ejercicio de estos derechos sin perjuicio de la moral, la salud o la seguridad pública; cooperación entre el Estado y empresas estatales o privadas, libertad de contratación, libre competencia, igualdad de condiciones para las inversiones nacionales y extranjeras, almacenamiento y disposición de divisas y adopción de normas dentro de la economía social de mercado. Protección interna y protección del consumidor. (p. 16) Por tanto, la iniciativa privada es libre, lo es y seguirá siendo, porque el Estado es el escudo constitucional del sistema económico y debemos conservarlo, tratar de corregir su realización y todo lo que interfiera en la creación de la igualdad para toda la sociedad y mejores oportunidades.

Asimismo, no hay menoscabo de por medio a la libertad de organización, cuando una empresa obtiene información privada de determinado cliente, la misma recibe la responsabilidad de otorgarle un adecuado procedente a esta información, la cual quedará obligada a lograr la salvaguarda de toda la información que se le brinde.

En cuanto a la pregunta **ocho** Quispe (2023), Pomacanchari Torre (2023), Medina (2023), Huacre (2023), Marín (2023), Maquera (2023) y Araujo (2023),

coinciden que muchas empresas que son víctimas de delitos informáticos se han enfrentado al robo de datos tanto informáticos como personales, accesos no autorizados a sistemas informáticos, daños informáticos en sistemas, así como pérdidas económicas. Puede decirse además que la ausencia de medidas preventivas en las regulaciones relacionadas con la privacidad de información induce a consecuencias legales, tales como sanciones y demandas, así como a graves repercusiones en la reputación de la empresa, incluyendo también pérdida de confianza de clientes, de negocios y de daños financieros. Siendo imprescindible que las empresas implementen ciertas medidas que sean sólidas de privacidad de datos para evitar de este modo consecuencias.

Mamani (2023) señala que para prevenir los delitos informáticos las empresas deben de incorporar tecnologías emergentes de la actualidad como la inteligencia artificial (IA) y el blockchain, esta combinación es poderosa para fortalecer la seguridad de la información, la IA tiene la capacidad de analizar patrones de comportamiento y detectar anomalías en el tráfico de datos. Al integrar la capacidad que brinda la IA para identificar comportamientos inusuales con la inmutabilidad de los registros en blockchain, se crea un sistema robusto para la detección de intrusiones y la prevención de ataques. En ese sentido, blockchain pueden ser utilizados para automatizar procesos de auditoría y la IA puede analizar los datos almacenados y ejecutar auditorias automáticas para verificar la integridad de los datos, asegurando que no haya manipulaciones maliciosas, asimismo, la IA puede procesar grandes volúmenes de datos y aprender patrones de amenazas de manera más eficiente.

Estos consideran además que las principales consecuencias legales vienen a ser: empresas que pueden ser demandas por clientes, socios comerciales así como otras partes afectadas por delito informático, que puede resultar en multas y en daños económicos, además de enfrentar sanciones regulatorias por tener incumplimiento de leyes de protección de datos, generándose de este modo finalmente pérdidas económicas producto de los ciberataques, crisis de seguridad en posición de sanciones, daño de reputación y finalmente pérdida de clientes.

Con relación a la pregunta **nueve** Quispe (2023), Pomacanchari Torre (2023), Medina (2023), Huacre (2023), Marín (2023), Maquera (2023) y Araujo (2023), señalan que es posible garantizar por medio de copias de seguridad o de

respaldos, empleando antivirus en el sistema informático, controlando el acceso a la información que comparte con sus usuarios, fomentando una cultura de contraseñas seguras entre otras. De este modo sostienen que, las empresas víctimas de delitos informáticos se enfrentan al secuestro de datos informáticos que buscan ser de índole personal, laboral y claves de seguridad, accesos no autorizados a sistemas informáticos.

Finalmente, Huacre (2023), expone además que un marco legal puntual es crucial que exista un marco legal claro y actualizado que defina los delitos informáticos, que establezcan las penas correspondientes, mientras que la cooperación internacional, dado que los delitos informáticos transcienden las fronteras nacionales, la cooperación internación es necesaria para prevenir los delitos.

Concluyendo, con nuestras **fichas de análisis documental** que dan soporte al **objetivo específico dos,** la **Resolución N. ° 071-2022-2023-OM-CR**, en el **apartado 2** sobre las de protección de los datos personales – **Ley N.º 29733**, con relación al **derecho de protección de datos,** el uso de los datos personales se denota como sensibles, se maneja con sumo cuidado puesto que el gobierno peruano debe velar por ello, para que no haya un perjuicio al usuario de parte de las empresas públicos o privados, así mismo, se debe brindar medidas de seguridad a las personas en general, no es fácil poder proteger una base de datos que se encuentren almacenados, por ello la protección de datos debe ir en colaboración de los clientes y entidades o empresas, brindándole seguridad, para garantizar la atención de derechos de acceso, rectificación, cancelación y oposición, asimismo, asegurar la atención de las solicitudes o requerimientos formulados por la autoridad de protección de datos personales.

En la misma línea la **Resolución Ministerial N.º 129-2012-PCM,** en el **numeral 8** sobre La Norma Técnica Peruana “NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información, con relación a la **libertad de organización de empresa** establece un Plan de Seguridad de la Información bajo normas Técnicas, esta se establece en la Agenda Digital Peruana 2.0, donde establece la necesidad de contar estrategias de ciberseguridad para evitar incidentes en recursos de información, las bases se encuentran en Códigos de buenas prácticas para las gestiones de seguridad de información.

Se logró los hallazgos del **objetivo específico 2**, en **Paraguay,** mediante el Decreto Nro. 7052 el 24 de abril del 2017 aprueba el plan nacional de ciberseguridad e integra la comisión nacional de ciberseguridad (Presidencia de la República del Paraguay, 2017) donde se establece líneas de acción para fortalecer la seguridad en los activos críticos y así lograr un ciberespacio seguro, resiliente y confiable respectivamente. Cuenta con áreas focales como la coordinación gubernamental, cooperación pública – privada, cooperación internacional y marco legal. De la misma forma, tiene un Comité Nacional de Seguridad Cibernética (Ministerio de Tecnologías de la Información y Comunicaciones, 2020).

Por su parte **Chile**, cuenta con la Política Nacional de Ciberseguridad 2017-2022, el pasado 26 de mayo del 2023 el Gobierno presentó su propuesta de nueva Política Nacional de Ciberseguridad incorpora 5 ejes como infraestructura resiliente, derecho de personas, cultura de ciberseguridad, coordinación nacional e internacional y fomento de la industria y la investigación científica (Ministerio de Interior y Seguridad Pública).

En **argentina**, el 5 de diciembre del 2022, mediante Resolución 17/2022, la secretaria de innovación pública aprobó el Comité Nacional de Blockchain y los lineamientos Nacional sobre Blockchain, cuyo objetivo es utilizar la tecnología como una herramienta para optimizar los procesos, políticas y seguridad de la información en la administración central, los organismos descentralizados, empresas y sociedades del Estado, los entes públicos y evitar, así, la falsificación y fraude en la gestión. La Resolución establece pilares para una buena normativa aplicable a la tecnología blockchain como la privacidad, identidad, seguridad y procedencia de los datos y gobernanza.

Colombia, la necesidad de regular la gestión de la información se desprende del artículo 15 de la Constitución política de 1991, la cual, establece el tratamiento y circulación de los datos utilizando la tecnología blockchain por que genera confianza en las partes al no existir un tercero que controle y centralice los datos, por ello no existe riesgo para ser filtrado o alterado.

Por lo que se puede inferir la existencia de la discrepancia de la Ley 29733 de Protección de Datos y el sistema de blockchain, porque, la Ley busca controlar la información porque es administrada por un tercero, mientras tanto, blockchain; la

información es descentralizada. Por ello, se requiere que esta nueva tecnología encripta la información.

Mendoza (2018) manifiesta que el derecho de protección de datos, en México si bien en cierto la regulación en materia de la protección de datos personales en empresas públicas y privadas garantiza un derecho humano, también es un beneficio económico a nivel internacional, la cual deben tener un alto nivel adecuado de protección de la información, ello para que el país se pueda declarar seguro en el intercambio comercial. (p.589)

Asimismo, **Aliaga** (2021) respecto a la libertad de organización de empresa, es el terreno donde la organización empresarial es un derecho, que, al crear formas diferentes para cada ordenamiento jurídico, las diversas manifestaciones del negocio o empresa a crear logran desarrollarse de manera más ordenada, teniendo en cuenta los deseos individuales o colectivos, realizando así el aporte más significativo al desarrollo de la economía. Social; Las empresas se definen de diferentes maneras, pero la atención se centra siempre en las condiciones económicas. (p. 184)

Po lo señalado en el objetivo **específico 2** de la tesis concluyó que las principales consecuencias legales vienen a ser: empresas que pueden ser demandas por clientes, socios comerciales así como otras partes afectadas por delito informático, que puede resultar en multas y en daños económicos, además de enfrentar sanciones regulatorias por tener incumplimiento de leyes de protección de datos, generándose de este modo finalmente pérdidas económicas producto de los ciberataques, crisis de seguridad en posición de sanciones, daño de reputación y finalmente pérdida de clientes. Asimismo, la Constitución Política del Perú ampara la libre organización de las empresas, con el fin de lograr para sí mismo una posición en el mercado laboral y ganancias económicas, pero ello también implica cumplir con parámetros establecidos por los legisladores, como es el proteger y salvaguardad la información personal y cesible que puedan llegar a obtener dependiendo en el área que se desempeñan, existiendo la ley de protección de datos personales, las empresas deben operar en entorna a esta ley.

Se afirmó en el **supuesto específico 2**, el derecho a la protección de los datos contribuye a la libertad de la organización empresarial como garantía constitucional, ya que el derecho a la protección de datos desempeña un papel

fundamental en la prevención y gestión del fraude informático, asimismo, coadyuva el respeto de este derecho por parte de las empresas a generar mayor confianza a los usuarios, logrando obtener una posición en el mercado mediante la reputación y generar mayores ingresos a las empresas.

V. CONCLUSIONES

Primera: En cuanto al análisis realizado, la presencia de los fraudes informáticos genera impacto significativo en la libertad de empresa de diversas maneras como las pérdidas económicas restringiendo su capacidad para operar, invertir y competir en el mercado, asimismo, daña la reputación de la empresa, pérdida de confianza de los clientes, socios comerciales, afecta la capacidad para atraer nuevos clientes y mantener relaciones comerciales existentes, también, puede paralizar temporal o completa de las operaciones de las empresas, dificultando brindar servicios de manera efectiva, perdida de información estratégica brindando que los competidores obtengan ventaja indebida, afectando la libertad de la empresa para innovar y competir, por otro lado, la empresa víctima del fraude informático enfrentan costos significativos para mitigar los daños, costos legales, en ese sentido, las empresas pueden enfrentar demandas, multas y sanciones regulatorias por no cumplir con las leyes de protección de datos. La norma de delitos informáticos se encuentra en ambigüedad, se evidencio que la mayoría de empresas no emplean medidas y estrategias de seguridad para prevenir o minimizar un posible fraude informático, entre las que se destacan el desarrollo de políticas de seguridad, la formación de empleados, la correcta protección de datos, el empleo de firewalls, los procesos de actualización, monitoreo, así como la gestión de acceso, la correcta evaluación de posibles proveedores, el empleo de la seguridad en la nube y el correcto uso de auditorías de seguridad cibernética.

Segunda: Se evidencio que existe desafíos potenciales en la protección de los datos empresariales frente a los avances de las tecnológicas emergentes de la actualidad, asimismo, no existe auditorias de seguridad periódicas para evaluar la seguridad de los sistemas y base de datos, tampoco un plan de respuesta a incidentes para ser abordados rápidamente las amenazas y minimizar el impacto de los delitos informáticos. De la misma manera, se carece de especialistas altamente capacitados en ciberseguridad. En ese sentido, para lograr de manera efectiva la protección de datos se requiere de un esfuerzo continuo y la combinación de tecnología, procesos y concienciación. Es esencial adaptarse a las nuevas amenazas y desafíos que puedan surgir en el panorama de la ciberseguridad, por ello, se requiere de una constante actualización de las normas para abordar los desafíos relacionados a la tecnología y la privacidad de la información. La evolución de la sofisticación de los ataques cibernéticos debe ser respondida de manera

dinámica y proporcional. Sin una respuesta estratégica, los esfuerzos nacionales en materia de seguridad cibernética serán insostenibles, esporádicos, ineficientes.

Tercera: El derecho a la protección de datos juega un papel importante en la prevención y mitigación del fraude informático, asimismo, apoya a la organización empresarial, sin embargo, la mala gestión de las medidas preventivas traen consecuencias legales en las industrias, como demandas interpuestas por las partes afectadas del delito informático, asimismo, puede resultar perjudicial por la imposición de multas, generando daños económicos producto de los ciberataques daño reputacional y perdida de cliente, además, de enfrentar sanciones por el incumplimiento de leyes vigentes de protección de datos como la Ley 29733. Asimismo, el art. 59 de la Constitución Política del Perú garantiza la libertad de empresa, comercio e industria, asimismo, en ese sentido, las empresas deben de proteger y salvaguardad la información personal utilizando la tecnología blockchain que tiene un gran potencial para mejorar la seguridad de la información y abordar algunos de los desafíos asociados con los ciberdelitos. Finalmente, la tecnología del blockchain es compatible con la Ley 29733, Ley de protección de datos por que la tecnología blockchain ofrece varios beneficios significativos en el ámbito de la seguridad de la información, lo que puede contribuir a mitigar y prevenir ataques cibernéticos.

VI. RECOMENDACIONES

Primera: Al Poder Legislativo que disponga la creación de un organismo (Seguridad Nacional Cibernética - SENACI) autónomo regulador, fiscalizador, que supervise tanto empresas públicas y privadas cumplan con las normas y políticas de seguridad de información para garantizar la prevención de los fraudes informáticos, con la finalidad de cumplir con las medidas y estrategias de seguridad para prevenir o minimizar un posible fraude informático, entre las que se destacan el desarrollo de políticas de seguridad, la formación de empleados, la correcta protección de datos, el empleo de firewalls, los procesos de actualización, monitoreo, así como la gestión de acceso, la correcta evaluación de posibles proveedores, el empleo de la seguridad en la nube, el correcto uso de auditorías de seguridad cibernética.

Segunda: A la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, disponga la creación del Plan Nacional de Blockchain, asimismo, la creación del Comité Nacional de Blockchain y lineamientos donde se establezca políticas a nivel gubernamental y nacional de estrategias para reforzar la seguridad de sus activos críticos y alcanzar un ciberespacio que sea seguro, confiable y resistente, el plan debe de contribuir en garantizar estabilidad económica, continuidad del negocio, asegurar que los datos e infraestructura criticas estén protegidos y seguros, asimismo, debe de ser fortalecida con la Ley N° 318114 que regula la inteligencia artificial – IA. En ese sentido, la IA tiene la capacidad de analizar patrones de comportamiento y detectar anomalías en el tráfico de datos. Al integrar la capacidad que brinda la IA en identificar comportamientos inusuales con la inmutabilidad de los registros en blockchain, se crea un sistema robusto para la detección de intrusiones y la prevención de ataques. Por ello, el blockchain pueden ser utilizados para automatizar procesos de auditoría y la IA puede analizar los datos almacenados y ejecutar auditorias automáticas para verificar la integridad de los datos, manipulaciones maliciosas. Por otro lado, las escuelas de posgrado de las universidades dispongan la creación de la maestría en TICs con énfasis en auditoria y seguridad de la información por la creciente sofisticación de las amenazas cibernéticas genera demanda significativa de profesionales altamente capacitados en auditoría y seguridad de la información.

Tercera: Al Gobierno Digital, con el fin de que establezcan conductas infractoras en materia de responsabilidad administrativa y penal para los casos de incumplimiento, con la finalidad de evitar crisis de seguridad en posición de sanciones, daño de reputación y finalmente pérdida de clientes. Asimismo, la Constitución Política del Perú ampara la libre organización de las empresas, con el fin de lograr para sí mismo una posición en el mercado laboral y ganancias económicas.

