FACULTAD DE DERECHO
ESCUELA PROFESIONAL DE DERECHO

Tesis

VULNERACIÓN DEL SECRETO EMPRESARIAL MEDIANTE ESPIONAJE EMPRESARIAL EN LIMA

PARA OBTENER EL TÍTULO DE
ABOGADO

Autores
ESPINOZA FABIAN, Lucero Alexandra (ORCID: 0000-0002-7737-3994)
HUAMAN COCHACHE, Bryan Alexander (ORCID: 0000-0001-7541-2825)

Asesora
YUNKOR ROMERO, Yurela Kosset (ORCID: 0000-0001-9902-5993)

Línea de investigación del programa
Enfoque interdisciplinario de la ciencia jurídica

Línea de acción RSU
Salud y Bienestar

LIMA, PERÚ, JULIO DE 2025

Referencia bibliográfica

Espinoza Fabian, L. A., & Huaman Cochache, B. A. (2025). *Vulneración del secreto empresarial mediante espionaje empresarial en Lima* [Tesis de pregrado, Universidad Autónoma del Perú]. Repositorio de la Universidad Autónoma del Perú.

HOJA DE METADATOS

Datos del autor	
Nombres y apellidos	Lucero Alexandra Espinoza Fabian
Tipo de documento de identidad	DNI
Número de documento de identidad	70420560
URL de ORCID	https://orcid.org/0000-0002-7737-3994
Datos del autor	
Nombres y apellidos	Bryan Alexander Huaman Cochache
Tipo de documento de identidad	DNI
Número de documento de identidad	71239571
URL de ORCID	https://orcid.org/0000-0001-7541-2825
Datos del asesor	
Nombres y apellidos	Yurela Kosett Yunkor Romero
Tipo de documento de identidad	DNI
Número de documento de identidad	20118250
URL de ORCID	https://orcid.org/0000-0001-9902-5993
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Carlos Antonio Agurto Gonzales
Tipo de documento	DNI
Número de documento de identidad	42378796
Secretario del jurado	
Nombres y apellidos	Alfonso Alvarado Vigo
Tipo de documento	DNI
Número de documento de identidad	45603621
Vocal del jurado	
Nombres y apellidos	Luis Angel Espinoza Pajuelo
Tipo de documento	DNI
Número de documento de identidad	10594662
Datos de la investigación	
Título de la investigación	Vulneración del secreto empresarial mediante espionaje empresarial en Lima

Línea de investigación Institucional	Persona, sociedad, empresa y estado
Línea de investigación del Programa	Enfoque interdisciplinario de la ciencia jurídica
Línea de acción RSU	Salud y bienestar
URL de disciplinas OCDE	https://purl.org/pe-repo/ocde/ford#5.05.01

FACULTAD DE DERECHO

ESCUELA PROFESIONAL DE DERECHO

ACTA DE SUSTENTACIÓN DE TESIS

En la ciudad de Lima, el jurado de sustentación de tesis conformado por: el DR. CARLOS ANTONIO AGURTO GONZALES como presidente, el MAG. ALFONSO ALVARADO VIGO como secretario y el DR. LUIS ANGEL ESPINOZA PAJUELO como vocal, reunidos en acto público para dictaminar la tesis titulada:

VULNERACIÓN DEL SECRETO EMPRESARIAL MEDIANTE ESPIONAJE EMPRESARIAL EN LIMA

Presentado por la bachiller:

LUCERO ALEXANDRA ESPINOZA FABIAN

Para obtener el **Título Profesional de Abogada**; luego de escuchar la sustentación de la misma y resueltas las preguntas del jurado se procedió a la calificación individual, obteniendo el dictamen de **Aprobado-Bueno** con una calificación de **DIECISEIS (16).**

En fe de lo cual firman los miembros del jurado, el 17 de julio de 2025

PRESIDENTE	**SECRETARIO**	**VOCAL**
CARLOS ANTONIO AGURTO GONZALES	MAG. ALFONSO ALVARADO VIGO	DR. LUIS ÁNGEL ESPINOZA PAJUELO

FACULTAD DE DERECHO

ESCUELA PROFESIONAL DE DERECHO

ACTA DE SUSTENTACIÓN DE TESIS

En la ciudad de Lima, el jurado de sustentación de tesis conformado por: el DR. CARLOS ANTONIO AGURTO GONZALES como presidente, el MAG. ALFONSO ALVARADO VIGO como secretario y el DR. LUIS ANGEL ESPINOZA PAJUELO como vocal, reunidos en acto público para dictaminar la tesis titulada:

VULNERACIÓN DEL SECRETO EMPRESARIAL MEDIANTE ESPIONAJE EMPRESARIAL EN LIMA

Presentado por el bachiller:

BRYAN ALEXANDER HUAMAN COCHACHE

Para obtener el **Título Profesional de Abogado**; luego de escuchar la sustentación de la misma y resueltas las preguntas del jurado se procedió a la calificación individual, obteniendo el dictamen de **Aprobado-Bueno** con una calificación de **DIECISEIS (16).**

En fe de lo cual firman los miembros del jurado, el 17 de julio de 2025

PRESIDENTE CARLOS ANTONIO AGURTO GONZALES	**SECRETARIO** MAG. ALFONSO ALVARADO VIGO	**VOCAL** DR. LUIS ÁNGEL ESPINOZA PAJUELO

ACTA DE APROBACIÓN DE ORIGINALIDAD

Yo Yurela Kosett Yunkor Romero docente de la Facultad de Derecho de la Escuela Profesional de Derecho de la Universidad Autónoma del Perú, en mi condición de asesora de la tesis titulada:

VULNERACIÓN DEL SECRETO EMPRESARIAL MEDIANTE ESPIONAJE EMPRESARIAL EN LIMA

De los bachilleres Lucero Alexandra Espinoza Fabian y Bryan Alexander Huaman Cochache, certifico que la tesis tiene un índice de similitud de 13% verificable en el reporte de similitud del software Turnitin que se adjunta.

La suscrita revisó y analizó dicho reporte a lo que concluyó 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 Autónoma del Perú.

Lima, 17 de julio de 2025

Yurela Kosett Yunkor Romero

DNI: 20118250

DEDICATORIA

A mis padres, por ser mi mayor ejemplo de amor, esfuerzo y dedicación, por sostenerme en cada caída y celebrar conmigo cada paso. A mis hermanos y cuñada, por su apoyo incondicional y por recordarme siempre que no estoy sola. A mi perrita, que con su tierna compañía me acompañó en cada desvelo, demostrando que el amor también se expresa en silencios y miradas.Este logro es tanto mío como de ustedes.

Lucero Alexandra Espinoza Fabian

Dedico esta tesis a todas las personas que me han acompañado en este proceso, con su amor, apoyo y paciencia. A mi familia, que siempre ha creído en mí, brindándome la fuerza para superar cada obstáculo; a mis hermanos, por su comprensión y compañía en los momentos difíciles; y a mis docentes, por compartir sus conocimientos y motivarme a seguir aprendiendo. Este logro es tanto mío como de todos ustedes.

Bryan Alexander Huaman Cochache

AGRADECIMIENTOS

A mis padres, por su amor incondicional y apoyo en cada paso de mi camino; a mis docentes, por su paciencia y valiosas enseñanzas que marcaron mi formación; a mi compañero de tesis, por su compromiso y esfuerzo compartido en este desafío; y a la Universidad Autónoma del Perú, por brindarme el conocimiento y las herramientas para mi desarrollo profesional. A todos ustedes, gracias por ser parte de este logro.

Lucero Alexandra Espinoza Fabian

Quiero expresar mi más profundo agradecimiento a todas las personas que hicieron posible la culminación de esta tesis. Agradezco a mis docentes, por su valiosa guía y por inspirarme a pensar críticamente sobre el Derecho. Mi más sincero agradecimiento a mi familia, por su apoyo incondicional, confianza y amor durante todo este camino. Finalmente, a todas aquellas personas que, de una u otra manera, contribuyeron a que este trabajo fuera posible. Este logro es el resultado de un esfuerzo colectivo, y me siento profundamente agradecido por ello.

Bryan Alexander Huaman Cochache

ÍNDICE

DEDICATORIA **2**
AGRADECIMIENTOS **3**
LISTA DE TABLAS **5**
RESUMEN **6**
ABSTRACT **7**
1. INTRODUCCIÓN **8**
2. MÉTODO **16**
2.1 Tipo y diseño de investigación 16
2.2 Escenario de Estudio 16
2.3 Hipótesis 16
2.4 Participantes 17
2.5 Técnicas e instrumentos de recolección de datos 17
2.6 Procedimiento 18
2.7 Análisis de datos 18
2.8 Aspecto Ético: 19
3. RESULTADOS **20**
4. DISCUSIÓN **27**
5. CONCLUSIONES **30**
6. RECOMENDACIONES **31**
REFERENCIAS **32**
ANEXOS

LISTA DE TABLAS

Tabla 1 Matriz de triangulación 1
Tabla 2 Matriz de triangulación 2
Tabla 3 Matriz de triangulación 3
Tabla 4 Matriz de triangulación 4
Tabla 5 Matriz de triangulación 5
Tabla 6 Matriz de triangulación 6
Tabla 7 Matriz de triangulación 7
Tabla 8 Matriz de triangulación 8

VULNERACIÓN DEL SECRETO EMPRESARIAL MEDIANTE ESPIONAJE EMPRESARIAL EN LIMA

LUCERO ALEXANDRA ESPINOZA FABIAN
BRYAN ALEXANDER HUAMÁN COCHACHE

UNIVERSIDAD AUTÓNOMA DEL PERÚ

RESUMEN

Esta investigación tuvo como objetivo analizar el impacto del espionaje empresarial en la protección de los secretos empresariales en Lima. El estudio fue de tipo aplicado y diseño no experimental. Se entrevistó a cinco magísteres en derecho corporativo y mercantil, seleccionados por su experiencia en el ámbito legal y empresarial. Las entrevistas, junto con el análisis documental, permitieron conocer en profundidad la situación actual. Los resultados mostraron que los participantes identificaron una débil protección de los secretos empresariales, atribuida a la falta de políticas internas claras, deficiencias en ciberseguridad y escasa capacitación del personal. También se evidenció que el espionaje empresarial es percibido como una amenaza real para la competitividad de las organizaciones en Lima. Se concluyó que es necesario fortalecer las políticas internas, implementar medidas de ciberseguridad y promover una cultura de protección de la información. Estas acciones contribuirían a reducir la vulnerabilidad de las empresas frente al espionaje y mejorar su seguridad.

Palabras clave: secreto empresarial, espionaje empresarial, políticas internas, ciberseguridad

BREACH OF TRADE SECRETS THROUGH CORPORATE ESPIONAGE IN LIMA

LUCERO ALEXANDRA ESPINOZA FABIAN
BRYAN ALEXANDER HUAMÁN COCHACHE

UNIVERSIDAD AUTÓNOMA DEL PERÚ

ABSTRACT

This research aimed to analyze the impact of corporate espionage on the protection of trade secrets in Lima. The study was applied in nature and used a non-experimental design. Five master's degree holders in corporate and commercial law were interviewed due to their experience in the legal and business fields. The interviews, along with document analysis, provided an in-depth understanding of the current situation. The results showed that participants identified weak protection of trade secrets, attributed to the lack of clear internal policies, cybersecurity deficiencies, and limited staff training. Corporate espionage was also perceived as a real threat to the competitiveness of organizations in Lima. It was concluded that it is necessary to strengthen internal policies, implement cybersecurity measures, and promote a culture of information protection. These actions would help reduce companies' vulnerability to espionage and improve their overall information security.