REFERENCIAS

Ablon, L. (2018). Data Thieves: The motivations of cyber threat actors and their use and monetization of stolen data. En *RAND Corporation eBooks*. https://doi.org/10.7249/ct490

Acosta, M., Benavides, M. y García, N. (2020). Cybercrime: Impunity organizational and its complexity in the business of the world. *Revista Venezolana de Gerencia, 25* (89). https://www.redalyc.org/journal/290/29062641023/html/

Acuario, S. (2016). *Delitos informáticos: generalidades*. UDGVirtual, 01-67. http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/599

Aliaga, L. A. (2021). La magnitud de la MYPE en el Perú. libertad para elegir la estructura empresarial. *Giuristi*, *2*(4), 181-199. https://doi.org/10.46631/giuristi.2021.v2n4.04

Barceló, R. (2021). El impacto de la tecnología blockchain en la contratación privada; ¿hacia una contratación inteligente? *Revista de Internet, Derecho y Política*, 33. https://doi.org/10.7238/idp.v0i33.375171

Beaumont, R. A. (2023). La libertad de empresa y su regulación por el derecho peruano. *Fondo editorial Universidad San Ignacio de Loyola*, *1*, 1-20. https://repositorio.usil.edu.pe/entities/publication/98feaa9a-1e27-4e1b-923c-6d5ded8b8347

Brenner, S. W. (2016). Bits, Bytes and Bicycles: Theft and «Cyber Theft». *ResearchGate*, *47*, 817. https://www.researchgate.net/publication/311064912_Bits_Bytes_and_Bicycles_Theft_and_Cyber_Theft

Cabrera, A. (2017). LA REGULACIÓN DEL DERECHO A LA LIBERTAD DE EXPRESIÓN EN INTERNET: ESTÁNDARES INTERAMERICANOS Y EL CASO DE FACEBOOK. *Revista Vox Juris*, *(33)1*, 2010-2222. https://eds.s.ebscohost.com/eds/detail/detail?vid=4&sid=cc0e2244-6e6b-4749-84d4-e8352ec222a6%40redis&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=124627413&db=fua

Campos, O. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. *Revista Científica Hallazgos21,* *4*(1), 100- 111. http://revistas.pucese.edu.ec/hallazgos21/

Carrasco, H. (2018). EL CONTENIDO Y LÍMITES DE LA LIBERTAD DE EMPRESA Y SU ARTICULACIÓN CON EL DERECHO DE LIBERTAD SINDICAL. *VI Congreso Nacional de Derecho del Trabajo y de la Seguridad Social*, 917-933. https://www.spdtss.org.pe/wp-content/uploads/2021/10/VI-Congreso-Nacional-full-917-933.pdf

Congreso de la República. (2011). *Ley N.º 2973.* Ley de Protección de Datos Personales. https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733

Echevarría, M. V., Garaycoa, M. A., & Tusev, A. (2020). ¿ESTÁN PREPARADOS LOS MILLENNIALS ECUATORIANOS CONTRA UN ATAQUE INFORMÁTICO? Chakiñan, 10, 73-86. https://doi.org/10.37135/chk.002.10.05

Esteban, N. (2018) Tipos de Investigación. Universidad Santo Domingo de Guzmán. https://core.ac.uk/download/pdf/250080756.pdf

Fernandes, A. Z. (2023*). Métodos de investigación: qué y cuáles son (con ejemplos)*. Toda Materia. https://www.todamateria.com/metodos-de-investigacion/

Fernández, W., & Vargas, C. (2018). ¿Son útiles las TIC para combatir la ciberdelincuencia? La relación entre la denuncia de delitos informáticos y el equipamiento tecnológico de las comisarias. *Revista de Direito*, *Estado e Telecomunicacoes*, 10(2), 37-52. https://link.gale.com/apps/doc/A568257005/AONE?u=univcv&sid=bookmark-AONE&xid=d9166d9b

Ferrero, F. (2018). Algunos aspectos éticos de la investigación en educación médica. *Archivos argentinos de pediatría*, *116*(6), 384–385. https://doi.org/10.5546/aap.2018.384

Gallardo, E. E. (2018). *Metodología de la Investigación.* Universidad Continental. 9-97.

https://repositorio.continental.edu.pe/bitstream/20.500.12394/4278/1/DO_UC_EG_MAI_UC0584_2018.pdf

Gordillo, V. (2021). BLOCKCHAIN Y PROTECCIÓN DE DATOS. *Revista Estudiantil de Derecho Privado*, *7*. https://red.uexternado.edu.co/blockchain-y-proteccion-de-datos

Heineman, K. (2019) Introducción a la metodología de la investigación empírica en las ciencias del deporte. Editorial Paidotribo. 2da ed.

Ibarra, S., Segredo, S., Juárez, L. G., & Tobón, S. (2018). Estudio de validez de contenido y confiabilidad de un instrumento para evaluar la metodología socioformativa en el diseño de cursos. *ESPACIOS*, *(39)53*, 24. https://www.revistaespacios.com/cited2017/cited2017-24.pdf

Iño, W. (2018). Investigación educativa desde un enfoque cualitativo: la historia oral como método. Voces de la educación, 3(6), 93–110.

Kynigopoulo, C. (2019). Cyber fraud and crime. *Mediterranean College, Egnatia* 2-4.https://www.researchgate.net/publication/349732591_Cyber_fraud_and_crime

Lux, L. M. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Ius Et Praxis*, 24(1), 159-206. https://doi.org/10.4067/s0718-00122018000100159

Lux, L. M., & Calderón, G. O. (2020). The Crime of Cyber Fraud: Definition and Delimitation. *Revista Chilena de Derecho y Tecnología*, 9(1), 151-184. https://revistaschilenas.uchile.cl/handle/2250/136605

Malik, J. & Choudhury, S. (2019). Privacy and surveillance: The Law relating to Cyber Crimes in India. *Journal of Engineering, Computing and Architecture* *9*(12), 74-98. https://www.researchgate.net/publication/340756434_Privacy_and_surveillance_The_Law_relating_to_Cyber_Crimes_in_India

Mendoza, O. A. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: Desafíos y cumplimiento. *Revista IUS*, *12 N.º 41*, 267-291. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267&lang=es

Mendoza, O. A. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *Revista IUS*, *15*(48), 179-207. https://doi.org/10.35487/rius.v15i48.2021.743

Minahim, M. A. de A., & Spinola, L. M. C. (2017). THE FRAUD COMMITTED BY COMPUTERISED MEANS UNDER THE OPTICS OF VITIMODOGMATIC/A FRAUDE COMETIDA POR MEIOS INFORMATICOS SOB O PRISMA DA VITIMODOGMATICA. *Revista de Direito Penal, Processo Penal e Constituicao*, 3(2), 144. https://go.gale.com/ps/i.do?p=AONE&u=univcv&id=GALE%7CA609817166&v=2.1&it=r&inPS=true

Ministerio de Tecnologías de la Información y Comunicación Paraguay. (s. f.). *Ciberseguridad y Protección de la información*. CERT - PY. https://www.mitic.gov.py/viceministerios/tecnologias-de-la-informacion-y-comunicacion/ciberseguridad-y-proteccion-a-la-informacion

Ñaupas, H., Valdivia, M., Palacios, J., & Romero, H. (2018). *Metodología de la investigación cuantitativa - Cualitativa y Redacción de la Tesis* (5.ª ed.). Ediciones de la U,9-559. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/MetodologiaInvestigacionNaupas.pdf

Páramo, P. (2018) La investigación de Ciencias Sociales: Técnicas de recolección de información. Bogotá: Universidad piloto de Gobiernos.

Peña, T. (2022). Etapas del análisis de la información documental. *Revista Interamericana de Bibliotecología*, *(45)3*, 1-7. http://www.scielo.org.co/pdf/rib/v45n3/2538-9866-rib-45-03-e4.pdf

Política Nacional de Ciberseguridad. (2023, 30 mayo). CSIRT. https://www.csirt.gob.cl/noticias/gobierno-presento-su-nueva-politica-nacional-de-ciberseguridad/

Presidencia de la República de Paraguay Ministerio de Relaciones Exteriores. (2017). *Decreto N.º 7052*. Por la cual se aprueba el plan nacional de ciberseguridad y se integra la comisión nacional de ciberseguridad. https://www.mspbs.gov.py/dependencias/dgtic/especiales/Decreto-Nro-7052-24-Abril-2017-Plan-Ciberseguridad.pdf

Quintana, L. y Hermida, J. (2019). La hermenéutica como método de interpretación de textos en la investigación psicoanalítica. *Perspectivas en Psicología: Revista de Psicología y Ciencias Afines, 16*(2), 73-80. https://www.redalyc.org/journal/4835/483568603007/

Rodríguez, C. (2016). PRINCIPIOS GENERALES DEL RÉGIMEN ECONÓMICO DE LA CONSTITUCIÓN POLÍTICA DEL PERÚ. *Quipukamayoc, 24*(45), 121–137. https://doi.org/10.15381/quipu.v24i45.12475

Rodríguez, V. (2021). Principio constitucional de la libre competencia. *Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas*, 44, 257-289. https://doi.org/10.14482/INDES.30.1.303.661

Rosales, M. I. (2023). *Enfoque cualitativo: Definición y Características*. Web y Empresas. https://www.webyempresas.com/enfoque-cualitativo-definicion-y-caracteristicas/

Secretaría Nacional de Tecnologías de la información y comunicación. (s. f.). *Plan Nacional de Ciberseguridad*. CERT - PY. https://www.cert.gov.py/wp-content/uploads/2020/07/CERT-PY-Plan_Nacional_Ciberseguridad.pdf

Sordini, M. (2019). La entrevista en profundidad en el ámbito de la gestión pública. *Revista Reflexiones, 98* (1), 75-88. https://doi.org/10.15517/rr.v98i1.33083

Téllez, J. A., Camus, F. B., & Silva, J. A. (2022). El abuso de la libertad de empresa en los contratos por adhesión: un nuevo enfoque para el análisis de las cláusulas abusivas. *Revista De Derecho (valdivia)*, *35*(1), 79-101. https://doi.org/10.4067/s0718-09502022000100079

Torres F., J. (2020). LIBERTAD DE EMPRESA. *Revista Electrónica de Derecho Comercial.* 01-14. http://www.derecho-comercial.com/Doctrina/torres01.pdf

Tribunal Constitucional (2014). Sentencia del tribunal constitucional. TC. https://www.tc.gob.pe/jurisprudencia/2019/03455-2014-AA.pdf

Vasconcelos, S., Menezes, P., Ribeiro, M., & Heitman, E. (2021, 5 febrero). Rigor científico y ciencia abierta: desafíos éticos y metodológicos en la investigación cualitativa. *SciELO en perpectiva*. https://blog.scielo.org/es/2021/02/05/rigor-cientifico-y-ciencia-abierta-desafios-eticos-y-metodologicos-en-la-investigacion-cualitativa/

Veliz, C. (2022). *Privacidad es poder: Datos, vigilancia y libertad en la era digital*. DEBATE, (17)49 1-304. https://books.google.es/books?hl=es&lr=&id=EDA0EAAAQBAJ&oi=fnd&pg=PT3&dq=libertad+de+organizacion+de+empresa&ots=1TRk96Calh&sig=LlSdOJPZAMD7avSkV4BvOrIK_QU#v=onepage&q=libertad%20de%20organizacion%20de%20empresa&f=false

Viera, C. (2016). LA LIBERTAD DE EMPRESA Y ALGUNOS LÍMITES DESDE LA PERSPECTIVA DEL ESTADO SOCIAL. *Revista Jurídica Universidad Autónoma de Madrid*, *21*, 197-224. https://revistas.uam.es/revistajuridica/article/view/6021

Zhang, Y. & Dong, H. Criminal law regulation of cyber fraud crimes—from the perspective of citizens' personal information protection in the era of edge computing. *Journal of Cloud Computing, 12* (64). https://doi.org/10.1186/s13677-023-00437-3

ANEXOS

Anexo 1: Matriz de Categorización Apriorística

FACULTAD DE DERECHOS Y HUMANIDADES

ESCUELA: Escuela Profesional de Derecho

NOMBRE DE LA ESTUDIANTE: Chumbe Huarhuachi, Briggit Bettsy

ÁMBITO TEMÁTICO: Delitos informáticos y garantías constitucionales

TÍTULO	
Fraude informático frente a la libertad de empresa como garantía constitucional de Lima, 2023	
PROBLEMAS	
Problema General	¿De qué manera el fraude informático afecta la libertad de empresa como garantía constitucional?
Problema Específico 1	¿De qué manera la ciberseguridad garantiza la libertad de acceso de mercado como garantía constitucional?
Problema Específico 2	¿De qué manera el derecho a la protección de datos contribuye a la libertad de la organización empresarial como garantía constitucional?
OBJETIVOS	
Objetivo General	Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional.
Objetivo Específico 1	Analizar de qué manera la ciberseguridad garantiza la libertad de acceso de mercado como garantía constitucional.

Objetivo Específico 2	Analizar de qué manera el derecho a la protección de datos contribuye a la libertad de la organización empresarial como garantía constitucional.
SUPUESTOS	
Supuesto General	El fraude informático afecta la libertad de empresa; los efectos que deja los fraudes informáticos a las empresas son pérdidas significativas de su economía, pérdida de clientes y socios, los atentados traer perdías de recursos financieros girando inestabilidad financiera de la empresa, pérdida de confianza y calidad de dicha empresa, trayendo quiebras e incluso en cierre de las empresas.
Supuesto Específico 1	la ciberseguridad se relaciona con la garantía a la continuidad de las operaciones comerciales por que los ataques cibernéticos pueden interrumpir las actividades comerciales, afectando directamente la libertad de acceso al mercado de los actores económicos. En ese sentido, un entorno cibernético seguro fomenta la confianza entre los participantes del mercado. La confianza es fundamental para el buen funcionamiento de las transacciones comerciales y, por ende, para la libertad de acceso al mercado. En relación con ello, la ciberseguridad debe de estar respaldada por regulaciones que busquen proteger los intereses económicos y la libertad de acceso al mercado.
Supuesto Específico 2	El derecho a la protección de los datos contribuye a la libertad de la organización empresarial como garantía constitucional, ya que el derecho a la protección de datos desempeña un papel fundamental en la prevención y gestión del fraude informático, asimismo, coadyuva el respeto de este derecho por parte de las empresas a generar mayor confianza a los usuarios, logrando obtener

	una posición en el mercado mediante la reputación y generar mayores ingresos a las empresas.

Categorización	**Categoría 1: fraude informático** Subcategoría 1: Ciberseguridad Subcategoría 2: Derecho de protección de datos **Categoría 2: Libertad de empresa** Subcategoría 1: Libertad de acceso de mercado Subcategoría 2: Libertad de organización de empresa
METODOLOGÍA	
Tipo y Diseño de investigación	- **Enfoque:** Cualitativo - **Diseño:** Teoría Fundamentada - **Tipo de investigación:** Básica - **Nivel de la investigación:** Descriptivo
Método de muestreo	- **Escenario de estudio:** Distrito de Cercado de Lima, ubicado en la parte central de Lima Metropolitana, provincia y región de Lima - Perú - **Participantes:** especialistas en derecho penal, derecho informático, Dirección de Investigación Criminal (DIRINCRI), fiscales provinciales - **Muestra no probabilística** - **Tipo:** de expertos. **Orientados por conveniencia**
Plan de análisis y trayectoria metodológica	**Técnica e instrumento de recolección de datos** **Técnica:** Entrevista y análisis documental **Instrumento:** Guía de Entrevista y Ficha de análisis de documentos.
Método de Análisis de información	Análisis hermenéutico, inductivo y descriptivo.

ANEXO 1.1. Matriz de triangulación de datos de entrevista

Problema General	Guía de entrevista P1 Quispe, Huacre y Mamani	Guía de entrevista P2 Pomacanchari, Valderrama y Araujo	Guía de entrevista P3 Medina, Gutierrez y Maquera	Categorías descubiertas	Categorías emergentes	Semejanzas	Diferencias	Conclusiones Aproximativas No definitivas
¿De qué manera el fraude informático afecta la libertad de empresa como garantía constitucional?,	el fraude informático afecta de manera directa, ya que cualquier persona puede ser víctimas de este tipo de delitos y en especial las personas jurídicas porque las empresas generalmente mueven mucho dinero para efectuar las actividades propias y para esto utilizan diversas plataformas	el fraude informático al ser una de las modalidades de delitos informáticos al tratarse de una nueva norma o ley no se encuentra debidamente implementada con la tecnología y logística correspondiente, la ley 30096 no tiene reglamentación especializada en delitos informáticos, en	El fraude informático afecta a la libertad de empresa al comprometer la propiedad intelectual y secretos comerciales, causar pérdidas financieras, dañar la reputación, requerir costos de mitigación, y frenar la innovación en el entorno empresarial	Plataformas digitales Propiedad intelectual Seguridad cibernética	Propiedad intelectual	Plataformas digitales Seguridad cibernética	Propiedad intelectual	Coinciden en señalar que este tipo de fraude informativo afecta de forma directa a las empresas, debido a que nadie está exento de ser víctima de este tipo de delito el cual genera una significativa afectación a la economía financiera de la empresa, asimismo se señala que este tipo de fraude puede

	digitales lo cual los convierte en principales blancos de los ciberdelincuentes	donde se tipifiqué en forma escrita los procesos, procedimientos y pautas para combatir los ciberdelitos y no evoluciona						considerarse una modalidad de delito informático, que lamentablemente a estas alturas dentro de la Ley 30096 no dispone de una tipificación real
Problema Específico 1	**Guía de entrevista P4 Quispe, Huacre y Mamani**	**Guía de entrevista P5 Pomacanchari, Valderrama y Araujo**	**Guía de entrevista P6 Medina, Gutierrez y Maquera**	**Categorías descubiertas**	**Categorías emergentes**	**Semejanzas**	**Diferencias**	**Conclusiones Aproximativas No definitivas**
Analizar de qué manera una base legal de la tecnología aporta en la libertad de acceso de mercado como garantía constitucional	Considero que tener un marco legal en tecnología ayudaría mucho a la libertad de empresas porque permitiría tener acceso a mediante internet a todos los servicios o productos que ofrecen las	La libertad de acceso al mercado de la empresa se encuentra normada, la que también implica la adquisición de deberes y protección a su usuario, quien tiene la obligación de velar por el	El artículo 59º de la Constitución reconoce el derecho a la libertad de empresa, garantizando a todas las personas una libertad de decisión no sólo para crear empresas, es	Base legal de la tecnología Políticas de ciberseguridad	Políticas de ciberseguridad	Base legal de la tecnología	Ciberseguridad Políticas de ciberseguridad	Coinciden que disponer de un marco legal en tecnología que ampare y proteja la seguridad informática, mediante legisladores capacitados y expertos en la materia de tecnología y el ciberespacio,

	empresas; así como se normaría y se trataría de dar la mayor seguridad informática posible a todos los clientes y/o usuarios.	bienestar de lo que se le otorga	para actuar en el mercado (libertad de acceso al mercado), también para establecer los propios objetivos de la empresa.					seria coparticipe de la libertad de empresas, permitiendo acceso por internet a cada uno de los servicios o productos ofertados por las empresas, disminuyendo delitos informáticos
Problema Específico 2	**Guía de entrevista P7 Quispe, Huacre y Mamani**	**Guía de entrevista P8 Pomacanchari, Valderrama y Araujo**	**Guía de entrevista P9 Medina, Gutierrez y Maquera**	**Categorías descubiertas**	**Categorías emergentes**	**Semejanzas**	**Diferencias**	**Conclusiones Aproximativas No definitivas**
Analizar de qué manera los derechos y privacidad apoyan en la libertad de la organización de empresa como garantía constitucional.	Considero que, si pude apoyar la privacidad de la información porque es necesario poder ejercer el derecho de la libertad de expresión,	El derecho a la privacidad de información tiene por objeto garantizar el derecho fundamental a la protección de los datos personales, a	El equilibrio entre los derechos y la privacidad de la información y la libertad de organización puede ser beneficioso al garantizar la	Libertad de expresión	Libertad de expresión	Libertad de expresión	Libertad de expresión	Señalan que si puede dar apoyo a la privacidad de la información debido a que es imprescindible ejercer el derecho de la libertad de expresión,

	evitando la violación de un derecho reconocido por ella.	través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen, en ese sentido las empresas en el caso de transferencias de datos personales dentro de grupos empresariales, sociedades subsidiarias afiliadas o vinculadas bajo el control común del mismo grupo del titular del banco de datos personales o	protección de los datos y la confianza en el mercado, pero también puede perjudicar si las regulaciones son excesivas y dificultan la operación de las empresas, limitan la recopilación de datos o no se equilibran adecuadamente con las necesidades de ciberseguridad. En resumen, se debe encontrar un equilibrio adecuado para proteger la información sin imponer cargas excesivas a las empresas					evitando de este modo violación de un derecho reconocido por esta, por lo que tal derecho a la privacidad de información trata de garantizar el derecho fundamental a la protección de datos personales, por medio de un idóneo tratamiento, dentro del respeto a los derechos que en ella se reconocen, tratando lograr de esta manera un acertado equilibrio entre derechos y

		responsable del tratamiento						privacidad de información

UNIVERSIDAD CÉSAR VALLEJO

Anexo 2: Instrumento de recolección de datos

GUIA DE ENTREVISTA

(ESPECIALISTAS)

Título: Fraude informático frente a la libertad de empresa como garantía constitucional, Lima 2023

Entrevistado/a:

Cargo/profesión/grado académico:

Objetivo general

Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional

Premisa: La Ley N.º 30096 que regula los delitos informáticos en el Perú, ayuda a proteger los datos comerciales y la propiedad intelectual de las empresas al penalizar el acceso no autorizado a sistemas informáticos y la divulgación no autorizada de información confidencial. Fraude informático es el delito que sanciona a toda persona que procura a través de las tecnologías de la información o de la comunicación, un beneficio o provecho ilícito para sí o para otro en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático.

Pregunta 1.- Desde su perspectiva, ¿cómo afecta el fraude informático al desarrollo de la libertad de empresa como garantía constitucional?

……

……

……

……

Pregunta 2.- En su máxima experiencia, ¿qué medidas y estrategias utilizan las empresas para prevenir y mitigar los efectos del avance tecnológico en el fraude informático para sí mismo?

……

……

……

……

……

Pregunta 3.- En ese escenario, ¿cómo la creación de un organismo supervisor de seguridad digital garantizaría la libertad de empresa en la prevención de los fraudes informáticos?

……

……

……

……

Objetivo específico 1

Analizar de qué manera la ciberseguridad garantiza la libertad de acceso de mercado como garantía constitucional.

Premisa: Ley N.º 28303 del Marco de Ciencia, Tecnología e Innovación Tecnológica hace referencia al base legal de la tecnología, ya que esta tiene la finalidad de diseñar el marco legal e institucional, sobre todo el de la administración de justicia. El artículo 59º de la Constitución reconoce el derecho a la libertad de empresa, garantizando a todas las personas una libertad de decisión no sólo para crear empresas, es para actuar en el mercado (libertad de acceso al mercado), también para establecer los propios objetivos de la empresa.

Pregunta 4.- En vista a la premisa acotada, bajo su propio concepto, ¿de qué manera mantener un marco legal en la tecnología aportaría a la libertad de acceso de mercado de la empresa?

……

……

……

……..

Pregunta 5.- Desde su perspectiva, ¿cómo se han desarrollado las políticas de ciberseguridad para promover o inhibir la entrada de nuevas empresas en el mercado?

……

……

……

……

Pregunta 6.- En Perú, ¿cómo se han adaptado las regulaciones internacionales sobre tecnología para equilibrar la libertad de acceso de mercado?

……

……

……

……..

Objetivo específico 2

Analizar de qué manera el derecho a la protección de datos contribuye a la libertad de la organización empresarial como garantía constitucional.

Premisa: Ley N.º 29733 de Protección de Datos Personales, con relación a los derechos y privacidad, la utilización de los datos personales y sensibles se maneja con sumo cuidado puesto que el gobierno peruano debe velar que no haya un perjuicio al usuario con fines públicos o privados. La libertad de organización de empresa establece un plan de seguridad de la información bajo normas técnicas, esta se establece en la Agenda Digital Peruana 2.0, donde establece la necesidad de contar estrategias de ciberseguridad para un accionar fluido en el mercado.

Pregunta 7.- En su opinión, ¿cómo pueden apoyar o perjudicar los derechos y privacidad de información en la libertad de la organización como garantía constitucional?

……

……

……

……

Pregunta 8.- ¿Qué consecuencias legales y reputacionales pueden enfrentar las empresas por la falta de medidas preventivas en las regulaciones sobre privacidad de información?

……

……

……

……

……

9.- Bajo un marco legal, ¿en qué medidas una libre organización de empresa garantizaría el uso de la información personal y sensible de los clientes y empleados?

……

……

……

……

_____

FIRMA Y SELO

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 2.1. Guía de entrevista

GUÍA DE ENTREVISTA

(ESPECIALISTA)

Título: Fraude informático frente a la libertad de empresa como garantía constitucional, Lima 2023

Entrevistado/a: Alan Roldan Araujo Chavez

Cargo/profesión/grado académico: Fiscal Adjunto al Provincial

Objetivo general

Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional

Premisa: La Ley N.° 30096 que regula los delitos informáticos en el Perú, ayuda a proteger los datos comerciales y la propiedad intelectual de las empresas al penalizar el acceso no autorizado a sistemas informáticos y la divulgación no autorizada de información confidencial. Fraude informático es el delito que sanciona a toda persona que procura a través de las tecnologías de la información o de la comunicación, un beneficio o provecho ilícito para sí o para otro en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático.

Pregunta 1.- Desde su perspectiva, ¿cómo afecta el fraude informático al desarrollo de la libertad de empresa como garantía constitucional?

Al igual como en todos los ámbitos de la vida, la comisión de los diferentes delitos miden negativamente en el goce de los derechos que tenemos y de igual

UNIVERSIDAD CÉSAR VALLEJO

manera el fraude informático puede negativamente en el derecho en lo referido al daño las empresas privadas a un alcance a sus datos o S. Informático que posea o tenga Propiedad de patrimonio

Pregunta 2.- En su máxima experiencia, ¿qué medidas y estrategias utilizan las empresas para prevenir y mitigar los efectos del avance tecnológico en el fraude informático para sí mismo?

Aplicación de técnicas de Ciberseguridad que permiten dotar de seguridad en la red, de la nube y sistema físico de los dispositivos que conforman la arquitectura de red de las empresas.

Pregunta 3.- En ese escenario, ¿cómo la creación de un organismo supervisor de seguridad digital garantizaría la libertad de empresa en la prevención de los fraudes informáticos?

En la actualidad existen diversos órganos que combaten este tipo de delitos. En ese sentido mediante D.L 1412 se aprobó la Ley de Gobierno Digital, con la cual se dota funciones relacionadas a seguridad digital a la Secretaría de Gobierno Digital.

Objetivo específico 1

Analizar de qué manera el impacto legal de la tecnología aporta en la libertad de acceso de mercado como garantía constitucional

Premisa: Ley N.° 28303 del Marco de Ciencia, Tecnología e Innovación Tecnológica hace referencia al impacto legal de la tecnología, ya que esta tiene la finalidad de diseñar el marco legal e institucional, sobre todo el de la administración de justicia. El artículo 59º de la Constitución reconoce el derecho a la libertad de empresa, garantizando a todas las personas una libertad de decisión no sólo para crear empresas, es para actuar en el mercado

(libertad de acceso al mercado), también para establecer los propios objetivos de la empresa.

Pregunta 4.- En vista a la premise acotada, bajo su propio concepto, ¿de qué manera mantener un marco legal en la tecnología aportaría a la libertad de acceso de mercado de la empresa?

Hace que sea más importante consolidar y actualizar un marco normativo relacionado a las tecnologías digitales, ya que las tecnologías en constante y presenta avances cada día. Lo cual trae consigo la creación de nuevos delitos, en ese contexto, tener un marco legal actualizado significa dar seguridad jurídica en relación a solucionar el derecho anteriormente

Pregunta 5.- Desde su perspectiva, ¿cómo se han desarrollado las políticas de ciberseguridad para promover o inhibir la entrada de nuevas empresas en el mercado?

Constante aparecen nuevas modalidades de ataques contra las empresas, se ha visto necesidad de implementar políticas de ciberseguridad de parte del Gobierno y de las particulares ya sea desde un ámbito preventivo o de uno de actuación ante

Pregunta 6.- En Perú, ¿cómo se han adaptado las regulaciones internacionales sobre tecnología para equilibrar la libertad de acceso de mercado?

Respecto a la normativa internacional en relación al tema comercial permite desarrollarse, sin embargo resulta muy conocido recientes decisiones respecto a la implementación de políticas de ciberseguridad en todas empresas a fin de dar confiabilidad a todos sus actores

UNIVERSIDAD CÉSAR VALLEJO

Objetivo específico 2

Analizar de qué manera los derechos y privacidad apoyan en la libertad de la organización de empresa como garantía constitucional.

Premisa: Ley N.º 29733 de Protección de Datos Personales, con relación a los derechos y privacidad, la utilización de los datos personales y sensibles se maneja con sumo cuidado puesto que el gobierno peruano debe velar que no haya un perjuicio al usuario con fines públicos o privados. La libertad de organización de empresa establece un plan de seguridad de la información bajo normas técnicas, esta se establece en la Agenda Digital Peruana 2.0, donde establece la necesidad de contar estrategias de ciberseguridad para un accionar fluido en el mercado.

Pregunta 7.- En su opinión, ¿cómo pueden apoyar o perjudicar los derechos y privacidad de información en la libertad de la organización como garantía constitucional?

Coadyuva el respeto de este derecho por parte de las empresas a la mayor confiabilidad de los particulares en los servicios que estos ofrecen.

Pregunta 8.- ¿Qué consecuencias legales y reputacionales pueden enfrentar las empresas por la falta de medidas preventivas en las regulaciones sobre privacidad de información?

Sanciones administrativas por los organos correspondientes, así como de ser el caso y bajo los alcances del principio de legalidad la comisión de delitos, debiendo tomarse en cuenta en dicho contexto además el principio de subsidiariedad.

UNIVERSIDAD CÉSAR VALLEJO

9.- Bajo un marco legal, ¿en qué medidas una libre organización de empresa garantizaría el uso de la información personal y sensible de los clientes y empleados?

Cumpliendo la normativa nacional aplicando y/o tomando en cuenta recomendaciones sobre ciberseguridad acorde a la vanguardia de protección de información que guarden en sus equipos, resaltando también su cumplimiento ideal de la criticidad en la presencia de un sistema de compliance.

FIRMA Y SELLO

Alan Roldan Araujo Chavez
Fiscal Adjunto al Provincial.
UFEC

UNIVERSIDAD CÉSAR VALLEJO

GUÍA DE ENTREVISTA

(ESPECIALISTA)

Lester Manahen Maquera Platero

Cargo: Fiscal adjunto provincial

Respuesta a pregunta 1:

Sin duda alguna el delito de fraude informático afecta al desarrollo de la libertad de empresa como garantía constitucional. Y lo hace, por un lado, respecto a la persona (natural o jurídica) titular del sistema informático afectado; así como, por otro lado, respecto a la persona (natural o jurídica) usuaria de dicho sistema informático. En relación a esta última, qué duda cabe, se ve afectada —por lo general— con el desvío de sus fondos hacia cuentas de terceros; lo que le genera pérdidas muchas veces irreparables y que incluso podrían perjudicar a dependientes de la afectada. Respecto a la primera de las nombras (persona titular del sistema informático), la afectación puede presentarse por tener que reintegrar el dinero desviado de sus usuarios; pero, sobre todo, creo yo, por la merma de su reputación como institución segura en las transacciones virtuales; lo que desincentiva a sus usuario el uso de, por ejemplo, tarjetas de crédito, tokens digitales, entre otros; lo que a su vez desacelera el consumo y la transformación digital en general y que, en buena cuenta, nos perjudica a todos también.