Keywords: trade secret, corporate espionage, internal policies, cybersecurity

1. INTRODUCCIÓN

El mundo empresarial actualmente se mantiene competitivo, el resguardo de los activos intangibles, como el secreto empresarial, es de vital importancia. Sin embargo, el desafío de salvaguardar esta información confidencial se ve a menudo amenazado por el fenómeno del espionaje empresarial. Está problemática tiene presencia en varios países, como Estados Unidos, territorio en el cual durante el año 2021 se determinó que diversas empresas estaban siendo afectadas por este fenómeno, como la empresa Tesla Inc, L'Oreal, Lidl, Google (López, 2012).

Los secretos empresariales son información confidencial y valiosa que una empresa mantiene para obtener ventajas competitivas en el mercado. Estos secretos pueden incluir una amplia gama de información, desde fórmulas químicas y procesos de fabricación hasta estrategias de marketing y listas de clientes (Aliaga, 2019).

En la problemática internacional, el mundo empresarial actualmente se mantiene competitivo, el resguardo de los activos intangibles, como el secreto empresarial, es de vital importancia. Sin embargo, el desafío de salvaguardar esta información confidencial se ve a menudo amenazado por el fenómeno del espionaje empresarial. Está problemática tiene presencia en varios países, como Estados Unidos, territorio en el cual durante el año 2021 se determinó que diversas empresas estaban siendo afectadas por este fenómeno (López, 2012). También se han reportado casos de presunta ciberespionaje y robo de propiedad intelectual como, por ejemplo, Micron Technology, una empresa de semiconductores de EE. UU., acusó a United Microelectronics Corporation (UMC) y a la empresa china Fujian Jinhua Integrated Circuit Co. de robar secretos comerciales relacionados con chips de memoria DRAM. Micrón presentó una demanda alegando infracción de derechos de propiedad intelectual. Este caso ilustra las preocupaciones sobre el robo de propiedad intelectual y el espionaje industrial en el sector de semiconductores (Aguerre, 2022).

La encuesta de EY (Ernst & Young) señala que la falta de mejora en los niveles globales de corrupción empresarial en los últimos seis años muestra que las empresas se mantienen vulnerables a impactos financieros y reputacionales significativos y la reducción del comportamiento antiético en los negocios sigue siendo un gran desafío, pese al incremento de la persecución de estas conductas de mala fe a nivel global (Cárdenas & Joffré, 2018).

En la problemática nacional, la salvaguarda de los secretos empresariales se rige principalmente por la Ley Nº29733, que establece disposiciones para resguardar

la información confidencial, reconociendo su papel crucial en la competitividad empresarial. Empresas de diversos sectores afrontan desafíos en proteger su información ante posibles actos de espionaje, ya sea mediante la infiltración de agentes, obtención no autorizada de documentos o vigilancia electrónica (Astudillo, 2019).

En Perú, la labor fundamental de Indecopi radica en resguardar los secretos empresariales. En términos simples, tiene el poder de intervenir en situaciones donde se violan derechos de propiedad intelectual y se compromete la competencia, especialmente en casos de infracción de secretos empresariales. Particularmente, los esfuerzos del Indecopi han sido reconocidos por distintas entidades y organizaciones extranjeras que persiguen fines similares vinculados a la protección transnacional de los derechos de Propiedad Intelectual. Entre diversas formas desleales, la violación de secretos empresariales experimentó escasas modificaciones en las normativas represivas sobre competencia desleal. De hecho, los cambios que se presentaron fueron únicamente de tipo técnico, es decir, se mejoró su redacción sin alterar su contenido, tal como lo señala el Decreto Legislativo 1044, Ley de Represión de la Competencia Desleal (Barbosa et al., 2021).

En la problemática local, las compañías frecuentemente se encuentran en riesgo de que sus empleados, especialmente aquellos con acceso a datos confidenciales, puedan abandonar la empresa llevándose consigo secretos empresariales o aplicándolos en favor de la competencia (Zermeño et al., 2021). Esto puede incluir información sobre clientes, estrategias comerciales, productos, procesos o datos financieros, si bien en los últimos 12 años Indecopi ha resuelto más de 20 casos denunciados bajo la figura de violación de secretos empresariales, 18 de estos fueron declarados infundados y el único caso fundado no fue por espionaje corporativo. Lo cierto es que los casos denunciados bajo el supuesto de violación de secretos empresariales difícilmente prosperan pues la extracción de la información comercial sensible resulta extremadamente difícil de acreditar y, además, la información a la que se tiene acceso no siempre es considerada confidencial (Valencia, 2023).

Se llevaron a cabo acciones internas sobre espionaje en las empresas residentes en Lima, realizadas por agentes económicos y empleados de confianza. Estos actos fueron considerados como formas atípicas de sabotaje empresarial, causando perjuicios a las empresas. Esto se debe a que al momento de la supervisión

lo hacen de una manera incorrecta en los casos, las personas involucradas no recibieron sanciones y fueron eximidos de los cargos imputados por la Comisión de INDECOPI. Estas decisiones, plasmadas en cuatro resoluciones administrativas controvertidas, destacaron la primacía de la libre competencia sobre los derechos afectados de los empleadores.

Es factible implementar un servicio de seguridad empresarial en Lima Metropolitana, ya que hay un mercado nacional que probablemente respalde y adopte el servicio debido al aumento de la inseguridad ciudadana, además, desde un punto de vista técnico, económico y financiero, la viabilidad del servicio parece estar respaldada (Cristea, 2017).

Así que, se planteó la interrogante principal: ¿Cómo el espionaje empresarial afecta la protección insuficiente del secreto empresarial en Lima, 2023? Igualmente, con el propósito de contribuir a resolver aquella interrogante, se delinearon los problemas específicos: ¿Cómo el espionaje empresarial, está afectando la protección de secretos empresariales? y ¿Cómo fortalecer la protección del secreto empresarial incluyendo estrategias de ciberseguridad, medidas de seguridad y políticas internas en Lima 2023?

Este trabajo de investigación se toma desde la problemática de la insuficiente protección del secreto empresarial emerge como un tema crítico en este contexto. Esta cuestión se centra en las deficiencias en las políticas, prácticas y conciencia empresarial que exponen a las empresas a riesgos significativos de pérdida de información confidencial a manos de competidores, empleados desleales o actores externos.

Este trabajo resalta la importancia al abordar la complejidad y los retos asociados con la administración de secretos empresariales en un contexto donde las amenazas pueden surgir internamente, incluso desde dentro de la propia empresa. Proporcionar recomendaciones prácticas y estrategias para abordar estos riesgos puede ser valioso tanto para las empresas como para la formulación de políticas y regulaciones relacionadas con la protección de secretos empresariales (Santos, 2023).

La relevancia jurídica de esta investigación es que destaca la importancia de abordar las amenazas a los secretos empresariales no solo desde un marco externo, sino también desde el interior de las organizaciones (Aguerre, 2022). Esto tiene implicaciones directas en términos de legislación y regulación relacionada con la

salvaguarda de información confidencial de las empresas. Al resaltar la posibilidad de que los trabajadores internos representan un riesgo para la seguridad de los secretos empresariales, la investigación podría influir en la formulación de políticas y leyes que busquen fortalecer la protección legal de esta información sensible. Podría inspirar cambios en las normativas laborales o en las disposiciones legales que regulan la gestión de secretos empresariales, considerando la necesidad de abordar amenazas internas.

Continuando con el marco teórico, compartiremos las distintas teorías y conceptos relacionados con la investigación científica, incluyendo trabajos previos y destacando los antecedentes pertinentes, especialmente aquellos derivados de tesis tanto nacionales como internacionales. El objetivo es proporcionar respuestas en consonancia con nuestros objetivos de investigación.

Por consiguiente, en los antecedentes internacionales acerca del espionaje empresarial en Alemania tenemos a Pazmiño (2020) en su tesis titulada "Espionaje y competitividad: la industria automotriz alemana en el juego comercial moderno de China" este trabajo tiene como objetivo evidenciar cómo el espionaje corporativo constituye una parte más del juego comercial moderno, particularmente en el contexto de la industria automotriz alemana en China, su metodología es cualitativa la cual cuenta con analizan los principales casos de espionaje chino de la industria alemana, las acciones defensivas emprendidas por Alemania y las estrategias que su industria automotriz prioriza para mantener la competitividad en un entorno de espionaje e incertidumbre, la cual concluye en que el espionaje corporativo se ha posicionado como una variable más del juego de posicionamiento comercial moderno en el mercado chino.

A pesar de que hay inconvenientes las empresas toman su propia decisión y deciden continuar con sus labores. Desde nuestra perspectiva, la investigación analiza las medidas defensivas adoptadas por Alemania, implementando estrategias de su sector automotriz para contrarrestar el riesgo de espionaje y la incertidumbre. Adicionalmente, es importante destacar que el espionaje ha adquirido un papel fundamental en el panorama del mercado chino.

En Venezuela el autor Gómez (2019) en su artículo científico titulado "EL sigilo de la información no divulgada o secretos empresariales con valor competitivo" su metodología fue descriptiva, tiene como objetivo determinar que en cada país deben usar mecanismos de defensa contra quienes vulneren esta barrera y así accedan a

información valiosa considerada como secreto de una empresa. Tras revisar este artículo, destacamos que las empresas perjudicadas tienen la opción de emprender acciones legales para resguardar sus secretos empresariales y buscar compensación por posibles daños en casos de infracción.

Siguiendo con los antecedentes nacionales, en Perú tenemos al autor Pérez (2022) en su artículo científico titulado el “secreto empresarial” utilizó una metodología descriptiva, explicativa, tiene como objetivo detallar que la información debe tener un valor comercial para que sea considerada como secreto de una empresa. Concluye que es una información confidencial que proporciona una ventaja competitiva a otra empresa que está en el mismo rubro. Como comentario, podemos decir que para que se considere dicha información como secreta deben cumplir requisitos formales.

Continuando con los autores León et al. (2022**)** en su artículo “Revisión de los avances y cambios en ciberseguridad en el Perú, para una transformación digital” tienen como objetivo explorar publicaciones donde ha sido tratado el tema de ciberseguridad en el Perú, su metodología es descriptivo exploratorio concluyendo que se presentan varias perspectivas en cuanto a los avances en el tema de ciberseguridad, pasando por la comparación en el área de inversiones en el contexto de Latinoamérica, la situación del Perú respecto a los ataques cibernéticos, la implementación de normas que buscan establecer un ordenamiento tanto para el ámbito estatal como privado. En este entorno, se cuentan con recursos digitales que pueden ser utilizados para preservar la confidencialidad y proteger la integridad de la información.

En Perú el autor García (2022) en su artículo científico titulado “la protección de los secretos empresariales” usó una metodología descriptiva, tiene como objetivo detallar lo importante que es establecer un límite entre la licitud (lo que sí está permitido) e ilicitud (lo no permitido por la ley) de la información que puedan utilizar los ex empleados de una empresa, concluye que los ex empleados deben ser personas inteligentes al no brindar información de una empresa. Es importante que las empresas en Perú tomen medidas para identificar y proteger adecuadamente sus secretos empresariales, así como para conocer y cumplir con las disposiciones legales.