Respuesta a pregunta 2:

Las medidas y estrategias que utilizan las empresas para prevenir y mitigar los efectos del avance tecnológico en el fraude informático son diversos, pasando desde la implementación de mecanismos de ciberseguridad (ISO 27001, entre otros) y la contratación de personal altamente capacitado al respecto, hasta la coordinación con las instituciones estatales pertinentes para la prevención, detección y sanción de la ciberdelincuencia.

Respuesta a pregunta 3:

No estoy tan seguro que la creación de un organismo supervisor de seguridad digital garantizaría la libertad de empresa en la prevención de los fraudes informáticos; toda vez que —por lo menos en mi experiencia— la comisión del citado delito en la mayoría de casos se debe a negligencias previas incurridas por parte del usuario (siendo que, a consecuencia de dichas negligencias, los ciberdelincuentes se apoderan de la información sensible de sus víctimas y con las que posteriormente realizan el fraude informático). Esto es, de existir un organismo supervisor (por cierto, desconozco si ahora mismo existe), y debido a lo anotado anteriormente, no creo que la situación cambie mucho. Ahora, no es que no exista supervisión alguna a las empresas en lo que a seguridad digital se refiere, toda vez que si, por ejemplo, se advierte que en un caso concreto el sistema de prevención de fraude falló de tal manera que permitió que desviaran fondos de la cuenta bancaria de un cliente; INDECOPI ordena que dicho banco reintegre al usuario el monto desviado. Esto último considero es una forma de supervisión de la seguridad digital de las empresas, aunque no de modo directo, claro está.

Respuesta a pregunta 4:

Considero que es positiva la implementación de un marco legal que promueve el uso de la tecnología en diversos ámbitos y especialmente en la libertad de acceso de mercado de la empresa. En efecto, el uso de la tecnología permite muchas veces no solo reducir costos de personal, de materiales y de tiempo, sino también realizar un mejor producto o brindar un mejor servicio. De tal manera que las personas que quieran acceder al mercado puedan hacerlo de manera más fácil y brindando un producto o servicio competitivo.

Respuesta a pregunta 5:

Las empresas no solo por normativa deben implementar mecanismos de ciberseguridad, sino que están en la necesidad de hacerlo; caso contrario, estarían prácticamente condenas a dejar de existir tarde o temprano. Sea para promover o inhibir la entrada de nuevas empresas al mercado, por lo general, el gobierno responde tarde en la regulación; al contrario, son las mismas empresas quienes implementan mecanismos se seguridad, algunos mejores que otros, claro está; sea para ingresar, sea para permanecer en el mercado.

Respuesta a pregunta 6:

No tengo mucho conocimiento sobre el tema comercial, en realidad; pero, como señalé antes, la implementación de mecanismos de ciberseguridad (a saber, ISO 27001, ISO 27032 o, mejor aún, NIST SP 800-53) constituyen estándares internacionales que le otorgan mayor confiabilidad y, por tanto, competitividad a las empresas para con sus clientes. Siendo que dichos mecanismos de seguridad son, pues, en su gran mayoría implementados por las grandes empresas en el país.

Respuesta a pregunta 7:

Considero que la privacidad de los datos personales de los usuarios en nada perjudica a la libertad de la organización de empresa. Por el contrario, el respeto al derecho inicialmente citado generaría una confianza de los usuarios que más adelante podrían generar mayores ingresos a la empresa.

Respuesta a pregunta 8:

Por supuesto que son varias las consecuencias legales y reputacionales que pueden enfrentar las empresas por falta de medidas preventivas en las regulaciones sobre privacidad de la información. Lo había señalado anteriormente, si una empresa incumple la correspondiente normativa, las sanciones podrían ir desde una simple multa hasta la disolución de la empresa (sin mencionar, eventualmente, las implicancias jurídico-penales para con sus representantes, si fuera el caso). Por otro lado (y tal vez de mayor trascendencia para con los intereses económicos de la empresa), en el aspecto reputacional, los clientes al advertir que una determina empresa no cumplen con las regulaciones debidas, pues, sencillamente elegirá a una empresa que sí las cumpla.

Respuesta a pregunta 9:

Cumpliendo con los estándares internacionales sobre ciberseguridad y demás normativa correspondiente; estando siempre a la vanguardia al respecto.

UNIVERSIDAD CÉSAR VALLEJO

GUÍA DE ENTREVISTA

(ESPECIALISTA)

Título: Fraude informático frente a la libertad de empresa como garantía constitucional, Lima 2023

Entrevistado/a: Juan Pablo QUISPE QUISPE**.**

Cargo/profesión/grado académico: EFECTIVO POLICIAL DE INVESTIGACIÓN EN LA DIVISION DE INVESTIGACION DE DELITOS DE ALTA TECNOLOGIA – DIRINCRI PNP.

Objetivo general

Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional

Premisa: La Ley N.º 30096 que regula los delitos informáticos en el Perú, ayuda a proteger los datos comerciales y la propiedad intelectual de las empresas al penalizar el acceso no autorizado a sistemas informáticos y la divulgación no autorizada de información confidencial. Fraude informático es el delito que sanciona a toda persona que procura a través de las tecnologías de la información o de la comunicación, un beneficio o provecho ilícito para sí o para otro en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático.

Pregunta 1.- Desde su perspectiva, ¿cómo afecta el fraude informático al desarrollo de la libertad de empresa como garantía constitucional?

Considero que el fraude informático afecta de manera directa, ya que cualquier persona puede ser víctimas de este tipo de delitos y en especial las personas jurídicas porque las empresas generalmente mueven mucho dinero para efectuar las actividades propias y para esto utilizan diversas plataformas digitales lo cual los convierte en principales blancos de los ciberdelincuentes,

al ser una empresa víctima del fraude informático afecta directamente la economía financiera de la empresa, ya sea por perdida de clientes y robo de información de su base de datos, cualquier caso sea, la empresa estaría reduciendo sus actividad empresariales y crecimiento de su bolsa de valores poniéndolo en una posición desventajosa ante otra empresa.

Pregunta 2.- En su máxima experiencia, ¿qué medidas y estrategias utilizan las empresas para prevenir y mitigar los efectos del avance tecnológico en el fraude informático para sí mismo?

En mi experiencia, pude apreciar que la mayoría de empresas aun no cuentan con medidas de protección de calidad ni a la misma altura de los avances tecnológicos, debo indicar que deben poner en ejecución medidas de ciberseguridad, capacitaciones a su personal para que puedan tener claro las diferentes modalidades que existe de fraude informático y así poder evitarlas o en todo caso contratar un equipo de profesionales para que pueda detectar las vulnerabilidades de sus sistema informático y en base a eso ejecutar mejoras; así como tener mucho cuidado con sus claves secretas y claves token, claves digitales entre otras ya que con estas pueden ejecutar las operaciones bancarias fraudulentas.

Pregunta 3.- En ese escenario, ¿cómo la creación de un organismo supervisor de seguridad digital garantizaría la libertad de empresa en la prevención de los fraudes informáticos?

Considero que un organismo supervisor de seguridad digital no podría garantizar que la empresa sea víctima de los fraudes informáticos, porque este tipo de delitos no tiene fronteras vale decir que se puede cometer desde cualquier parte del mundo y si se crea un organismo sería algo interno y considero que no solucionaría el problema.

Objetivo específico 1

Analizar de qué manera la ciberseguridad garantiza la libertad de acceso de mercado como garantía constitucional

Premisa: Ley N.º 28303 del Marco de Ciencia, Tecnología e Innovación Tecnológica hace referencia al base legal de la tecnología, ya que esta tiene la finalidad de diseñar el marco legal e institucional, sobre todo el de la administración de justicia. El artículo 59º de la Constitución reconoce el derecho a la libertad de empresa, garantizando a todas las personas una libertad de decisión no sólo para crear empresas, es para actuar en el mercado (libertad de acceso al mercado), también para establecer los propios objetivos de la empresa.

Pregunta 4.- En vista a la premisa acotada, bajo su propio concepto, ¿de qué manera mantener un marco legal en la tecnología aportaría a la libertad de acceso de mercado de la empresa?

Considero que tener un marco legal en tecnología ayudaría mucho a la libertad de empresas porque permitiría tener acceso a mediante internet a todos los servicios o productos que ofrecen las empresas; así como se normaría y se trataría de dar la mayor seguridad informática posible a todos los clientes y/o usuarios.

Pregunta 5.- Desde su perspectiva, ¿cómo se han desarrollado las políticas de ciberseguridad para promover o inhibir la entrada de nuevas empresas en el mercado?

Considero que aún no se ha desarrollado correctamente las políticas de ciberseguridad porque en los últimos tiempos y por los diferentes problemas que enfrenta el país priva la entrada de nuevas empresas; es decir, aún falta incrementar con eficiencia estas políticas de seguridad.

Pregunta 6.- En Perú, ¿cómo se han adaptado las regulaciones internacionales sobre tecnología para equilibrar la libertad de acceso de mercado?

La difícil realidad económica del Perú es una consecuencia de una falta de productos y servicios competitivos en el mercado globalizado; por falta de conocimientos científicos y tecnológicos; debido a que no se promueve la investigación con presupuestos adecuados.

UNIVERSIDAD CÉSAR VALLEJO

Objetivo específico 2

Analizar de qué manera el derecho a la protección de datos contribuye a la libertad de la organización empresarial como garantía constitucional.

Premisa: Ley N.º 29733 de Protección de Datos Personales, con relación a los derechos y privacidad, la utilización de los datos personales y sensibles se maneja con sumo cuidado puesto que el gobierno peruano debe velar que no haya un perjuicio al usuario con fines públicos o privados. La libertad de organización de empresa establece un plan de seguridad de la información bajo normas técnicas, esta se establece en la Agenda Digital Peruana 2.0, donde establece la necesidad de contar estrategias de ciberseguridad para un accionar fluido en el mercado.

Pregunta 7.- En su opinión, ¿cómo pueden apoyar o perjudicar los derechos y privacidad de información en la libertad de la organización como garantía constitucional?

Considero que, si pude apoyar la privacidad de la información porque es necesario poder ejercer el derecho de la libertad de expresión, evitando la violación de un derecho reconocido por ella.

Pregunta 8.- ¿Qué consecuencias legales y reputacionales pueden enfrentar las empresas por la falta de medidas preventivas en las regulaciones sobre privacidad de información?

Las consecuencias que podrían enfrenar las empresas serias que su data sea expuesta, que sea víctima de los ciberdelincuentes, que su acceso a sus datos sea más restringido, que la información que comparten con sus clientes se encuentre cifrado, que implemente una política de confidencialidad y retención de datos, entre otros.

9.- Bajo un marco legal, ¿en qué medidas una libre organización de empresa garantizaría el uso de la información personal y sensible de los clientes y empleados?

Se puede garantizar mediante copias de seguridad o respaldos, utilizando antivirus en el sistema informático, controlando el acceso a la información que comparte con sus usuarios, fomentando una cultura de contraseñas seguras entre otras.

GUÍA DE ENTREVISTA

(ESPECIALISTA)

Título: Fraude informático frente a la libertad de empresa como garantía constitucional, Lima 2023

Entrevistado/a: POMACANCHARI TORRE JORGE.

Cargo/profesión/grado académico: Mg. EN DERECHO PENAL, MENCIÓN EN CIENCIAS PENALES; FISCAL ADJUNTO PROVINCIAL.

Objetivo general

Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional

Premisa: La Ley N.º 30096 que regula los delitos informáticos en el Perú, ayuda a proteger los datos comerciales y la propiedad intelectual de las empresas al penalizar el acceso no autorizado a sistemas informáticos y la divulgación no

autorizada de información confidencial. Fraude informático es el delito que sanciona a toda persona que procura a través de las tecnologías de la información o de la comunicación, un beneficio o provecho ilícito para sí o para otro en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático.

Pregunta 1.- Desde su perspectiva, ¿cómo afecta el fraude informático al desarrollo de la libertad de empresa como garantía constitucional?

Considero que, el fraude informático al ser una de las modalidades de delitos informáticos al tratarse de una nueva norma o ley no se encuentra debidamente implementada con la tecnología y logística correspondiente, la ley 30096 no tiene reglamentación especializada en delitos informáticos, en donde se tipifiqué en forma escrita los procesos, procedimientos y pautas para combatir los ciberdelitos y no evoluciona, ni cambia constante como las nuevas modalidades de ciberdelitos que aparecen constantemente en la actualidad, toda vez que el ministerio público en gran parte de supervisiones no se encuentra capacitado o especializados en ese tipo de delitos teniendo en cuenta que conforme a la doctrina nacional recién se puede apreciar la especialización del derecho en el sector justicia, por lo cual las empresas no constan de un marco legal de protección.

Pregunta 2.- En su máxima experiencia, ¿qué medidas y estrategias utilizan las empresas para prevenir y mitigar los efectos del avance tecnológico en el fraude informático para sí mismo?

Considero que las empresas tienen reglamentos internos que deben cumplir para salvaguardar el bienestar de la empresa, más no medidas ni estrategias para efectos de protección, los efectos del avance tecnológico son positivos como herramientas mas activas para el bienestar económico de cualquier actividad comercial, a su vez traes consigo actos ilícitos que son cometidos detrás de una pantalla tecnológica, la cual tendría que ser contrarrestado con un mismo mecanismo de tecnología creado por expertos en la materia para

salvaguardar una infraestructura compuesta por bases de datos concernientes.

Pregunta 3.- En ese escenario, ¿cómo la creación de un organismo supervisor de seguridad digital garantizaría la libertad de empresa en la prevención de los fraudes informáticos?

Es muy importante, primero implementar y sensibilizar la ley 30096 frente a la sociedad y que con ello un organismo supervisor seria de total importancia, por cuanto al tener un órgano supervisor tendremos un control del uso de la cibernética como una herramienta muy importante para el desarrollo de la libertad de empresa, como también la existencia de un seguro cibernético ayudaría a disminuir las cifras de delitos informáticos.

Objetivo específico 1

Analizar de qué manera la ciberseguridad garantiza la libertad de acceso de mercado como garantía constitucional

Premisa: Ley N.º 28303 del Marco de Ciencia, Tecnología e Innovación Tecnológica hace referencia al base legal de la tecnología, ya que esta tiene la finalidad de diseñar el marco legal e institucional, sobre todo el de la administración de justicia. El artículo 59º de la Constitución reconoce el derecho a la libertad de empresa, garantizando a todas las personas una libertad de decisión no sólo para crear empresas, es para actuar en el mercado (libertad de acceso al mercado), también para establecer los propios objetivos de la empresa.

Pregunta 4.- En vista a la premisa acotada, bajo su propio concepto, ¿de qué manera mantener un marco legal en la tecnología aportaría a la libertad de acceso de mercado de la empresa?

Considero que al existir un marco legar que ampare y proteja la seguridad informática, mediante legisladores capacitados y expertos en la materia de tecnología y el ciberespacio, ayudaría a disminuir los delitos informáticos por

las cuales son víctimas las empresas y usuarios, al ejecutar medidas de protección las cuales tendrían que ser implementadas en cada empresa obligatoriamente, se estaría protegiendo a las empresas y usuarias de ser víctimas de fraude informático entre otras modalidades.

Pregunta 5.- Desde su perspectiva, ¿cómo se han desarrollado las políticas de ciberseguridad para promover o inhibir la entrada de nuevas empresas en el mercado?

Considero que la política de ciberseguridad es diversa las cuales se deben incluir necesariamente a agentes estatales, económicos y sociales, esclarecer cómo se ponderan los distintos objetivos entre sí e identificar claramente el papel que cumple el Estado en sus diversas funciones. El Perú cuenta con políticas de ciberseguridad, pero estas no son ejecutadas, no existe un adecuado seguimiento a ello.

Pregunta 6.- En Perú, ¿cómo se han adaptado las regulaciones internacionales sobre tecnología para equilibrar la libertad de acceso de mercado?

El Perú logro tener un acceso valioso como es el convenio de Budapest, el cual contiene un marco legal internacional para salvaguardar la seguridad informática, pero lamentablemente esta no está siendo explotada por los letrados para el uso de nuestra legislación peruana.