Por otra parte, Cotrina (2020**)** en su tesis titulada “El espionaje corporativo y su incidencia en el funcionamiento interno de las empresas privadas del periodo 2007-2013" donde su objetivo es determinar de qué manera incide el vacío del tipo penal

de espionaje corporativo en el funcionamiento de las empresas privadas fiscalizadas por la comisión de Indecopi de Lima, está cuenta con una metodología cualitativa, descriptiva y no experimental en la cual concluye que el espionaje empresarial incide negativamente en lo que es el funcionamiento internos en las empresas privadas debido a las conductas malas y fraudulentas que son realizadas por trabajadores espías, los empleados y terceras personas que generan daños negativos a la empresa.

Entonces podemos decir que, la carencia de regulación legal-penal para el espionaje corporativo en Perú crea un entorno propicio para que actores deshonestos busquen beneficios económicos mediante el uso no autorizado de información confidencial de empresas y esto no solo amenaza el funcionamiento interno de las compañías privadas en Perú, sino que también perturba su capacidad competitiva y financiera (Viera, 2020).

Respecto a los antecedentes locales Fernández (2018) en su tesis “La violación de un secreto empresarial por un trabajador: un análisis de la jurisprudencia de la sala especializada del Tribunal del INDECOPI sobre represión de la competencia desleal” analiza los secretos empresariales desde la jurisprudencia que ha emitido el INDECOPI con relación a la supuesta comisión de actos de competencia desleal en la modalidad de violación de secretos en Lima. La ley de Represión de la Competencia Desleal fija directrices y procedimientos para prevenir y castigar prácticas que distorsionen o impidan el mantenimiento de una competencia justa en el mercado peruano. INDECOPI acepta denuncias vinculadas a la competencia desleal, permitiendo que las partes afectadas presenten quejas. Después, se realiza una investigación para verificar la presencia de conductas desleales. En caso de confirmarse la existencia de competencia desleal, INDECOPI puede aplicar medidas correctivas y sanciones. Estas medidas abarcan desde la cesación de la práctica desleal hasta la imposición de multas y otras acciones dirigidas a restablecer una competencia justa en el mercado.

Para Quilia (2020) en su tesis titulada “Desafíos en la gestión empresarial de las MyPEs en tiempos de Covid-19, Lima” tuvo como objetivo analizar los desafíos empresariales en las MyPEs en tiempos de Covid-19, Lima, 2020, según los consultores empresariales y empresarios. La gestión empresarial en Lima durante la pandemia del Covid-19 ha enfrentado desafíos notables, exigiendo adaptaciones rápidas para garantizar la continuidad operativa y salvaguardar la seguridad de

empleados y clientes. Las estrategias de comercio electrónico han desempeñado un papel crucial al permitir a las empresas incursionar en el ámbito virtual para llegar a sus clientes. La presencia en la web y la capacidad de realizar transacciones digitales son aspectos cruciales para la viabilidad de cualquier empresa. Es imperativo que las empresas sigan vigilando la situación y ajustando sus estrategias en respuesta a las circunstancias cambiantes.

La autora García (2023) en su tesis titulada “Existe gran controversia como se aplica el secreto empresarial en las empresas de Lima” utilizó una metodología descriptiva, tiene como objetivo determinar que las empresas de Lima la mayoría no saben cómo aplicar o sancionar a los trabajadores que dejan de laborar para una empresa y empiezan a dar información confidencial a una empresa competidora del mismo rubro, concluye que las empresas deben hacerle firmar un contrato de compromiso a los trabajadores antes de entrar a laborar en la empresa. Compartiendo la misma línea de la autora podemos decir que las empresas en la actualidad no saben si es el ex trabajador el que da información confidencial a otra empresa o trabajadores de la misma empresa que se encargan de vender valiosa información.

Siguiendo con las bases teóricas, el espionaje empresarial se enriquece mediante la exploración de diversas teorías y principios. La Teoría del Delito se utiliza como fundamento para analizar si el espionaje cumple con los criterios establecidos para ser catalogado como un delito. La Responsabilidad Penal de las Personas Jurídicas examina la viabilidad de que las empresas asuman responsabilidad penal por actividades de espionaje. Además, los Delitos Económicos y Contra la Propiedad Intelectual sitúan el espionaje empresarial en el marco de los delitos económicos y contra la propiedad intelectual (González, 2024).

Para Ramos (2019) lo relaciona con la teoría de la asociación diferencial, que examina cómo las interacciones sociales influyen en la conducta delictiva, sus ideas podrían aplicarse a la comprensión de las motivaciones detrás del espionaje empresarial.

La salvaguarda de los secretos empresariales se rige principalmente por la Ley Nº29733, que establece disposiciones para resguardar la información confidencial, reconociendo su papel crucial en la competitividad empresarial. Empresas de diversos sectores afrontan desafíos en proteger su información ante posibles actos de espionaje, ya sea mediante la infiltración de agentes, obtención no autorizada de documentos o vigilancia electrónica (Desk, 2019).

En el contexto de la protección del secreto empresarial, Donatello (2020) nos dice que la teoría de la asimetría de información examina cómo la posesión de información valiosa afecta las transacciones comerciales. Asimismo, Espejo y Manuel (2020) exploran cómo las leyes de propiedad intelectual, como patentes y derechos de autor, impactan en la creación y protección del conocimiento en la sociedad de la información.

En el caso de las medidas de protección de secretos empresariales son un conjunto de estrategias y acciones implementadas por una empresa para salvaguardar su información confidencial, que le proporciona una ventaja competitiva en el mercado. Existen 2 medidas para las amenazas internas y externas, en el caso de las amenazas internas las medidas de protección son: Contratos de trabajo, políticas de confidencialidad, procedimientos de empleo, supervisión continua de los empleados. Asimismo, en el caso de las amenazas externas las medidas son: Contratos, aplicar la diligencia debida (Dorneles, 2015).

La presente investigación posee una justificación teórica, puesto que aportará y reforzará conocimientos para futuras investigaciones acerca de la afectación del espionaje empresarial y la protección del secreto empresarial. Asimismo, se presenta una justificación práctica, ya que se pretende que las empresas deseen mejorar sus prácticas de protección de información confidencial al identificar las deficiencias y proponer recomendaciones basadas en la investigación (Gallardo, 2020).

Finalmente, esta investigación tiene una justificación metodológica, toda vez que se contribuirá con aportes a las empresas y comunidad científica en el rubro del derecho corporativo, dado que los instrumentos de recolección de datos son nuevos y servirán como referencia para posteriores estudios relacionados con las categorías bajo investigación. Este trabajo resalta la importancia al abordar la complejidad y los retos asociados con la administración de secretos empresariales en un contexto donde las amenazas pueden surgir internamente, incluso desde dentro de la propia empresa (León, 2018).

En tal sentido, se formuló el objetivo general: Analizar cómo el fenómeno del espionaje empresarial incide en la falta de protección adecuada de los secretos empresariales en Lima durante el año 2023 y como objetivos específicos: Evaluar el impacto del espionaje empresarial en la protección de secretos empresariales y Proporcionar recomendaciones para fortalecer la protección del secreto empresarial.

2. MÉTODO

2.1 Tipo y diseño de la investigación

Este proyecto de tesis, adopta un enfoque cualitativo exploratorio, centrándose en comprender a fondo el impacto del espionaje empresarial y la protección insuficiente del secreto empresarial en Lima durante 2023 (Sanín, 2013). Utilizaremos la entrevista como la principal herramienta para recolectar información. El diseño de investigación se alinea con un enfoque descriptivo cualitativo, buscando describir detalladamente la situación en su contexto natural sin intervención manipulativa (Girona, 2021).

Esta elección me permitirá obtener perspectivas directas y experiencias que revelen de manera integral la dinámica de este fenómeno en el entorno empresarial limeño de 2023. La selección del tipo y diseño de investigación está determinada por el objetivo, la esencia del problema de investigación y los recursos a disposición. Elegir la combinación apropiada es crucial para obtener resultados válidos y significativos (Rodríguez, 2022).

2.2 Escenario de estudio

El estudio se llevará a cabo en el entorno empresarial de Lima a lo largo del año 2023. En este entorno dinámico, me sumergiré en entrevistas con magísteres en Derecho Corporativo, quienes desempeñan un papel clave en el ámbito legal y empresarial (Fernández, 2018).

Este escenario limeño del 2023 proporcionará el contexto necesario para explorar en detalle el impacto del espionaje empresarial y la protección insuficiente del secreto empresarial. La intersección entre la experticia legal de los Magísteres y las complejidades del entorno empresarial en Lima será esencial para obtener una comprensión integral de la problemática en investigación. El ámbito de investigación se relaciona con el entorno o contexto en el que se realiza el estudio. Este escenario proporciona el marco dentro del cual se recopilan datos, se realizan observaciones y se llevan a cabo análisis.

2.3 Hipótesis

Se plantea la hipótesis de que, en Lima, durante el año 2023, el impacto del espionaje empresarial está estrechamente ligado a la falta de protección adecuada del secreto empresarial. Se espera demostrar que proporcionar recomendaciones específicas a las empresas para fortalecer la seguridad de sus secretos

empresariales, a través de estrategias de ciberseguridad y políticas internas, contribuirá a mitigar los riesgos asociados al espionaje.

Asimismo, se anticipa que, al examinar y explicar las medidas de prevención del espionaje empresarial implementadas por las empresas en Lima en 2023, se obtendrán insights fundamentales para comprender y abordar esta problemática de manera más efectiva. Es importante tener en cuenta que una hipótesis debe ser específica, falsificable y testable. Además, puede haber una hipótesis nula que afirma la ausencia de relación entre las variables o que no haya efecto. Durante el proceso de investigación, los datos recopilados se utilizan para para aceptar o rechazar la hipótesis nula, lo que contribuye a la comprensión del fenómeno estudiado (Ruíz, 2020).

2.4 Participantes

Los participantes clave de esta investigación serán Magísteres en Derecho Corporativo que estén inmersos en el entorno empresarial de Lima durante el año 2023. Estos profesionales expertos ofrecerán una perspectiva valiosa sobre cómo el espionaje empresarial y la insuficiente protección del secreto empresarial impactan en los ámbitos legal y corporativo (Sini, 2012). Sus experiencias y conocimientos especializados resultan esenciales para abordar las complejidades de la seguridad de la información empresarial en este contexto particular. Seleccionar adecuadamente a los entrevistados contribuye de manera importante a la validez y confiabilidad de los resultados de una investigación. Asegúrense de documentar detalladamente el proceso de selección y cualquier desafío encontrado durante la investigación (Alexis, 2020).

2.5 Técnicas e instrumentos de recolección de información

En la investigación, se empleó entrevistas en profundidad como el principal instrumento de recolección de datos. Nos centramos en Magísteres en Derecho Corporativo que están activos en el entorno empresarial de Lima. A través de estas entrevistas, nuestro objetivo es obtener una comprensión profunda de las perspectivas actuales en cuanto al impacto del espionaje empresarial y la falta de protección del secreto empresarial (Herrero, 2023).

Adicionalmente, realizamos un análisis documental en tiempo real de políticas internas, estrategias de ciberseguridad y otros documentos relevantes proporcionados por las empresas participantes. La combinación de entrevistas y

análisis documental que estamos utilizando en este momento nos permite capturar de manera precisa la dinámica actual en el ámbito empresarial y legal vinculada a la seguridad de la información en Lima. La selección de la técnica y el instrumento para recopilar datos debe estar en sintonía con los objetivos de la investigación y la naturaleza de las variables que se están estudiando. Además, la validez y la confiabilidad de los instrumentos son aspectos críticos a considerar en el diseño de la investigación (De Dret, 2015).