Objetivo específico 2

Analizar de qué manera el derecho a la protección de datos contribuye a la libertad de la organización empresarial como garantía constitucional

Premisa: Ley N.º 29733 de Protección de Datos Personales, con relación a los derechos y privacidad, la utilización de los datos personales y sensibles se maneja con sumo cuidado puesto que el gobierno peruano debe velar que no haya un perjuicio al usuario con fines públicos o privados. La libertad de organización de empresa establece un plan de seguridad de la información bajo normas técnicas,

esta se establece en la Agenda Digital Peruana 2.0, donde establece la necesidad de contar estrategias de ciberseguridad para un accionar fluido en el mercado.

Pregunta 7.- En su opinión, ¿cómo pueden apoyar o perjudicar los derechos y privacidad de información en la libertad de la organización como garantía constitucional?

El derecho a la privacidad de información tiene por objeto garantizar el derecho fundamental a la protección de los datos personales, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen, en ese sentido las empresas en el caso de transferencias de datos personales dentro de grupos empresariales, sociedades subsidiarias afiliadas o vinculadas bajo el control común del mismo grupo del titular del banco de datos personales o responsable del tratamiento, o a aquellas afiliadas o vinculadas a una sociedad matriz o a cualquier sociedad del mismo grupo del titular del banco de datos o responsable del tratamiento, se cumple con garantizar el tratamiento de datos personales, si se cuenta con un código de conducta que establezca las normas internas de protección de datos personales.

Pregunta 8.- ¿Qué consecuencias legales y reputacionales pueden enfrentar las empresas por la falta de medidas preventivas en las regulaciones sobre privacidad de información?

Las empresas víctimas de delitos informáticos se enfrentan al robo de datos informáticos y datos personales, accesos no autorizados a sistemas informáticos, daños informáticos en sistemas y las pérdidas económicas que producen en la víctima, entre otros.

9.- Bajo un marco legal, ¿en qué medidas una libre organización de empresa garantizaría el uso de la información personal y sensible de los clientes y empleados?

La Constitución Política del Perú ampara la libre organización de las empresas, con el fin de lograr para sí mismo una posición en el mercado laboral y ganancias económicas, pero ello también implica cumplir con parámetros establecidos por los legisladores, como es el proteger y

salvaguardad la información personal y cesible que puedan llegar a obtener dependiendo en el área que se desempeñan, existiendo la ley de protección de datos personales, las empresas deben operar en entorna a esta ley.

GUÍA DE ENTREVISTA

(ESPECIALISTA)

Título: Fraude informático frente a la libertad de empresa como garantía constitucional, Lima 2023

Entrevistado/a: MEDINA ARCE ANTONY KEVIN

Cargo/profesión/grado académico: INGENIERO DE SISTEMAS Y BACHILLER EN DERECHO, RESPONSABLE DE LA UNIDAD DE ESTADÍSTICAS E INFORMÁTICA DE LA DIRECCIÓN DE SALUD VIRGEN DE COCHARCAS – CHINCHEROS.

Objetivo general

Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional

Premisa: La Ley N.º 30096 que regula los delitos informáticos en el Perú, ayuda a proteger los datos comerciales y la propiedad intelectual de las empresas al penalizar el acceso no autorizado a sistemas informáticos y la divulgación no autorizada de información confidencial. Fraude informático es el delito que sanciona

a toda persona que procura a través de las tecnologías de la información o de la comunicación, un beneficio o provecho ilícito para sí o para otro en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático.

Pregunta 1.- Desde su perspectiva, ¿cómo afecta el fraude informático al desarrollo de la libertad de empresa como garantía constitucional?

El fraude informático afecta a la libertad de empresa al comprometer la propiedad intelectual y secretos comerciales, causar pérdidas financieras, dañar la reputación, requerir costos de mitigación, y frenar la innovación en el entorno empresarial. Esto socava la confianza y obstaculiza la capacidad de las empresas para competir en la era digital. La protección de datos comerciales y propiedad intelectual es esencial para garantizar la libertad de empresa como garantía constitucional.

Pregunta 2.- En su máxima experiencia, ¿qué medidas y estrategias utilizan las empresas para prevenir y mitigar los efectos del avance tecnológico en el fraude informático para sí mismo?

Las empresas utilizan una variedad de medidas y estrategias para prevenir y mitigar el fraude informático, incluyendo políticas de seguridad, formación de empleados, protección de datos, firewalls, actualizaciones, monitoreo, gestión de acceso, respuesta a incidentes, evaluación de proveedores, seguridad en la nube, auditorías de seguridad y más. La seguridad cibernética se ha vuelto esencial en el entorno empresarial moderno.

Pregunta 3.- En ese escenario, ¿cómo la creación de un organismo supervisor de seguridad digital garantizaría la libertad de empresa en la prevención de los fraudes informáticos?

La creación de un organismo supervisor de seguridad digital garantizaría la libertad de empresa en la prevención de fraudes informáticos al establecer estándares, proporcionar orientación, fomentar la colaboración, supervisar el cumplimiento, impulsar la investigación, coordinar respuestas a incidentes y promover la confianza en un entorno empresarial más seguro y regulado en términos de seguridad cibernética.

Objetivo específico 1

Analizar de qué manera la ciberseguridad garantiza la libertad de acceso de mercado como garantía constitucional

Premisa: Ley N.º 28303 del Marco de Ciencia, Tecnología e Innovación Tecnológica hace referencia al base legal de la tecnología, ya que esta tiene la finalidad de diseñar el marco legal e institucional, sobre todo el de la administración de justicia. El artículo 59º de la Constitución reconoce el derecho a la libertad de empresa, garantizando a todas las personas una libertad de decisión no sólo para crear empresas, es para actuar en el mercado (libertad de acceso al mercado), también para establecer los propios objetivos de la empresa.

Pregunta 4.- En vista a la premisa acotada, bajo su propio concepto, ¿de qué manera mantener un marco legal en la tecnología aportaría a la libertad de acceso de mercado de la empresa?

Un marco legal sólido en tecnología contribuye a la libertad de acceso al mercado de la empresa al fomentar la innovación, proteger la propiedad intelectual, asegurar una competencia justa, abordar preocupaciones de seguridad y privacidad, promover el cumplimiento de estándares globales y facilitar la resolución de disputas. Esto crea un ambiente favorable para que las empresas ingresen y operen en mercados competitivos y tecnológicamente avanzados.

Pregunta 5.- Desde su perspectiva, ¿cómo se han desarrollado las políticas de ciberseguridad para promover o inhibir la entrada de nuevas empresas en el mercado?

Las políticas de ciberseguridad pueden tanto promover como inhibir la entrada de nuevas empresas en el mercado. Para promover, las políticas de ciberseguridad ofrecen un entorno seguro y confiable que fomenta la inversión en tecnología y la innovación. Sin embargo, políticas excesivamente restrictivas o costosas pueden actuar como barreras de entrada y desincentivar a nuevas empresas debido a los

altos costos de cumplimiento. Por lo tanto, el impacto de las políticas de ciberseguridad en la entrada de nuevas empresas en el mercado depende de su equilibrio entre la protección y la facilitación de la innovación.

Pregunta 6.- En Perú, ¿cómo se han adaptado las regulaciones internacionales sobre tecnología para equilibrar la libertad de acceso de mercado?

Perú ha adaptado las regulaciones internacionales sobre tecnología para equilibrar la libertad de acceso al mercado a través de la armonización normativa, la participación en tratados internacionales, la promoción de la innovación, la creación de agencias reguladoras especializadas y el fomento de la inversión extranjera en el sector tecnológico. Estas medidas buscan promover un ambiente empresarial más competitivo y facilitar el acceso al mercado para las empresas tecnológicas.

Objetivo específico 2

Analizar de qué manera el derecho a la protección de datos contribuye a la libertad de la organización empresarial como garantía constitucional

Premisa: Ley N.º 29733 de Protección de Datos Personales, con relación a los derechos y privacidad, la utilización de los datos personales y sensibles se maneja con sumo cuidado puesto que el gobierno peruano debe velar que no haya un perjuicio al usuario con fines públicos o privados. La libertad de organización de empresa establece un plan de seguridad de la información bajo normas técnicas, esta se establece en la Agenda Digital Peruana 2.0, donde establece la necesidad de contar estrategias de ciberseguridad para un accionar fluido en el mercado.

Pregunta 7.- En su opinión, ¿cómo pueden apoyar o perjudicar los derechos y privacidad de información en la libertad de la organización como garantía constitucional?

El equilibrio entre los derechos y la privacidad de la información y la libertad de organización puede ser beneficioso al garantizar la protección de los datos y la confianza en el mercado, pero también puede perjudicar si las regulaciones son

excesivas y dificultan la operación de las empresas, limitan la recopilación de datos o no se equilibran adecuadamente con las necesidades de ciberseguridad. En resumen, se debe encontrar un equilibrio adecuado para proteger la información sin imponer cargas excesivas a las empresas.

Pregunta 8.- ¿Qué consecuencias legales y reputacionales pueden enfrentar las empresas por la falta de medidas preventivas en las regulaciones sobre privacidad de información?

La falta de medidas preventivas en las regulaciones sobre privacidad de información puede llevar a consecuencias legales, como sanciones y demandas, y a graves repercusiones en la reputación de la empresa, incluyendo la pérdida de confianza de clientes, pérdida de negocios y daños financieros. Es fundamental que las empresas implementen medidas sólidas de privacidad de datos para evitar estas consecuencias.

9.- Bajo un marco legal, ¿en qué medidas una libre organización de empresa garantizaría el uso de la información personal y sensible de los clientes y empleados?

Bajo un marco legal, una libre organización de empresa garantiza el uso adecuado de la información personal y sensible de clientes y empleados mediante medidas que incluyen el consentimiento informado, la limitación de la recopilación, la seguridad de datos, la transparencia, el respeto de los derechos individuales, notificaciones de brechas de seguridad, auditorías de cumplimiento, capacitación del personal, evaluación de riesgos, la designación de un responsable de protección de datos y el cumplimiento normativo. Estas medidas aseguran el cumplimiento de las regulaciones de privacidad y la protección de los datos personales y sensibles.

UNIVERSIDAD CÉSAR VALLEJO

GUÍA DE ENTREVISTA

(ESPECIALISTA)

Título: Fraude informático frente a la libertad de empresa como garantía constitucional, Lima 2023

Entrevistado/a: MIGUEL HUACRE MÉNDEZ

Cargo/profesión/grado académico: ABOGADO PENALISTA, ALCALDE DE LA MUNICIPALIDAD PROVINCIAL – APURÍMAC

Objetivo general

Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional

Premisa: La Ley N.º 30096 que regula los delitos informáticos en el Perú, ayuda a proteger los datos comerciales y la propiedad intelectual de las empresas al penalizar el acceso no autorizado a sistemas informáticos y la divulgación no autorizada de información confidencial. Fraude informático es el delito que sanciona a toda persona que procura a través de las tecnologías de la información o de la comunicación, un beneficio o provecho ilícito para sí o para otro en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático.

Pregunta 1.- Desde su perspectiva, ¿cómo afecta el fraude informático al desarrollo de la libertad de empresa como garantía constitucional?

El fraude informático es el delito que comete el que manipula un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o lo hace a través de cualquier interferencia en el funcionamiento de un sistema informático, siendo una empresa víctima del este ilícito puede verse interrumpida el área administrativo de operaciones, ocasionando retrasos en su plan de cada año, afectado también a sus

usuarios o consumidore, los cuales pueden tomar medidas legales, causándoles una mala reputación y pérdidas económicas considerables.

Pregunta 2.- En su máxima experiencia, ¿qué medidas y estrategias utilizan las empresas para prevenir y mitigar los efectos del avance tecnológico en el fraude informático para sí mismo?

Teniendo en cuenta los grandes riesgos que implican la manipulación de las bases de datos de empresas, instituciones y organizaciones, cada una de ellas está en la obligación de establecer mecanismos de resguardo y protección de cada una de las piezas de información.

Pregunta 3.- En ese escenario, ¿cómo la creación de un organismo supervisor de seguridad digital garantizaría la libertad de empresa en la prevención de los fraudes informáticos?

la creación de un organismo o unidad especializada que supervise y fiscalice el cumplimiento de las normas y políticas de seguridad de la información, este organismo puede cumplir las siguientes funciones: estableces normas y políticas de seguridad de la información, supervisar el cumplimiento de las normas y proporcionar educación y formación.

Objetivo específico 1

Analizar de qué manera la ciberseguridad garantiza la libertad de acceso de mercado como garantía constitucional

Premisa: Ley N.º 28303 del Marco de Ciencia, Tecnología e Innovación Tecnológica hace referencia al base legal de la tecnología, ya que esta tiene la finalidad de diseñar el marco legal e institucional, sobre todo el de la administración de justicia. El artículo 59º de la Constitución reconoce el derecho a la libertad de empresa, garantizando a todas las personas una libertad de decisión no sólo para crear empresas, es para actuar en el mercado (libertad de acceso al mercado), también para establecer los propios objetivos de la empresa.

Pregunta 4.- En vista a la premisa acotada, bajo su propio concepto, ¿de qué manera mantener un marco legal en la tecnología aportaría a la libertad de acceso de mercado de la empresa?

Considero que tener un marco legal en tecnología ayudaría mucho a la libertad de empresas porque permitiría tener acceso a mediante internet a todos los servicios o productos que ofrecen las empresas; así como se normaría y se trataría de dar la mayor seguridad informática posible a todos los clientes y/o usuarios.

Pregunta 5.- Desde su perspectiva, ¿cómo se han desarrollado las políticas de ciberseguridad para promover o inhibir la entrada de nuevas empresas en el mercado?

Las instituciones encargadas de prevenir los delitos informáticos a menudo promueven capacitaciones transversales especialidad y por niveles (básico y avanzado) para fiscales, peritos de especialidad. Además, también se realizan esfuerzos para sensibilizar al público en general, para prevenir el ciberdelito.

Pregunta 6.- En Perú, ¿cómo se han adaptado las regulaciones internacionales sobre tecnología para equilibrar la libertad de acceso de mercado?

Los avances tecnológicos que puedan manejar las empresas para proteger su información pueden significar una ventaja competitiva muy importante ante otras empresas. No es común que la información generada, un estudio de mercado o el desarrollo de un nuevo producto o servicio se publique antes de que se haya masificado entre los clientes, salvo que se vulnere la seguridad de la compañía.

Objetivo específico 2

Analizar de qué manera el derecho a la protección de datos contribuye a la libertad de la organización empresarial como garantía constitucional

Premisa: Ley N.º 29733 de Protección de Datos Personales, con relación a los derechos y privacidad, la utilización de los datos personales y sensibles se maneja

con sumo cuidado puesto que el gobierno peruano debe velar que no haya un perjuicio al usuario con fines públicos o privados. La libertad de organización de empresa establece un plan de seguridad de la información bajo normas técnicas, esta se establece en la Agenda Digital Peruana 2.0, donde establece la necesidad de contar estrategias de ciberseguridad para un accionar fluido en el mercado.

Pregunta 7.- En su opinión, ¿cómo pueden apoyar o perjudicar los derechos y privacidad de información en la libertad de la organización como garantía constitucional?

No existe perjuicio de por medio a la libertad de organización, cuando una empresa adquiere información privada de un cliente, esta adquiere la responsabilidad de darle un buen procedente a tal información, la cual estará obligada salvaguardar toda información que se le sea brindada.

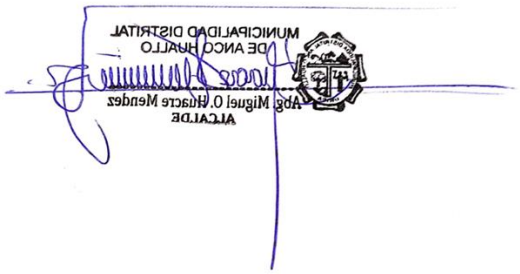
Pregunta 8.- ¿Qué consecuencias legales y reputacionales pueden enfrentar las empresas por la falta de medidas preventivas en las regulaciones sobre privacidad de información?

Las consecuencias legales son las siguientes: las empresas pueden ser demandas por clientes, socios comerciales y otras partes afectadas por el delito informático, los que puede resultar en multas y daños económicos, además de enfrentar sanciones regulatorias por incumplir las leyes de protección de datos

9.- Bajo un marco legal, ¿en qué medidas una libre organización de empresa garantizaría el uso de la información personal y sensible de los clientes y empleados?

1.- Marco legal claro: es crucial que exista un marco legal claro y actualizado que defina los delitos informáticos, que establezcan las penas correspondientes.

2.- Cooperación internacional: dado que los delitos informáticos transcienden las fronteras nacionales, la cooperación internación es esencial para prevenir los delitos.



UNIVERSIDAD CÉSAR VALLEJO

GUÍA DE ENTREVISTA

(ESPECIALISTA)

Título: Fraude informático frente a la libertad de empresa como garantía constitucional, Lima 2023

Entrevistado/a: MARÍN VALDERRAMA JUAN DAVID

Cargo/profesión/grado académico: ABOGADO PENALISTA, ASISTENTE EN FUNCIÓN FISCAL - MINISTERIO PÚBLICO

Objetivo general

Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional

Premisa: La Ley N.º 30096 que regula los delitos informáticos en el Perú, ayuda a proteger los datos comerciales y la propiedad intelectual de las empresas al penalizar el acceso no autorizado a sistemas informáticos y la divulgación no autorizada de información confidencial. Fraude informático es el delito que sanciona a toda persona que procura a través de las tecnologías de la información o de la comunicación, un beneficio o provecho ilícito para sí o para otro en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático.

Pregunta 1.- Desde su perspectiva, ¿cómo afecta el fraude informático al desarrollo de la libertad de empresa como garantía constitucional?

La libertad de empresa es una garantía constitucional, la cual está amparado en la Constitución Política del Perú, al ser ella una víctima del fraude informático vulnerando la estabilidad de redes de internet que estar información confidencial del cliente, la cual le puede traer consecuencias legales y pérdidas económicas

Pregunta 2.- En su máxima experiencia, ¿qué medidas y estrategias utilizan las empresas para prevenir y mitigar los efectos del avance tecnológico en el fraude informático para sí mismo?

Las estrategias implementadas por algunas empresas, son los antivirus, herramienta ineficiente para usarlo como protección ante una base de datos grande y confidencial, una herramienta segura deber ser acorde a los avances tecnológicos y especialidades para cada según se necesidad sea

Pregunta 3.- En ese escenario, ¿cómo la creación de un organismo supervisor de seguridad digital garantizaría la libertad de empresa en la prevención de los fraudes informáticos?

La creación de un organismo en mención, con la gestación de un instituto especializado para formar a investigadores y peritos especializados en delitos informáticos y enfrenten a este flagelo delictivo. Asimismo, se debe reformar los organismos autónomos con el Ministerio Público y el Poder Judicial, de tal suerte que la administración de justicia sea respetando todos los cánones jurídico- normativos y legales, desterrando la corrupción que debilita estas entidades tutelares de la justicia

Objetivo específico 1

Analizar de qué manera la ciberseguridad garantiza la libertad de acceso de mercado como garantía constitucional

Premisa: Ley N.º 28303 del Marco de Ciencia, Tecnología e Innovación Tecnológica hace referencia al base legal de la tecnología, ya que esta tiene la finalidad de diseñar el marco legal e institucional, sobre todo el de la administración de justicia. El artículo 59º de la Constitución reconoce el derecho a la libertad de empresa, garantizando a todas las personas una libertad de decisión no sólo para crear empresas, es para actuar en el mercado (libertad de acceso al mercado), también para establecer los propios objetivos de la empresa.

Pregunta 4.- En vista a la premisa acotada, bajo su propio concepto, ¿de qué manera mantener un marco legal en la tecnología aportaría a la libertad de acceso de mercado de la empresa?

La libertad de acceso al mercado de la empresa se encuentra normada, la que también implica la adquisición de deberes y protección a su usuario, quien tiene la obligación de velar por el bienestar de lo que se le otorga.

Pregunta 5.- Desde su perspectiva, ¿cómo se han desarrollado las políticas de ciberseguridad para promover o inhibir la entrada de nuevas empresas en el mercado?

La estrategia Nacional de Ciberseguridad Española en el contexto de la Estrategia de Seguridad Nacional es el resultado de un importante esfuerzo de nuestra Administración para enfrentar con la mayor seguridad, confianza y con las mejores garantías posibles los retos que tenemos como país, en un contexto internacional claramente dominado por el uso masivo y exponencialmente creciente de la tecnología.

Pregunta 6.- En Perú, ¿cómo se han adaptado las regulaciones internacionales sobre tecnología para equilibrar la libertad de acceso de mercado?

La regulación internacional sobre la tecnología va en avance y actualización constante de acorde con la actualidad, las cuales tienen como medida de protección la implementación de las normas ISO.

Objetivo específico 2

Analizar de qué manera el derecho a la protección de datos contribuye a la libertad de la organización empresarial como garantía constitucional

Premisa: Ley N.º 29733 de Protección de Datos Personales, con relación a los derechos y privacidad, la utilización de los datos personales y sensibles se maneja con sumo cuidado puesto que el gobierno peruano debe velar que no haya un

perjuicio al usuario con fines públicos o privados. La libertad de organización de empresa establece un plan de seguridad de la información bajo normas técnicas, esta se establece en la Agenda Digital Peruana 2.0, donde establece la necesidad de contar estrategias de ciberseguridad para un accionar fluido en el mercado.

Pregunta 7.- En su opinión, ¿cómo pueden apoyar o perjudicar los derechos y privacidad de información en la libertad de la organización como garantía constitucional?

Las empresas están en la obligación cumplir bajo el marco legal de adquirir la protección adecuada, no solo los beneficiando a los usuarios, sino también para sí misma, para disminuir las quiebras de las empresas

Pregunta 8.- ¿Qué consecuencias legales y reputacionales pueden enfrentar las empresas por la falta de medidas preventivas en las regulaciones sobre privacidad de información?

Las consecuencias se estiman en las pérdidas económicas a consecuencia de los ciberataques, crisis de seguridad en posición de sanciones, daño de reputación y esta finalmente conlleva a la pérdida de clientes.

9.- Bajo un marco legal, ¿en qué medidas una libre organización de empresa garantizaría el uso de la información personal y sensible de los clientes y empleados?

Este seria bajo en cumplimiento de las no mamas en mención para una adecuada protección que sea de conocimiento del estado y así conservar a los trabajadores que quieren ponerse de acuerdo

UNIVERSIDAD CÉSAR VALLEJO

GUÍA DE ENTREVISTA

(ESPECIALISTA)

Título: Fraude informático frente a la libertad de empresa como garantía constitucional, Lima 2023

Entrevistado/a: YANIRA TERESA GUTIÉRREZ PALOMINO

Cargo/profesión/grado académico: ABOGADA - ESPECIALISTA EN DERECHO PENAL

Objetivo general

Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional

Premisa: La Ley N.º 30096 que regula los delitos informáticos en el Perú, ayuda a proteger los datos comerciales y la propiedad intelectual de las empresas al penalizar el acceso no autorizado a sistemas informáticos y la divulgación no autorizada de información confidencial. Fraude informático es el delito que sanciona a toda persona que procura a través de las tecnologías de la información o de la comunicación, un beneficio o provecho ilícito para sí o para otro en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático.

Pregunta 1.- Desde su perspectiva, ¿cómo afecta el fraude informático al desarrollo de la libertad de empresa como garantía constitucional?

……
……
……
……

Pregunta 2.- En su máxima experiencia, ¿qué medidas y estrategias utilizan las empresas para prevenir y mitigar los efectos del avance tecnológico en el fraude informático para sí mismo?

……
……
……
……..

Pregunta 3.- En ese escenario, ¿cómo la creación de un organismo supervisor de seguridad digital garantizaría la libertad de empresa en la prevención de los fraudes informáticos?

Considero que los organismos reguladores son una garantía que ayuda a cumplir las normas y esto es una garantía para prevenir ilícitos informáticos.

Objetivo específico 1

Analizar de qué manera la ciberseguridad garantiza la libertad de acceso de mercado como garantía constitucional

Premisa: Ley N.º 28303 del Marco de Ciencia, Tecnología e Innovación Tecnológica hace referencia al base legal de la tecnología, ya que esta tiene la finalidad de diseñar el marco legal e institucional, sobre todo el de la administración de justicia. El artículo 59º de la Constitución reconoce el derecho a la libertad de empresa, garantizando a todas las personas una libertad de decisión no sólo para crear empresas, es para actuar en el mercado (libertad de acceso al mercado), también para establecer los propios objetivos de la empresa.

Pregunta 4.- En vista a la premisa acotada, bajo su propio concepto, ¿de qué manera mantener un marco legal en la tecnología aportaría a la libertad de acceso de mercado de la empresa?

……
……

.....

.....

.....

Pregunta 5.- Desde su perspectiva, ¿cómo se han desarrollado las políticas de ciberseguridad para promover o inhibir la entrada de nuevas empresas en el mercado?

.....

.....

.....

.....

.....

Pregunta 6.- En Perú, ¿cómo se han adaptado las regulaciones internacionales sobre tecnología para equilibrar la libertad de acceso de mercado?

.....

.....

.....

.....

.....

Objetivo específico 2

Analizar de qué manera el derecho a la protección de datos contribuye a la libertad de la organización empresarial como garantía constitucional

Premisa: Ley N.º 29733 de Protección de Datos Personales, con relación a los derechos y privacidad, la utilización de los datos personales y sensibles se maneja con sumo cuidado puesto que el gobierno peruano debe velar que no haya un perjuicio al usuario con fines públicos o privados. La libertad de organización de empresa establece un plan de seguridad de la información bajo normas técnicas, esta se establece en la Agenda Digital Peruana 2.0, donde establece la necesidad de contar estrategias de ciberseguridad para un accionar fluido en el mercado.

Pregunta 7.- En su opinión, ¿cómo pueden apoyar o perjudicar los derechos y privacidad de información en la libertad de la organización como garantía constitucional?

Las empresas están en la obligación cumplir bajo el marco legal de adquirir la protección adecuada, no solo los beneficiando a los usuarios, sino también para sí misma, para disminuir las quiebras de las empresas

Pregunta 8.- ¿Qué consecuencias legales y reputacionales pueden enfrentar las empresas por la falta de medidas preventivas en las regulaciones sobre privacidad de información?

La difusión de los delitos informáticos es el primer papel de las autoridades, luego la prevención, regulación de las normas y cumplimiento de las mismas normas.

9.- Bajo un marco legal, ¿en qué medidas una libre organización de empresa garantizaría el uso de la información personal y sensible de los clientes y empleados?

……
……
……
……
……

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 2.2: Ficha de análisis de fuente de documentos

INSTRUMENTO DE RECOLECCIÓN DE DATOS

FICHA DE ANÁLISIS DE FUENTE DE DOCUMENTOS

Título de la investigación:

Fraude informático frente a la libertad de empresa como garantía constitucional, Lima 2023

Objetivo general

Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional.

I. ANÁLISIS DE LEY N°30096 – LEY DE DELITOS INFORMATICOS

Ficha de análisis de fuente de documentos – Ley de delitos informáticos	
Identificación de la Fuente: LEY DE DELITOS INFORMÁTICOS LEY Nº 30096 Link: https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf	
Texto relevante	**Análisis del contenido**
Según lo expuesto por la Ley N° 30096 – Ley de Delitos Informáticos, en el **artículo 1** del desarrollo del objeto es prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia, con relación al	La Ley N° 30096 hace referencia a los delitos informáticos, en la cual una de las modalidades es el **fraude informático;** La ciberseguridad y la libertad empresarial son componentes críticos de la economía digital y la sociedad actual. El equilibrio entre leyes que protegen la ciberseguridad y políticas que promueven la libertad empresarial es esencial para

artículo 8 sobre el **fraude informático**, considera: Las medianas y pequeñas empresas no pueden asumir realizar una inversión en herramientas de ciberseguridad o contratar servicios dirigidos a la protección de sus activos inmateriales más valiosos y esenciales. No olvidemos que en la actualidad nos encontramos en plena ola de digitalización de las empresas, donde los datos fluyen por la red a niveles inimaginables convirtiéndose en el nuevo “oro” de cualquier compañía. Cabe resaltar, dicha línea de acción se encuentra amparada en el **artículo 8, fraude informático** el que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado	garantizar un entorno en línea seguro y próspero. Así como el gobierno, las grandes industrias manejan un sinfín de información instaladas en sistemas informáticos, por lo que para una correcta actividad comercial deben asegurar la existencia de leyes para evitar dichas delincuencias informáticas.

destinado a fines asistenciales o a programas de apoyo social.	
Ponderamiento	
A manera de conclusión, se puede indicar que, en la **Ley N° 30096 – Ley de Delitos Informáticos** en el **artículo 1** tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, que son cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de poder garantizar la lucha eficaz contra la ciberdelincuencia. En la cual se puede evidenciar que las empresas están siendo atacadas mediante una modalidad que se encuentra en el **artículo 8 fraude informático,** el cual impide la libertad de empresa como garantía constitucional.	

II. ANÁLISIS DE LA SENTENCIA DEL TRIBUNAL CONSTITUCIONAL

Ficha de análisis de fuente de documentos – Sentencia del Tribunal Constitucional	
Identificación de la Fuente: Sentencia del Tribunal Constitucional EXP. N.° 0011-2013-PI/TC - LIMA Link: https://www.tc.gob.pe/jurisprudencia/2015/00011-2013-AI.html#:~:text=La%20libertad%20de%20empresa%20es,bienes%20o%20prestaci%C3%B3n%20de%20servicios%2C	
Texto relevante	**Análisis del contenido**
De manera que, la Sentencia del Tribunal Constitucional del expediente N.° 0011-2013-PI/TC - Lima, en el apartado B consideraciones del Tribunal Constitucional en el **numeral treinta** conformes la **libertad de empresa**, narra que: El artículo 59 de la Constitución reconoce el derecho a la libertad de empresa en los términos	La presente sentencia alude a la **libertad de empresa,** ello es una representación de la libertad individual, por lo que, al ser consustancial con la libertad, el Estado debe permitir la existencia, actividad y permanencia de la empresa. En tal línea, la presencia del estado debe

siguientes: "*El Estado estimula la creación de riqueza y garantiza la libertad de trabajo y la libertad de empresa, comercio e industria […]*" La libertad de empresa es un derecho fundamental mediante el cual se garantiza la facultad de toda persona a elegir y crear libremente una institución u organización con el objeto de dedicarla a la realización de actividades que tengan fines económicos, ya sea de producción de bienes o prestación de servicios, orientados a satisfacer necesidades, y disfrutar de su rendimiento económico y satisfacción espiritual. Tribunal recordó que el contenido constitucionalmente protegido de la libertad de empresa está compuesto por tres posiciones ius-fundamentales básicas: 1 Acceso. - A través de la llamada libertad de fundación de una empresa, mediante la cual se garantiza la potestad de decidir no solo crear empresas, sino también actuar en el mercado, según la denominada libertad de acceso al mercado. 2 autoorganización. - A través del reconocimiento a la libertad de organización de la empresa, que garantiza al empresario la facultad de establecer los objetivos propios de la empresa, con el fin de dirigir y planificar su actividad (libertad de dirección de la empresa) en atención a sus recursos y a	proteger a las empresas y usuarios de los delitos informáticos hace que las empresas se encuentren vulnerables mediante los fraudes informáticos, lo que impide el crecimiento económico social de mercado, la cual protege el artículo 59 de la Constitución Política del Perú, a la libertad de empresa como garantía constitucional.

las condiciones del mercado. 3 cesación. - A través del cual se reconoce la potestad de decidir la salida del mercado de la empresa.	
Ponderamiento	
En consecuencia, se infiere de la Sentencia del Tribunal Constitucional del expediente N.° 0011-2013-PI/TC - Lima, en el apartado B consideraciones del Tribunal Constitucional en el **numeral treinta** conformes a **la libertad de empresa** es la representación de la libertad individual, por lo que al ser consustancial con la libertad, el Estado debe permitir la existencia, actividad y permanencia de la empresa, es por ello que la intervención del Estado debe garantizar la libertad de trabajo y la libertad de empresa sin límites, como se encuentra amparada en el artículo 59 de la Constitución Política del Perú.	