2.6 Procedimiento

El procedimiento de la investigación sigue un enfoque meticuloso. En primer lugar, identificamos y seleccionamos a los Magísteres en Derecho Corporativo activos en el entorno empresarial de Lima como participantes clave (Pazmiño, 2020). Luego, llevamos a cabo entrevistas en profundidad con cada uno de ellos para explorar sus perspectivas sobre el impacto del espionaje empresarial y la protección insuficiente del secreto empresarial (Lezama, 2023). Simultáneamente, realizamos un análisis documental en tiempo real, examinando políticas internas, estrategias de ciberseguridad y otros documentos proporcionados por las empresas participantes. Esta unión nos permite adquirir información detallada y actualizada sobre la dinámica empresarial y legal relacionada con la seguridad de la información en Lima.

El proceso de recopilación de datos está en marcha y nos aseguramos de mantener un enfoque ético y respetuoso durante las entrevistas, garantizando la confidencialidad de la información recopilada y cumpliendo con los protocolos éticos de investigación. Los procedimientos son fundamentales para velar por la excelencia y coherencia en la investigación. Un diseño y ejecución meticulosos de los procedimientos contribuyen a la validez interna y externa de los resultados, así como a la posibilidad de replicación por otros investigadores (Gómez, 2019).

2.7 Análisis de datos

Durante la fase de análisis de datos para nuestra investigación, estamos adoptando un enfoque minucioso. Después de transcribir detalladamente las entrevistas con los Magísteres en Derecho Corporativo, aplicamos un análisis de contenido para descubrir patrones, temas recurrentes y perspectivas clave. Paralelamente, el análisis documental se centra en examinar a fondo las políticas internas y estrategias de ciberseguridad proporcionadas por las empresas participantes. Utilizamos técnicas cualitativas para extraer información relevante y contextualizarla en el contexto de la protección del secreto empresarial y la

prevención del espionaje (Schulz, 2023). Este proceso de análisis es continuo, con una atención constante a la fiabilidad y validez de los resultados. La triangulación de datos provenientes de entrevistas y análisis documental fortalece la robustez de nuestras conclusiones, brindando una comprensión completa y contextualizada de la problemática que estamos investigando. El análisis de datos representa una etapa crucial en la investigación, Contribuyendo a la generación de conocimiento y a la toma de decisiones basada en información.

2.8 Aspectos éticos

En nuestra investigación, nos comprometemos de manera sólida con normas éticas para asegurar la integridad y el respeto hacia nuestros partícipes, así como la credibilidad de nuestros hallazgos (De Pitta, 2021). Antes de iniciar las entrevistas, suministramos detalles acerca del propósito de la investigación y solicitamos la aprobación informada de los Magísteres en Derecho Corporativo.

Aseguramos la reserva de información obtenida mediante la asignación de códigos anónimos a los participantes y protegiendo sus identidades. En el análisis de datos, mantenemos un enfoque ético al honrar la privacidad y confidencialidad de la información sensible proporcionada por las empresas participantes en el análisis documental (Ganz et al., 2020).

Cualquier información identificable se maneja con la debida discreción y se presenta de manera agregada y anónima en los informes finales. Además, cumplimos rigurosamente con los protocolos éticos de investigación y estamos abiertos a la retroalimentación de los participantes en cualquier etapa del proceso. Nos comprometemos a realizar la investigación de forma ética y responsable, garantizando el respeto a los derechos y la dignidad de todos los involucrados. Los aspectos éticos en la investigación son principios y normas que guían la conducta ética de los investigadores y protegen los derechos, bienestar y dignidad de los participantes humanos involucrados en el estudio (Antoni, 2017).

3. RESULTADOS

Tabla 1

Matriz de triangulación 1

Entrevistado(a)	Pregunta 1.- ¿Cómo afecta el espionaje empresarial a la protección de la propiedad intelectual en las empresas de Lima?
Dr. Gerardo Manuel Aybar Izaguirre	En el Perú, la libertad de empresa y la protección de la propiedad intelectual son fundamentales según la legislación, aunque el espionaje empresarial puede dañar la reputación y economía de las empresas, destacando la necesidad de medidas de protección efectivas.
Dr. Moises Huaman Picchuaman	La protección de la información empresarial es crucial, ya que las empresas desarrollan datos, actividades y procesos para lograr mayor productividad.
Dra. Pamela Avalos Farfan	El espionaje empresarial afecta a las empresas causando daños económicos, deterioro de la reputación y pérdida de información confidencial, ya que los competidores pueden utilizar estos datos para superarlas.
Dr. Martin Vicente Tovar Cerquen	El espionaje empresarial revela una debilidad legal en Perú, reflejada en los expedientes de Indecopi, y no aborda adecuadamente las necesidades de las empresas.
Dr. Alexander Solorzano Maguiña	El espionaje empresarial afecta negativamente a las empresas al permitir que los competidores conozcan su producción y estrategias, usando recursos para superarlas.

Interpretación: Todos los entrevistados coinciden en que el espionaje empresarial causa un perjuicio económico significativo y daña la reputación de las empresas.

Tabla 2

Matriz de triangulación 2

Entrevistado(a)	Pregunta 2.- ¿Qué papel cree que debe desempeñar INDECOPI en la prevención del espionaje empresarial para proteger la propiedad intelectual?
Dr. Gerardo Manuel Aybar Izaguirre	Indecopi debe cumplir su mandato según la Comisión Política del Perú para tomar acciones administrativas y sancionar a las empresas que incurran en espionaje, protegiendo así a otras empresas de perjuicios económicos por robo o pérdida de información.

Dr. Moises Huaman Picchuaman	La propiedad intelectual es protegida por Indecopi, que inscribe secretos industriales y comerciales, supervisa y sanciona a las empresas que incumplen las normativas vigentes para asegurar la protección nacional de la información trascendental de las empresas.
Dra. Pamela Avalos Farfan	Indecopi debe sancionar a las empresas o personas que vulneren derechos de propiedad intelectual, ya que es el organismo regulador encargado de garantizar su protección y el cumplimiento de las normativas vigentes.
Dr. Martin Vicente Tovar Cerquen	Hoy en día, las sentencias de Indecopi muestran una vulnerabilidad para los trabajadores de las empresas, revelando que la falta de una correlación normativa penal adecuado deja a Indecopi en un desamparo total, lo que impide una sanción clara y efectiva.
Dr. Alexander Solorzano Maguiña	El espionaje empresarial es una infracción que merece sanción, y la función de Indecopi es verificar y sancionar tanto a las empresas que realizan espionaje como a las que las contratan para llevarlo a cabo.

Interpretación: En Perú, Indecopi cumple un rol clave en la lucha contra el espionaje empresarial, pero su efectividad se ve limitada por la falta de medidas legales claras, lo que debilita su capacidad para sancionar adecuadamente estas conductas.

Tabla 3

Matriz de triangulación 3

Entrevistado(a)	Pregunta 3.- ¿Cuáles son las principales vulnerabilidades en la protección de la información confidencial que han observado en las empresas de Lima?
Dr. Gerardo Manuel Aybar Izaguirre	Existe una debilidad legal debido a la ausencia de acuerdos de confidencialidad y sanciones claras, lo que deja desprotegida la información empresarial frente a posibles filtraciones.
Dr. Moises Huaman Picchuaman	Con el auge de la digitalización, las empresas almacenan información en archivos digitales y servidores, lo que las expone a piratas informáticos y riesgos de seguridad jurídica, por lo que deben utilizar herramientas legales y tecnológicas para controlar estos riesgos.
Dra. Pamela Avalos Farfan	La escasa aplicación de acuerdos de confidencialidad y la debilidad en la seguridad digital exponen a las empresas a riesgos, por lo que se requiere reforzar tanto las medidas legales como tecnológicas para proteger la información.

Dr. Martin Vicente Tovar Cerquen	El espionaje empresarial y los contratos atípicos reflejan la realidad actual de las cláusulas de confidencialidad para los trabajadores; el sabotaje empresarial y las ventajas competitivas a través de estas prácticas pueden afectar el patrimonio de las personas jurídicas en el sector privado.
Dr. Alexander Solorzano Maguiña	Las principales vulnerabilidades en las empresas objeto de espionaje incluyen la falta de medidas de seguridad y la falta de conciencia sobre el riesgo de ser espiadas; muchas empresas no integran estas preocupaciones en sus políticas empresariales, lo que las deja expuestas.

Interpretación: En las empresas de Lima, la información confidencial está en riesgo principalmente por la falta de acuerdos de confidencialidad sólidos, sanciones insuficientes y vulnerabilidades en los sistemas digitales.

Tabla 4

Matriz de triangulación 4

Entrevistado(a)	Pregunta 4.- ¿Qué sistemas informáticos y/o software recomienda implementar para fortalecer la seguridad de la información confidencial frente al espionaje empresarial?
Dr. Gerardo Manuel Aybar Izaguirre	Se deben adquirir todos los software y equipos tecnológicos necesarios para proteger a las empresas contra virus, malware y ataques cibernéticos, evitando así vulneraciones de información que puedan causar perjuicios económicos a la sociedad.
Dr. Moises Huaman Picchuaman	La protección de la información sensible en las empresas no solo depende de la normativa vigente, sino también de medidas internas como los acuerdos de confidencialidad y restricciones al uso de dispositivos externos como USBs.
Dra. Pamela Avalos Farfan	Para evitar la pérdida de información sensible, las empresas deben aplicar medidas como instalar dispositivos de vigilancia, restringir la impresión de documentos confidenciales y reforzar los acuerdos de confidencialidad junto con herramientas de seguridad.
Dr. Martin Vicente Tovar Cerquen	Actualmente no existe un software perfecto para la seguridad empresarial, pero la inteligencia artificial y la adopción de tecnologías de otros países pueden ayudar a reducir las vulnerabilidades.

Dr. Alexander Solorzano Maguiña	La implementación de medidas de seguridad debe estar a cargo de expertos en informática, quienes pueden establecer sistemas de protección adecuados; sin embargo, es fundamental que las empresas busquen fortalecer sus sistemas con herramientas seguras y personal capacitado.

Interpretación: Para fortalecer la seguridad frente al espionaje empresarial en Lima, las empresas deben implementar herramientas tecnológicas y medidas de protección, contando con el apoyo de expertos en informática para su correcta aplicación.

Tabla 5

Matriz de triangulación 5

Entrevistado(a)	Pregunta 5.- ¿Considera que Indecopi sanciona eficazmente a las personas y/o empresas que acceden ilícitamente a información empresarial confidencial?
Dr. Gerardo Manuel Aybar Izaguirre	Indecopi actualmente no tiene la capacidad para sancionar eficazmente a las empresas que incurren en espionaje, ya que están más concentrados en sancionar a las grandes empresas y en cuestiones que afectan económicamente al desarrollo del país.
Dr. Moises Huaman Picchuaman	Indecopi sigue un proceso formal para sancionar el espionaje empresarial, que incluye investigación, defensa y multas elevadas, en línea con la política estatal de proteger a las empresas y el desarrollo económico del país.
Dra. Pamela Avalos Farfan	Indecopi, a través de sus multas, busca sancionar las conductas de espionaje empresarial, pero considero que no todas las empresas denuncian estos actos ilícitos, lo que limita la efectividad de sus sanciones.
Dr. Martin Vicente Tovar Cerquen	En las lecturas sobre Indecopi he observado una vulnerabilidad en su labor para proteger la información sensible de las personas jurídicas, ya que no existe una labor eficaz para sancionar a quienes utilizan ilegalmente dicha información.
Dr. Alexander Solorzano Maguiña	Se critica a Indecopi por no cumplir eficazmente con su rol de sancionar el espionaje empresarial, señalando que el organismo no está funcionando adecuadamente para proteger a las empresas de conductas desleales.