Objetivo específico 1

Analizar de qué manera se previene el base legal de la tecnología en la libertad de acceso de mercado como garantía constitucional.

I. ANÁLISIS DE LA RESOLUCIÓN PRESIDENCIA N.º 097-2020-CONCYTEC-P

Ficha de análisis de fuente de documentos – Resolución Presidencial	
Identificación de la fuente: Resolución Presidencia N.º 097-2020-CONCYTEC-P https: https://www.urp.edu.pe/pdf/id/24967/n/r.p.-097-2020-concytec-p-aprueba-guia-proyectos-de-investigacionf.pdf	
Texto relevante	**Análisis del contenido**
Sen lo expuesto por la Resolución Presidencial N.º 097-2020-CONCYTEC-P, en el **numeral 3.** De la Ley Marco de Ciencia, Tecnología	La Resolución Presidencial menciona la Ley Marco de Ciencia, Tecnología e Innovación Tecnológica, con relación a la **ciberseguridad,** el rol del estado es poder

e Innovación Tecnológica, con relación a la **ciberseguridad,** considera: Que, a través del Informe de Vistos, la Oficina General de Asesoría Jurídica, señala que de acuerdo al artículo 4 de la Ley N.º 28613, Ley del CONCYTEC, éste tiene por finalidad normar, dirigir, orientar, fomentar, coordinar, supervisar y evaluar las acciones del Estado en el ámbito de la ciencia, tecnología e innovación tecnológica y promover e impulsar su desarrollo mediante la acción concertada y la complementariedad entre los programas y proyectos de las instituciones públicas, académicas, empresariales, organizaciones sociales y personas integrantes del Sistema Nacional de Ciencia, Tecnología e Innovación Tecnológica (SINACYT). Conceder los derechos de uso y/o explotación de la riqueza nacional, fijando las condiciones de su aprovechamiento sustentable y rentabilidad, tanto para los concesionarios como para la colectividad nacional.	consolidar y perfeccionar el sistema democrático, como forma de vida de la sociedad peruana y de gobierno de la República, expresado en la vigencia real de los derechos económicos y sociales de la persona, contenidos en nuestra Carta Política.
Ponderamiento	
A manera de conclusión, se puede indicar que, en la **Resolución Presidencial N.º 097-2020-CONCYTEC-P** en el **numeral 3** de la Ley Marco de Ciencia, Tecnología e Innovación Tecnológica hace referencia a la **ciberseguridad,** ya que esta tiene la finalidad de diseñar el marco legal e institucional, sobre todo el de la	

administración de justicia, dentro del cual, tanto las personas naturales como las empresas productivas, dispongan de un orden jurídico que les brinde estabilidad y certidumbre en la disposición y ejercicio de sus derechos adquiridos dentro de la ley.

II. ANÁLISIS DE LA SENTENCIA DEL TRIBUNAL CONSTITUCIONAL

Ficha de análisis de fuente de documentos – Sentencia del Tribunal Constitucional	
Identificación de la Fuente: Sentencia del Tribunal Constitucional EXP. N.º 01405-2010-PA/TC - CALLAO Link: https://www.tc.gob.pe/jurisprudencia/2011/01405-2010-AA.html	
Texto relevante	**Análisis del contenido**
De manera que en la Sentencia del Tribunal Constitucional del EXP. N.º 01405-2010-PA/TC – Callao, Consideraciones del Tribunal Constitucional en el **apartado 15** conforme a la **libertad de acceso de mercado** narra que: El artículo 59º de la Constitución reconoce el derecho a la libertad de empresa está garantizando a todas las personas una libertad de decisión no sólo para crear empresas (libertad de fundación de una empresa), y por tanto, para actuar en el mercado (libertad de acceso al mercado), sino también para establecer los propios objetivos de la empresa (libertad de organización del empresario) y dirigir y planificar su actividad (libertad de dirección de la empresa) en atención a sus recursos y a las condiciones del propio mercado, así como la libertad de cesación o de salida del	La presente sentencia alude en razón a la **libertad de acceso de mercado,** el Estado debe remover los obstáculos que impidan o restrinjan el libre acceso a los mercados de bienes y servicios, así como toda práctica que produzca o pueda producir el efecto de limitar, impedir, restringir o falsear la libre competencia, para lo cual debe formular y establecer todos los mecanismos jurídicos necesarios a fin de salvaguardar la libre competencia.

mercado. Por dicha razón, el artículo 61º de la Constitución reconoce que el Estado: a) facilita y vigila la libre competencia; b) combate toda práctica que limite la libre competencia; y c) combate el abuso de posiciones dominantes o monopólicas.	
Ponderamiento	
En consecuencia, se infiere a la Sentencia del Tribunal Constitucional del EXP. N.º 01405-2010-PA/TC – Callao, Consideraciones del Tribunal Constitucional, en el **apartado 15** conforme a la **libertad de acceso de mercado,** el artículo 59 de la Constitución Política del Perú garantiza a todas las personas una libertad de decisión no sólo para crear empresas (libertad de fundación de una empresa), y por tanto, para actuar en el mercado (libertad de acceso al mercado), sino también para establecer los propios objetivos de la empresa (libertad de organización del empresario) y dirigir y planificar su actividad (libertad de dirección de la empresa) en atención a sus recursos y a las condiciones del propio mercado, así como la libertad de cesación o de salida del mercado.	

Objetivo específico 2

Analizar de qué manera los derechos y privacidad apoyan en la libertad de la organización de empresa como garantía constitucional.

I. ANÁLISIS DE LA RESOLUCIÓN N.° 071-2022-2023-OM-CR

Ficha de análisis de fuente de documentos – Resolución N.º 071-2022-2023-OM-CR	
Identificación De La Fuente: Resolución N. ° 071-2022-2023-OM-CR Link: https://www.congreso.gob.pe/Docs/spa/files/resoluciones/2023/resolucion-071-2022-2023-om.pdf	
Texto relevante	**Análisis del contenido**

Según lo expuesto por la Resolución N.º 071-2022-2023-OM-CR, en el **numeral 2** sobre la Ley de Protección de Datos Personales – Ley N.º 29733, con relación al **derecho de protección de datos,** considera: La ley 29733 denota que los datos personales como sensibles dentro de un registro o base con titularidad correspondiente a una entidad pública se encuentra sujeto a penalización por un marco constitucional de los derechos fundamentales. Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú. Ley se aplica a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. Son objeto de especial protección los datos sensibles, ya que están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes, como también esta obligación subsiste aun después de finalizadas las relaciones con el titular del banco de datos personales. Los ambientes en los que se procese almacenen o transmita la información deberán ser implementados, con	La resolución infiere en la Superintendencia Nacional de Protección de Datos Personales, en relación al **derecho de protección de datos,** la Ley N.º 29733 es la encargada de supervisa y regula el cumplimiento de la ley en el país, puesto que es un derecho fundamental, no proteger los datos personales puede tener consecuencias graves y variadas, que van desde la violación de la privacidad hasta sanciones legales y pérdidas financieras significativas. Por lo tanto, es esencial que las organizaciones y las entidades gubernamentales tomen medidas adecuadas para proteger los datos personales y cumplir con las leyes de protección de datos.

controles de seguridad apropiados, tomando como referencia las recomendaciones de seguridad física y ambiental recomendados en la "NTP ISO/IEC 17799 EDI. Tecnología de la Información.	
Ponderamiento	
A manera de conclusión, se puede indicar que, en la **Resolución N. ° 071-2022-2023-OM-CR**, en el **numeral 2** sobre la Ley de Protección de Datos Personales – Ley N.º 29733, con relación al **derecho de protección de datos,** la utilización de los datos personales y sensibles se maneja con sumo cuidado puesto que el gobierno peruano debe velar que no haya un perjuicio al usuario con fines públicos o privados, Brindar medidas de seguridad a los titulares de los datos personales para garantizar la atención de derechos de acceso, rectificación, cancelación y oposición, asimismo, asegurar la atención de las solicitudes o requerimientos formulados por la Autoridad Nacional de Protección de Datos Personales.	

II. ANÁLISIS DE RESOLUCIÓN MINISTERIAL N.º 129-2012-PCM

Ficha de análisis de fuente de documentos – Resolución Ministerial	
Identificación de la Fuente: Resolución Ministerial N.º 129-2012-PCM Link: https://cdn.www.gob.pe/uploads/document/file/303765/RM_129_2012PCM.pdf?v=1553808064	
Texto relevante	**Análisis del contenido**
Según lo expuesto por la Resolución Ministerial N.º 129-2012-PCM, en el **numeral 8** sobre La Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información, con relación a la **libertad de organización de empresa,** considera: considera que la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007	La Resolución Ministerial infiere en el ISO/IEC 17799:2007 EDI. Tecnología de la Información, con relación a **la libertad de organización de**

EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información, 2° Edición" establece la recomendación de seguridad, así como, las buenas prácticas para la implementación de controles que realizan los Sistemas de Gestión de Seguridad de la información; pero no define la forma de realizar la entrega, por lo que es necesario incorporar una forma de verificar la efectividad y eficiencia de lo implementado. Que, de acuerdo a lo establecido en el numeral 4.8 del artículo 4 y el artículo 49 del Reglamento de Organización y Funciones de la Presidencia del Consejo de ministros actúa como ente rector del Sistema Nacional de informática a través de la Oficina Nacional de Gobierno Electrónico e informática (ONGEI), siendo esta la encargada de implementar la Política Nacional de Gobierno Electrónico e informática. Así mismo, es política de Estado promover, facilitar e incorporar el uso de las nuevas Tecnologías de la Información y la Comunicación (TIC) en la difusión de los avances de la infraestructura de datos espaciales del país, con el propósito de brindar a la población facilidades de acceso a la información y a los servicios gubernamentales, en menor tiempo e independientemente del lugar geográfico donde se realicen los requerimientos de la ciudadanía.	**empresa,** el contenido analizado se centra en la gestión de la seguridad de la información y el fomento de las Tecnologías de la Información y la Comunicación (TIC) en el contexto del gobierno peruano, se menciona la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI" como referencia para la seguridad de la información, pero se destaca la necesidad de desarrollar un enfoque de evaluación eficaz. La Presidencia del Consejo de ministros (PCM), a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), ejerce un papel rector en el Sistema Nacional de Informática en Perú, subrayando su relevancia en la regulación de las iniciativas tecnológicas, se enfatiza la política estatal de impulsar las TIC para mejorar la accesibilidad y eficiencia de los servicios

	gubernamentales, demostrando un compromiso gubernamental con la modernización de servicios y el acceso a la información.
Ponderamiento	
A manera de conclusión, se puede indicar que, en la **Resolución Ministerial N.º 129-2012-PCM,** en el **numeral 8** sobre La Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información, con relación a la **libertad de organización de empresa** establece un Plan de Seguridad de la Información bajo normas Técnicas, esta se establece en la Agenda Digital Peruana 2.0, donde establece la necesidad de contar estrategias de ciberseguridad para evitar incidentes en recursos de información, las bases se encuentran en Códigos de buenas prácticas para la gestión de seguridad de la información.	

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 3: EVALUACIÓN POR JUICIO DE EXPERTOS

ANEXO 3.1.: VALIDACIÓN DE INSTRUMENTO

CARTA DE PRESENTACIÓN

Señor: Mg. MARCHINARES RAMOS, Lucrecia

Presente

Asunto: **VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO**.

Me es muy grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que, siendo estudiante del Programa de Pregrado de la Escuela de Derecho de la UCV, sección C2, en la sede LIMA NORTE, ciclo 2023 - II, requiero validar los instrumentos con los cuales se recogerá la información necesaria para poder desarrollar mi investigación y con la que sustentaré mis competencias investigativas en la Experiencia curricular de Proyecto de investigación.

El nombre de mi título de investigación es: **"Fraude informático frente a la libertad de empresa como garantía constitucional de Lima, 2023"** y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, se ha considerado conveniente recurrir a usted, ante su connotada experiencia en temas educativos y/o investigación educativa.

El expediente de validación, que le hacemos llegar contiene:

- Carta de presentación.
- Formato de validación.
- Certificado de validez de contenido de los instrumentos.
- Guía de entrevista.
- Matriz de categorización

Expresándole mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

UNIVERSIDAD CÉSAR VALLEJO

Evaluación por **CHUMBE HUARHUACHI BRIGGIT BETTSY** **juicio de expertos**
DNI: 71029302

Respetado Juez: Usted ha sido seleccionado para evaluar el instrumento de "Guía de entrevista". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al que hacer jurídico. Agradecemos su valiosa colaboración.

1. Datos generales del abogado: Mg. MARCHINARES RAMOS, Lidia Lucrecia

Nombre del abogado:	Mg. MARCHINARES RAMOS, Lidia Lucrecia
Grado profesional:	Maestría (**X**) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa (X) Organizacional ( )
Áreas de experiencia profesional:	
Institución donde labora:	
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Jurídica: (si corresponde)	Mas de 8 años de experiencia en investigación

2. Propósito de la evaluación:

3. Datos de la escala

Nombre de la Prueba:	Guía de entrevista
Autor(a)(es):	Chumbe Huarhuachi, Briggit Bettsy
Procedencia:	Lima - Perú
Administración:	Propia
Tiempo de aplicación:	60 minutos
Ámbito de aplicación:	Distrito Fiscal Lima Centro
Significación:	La investigación tiene como **categoría 1**: Fraude informático**,** con subcategorías: Base legal de la tecnología y derechos y privacidad; como **categoría 2**: Libertad de empresa**,** con subcategorías: Libertad de acceso de mercado y libertad de organización de empresa; cuyo objetivo general es: Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional en Lima, 2023.

4. Soporte teórico

Escala/ÁREA	Sub categorías	Definición
Fraude informático	**Base legal de la tecnología** **Derechos y privacidad**	Lux y Calderón (2020) sostienen que el fraude informático esta vincula con al perjuicio patrimonial, mediante manipulación o alteración de datos o programas de sistemas informáticos, sin embargo, debe reconocerse que esta forma de definir al fraude informático corresponde a lo que podría denominarse un concepto estricto de éste, lo que significa que existen otras formas más laxas de comprender ese comportamiento.
Libertad de empresa	**Libertad de acceso de mercado** **Libertad de organización**	Para Guzmán (2023) Se define como el derecho a iniciar un negocio sin gravámenes gubernamentales, tal asignación puede ser hecha por una persona o grupo asociado.

	de empresa	

5. Presentación de instrucciones para el juez:

A continuación, a usted le presento la guía de entrevista elaborada por **Chumbe Huarhuachi, Briggit Bettsy** en el año 2023. De acuerdo con lossiguientes indicadores a fin de que califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica ysemántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (nocumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (altonivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencialo	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.

importante, es decir debe ser incluido.	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1. No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Categorías y subcategorías del instrumento:

Categorías	Subcategorías
Categoría 1: Fraude informáticos	Base legal de la tecnología
	Derechos y privacidad
Categoría 2: Libertad de empresa	Libertad de acceso de mercado
	Libertad de organización de empresa

OBJETIVOS	ÍTEM	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES/ RECOMENDACIONES
Objetivo general: Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional en Lima, 2023.	Desde su perspectiva, ¿cómo afecta el fraude informático al desarrollo de la libertad de empresa como garantía constitucional?	3	4	4	
	En su máxima experiencia, ¿qué medidas y estrategias utilizan las empresas para prevenir y mitigar los efectos del avance tecnológico en el fraude informático para sí mismo?	4	3	4	
	En ese escenario, ¿cómo la creación de un organismo supervisor de seguridad digital garantizaría la libertad de empresa en la prevención	3	4	4	

	de los fraudes informáticos?				
Objetivo específico 1: Analizar de qué manera el base legal de la tecnología aporta en la libertad de acceso de mercado como garantía constitucional.	En vista a la premisa acotada, bajo su propio concepto, ¿de qué manera mantener un marco legal en la tecnología aportaría a la libertad de acceso de mercado de la empresa?	4	3	4	
	Desde su perspectiva, ¿cómo se han desarrollado las políticas de ciberseguridad para promover o inhibir la entrada de nuevas empresas en el mercado?	4	4	3	
	En Perú, ¿cómo se han adaptado las regulaciones internacionales sobre tecnología para equilibrar la libertad de acceso de mercado?	4	4	4	
Objetivo específico 2: Analizar de qué manera los derechos y privacidad apoyan en la libertad de la organización de empresa como garantía constitucional.	En su opinión, ¿cómo pueden apoyar o perjudicar los derechos y privacidad de información en la libertad de la organización como garantía constitucional?	3	4	4	
	¿Qué consecuencias legales y reputacionales pueden enfrentar las empresas por la falta de medidas preventivas en las regulaciones sobre privacidad de información?	4	3	3	
	Bajo un marco legal, ¿en qué medidas una libre organización de empresa garantizaría el uso de la información personal y sensible de los clientes y empleados?	4	3	4	

Observaciones (precisar si hay suficiencia):

_____

_____

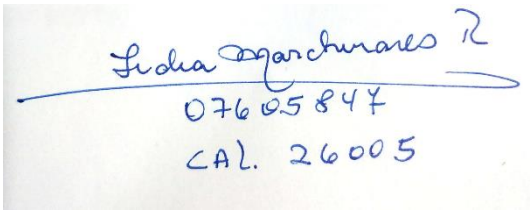
_____

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ]

No aplicable [ ]

Apellidos y nombres del juez validador: Mg. MARCHINARES RAMOS, Lidia Lucrecia

Especialidad del validador: Docente Universitario



Lima, 27 de setiembre del 2023.

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 3.2.: VALIDACIÓN DE INSTRUMENTO

CARTA DE PRESENTACIÓN

Señor: Mg. Vilela Apón, Rolando Javier

Presente

Asunto: **VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO**.

Me es muy grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que, siendo estudiante del Programa de Pregrado de la Escuela de Derecho de la UCV, sección C2, en la sede LIMA NORTE, ciclo 2023 - II, requiero validar los instrumentos con los cuales se recogerá la información necesaria para poder desarrollar mi investigación y con la que sustentaré mis competencias investigativas en la Experiencia curricular de Proyecto de investigación.

El nombre de mi título de investigación es: **"Fraude informático frente a la libertad de empresa como garantía constitucional de Lima, 2023"** y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, se ha considerado conveniente recurrir a usted, ante su connotada experiencia en temas educativos y/o investigación educativa.

El expediente de validación, que le hacemos llegar contiene:

- Carta de presentación.
- Formato de validación.
- Certificado de validez de contenido de los instrumentos.
- Guía de entrevista.
- Matriz de categorización

Expresándole mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

CHUMBE HUARHUACHI BRIGGIT BETTSY
DNI: 71029302

UNIVERSIDAD CÉSAR VALLEJO

Evaluación por juicio de expertos

Respetado Juez: Usted ha sido seleccionado para evaluar el instrumento de "Guía de entrevista". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al que hacer jurídico. Agradecemos su valiosa colaboración.

1. Datos generales del abogado:

Nombre del abogado:	Mg. Vilela Apón, Rolando Javier
Grado profesional:	Maestría (**X**) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa ( ) Organizacional ( )
Áreas de experiencia profesional:	
Institución donde labora:	
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Jurídica: (si corresponde)	

6. Propósito de la evaluación:

7. Datos de la escala

Nombre de la Prueba:	Guía de entrevista
Autor(a)(es):	Chumbe Huarhuachi, Briggit Bettsy
Procedencia:	Lima - Perú
Administración:	Propia
Tiempo de aplicación:	60 minutos
Ámbito de aplicación:	Distrito Fiscal Lima Centro
Significación:	La investigación tiene como **categoría 1**: Fraude informático**,** con subcategorías: Base legal de la tecnología y derechos y privacidad; como **categoría 2**: Libertad de empresa**,** con subcategorías: Libertad de acceso de mercado y libertad de organización de empresa; cuyo objetivo general es: Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional en Lima, 2023.

8. Soporte teórico

Escala/ÁREA	Sub categorías	Definición
Fraude informático	**Base legal de la tecnología** **Derechos y privacidad**	Lux y Calderón (2020) sostienen que el fraude informático esta vincula con al perjuicio patrimonial, mediante manipulación o alteración de datos o programas de sistemas informáticos, sin embargo, debe reconocerse que esta forma de definir al fraude informático corresponde a lo que podría denominarse un concepto estricto de éste, lo que significa que existen otras formas más laxas de comprender ese comportamiento.
Libertad de empresa	**Libertad de acceso de mercado** **Libertad de organización**	Para Guzmán (2023) Se define como el derecho a iniciar un negocio sin gravámenes gubernamentales, tal asignación puede ser hecha por una persona o grupo asociado.

	de empresa	

9. Presentación de instrucciones para el juez:

A continuación, a usted le presento la guía de entrevista elaborada por **Chumbe Huarhuachi, Briggit Bettsy** en el año 2023. De acuerdo con lossiguientes indicadores a fin de que califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica ysemántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (nocumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (altonivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencialo	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.

importante, es decir debe ser incluido.	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1. No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Categorías y subcategorías del instrumento:

Categorías	Subcategorías
Categoría 1: Fraude informáticos	Base legal de la tecnología
	Derechos y privacidad
Categoría 2: Libertad de empresa	Libertad de acceso de mercado
	Libertad de organización de empresa

OBJETIVOS	ÍTEM	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES/ RECOMENDACIONES
Objetivo general: Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional en Lima, 2023.	Desde su perspectiva, ¿cómo afecta el fraude informático al desarrollo de la libertad de empresa como garantía constitucional?	4	3	4	
	En su máxima experiencia, ¿qué medidas y estrategias utilizan las empresas para prevenir y mitigar los efectos del avance tecnológico en el fraude informático para sí mismo?	3	4	4	
	En ese escenario, ¿cómo la creación de un organismo supervisor de seguridad digital garantizaría la libertad de empresa en la prevención	3	4	3	

	de los fraudes informáticos?				
Objetivo específico 1: Analizar de qué manera el base legal de la tecnología aporta en la libertad de acceso de mercado como garantía constitucional.	En vista a la premisa acotada, bajo su propio concepto, ¿de qué manera mantener un marco legal en la tecnología aportaría a la libertad de acceso de mercado de la empresa?	4	4	3	
	Desde su perspectiva, ¿cómo se han desarrollado las políticas de ciberseguridad para promover o inhibir la entrada de nuevas empresas en el mercado?	4	3	4	
	En Perú, ¿cómo se han adaptado las regulaciones internacionales sobre tecnología para equilibrar la libertad de acceso de mercado?	4	4	3	
Objetivo específico 2: Analizar de qué manera los derechos y privacidad apoyan en la libertad de la organización de empresa como garantía constitucional.	En su opinión, ¿cómo pueden apoyar o perjudicar los derechos y privacidad de información en la libertad de la organización como garantía constitucional?	3	4	4	
	¿Qué consecuencias legales y reputacionales pueden enfrentar las empresas por la falta de medidas preventivas en las regulaciones sobre privacidad de información?	3	4	3	
	Bajo un marco legal, ¿en qué medidas una libre organización de empresa garantizaría el uso de la información personal y sensible de los clientes y empleados?	4	4	4	

Observaciones (precisar si hay suficiencia):

_____

_____

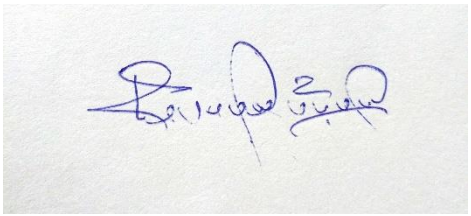
_____

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ]

No aplicable [ ]

Apellidos y nombres del juez validador: Mg. Vilela Apón, Rolando Javier

Especialidad del validador: Derecho Penal



Lima, 30 de octubre del 2023.

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 3.3.: VALIDACIÓN DE INSTRUMENTO

CARTA DE PRESENTACIÓN

Señor: La Torre Guerrero, Ángel Fernando

Presente

Asunto: **VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO**.

Me es muy grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que, siendo estudiante del Programa de Pregrado de la Escuela de Derecho de la UCV, sección C2, en la sede LIMA NORTE, ciclo 2023 - II, requiero validar los instrumentos con los cuales se recogerá la información necesaria para poder desarrollar mi investigación y con la que sustentaré mis competencias investigativas en la Experiencia curricular de Proyecto de investigación.

El nombre de mi título de investigación es: **"Fraude informático frente a la libertad de empresa como garantía constitucional de Lima, 2023"** y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, se ha considerado conveniente recurrir a usted, ante su connotada experiencia en temas educativos y/o investigación educativa.

El expediente de validación, que le hacemos llegar contiene:

- Carta de presentación.
- Formato de validación.
- Certificado de validez de contenido de los instrumentos.
- Guía de entrevista.
- Matriz de categorización

Expresándole mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

CHUMBE HUARHUACHI BRIGGIT BETTSY
DNI: 71029302

UNIVERSIDAD CÉSAR VALLEJO

Evaluación por juicio de expertos

Respetado Juez: Usted ha sido seleccionado para evaluar el instrumento de "Guía de entrevista". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al que hacer jurídico. Agradecemos su valiosa colaboración.

1. Datos generales del abogado:

Nombre del abogado:	La Torre Guerrero, Ángel Fernando
Grado profesional:	Maestría (**X**) Doctor ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa (X) Organizacional ( )
Áreas de experiencia profesional:	Docente universitario
Institución donde labora:	
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Jurídica: (si corresponde)	

10. Propósito de la evaluación:

11. Datos de la escala

Nombre de la Prueba:	Guía de entrevista
Autor(a)(es):	Chumbe Huarhuachi, Briggit Bettsy
Procedencia:	Lima - Perú
Administración:	Propia
Tiempo de aplicación:	60 minutos
Ámbito de aplicación:	Distrito Fiscal Lima Centro
Significación:	La investigación tiene como **categoría 1**: Fraude informático**,** con subcategorías: Base legal de la tecnología y derechos y privacidad; como **categoría 2**: Libertad de empresa**,** con subcategorías: Libertad de acceso de mercado y libertad de organización de empresa; cuyo objetivo general es: Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional en Lima, 2023.

12. Soporte teórico

Escala/ÁREA	Sub categorías	Definición
Fraude informático	**Base legal de la tecnología** **Derechos y privacidad**	Lux y Calderón (2020) sostienen que el fraude informático esta vincula con al perjuicio patrimonial, mediante manipulación o alteración de datos o programas de sistemas informáticos, sin embargo, debe reconocerse que esta forma de definir al fraude informático corresponde a lo que podría denominarse un concepto estricto de éste, lo que significa que existen otras formas más laxas de comprender ese comportamiento.
Libertad de empresa	**Libertad de acceso de mercado** **Libertad de organización**	Para Guzmán (2023) Se define como el derecho a iniciar un negocio sin gravámenes gubernamentales, tal asignación puede ser hecha por una persona o grupo asociado.

	de empresa	

13. <u>Presentación de instrucciones para el juez</u>:

A continuación, a usted le presento la guía de entrevista elaborada por **Chumbe Huarhuachi, Briggit Bettsy** en el año 2023. De acuerdo con lossiguientes indicadores a fin de que califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica ysemántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (nocumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (altonivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencialo	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.

importante, es decir debe ser incluido.	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1. No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Categorías y subcategorías del instrumento:

Categorías	Subcategorías
Categoría 1: Fraude informáticos	Base legal de la tecnología
	Derechos y privacidad
Categoría 2: Libertad de empresa	Libertad de acceso de mercado
	Libertad de organización de empresa

OBJETIVOS	ÍTEM	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES/ RECOMENDACIONES
Objetivo general: Analizar de qué manera el fraude informático afecta la libertad de empresa como garantía constitucional en Lima, 2023.	Desde su perspectiva, ¿cómo afecta el fraude informático al desarrollo de la libertad de empresa como garantía constitucional?	4	3	4	
	En su máxima experiencia, ¿qué medidas y estrategias utilizan las empresas para prevenir y mitigar los efectos del avance tecnológico en el fraude informático para sí mismo?	4	4	3	
	En ese escenario, ¿cómo la creación de un organismo supervisor de seguridad digital garantizaría la libertad de empresa en la prevención	3	3	3	

	de los fraudes informáticos?				
Objetivo específico 1: Analizar de qué manera el base legal de la tecnología aporta en la libertad de acceso de mercado como garantía constitucional.	En vista a la premisa acotada, bajo su propio concepto, ¿de qué manera mantener un marco legal en la tecnología aportaría a la libertad de acceso de mercado de la empresa?	3	4	4	
	Desde su perspectiva, ¿cómo se han desarrollado las políticas de ciberseguridad para promover o inhibir la entrada de nuevas empresas en el mercado?	4	4	4	
	En Perú, ¿cómo se han adaptado las regulaciones internacionales sobre tecnología para equilibrar la libertad de acceso de mercado?	4	3	3	
Objetivo específico 2: Analizar de qué manera los derechos y privacidad apoyan en la libertad de la organización de empresa como garantía constitucional.	En su opinión, ¿cómo pueden apoyar o perjudicar los derechos y privacidad de información en la libertad de la organización como garantía constitucional?	4	4	3	
	¿Qué consecuencias legales y reputacionales pueden enfrentar las empresas por la falta de medidas preventivas en las regulaciones sobre privacidad de información?	4	4	3	
	Bajo un marco legal, ¿en qué medidas una libre organización de empresa garantizaría el uso de la información personal y sensible de los clientes y empleados?	3	4	4	

Observaciones (precisar si hay suficiencia):

_____

_____

_____

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ]

No aplicable [ ]

Apellidos y nombres del juez validador: La Torre Guerrero, Ángel Fernando

Especialidad del validador: Docente universitario

Lima, 30 de octubre del 2023.

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 3.4. Validación de instrumento – ficha de análisis de fuente documental

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

I.1 Apellidos y Nombres: Dr. Santisteban Llontop, Pedro.
I.2 Cargo e institución donde labora: Docente UCV.
I.3 Nombre del instrumento motivo de evaluación: **Análisis de fuente Jurisprudencial**
I.4 Autor de Instrumento: Chumbe Huarhuachi, Briggit Bettsy

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. PRESENTACIÓN	Responde a la formalidad de la investigación												X	
2. OBJETIVIDAD	Contiene la información comprendida en la cualidad deobjetivo y la adecuación al objeto investigado												X	
3. ACTUALIDAD	Contiene la información de acorde a los aportes recientes al derecho												X	
4. INTENCIONALIDA D	Contiene la información adecuada para valorar las Categorías.												X	
5. COHERENCIA	La información tiene coherencia entre los problemas, objetivos e hipótesis												X	
6. METODOLOGÍA	El instrumento responde al objetivo de la Investigación: Tipo, diseño, categorías.												X	
7. PERTINENCIA	El instrumento contiene información que considera un problema crucial, tiene relevancia global.												X	

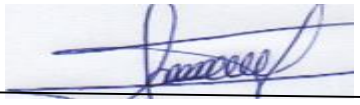
III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación — SI
- El Instrumento no cumple con Los requisitos para su aplicación

IV. PROMEDIO DE VALORACIÓN:

95

Lima, 10 de octubre 2023



FIRMA DEL EXPERTO INFORMANTE
Dr. Santisteban Llontop, Pedro
DNI No 09803311
Telf: 9832786

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Autenticidad del Asesor

Yo, SANTISTEBAN LLONTOP PEDRO PABLO, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Fraude informático frente a la libertad de empresa como garantía constitucional, Lima, 2023", cuyo autor es CHUMBE HUARHUACHI BRIGGIT BETTSY, constato que la investigación tiene un índice de similitud de 16.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 01 de Diciembre del 2023

Apellidos y Nombres del Asesor:	**Firma**
SANTISTEBAN LLONTOP PEDRO PABLO **DNI:** 09803311 **ORCID:** 0000-0003-0998-0538	Firmado electrónicamente por: PSANTISTEBANL el 01-12-2023 10:42:46

Código documento Trilce: TRI - 0675704

INVESTIGA UCV