Interpretación: Se critica a Indecopi por su falta de capacidad para sancionar

eficazmente el espionaje empresarial, debido a su enfoque en grandes empresas y la escasez de denuncias.

Tabla 6

Matriz de triangulación 6

Entrevistado(a)	Pregunta 6.- ¿Cuáles son las modalidades más utilizadas para acceder ilícitamente a información empresarial confidencial de las empresas de Lima?
Dr. Gerardo Manuel Aybar Izaguirre	Los hackers venden información empresarial en mercados negros como en el centro de Lima (Wilson), y la transgresión de acuerdos de confidencialidad por trabajadores agrava la exposición de información sensible, aumentando los riesgos para las empresas.
Dr. Moises Huaman Picchuaman	El espionaje empresarial incluye el hackeo de información sensible y la compra ilícita de bases de datos, y las empresas deben invertir en proteger su conocimiento y métodos, dada su alta inversión en la producción de esta información.
Dra. Pamela Avalos Farfan	El espionaje empresarial se manifiesta en la vulneración de convenios de confidencialidad y el robo de información mediante hackers; por ello, las empresas deben implementar medidas de seguridad
Dr. Martin Vicente Tovar Cerquen	La falta de una legislación penal clara sobre espionaje corporativo, especialmente en contratos atípicos como los del Estado, puede facilitar el acceso ilegal a información secreta.
Dr. Alexander Solorzano Maguiña	El espionaje empresarial puede adoptar formas materiales, como infiltrar a una persona para obtener información a través de empleados, o digitales, como el hackeo por parte de hackers.

Interpretación: Es esencial fortalecer los acuerdos de confidencialidad, mejorar las medidas de seguridad tecnológica, y abordar las lagunas legales que facilitan el acceso ilícito a información confidencial.

Tabla 7

Matriz de triangulación 7

Entrevistado(a)	Pregunta 7.- ¿Qué incentivos económicos se podrían implementar para que las empresas no compitan deslealmente mediante actos de espionaje empresarial?
Dr. Gerardo Manuel Aybar Izaguirre	Se sugiere implementar incentivos económicos para denuncias de espionaje empresarial, aplicar sanciones como multas y establecer un registro de infractores.

Dr. Moises Huaman Picchuaman	Se debería considerar que Indecopi endurezca las sanciones para las empresas que incurran en espionaje, promoviendo la protección de información sensible; además, las sanciones podrían extenderse al ámbito penal para asegurar el cumplimiento de las normativas.
Dra. Pamela Avalos Farfan	Para reducir las conductas anticompetitivas en las empresas, se deben aplicar mayores sanciones; endurecer las multas y considerar sanciones penales pueden ser estrategias efectivas para disminuir el espionaje empresarial y promover la competencia justa en el mercado.
Dr. Martin Vicente Tovar Cerquen	En el sector público existen incentivos económicos para quienes denuncian actos ilícitos, pero no en el sector privado. Se sugiere la creación de incentivos económicos en este sector para reducir el espionaje empresarial y promover una competencia justa.
Dr. Alexander Solorzano Maguiña	La falta de una política estatal efectiva para enfrentar la competencia desleal por espionaje y la insuficiencia de acciones de Indecopi han permitido que pocas empresas sean sancionadas por contratar espías, a pesar de la prevalencia de esta práctica.

Interpretación: Aunque existe un consenso sobre la necesidad de sanciones más rigurosas y medidas para fomentar las denuncias, hay diferencias en las propuestas específicas para lograr estos objetivos y en la evaluación de la efectividad actual de las políticas y prácticas de Indecopi.

Tabla 8

Matriz de triangulación 8

Entrevistado(a)	Pregunta 8.- ¿Cuáles son los principales retos que enfrentan las empresas en Lima para proteger sus secretos empresariales frente al espionaje empresarial?
Dr. Gerardo Manuel Aybar Izaguirre	Las empresas deberían implementar una política efectiva de protección de datos que incluya la compra de software adecuado, sistemas en la nube con encriptación y una custodia rigurosa de los datos, para evitar vulneraciones que puedan afectar su economía y reputación.
Dr. Moises Huaman Picchuaman	Las empresas deben instalar sistemas de seguridad digital y firmar contratos de confidencialidad con sus empleados para proteger información sensible. Estas medidas deben adaptarse al sector de la empresa para evitar vulneraciones que afecten su economía y reputación.

Dra. Pamela Avalos Farfan	Es fundamental que las empresas firmen acuerdos de confidencialidad sólidos y adopten políticas adecuadas para el manejo de datos, personalizadas según su sector, para proteger la información sensible y evitar daños económicos y reputacionales.
Dr. Martin Vicente Tovar Cerquen	Para gestionar el espionaje empresarial, es crucial hacer un análisis de pérdidas económicas tanto cuantitativo como cualitativo, establecer un registro de estas pérdidas, y colaborar para crear normas penales efectivas y evaluar los resultados mediante los expedientes de Indecopi.
Dr. Alexander Solorzano Maguiña	Las empresas deben ser conscientes de que el espionaje es una guerra comercial y deben proteger su know-how, producción y políticas de inversión. Para ello, es fundamental fidelizar al personal y establecer acuerdos de confidencialidad sólidos.

Interpretación: Aunque hay consenso en la necesidad de medidas de protección de datos y acuerdos de confidencialidad, también hay diferencias en el enfoque de las soluciones, abarcando desde la seguridad digital hasta el desarrollo de normativas legales más robustas.

4. DISCUSIÓN

En contraste con la matriz de triangulación Nº1, se demuestra que los entrevistados 1,2,3,4 tienen una postura a favor indicando que el espionaje empresarial afecta en diferentes aspectos principalmente en lo económico ya que disminuye ingresos a las empresas esto es debido a que las empresas invierten dinero, tiempo en estos secretos empresariales. Mientras que el entrevistado 5 indica que el espionaje mayormente se da por los hackers, utilizando medios electrónicos de esa manera obtienen información. Al proteger la información confidencial, las compañías pueden mantener su ventaja competitiva y asegurar su posición en el mercado (Rubio, 2018). Asimismo, coinciden que mayormente se ve en que estos casos de espionaje se dan mediante un empleado o ex empleado de la empresa al divulgar información valiosa.

Así como mencionamos anteriormente sobre un estudio que fue realizado por el autor Acuña (2018) quien indica que la violación de un secreto empresarial por parte de un trabajador es una infracción grave que puede tener consecuencias significativas tanto para el empleado como para la empresa. Los secretos empresariales incluyen información confidencial, como estrategias comerciales, listas de clientes, fórmulas de productos, planes de marketing y cualquier otro tipo de conocimiento que brinde una ventaja competitiva a la empresa.

De acuerdo a la Matriz de Triangulación Nº2 donde todos los entrevistados coinciden en que la propiedad intelectual es vulnerada de manera muy factible y peor que las sanciones no son bien aplicadas por Indecopi, dentro de esta entidad está la Comisión de Competencia Desleal que se encarga de recibir los casos, indicando que Indecopi debe mejorar su sanción y hacerla cumplir para empresas y personas naturales ya que de esa manera se pueden establecer antecedentes en el sistema legal peruano. En la misma línea hemos mencionado sobre un estudio realizado por el autor García (2020) indicando que actualmente se ve muy factible en las empresas que vulneran su información confidencial mediante el espionaje empresarial por eso el da opciones que pueden fortalecer el sistema de seguridad y de esa manera se van a disminuir casos de espionaje empresarial. También indica que de la manera como lo protegen y lo sancionan en el Perú es muy sencillo, las sanciones deben ser drásticas para las personas que cometen o vulneren la propiedad intelectual, secreto empresarial, entre otra información valiosa de una empresa.

En contraste con la Matriz de Triangulación Nº4 todos los entrevistados coinciden con la idea de perfeccionar los acuerdos de confidencialidad entre el empleador y empleado, implementar todos los softwares, webcam, micrófonos, prohibir la impresión de documentos confidenciales al momento de implementar todo lo mencionado se va a proteger mejor la información confidencial de las empresas y así va a disminuir casos de espionaje empresarial (Muñoz, 2020).

En un estudio realizado por los autores León et al. (2022) indican que la ciberseguridad en el contexto de espionaje empresarial ha cobrado una importancia crítica en Perú, debido al aumento de la sofisticación y frecuencia de los ciberataques. Si hay avances de ciberseguridad en el Perú, primeramente, el fortalecimiento de la legislación de la Ley de Protección de Datos Personales para incluir medidas específicas contra el acceso no autorizado a la información corporativa. El gobierno peruano ha lanzado varias iniciativas para mejorar la ciberseguridad a nivel nacional. Estas incluyen la creación del Centro Nacional de Seguridad Digital (CNSD), cuyo objetivo es coordinar las políticas de ciberseguridad y ofrecer apoyo técnico a las instituciones públicas y privadas.

En contraste con la Matriz de Triangulación Nº6 los entrevistados 1,2,3,5 comparten que debe darse una correcta política de protección de los datos de la empresa, datos personales, tener seguridad digital, acuerdos de confidencialidad de esa manera brindar seguridad a la información confidencial de la empresa. Mientras que el entrevistado 4 prioriza las diferencias en el ámbito público y privado como se da el espionaje empresarial menciona ejemplos donde nos absuelve la duda de la mejor manera (Pospichil et al., 2020).

Asimismo, menciona que tenemos un vacío de tipo penal sobre el espionaje corporativo. De acuerdo a lo detallado hasta el momento no podemos dejar de lado que el Decreto Supremo Nº030-2019 facilita la comprensión y aplicación de la ley tanto para las autoridades como para las empresas (Pereira et al., 2020). Esto contribuye a una mayor transparencia y previsibilidad en la regulación de las conductas anticompetitivas. El Decreto establece un régimen de sanciones que incluye multas significativas y medidas correctivas para las empresas que infrinjan la ley. Esto actúa como un disuasivo poderoso contra la realización de prácticas anticompetitivas y garantiza que las infracciones sean adecuadamente penalizadas. Sin olvidar de mencionar a la Teoría de la Asimetría de Información es una teoría fundamental que ayuda a explicar las dinámicas e ineficiencias de los mercados.

Comprenderla es crucial para el diseño de políticas y mecanismos que promuevan mercados más justos y eficientes.

Finalmente, el Código Penal Peruano establece sanciones claras y específicas para el espionaje empresarial, reflejando la gravedad de este delito y su impacto potencial en la economía y la competitividad del mercado, pero en la realidad no son bien aplicadas en el sistema peruano debe haber una cooperación mutua para que se pueda sancionar correctamente (Payan, 2011).

Las penas incluyen tanto la privación de libertad como multas económicas, con la intención de disuadir a los potenciales infractores y proteger los secretos empresariales de las empresas. La sanción de delitos como el espionaje empresarial por parte de Indecopi es un tema complejo debido a ciertas razones (Naoui et al., 2020). La legislación que se aplica a los delitos de espionaje puede no estar completamente detallada es por ello que se dificulta la persecución y sanción adecuada de estos delitos. Reunir pruebas contundentes que demuestren la comisión del delito y la responsabilidad de las partes involucradas es un desafío significativo. En algunos casos, puede haber presiones políticas y económicas que influyan en la capacidad de Indecopi para sancionar a los infractores (Nasheri, 2004). Las empresas poderosas pueden tener influencia que dificulte la aplicación de sanciones.

5. CONCLUSIONES

Primero. - El fenómeno del espionaje empresarial en Lima en el año 2023 representa una seria amenaza para la protección del secreto empresarial. La falta de medidas adecuadas de protección expone a las empresas a riesgos significativos, tanto internos como externos, que pueden comprometer la confidencialidad y la competitividad en el mercado.

Segundo. - El espionaje empresarial afecta directamente la protección de los secretos empresariales al facilitar el acceso no autorizado a información estratégica. Esta vulnerabilidad pone en riesgo la seguridad y sostenibilidad de las empresas en Lima, ya que la información confidencial es un activo invaluable que puede determinar el éxito o fracaso en el mercado.

Tercero. - La implementación de estrategias de ciberseguridad, medidas de seguridad y políticas internas de protección de datos se presenta como una solución clave para fortalecer la seguridad de los secretos empresariales y reducir el riesgo de espionaje empresarial. Estas medidas preventivas son esenciales para garantizar la integridad de la información confidencial de las empresas en un entorno empresarial cada vez más digitalizado y competitivo. Los hallazgos de la investigación resaltaron la importancia de adoptar medidas preventivas para garantizar la integridad de la información confidencial en un entorno empresarial digitalizado y competitivo.

Cuarto. - La investigación ha logrado analizar de manera exhaustiva cómo el fenómeno del espionaje empresarial incide en la falta de protección adecuada de los secretos empresariales en el contexto empresarial de Lima en el año 2023. Este análisis ha permitido comprender la magnitud de la amenaza y la importancia de abordarla de manera proactiva.

6. RECOMENDACIONES

Primero. - Considerar cómo los hallazgos de la investigación pueden inspirar cambios en las normativas laborales, en las disposiciones legales relacionadas con la gestión de secretos empresariales y en la promoción de prácticas éticas en el ámbito empresarial.

S**egundo. -** Considerar la posibilidad de adoptar un enfoque interdisciplinario que combine conocimientos de áreas como derecho, tecnología, ética empresarial y seguridad informática para abordar de manera integral el tema del espionaje empresarial.

Tercero. - Considerar la importancia de divulgar los resultados de la investigación de manera accesible y comprensible para diferentes audiencias, incluyendo empresas, académicos, autoridades gubernamentales y la sociedad en general.

Cuarto. - Reflexionar sobre el impacto social y económico del espionaje empresarial en la comunidad empresarial local y proponer acciones concretas para sensibilizar y prevenir esta práctica.

Quinto. - Mantenerse actualizado sobre las tendencias y desarrollos en el campo del espionaje empresarial y la protección del secreto empresarial, ya que es un tema en constante evolución que requiere adaptación continua.

REFERENCIAS

Acuña, T. (2018). El secreto empresarial como herramienta de valor para la competitividad y la innovación. *Revista Suma de Negocios, 10*(21), 17-24. https://www.redalyc.org/journal/6099/609964310003/

Aguerre, L. (2022). *La protección jurídica del secreto empresarial: Un estudio comparado entre las legislaciones española y uruguaya* [Tesis de pregrado, Universidad de Piura]. Repositorio de la Universidad de Piura. https://pirhua.udep.edu.pe/

Aguerre, L. (2022). *La protección jurídica del secreto empresarial* [Tesis de maestría, Universidad Pompeu Fabra]. Repositorio de la Universidad Pompeu Fabra https://repositori.upf.edu/bitstream/handle/10230/54212/TFMDret2022AguerreProtec.pdf?sequence=1&isAllowed=y

Alexis, N. (2020). *Desafíos en la gestión empresarial de las MYPeS en tiempos de COVID-19, Perú* [Tesis de maestría, Universidad César Vallejo]. Repositorio de la Universidad César Vallejo. https://repositorio.ucv.edu.pe/handle/20.500.12692/48291

Aliaga, A. (2019). *La incidencia de los delitos informáticos en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022* [Tesis de pregrado, Universidad Peruana de las Américas]. Repositorio de la Universidad Peruana de las Américas. http://repositorio.ulasamericas.edu.pe/bitstream/handle/upa/1127/ALIAGA%20SWIDIN.pdf?sequence=1&isAllowed=y

Antoni, G. P. (2017). *El delito de acceso ilícito a un sistema informático.* (2° ed.). Dialnet.

Astudillo, F. (2019). El sigilo de la información no divulgada o secretos empresariales con valor competitivo. *Anuario Dominicano de Propiedad Intelectual, 5*(6), 17–40. https://dialnet.unirioja.es/servlet/articulo?codigo=8270009

Barbosa, F., De Oliveira, J., Nascimento, J., & De Almeida, F. (2021). Corporate governance, dynamic capabilities and business performance in companies listed in brasil, bolsa, balcão s/a (B3 S/A). *Revista de Administracao de USFM, 1*(14), 182-201. https://www.redalyc.org/journal/2734/273467496010/

Cárdenas, P., & Joffré, L. (2018). *Estudio de prefactibilidad de una empresa de seguridad en Lima Metropolitana* [Tesis de pregrado, Universidad de Lima]. Repositorio de la Universidad de Lima.

https://repositorio.ulima.edu.pe/bitstream/handle/20.500.12724/7475/C%C3%A1rde

Cotrina, R. (2020). *El espionaje corporativo y su incidencia en el funcionamiento interno de las empresas privadas del periodo 2007-2013* [Tesis de pregrado, Universidad Privada del Norte]. Repositorio de la Universidad Privada del Norte. https://goo.su/UZzvO

Cristea, L. (2017). *La protección de datos de carácter sensible en el ámbito europeo* [Tesis doctoral, Universitat Abat Oliba]. Repositorio de la Universitat Abat Oliba. https://www.tdx.cat/bitstream/handle/10803/442972/Tlcu.pdf?sequence=1

De Dret, U. (2015). *Dogmática jurídica de los delitos de violación de secreto empresarial* [Tesis de pregrado, Universitat Pompeu Fabra]. Repositorio de la http://hdl.handle.net/10803/323082. http://hdl.handle.net/10803/323082

De Pitta, P. (2021). *O segredo comercial e a sua relevância jurídica no domínio comercial contemporáneo* [Tesis de pregrado, Universidade Católica Portuguesa]. Repositorio de la Universidades Católica Portuguesa. https://repositorio.ucp.pt/handle/10400.14/36333

Desk, S. (2019, 13 enero). China refuerza las leyes de propiedad intelectual para protegar las marcas. *China Briefing News*. https://www.china-briefing.com/news/china-refuerza-las-leyes-de-propiedad-intelectual-para-proteger-marcas-y-secretos-comerciales/

Dorneles, R. (2015). *Capacitación de las fuerzas armadas en ciberseguridad para la seguridad, defensa y desarrollo del estado plurinacional de Bolivia* [Tesis de pregrado, Universidad Militar]. Repositorio de la Universidad Militar. https://bdex.eb.mil.br/jspui/bitstream/1/1015/1/TESE_DORNELES.pdf

Donatello, L., Galán, V., & Velisone, J. (2020). Deinstitutionalization of beliefs and Corporate Social Responsibility: Between neo-Pentecostalism and spirituality. *Revista de Cesla, 13*(26), 1-19. https://www.redalyc.org/journal/2433/243364810021/

Espejo, D., & Manuel, C. (2020). *La violación de un secreto empresarial por un trabajador: Un análisis de la jurisprudencia de la Sala Especializada del Tribunal del INDECOPI sobre Represión de la competencia desleal* [Tesis de pregrado, Universidad de Piura]. Repositorio de la Universidad de Piura. https://hdl.handle.net/11042/4529

Fernández, C. (2018). La amenaza de las nuevas tecnologías en los negocios: El ciber espionaje empresarial. *Revista de Derecho, 14*(13), 1-42. https://revistas.uned.es/index.php/RDUNED/article/view/24001/19054

Fernández, C. (2018). El delito de daños y el espionaje empresarial: Dos ataques compatibles contra la información como bien inmaterial. *Revista de Derecho, 5*(6), 13-43. https://indret.com/wp-content/uploads/2020/05/1352b.pdf

Gallardo, A. (2020). *Innovaciones en la tipificación de delitos con la ratificación del convenio contra el cibercrimen, en el Perú el año 2019* [Tesis de pregrado, Universidad Científica del Perú]. Repositorio de la Universidad Científica del Perú.http://repositorio.ucp.edu.pe/bitstream/handle/UCP/984/GALLARDO_DER_TESIS_TITULO_2020.pdf?sequence=1

Ganz, A., Schlotefeldt, J., & Rodrigues, M., (2020). *Corporate governance and capital asset pricing models* [Tesis de pregrado, Universidad Privada RBE]. Repositorio de la Universidad Privada RBE. https://www.redalyc.org/journal/1954/195463513004/

García, J. (2020). *Vigilancia tecnológica por big data de patentes y espionaje industrial* [Tesis de maestría, Universidad Pontificia Comillas]. Repositorio de la Universidad Pontificia Comillas. https://goo.su/temp3r

García, M. (2022). La Protección de los secretos empresariales en el régimen andino. *Revista de Ciencias Sociales y Humanas, 22*(43), 1-20. http://www.scielo.org.co/scielo.php?pid=S1657-89532022000200208&script=sci_arttext

García, S. (2023). *Acceso a la información financiera protegida por el secreto bancario y transparencia financiera del estado peruano* [Tesis doctoral, Universidad San Ignacio de Loyola]. Repositorio de la Universidad San Ignacio de Loyola. .https://repositorio.usil.edu.pe/server/api/core/bitstreams/bc3aa711-63b2-46f6-8ce1-2e87afa8dc9c/content

Girona, R. M. (2021). *Las acciones civiles en defensa del secreto empresarial* [Tesis doctoral, Universitat de València]. Repositorio de la Universitat de València. https://dialnet.unirioja.es/servlet/tesis?codigo=308721

Gómez, F. (2019). El sigilo de la información no divulgada o secretos empresariales con valor competitivo. *Revista Dialnet, 6*(10), 1-24. https://dialnet.unirioja.es/servlet/articulo?codigo=8270009

González, D. (2024). *Los secretos empresariales y la Ley 1/2019, de 20 de febrero* [Trabajo de pregrado, Universidad de Oviedo]. Repositorio de la Universidad de Oviedo. https://digibuo.uniovi.es/dspace/handle/10651/71733

Herrero, P. (2023). Von Bismarck y su ¿predicción? sobre la compraventa de los secretos empresariales. *Revista Práctica de Derecho, 5*(10), 5-30. https://doi.org/10.51302/ceflegal.2023.18843

León, P. (2018). *La propiedad intelectual y el incremento en la exportación: departamento de Junín 2016* [Tesis de pregrado, Universidad Alas Peruanas]. Repositorio de la Universidad Alas Peruanas. https://repositorio.uap.edu.pe/jspui/bitstream/20.500.12990/6633/1/Tesis_propiedad%20intelectual_incremento_exportaci%C3%B3n_departamento%20Jun%C3%ADn_2016.pdf

León, E., Tesillo, C., Escobar, Y., & Godoy, L. (2022). Revisión de los avances y cambios en ciberseguridad en el Perú, para una transformación digital. *Innovación y Software, 3*(2), 1-13. https://www.redalyc.org/journal/6738/673870841009/673870841009.pdf

Lezama, C. (2023). Ciberdefensa y ciberseguridad en el Perú: realidad y retos en torno a la capacidad de las FF. AA. para neutralizar ciberataques que atenten contra la seguridad nacional. *Revista de Ciencia e Investigación en Defensa - CAEN, 4*(1), 55-76. https://doi.org/10.58211/recide.v4i1.99

López, M. (2012). La tutela penal del secreto empresarial [Tesis de maestría, Universidad de Panamá]. Repositorio de la Universidad de Panamá. http://up-rid.up.ac.pa/3616/1/maria_lopez.pdf

Muñoz, C. E. (2020). Revelación de secretos empresariales. *Revista de Derecho, 35*(49),114–125. https://goo.su/xGITN

Naoui, M., Lejdel, B., & Ayad, M. (2020). Using K-means algorithm for regression curve in big data system for business environment. *Revista Cubana de Ciencias Informáticas, 14*(2), 34-48. https://www.redalyc.org/journal/3783/378365833003/

Nasheri, H. (2004, 24 de junio). Economic Espionage and Industrial Spying. *ResearchGate.* https://goo.su/hfJMsQE

Payan, C. (2011). Secreto empresarial, vigencia como mecanismo de protección en la propiedad intelectual. *Revista de Derecho, 25*(34), 1-8. https://revistas.uexternado.edu.co/index.php/propin/article/view/3006/3656#:~:

text=Un%20secreto%20empresarial%20se%20considera,de%20lealtad%2C%20o%20la%20instigaci%C3%B3n

Pazmiño, D. (2020). Espionage and Competitiveness: The German Automotive Industry in China's Modern Commercial Game. *Urvio, 25*(*26)*, 93-103. https://doi.org/10.17141/urvio.26.2020.4221

Pazmiño, D. C. (2020). Espionaje y competitividad: la industria automotriz alemana en el juego comercial moderno de China. *Revista Latinoamérica de Estudios de Seguridad, 26*(34), 1-13. https://www.redalyc.org/journal/5526/552662410006/

Pereira, A., Stocker, F., De Mascena, K., & Boaventura, J. (2020). Corporate Social Performance and Financial Performance in Brazilian Companies: Analysis of the Influence of Disclosure. *Brazilian Business Review, 17*(5), 540-558. https://www.redalyc.org/journal/1230/123064464004/

Pérez, A. E. (2022). *Informe jurídico sobre la Resolución Nº 0177-2018/SDC-INDECOPI* [Tesis de pregrado, Pontificia Universidad Católica del Perú]. Repositorio de la Pontificia Universidad Católica del Perú. https://tesis.pucp.edu.pe/handle/20.500.12404/23456

Pospichil, B., Froehlich, C., Nodari, C., Schmidt, S., & Machado, R. (2020). The Contribution of the Dynamic Capabilities to Promote Sustainability in Industrial and Service Companies. *Brazilian Business Review, 17*(2), 180-210. https://www.redalyc.org/journal/3372/337264549003/html/#:~:text=Decrease%20operational%20costs%3B%20create%2C%20expand,improve%20the%20economic%20life%20cycle.&text=Protect%20ecosystems%3B%20improve%20air%20and,preserve%20natural%20and%20renewable%20resources.

Quilia, J. (2020). *Desafíos en la gestión empresarial de las MyPEs en tiempos de COVID-19, Perú* [Tesis de maestría, Universidad César Vallejo]. Repositorio de la Universidad César Vallejo. https://hdl.handle.net/20.500.12692/48291

Ramos, A. (2019). *La nueva normativa española para la protección de los secretos empresariales. En particular, su aplicación a los listados de clientela* [Tesis de pregrado, Universidad de Zaragoza]. Repositorio de la Universidad de Zaragoza. https://zaguan.unizar.es/record/90203/files/TAZ-TFG-2019-1208.pdf

Rodríguez, A. (2022). *La competencia desleal y la publicidad en las publicaciones de los influencers de Instagram en Lima 2021* [Tesis de pregrado, Universidad

Privada del Norte]. Repositorio de la Universidad Privada del Norte. https://repositorio.upn.edu.pe/handle/11537/31008

Rubio, A. (2018). *Técnicas de ciberataque y su relación con el espionaje industrial y económico* [Tesis de pregrado, Universidad Nacional Abierta y a Distancia]. Repositorio de la Universidad Nacional Abierta y a Distancia. https://repository.unad.edu.co/bitstream/handle/10596/31843/jmrubios.pdf?sequence=1&isAllowed=y

Ruíz, J. (2020). La hipótesis en la investigación científica – jurídica. *Revista Jurídica de Investigación e Innovación Educativa, 22*(25), 135-160. https://revistas.uma.es/index.php/rejienuevaepoca/article/view/7902/7372

Sanín, J. (2013). El secreto empresarial: Concepto teórico y fallas a la hora de alegar su violación ante la superintendencia de industria y comercio. *Revista de Derecho Privado, 23*(49), 1-34. https://www.redalyc.org/pdf/3600/360033220003.pdf

Santos, D. (2023). Como recolectar datos: métodos, ejemplos y herramientas clave. *Hubspot.* https://blog.hubspot.es/marketing/recoleccion-de-datos

Schulz, S. (2023, 23 de mayo). China sancionó a la empresa estadounidense Micron y agudizó la disputa por los semiconductores. *La Ruta China.* https://larutachina.com/china-sanciono-a-la-empresa-estadounidense-micron-y-agudizo-la-disputa-por-los-semiconductores/

Sini, G. (2012, 12 de junio). Espionaje industrial va en aumento en Perú. *Common Digital.* http://commondigital.pe/index.php/locales/11354-espionaje-industrial-va-en-aumento-en-peru

Valencia, A. (2023, 28 febrero). Espionaje corporativo en el Perú: el caso del "ejecutivo topo". *Bullard Falla Ezcurra.* https://bullardfallaezcurra.com/boletin/2021/05/04/espionaje-corporativo-en-el-peru-el-caso-del-ejecutivo-topo/

Viera, M. (2020). Trade Secrets, a key factor in the successful internationalization of a world-class Italian drink: The Campari case. *Revista Facultad de Jurisprudencia, 6*(7), 296-318. https://www.redalyc.org/journal/6002/600263428003/

Zermeño, J., Garza, M., & Rodríguez, M. (2021). El conocimiento en materia de propiedad intelectual como ventaja para la investigación científica. *Inquietud Empresarial, 21*(1), 103–116 https://doi.org/10.19053/01211048.11533

ANEXOS

Validación de Instrumento

Figura 1

Primera validación

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA CATEGORÍA RESPONSABILIDAD SECRETO EMPRESARIAL

N°	SUBCATEGORÍA S/ ítems	Veracidad[1]		Aplicabilidad[2]		Consistencia[3]		Neutralidad[4]		Sugerencias
	SUBCATEGORÍA 1: Propiedad Intelectual	Si	No	Si	No	Si	No	Si	No	
1	¿Cómo afecta el espionaje empresarial a la protección de la propiedad intelectual en las empresas de Lima?	X		X		X		X		-
2	¿Qué papel cree que debe desempeñar INDECOPI en la prevención del espionaje empresarial para proteger la propiedad intelectual?	X		X		X		X		-
	SUBCATEGORÍA 2: Información Confidencial	Si	No	Si	No	Si	No	Si	No	
1	¿Cuáles son las principales vulnerabilidades en la protección de la información confidencial que han observado en las empresas de Lima?	X		X		X		X		-
2	¿Qué sistemas informáticos y/o software recomienda implementar para fortalecer la seguridad de la información confidencial frente al espionaje empresarial?	X		X		X		X		-

Observaciones (precisar si hay suficiencia[5]):

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador: Zamaolla Yacheco, Juan Armando
DNI: 09263520
Especialidad del validador: Abogado en Derecho Corporativo

[1]**Veracidad:** Autenticidad y credibilidad. Los resultados son verdaderos para las personas que fueron estudiadas y para otras personas que han experimentado o estado en contacto con el fenómeno investigado.
[2]**Aplicabilidad:** Transferibilidad o exportabilidad. La transferibilidad consiste en la posibilidad de transferir los resultados a otros contextos o grupos.
[3]**Consistencia:** Dependencia o estabilidad de los datos.
[4]**Neutralidad:** Confirmabilidad. Se refiere a la neutralidad de la interpretación o análisis de la información, que se logra cuando otro (s) investigador (es) puede seguir «la pista» al investigador original y llegar a hallazgos similares
[5]**Suficiencia:** Los ítems planteados son suficientes para medir la dimensión

Lima, mayo de 2023

Firma del Experto Informante

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA CATEGORÍA ESPIONAJE EMPRESARIAL

N°	SUBCATEGORÍAS/ ítems	Veracidad[1]		Aplicabilidad[2]		Consistencia[3]		Neutralidad[4]		Sugerencias
	SUBCATEGORÍA 1: Acceso Ilícito	Si	No	Si	No	Si	No	Si	No	
1	¿Considera que Indecopi sanciona eficazmente a las personas y/o empresas que acceden ilícitamente a información empresarial confidencial?	X		x		X		x		-
2	¿Cuáles son las modalidades más utilizadas para acceder ilícitamente a información empresarial confidencial de las empresas de Lima?	X		X		X		X		-
	SUBCATEGORÍA 2: Competencia Desleal	Si	No	Si	No	Si	No	Si	No	
1	¿Qué incentivos económicos se podrían implementar para que las empresas no compitan deslealmente mediante actos de espionaje empresarial?	X		X		X		X		-
2	¿Cuáles son los principales retos que enfrentan las empresas en Lima para proteger sus secretos empresariales frente al espionaje empresarial?	x		X		x		X		-

Observaciones (precisar si hay suficiencia[5]):

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador: Zamaolla Yacheco, Juan Armando
DNI: 9263520
Especialidad del validador: Abogado en Derecho Corporativo

Lima, setiembre de 2023

[1]**Veracidad:** Autenticidad y credibilidad. Los resultados son verdaderos para las personas que fueron estudiadas y para otras personas que han experimentado o estado en contacto con el fenómeno investigado.
[2]**Aplicabilidad:** Transferibilidad o exportabilidad. La transferibilidad consiste en la posibilidad de transferir los resultados a otros contextos o grupos.
[3]**Consistencia:** Dependencia o estabilidad de los datos.
[4]**Neutralidad:** Confirmabilidad. Se refiere a la neutralidad de la interpretación o análisis de la información, que se logra cuando otro (s) investigador (es) puede seguir «la pista» al investigador original y llegar a hallazgos similares
[5]**Suficiencia:** Los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

Figura 2

Segunda validación

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA CATEGORÍA RESPONSABILIDAD SECRETO EMPRESARIAL

N°	SUBCATEGORÍAS/ ítems	Veracidad[1]		Aplicabilidad[2]		Consistencia[3]		Neutralidad[4]		Sugerencias
	SUBCATEGORÍA 1: Propiedad Intelectual	Si	No	Si	No	Si	No	Si	No	
1	¿Cómo afecta el espionaje empresarial a la protección de la propiedad intelectual en las empresas de Lima?	X		X		X		X		-
2	¿Qué papel cree que debe desempeñar INDECOPI en la prevención del espionaje empresarial para proteger la propiedad intelectual?	X		X		X		X		-
	SUBCATEGORÍA 2: Información Confidencial	Si	No	Si	No	Si	No	Si	No	
1	¿Cuáles son las principales vulnerabilidades en la protección de la información confidencial que han observado en las empresas de Lima?	X		X		X		X		-
2	¿Qué sistemas informáticos y/o software recomienda implementar para fortalecer la seguridad de la información confidencial frente al espionaje empresarial?	X		X		X		X		-

Observaciones (precisar si hay suficiencia[5]):

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador: Quiroz Cubas, Lars Anibal
DNI: 71249867
Especialidad del validador: Abogado en Derecho Corporativo

Lima, mayo de 2023

[1]**Veracidad:** Autenticidad y credibilidad. Los resultados son verdaderos para las personas que fueron estudiadas y para otras personas que han experimentado o estado en contacto con el fenómeno investigado.
[2]**Aplicabilidad:** Transferibilidad o exportabilidad. La transferibilidad consiste en la posibilidad de transferir los resultados a otros contextos o grupos.
[3]**Consistencia:** Dependencia o estabilidad de los datos.
[4]**Neutralidad:** Confirmabilidad. Se refiere a la neutralidad de la interpretación o análisis de la información, que se logra cuando otro (s) investigador (es) puede seguir «la pista» al investigador original y llegar a hallazgos similares
[5]**Suficiencia:** Los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA CATEGORÍA ESPIONAJE EMPRESARIAL

N°	SUBCATEGORÍAS/ ítems	Veracidad[1]		Aplicabilidad[2]		Consistencia[3]		Neutralidad[4]		Sugerencias
	SUBCATEGORÍA 1: Acceso Ilícito	Si	No	Si	No	Si	No	Si	No	
1	¿Considera que Indecopi sanciona eficazmente a las personas y/o empresas que acceden ilícitamente a información empresarial confidencial?	X		x		X		x		-
2	¿Cuáles son las modalidades más utilizadas para acceder ilícitamente a información empresarial confidencial de las empresas de Lima?	X		X		X		X		-
	SUBCATEGORÍA 2: Competencia Desleal	Si	No	Si	No	Si	No	Si	No	
1	¿Qué incentivos económicos se podrían implementar para que las empresas no compitan deslealmente mediante actos de espionaje empresarial?	X		X		X		X		-
2	¿Cuáles son los principales retos que enfrentan las empresas en Lima para proteger sus secretos empresariales frente al espionaje empresarial?	x		X		x		X		-

Observaciones (precisar si hay suficiencia[5]):

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador: Quiroz Cubas, Lars Anibal
DNI: 71249867
Especialidad del validador: Abogado en Derecho Corporativo

Lima, setiembre de 2023

[1]**Veracidad:** Autenticidad y credibilidad. Los resultados son verdaderos para las personas que fueron estudiadas y para otras personas que han experimentado o estado en contacto con el fenómeno investigado.
[2]**Aplicabilidad:** Transferibilidad o exportabilidad. La transferibilidad consiste en la posibilidad de transferir los resultados a otros contextos o grupos.
[3]**Consistencia:** Dependencia o estabilidad de los datos.
[4]**Neutralidad:** Confirmabilidad. Se refiere a la neutralidad de la interpretación o análisis de la información, que se logra cuando otro (s) investigador (es) puede seguir «la pista» al investigador original y llegar a hallazgos similares
[5]**Suficiencia:** Los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

Figura 3:

Tercera validación

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA CATEGORÍA RESPONSABILIDAD SECRETO EMPRESARIAL

N°	SUBCATEGORÍAS/ ítems	Veracidad[1]		Aplicabilidad[2]		Consistencia[3]		Neutralidad[4]		Sugerencias
	SUBCATEGORÍA 1: Propiedad Intelectual	Si	No	Si	No	Si	No	Si	No	
1	¿Cómo afecta el espionaje empresarial a la protección de la propiedad intelectual en las empresas de Lima?	X		X		X		X		-
2	¿Qué papel cree que debe desempeñar INDECOPI en la prevención del espionaje empresarial para proteger la propiedad intelectual?	X		X		X		X		-
	SUBCATEGORÍA 2: Información Confidencial	Si	No	Si	No	Si	No	Si	No	
1	¿Cuáles son las principales vulnerabilidades en la protección de la información confidencial que han observado en las empresas de Lima?	X		X		X		X		-
2	¿Qué sistemas informáticos y/o software recomienda implementar para fortalecer la seguridad de la información confidencial frente al espionaje empresarial?	X		X		X		X		-

Observaciones (precisar si hay suficiencia[5]):

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador: Rivera Arellano, Carlos Enrique
DNI: 07438888
Especialidad del validador: Magister en Derecho Administrativo

Lima, mayo de 2023

[1]**Veracidad:** Autenticidad y credibilidad. Los resultados son verdaderos para las personas que fueron estudiadas y para otras personas que han experimentado o estado en contacto con el fenómeno investigado.
[2]**Aplicabilidad:** Transferibilidad o exportabilidad. La transferibilidad consiste en la posibilidad de transferir los resultados a otros contextos o grupos.
[3]**Consistencia:** Dependencia o estabilidad de los datos.
[4]**Neutralidad:** Confirmabilidad. Se refiere a la neutralidad de la interpretación o análisis de la información, que se logra cuando otro (s) investigador (es) puede seguir «la pista» al investigador original y llegar a hallazgos similares
[5]**Suficiencia:** Los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LA CATEGORÍA ESPIONAJE EMPRESARIAL

N°	SUBCATEGORÍAS/ ítems	Veracidad[1]		Aplicabilidad[2]		Consistencia[3]		Neutralidad[4]		Sugerencias
	SUBCATEGORÍA 1: Acceso Ilícito	Si	No	Si	No	Si	No	Si	No	
1	¿Considera que Indecopi sanciona eficazmente a las personas y/o empresas que acceden ilícitamente a información empresarial confidencial?	X		x		X		x		-
2	¿Cuáles son las modalidades más utilizadas para acceder ilícitamente a información empresarial confidencial de las empresas de Lima?	X		X		X		X		-
	SUBCATEGORÍA 2: Competencia Desleal	Si	No	Si	No	Si	No	Si	No	
1	¿Qué incentivos económicos se podrían implementar para que las empresas no compitan deslealmente mediante actos de espionaje empresarial?	X		X		X		X		-
2	¿Cuáles son los principales retos que enfrentan las empresas en Lima para proteger sus secretos empresariales frente al espionaje empresarial?	x		X		x		X		-

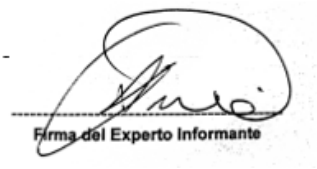
Observaciones (precisar si hay suficiencia[5]):

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador: Rivera Arellano, Carlos Enrique
DNI: 07438888
Especialidad del validador: Magister en Derecho Administrativo

Lima, setiembre de 2023

[1]**Veracidad:** Autenticidad y credibilidad. Los resultados son verdaderos para las personas que fueron estudiadas y para otras personas que han experimentado o estado en contacto con el fenómeno investigado.
[2]**Aplicabilidad:** Transferibilidad o exportabilidad. La transferibilidad consiste en la posibilidad de transferir los resultados a otros contextos o grupos.
[3]**Consistencia:** Dependencia o estabilidad de los datos.
[4]**Neutralidad:** Confirmabilidad. Se refiere a la neutralidad de la interpretación o análisis de la información, que se logra cuando otro (s) investigador (es) puede seguir «la pista» al investigador original y llegar a hallazgos similares
[5]**Suficiencia:** Los ítems planteados son suficientes para medir la dimensión



Firma del Experto Informante

(Anexo 5): Consentimiento informados

Figura 4

Consentimiento informado del primer entrevistado

DECLARACIÓN DEL PARTICIPANTE

El que firma y autoriza el presente documento, reconoce que la información facilitada en el proceso de ejecución de la presente investigación es estrictamente confidencial y no será usada para ningún otro propósito fuera de los de este estudio sin mi consentimiento. He sido informado de que puedo hacer preguntas sobre la propuesta de investigación en cualquier momento y que puedo retirarme del mismo cuando así lo decida, sin que esto implique responsabilidad para mi persona. De tener preguntas sobre mi participación en este estudio, **puedo contactar al correo electrónico** bhuamanc@autonoma.edu.pe así como al lespinozaf@autonoma.edu.pe

Se me otorga una copia digital del presente documento y solicito sea notificado al siguiente correo electrónico gaybary@autonoma.edu.pe, a fin de conocer sobre los resultados de la presente investigación.

COMPROMISOS ASUMIDOS POR EL PARTICIPANTE

De estar conforme con las condiciones señaladas, solicitamos consignar si autoriza o no vuestra participación.

AUTORIZACION: (SÍ) (NO)

Asimismo, de permitir la revelación de vuestra identidad, consignar (SÍ) o (NO), colocando vuestra firma en el siguiente recuadro:

AUTORIZACION: (SÍ) (NO)

APELLIDOS Y NOMBRES DEL PARTICIPANTE: Aybar Izaguirre, Gerardo Manuel

Figura 5

Consentimiento informado del segundo entrevistado

DECLARACIÓN DEL PARTICIPANTE

El que firma y autoriza el presente documento, reconoce que la información facilitada en el proceso de ejecución de la presente investigación es estrictamente confidencial y no será usada para ningún otro propósito fuera de los de este estudio sin mi consentimiento. He sido informado de que puedo hacer preguntas sobre la propuesta de investigación en cualquier momento y que puedo retirarme del mismo cuando así lo decida, sin que esto implique responsabilidad para mi persona. De tener preguntas sobre mi participación en este estudio, **puedo contactar al correo electrónico** bhuamanc@autonoma.edu.pe así como al lespinozaf@autonoma.edu.pe

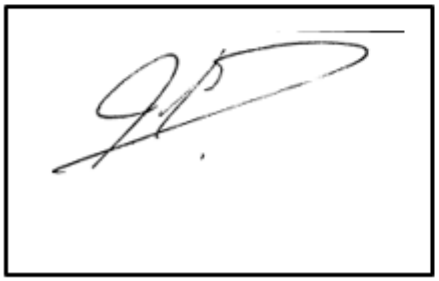
Se me otorga una copia digital del presente documento y solicito sea notificado al siguiente correo electrónico mhuamanh10@autonoma.edu.pe, a fin de conocer sobre los resultados de la presente investigación.

COMPROMISOS ASUMIDOS POR EL PARTICIPANTE

De estar conforme con las condiciones señaladas, solicitamos consignar si autoriza o no vuestra participación.

AUTORIZACION: (SÍ) (NO)

Asimismo, de permitir la revelación de vuestra identidad, consignar (SÍ) o (NO), colocando vuestra firma en el siguiente recuadro:



AUTORIZACION: (SÍ) (NO)

APELLIDOS Y NOMBRES DEL PARTICIPANTE: Huamán Pillhuaman, Moisés Noé

Figura 6

Consentimiento informado del tercer entrevistado

DECLARACIÓN DEL PARTICIPANTE

El que firma y autoriza el presente documento, reconoce que la información facilitada en el proceso de ejecución de la presente investigación es estrictamente confidencial y no será usada para ningún otro propósito fuera de los de este estudio sin mi consentimiento. He sido informado de que puedo hacer preguntas sobre la propuesta de investigación en cualquier momento y que puedo retirarme del mismo cuando así lo decida, sin que esto implique responsabilidad para mi persona. De tener preguntas sobre mi participación en este estudio, **puedo contactar al correo electrónico** bhuamanc@autonoma.edu.pe así como al lespinozaf@autonoma.edu.pe

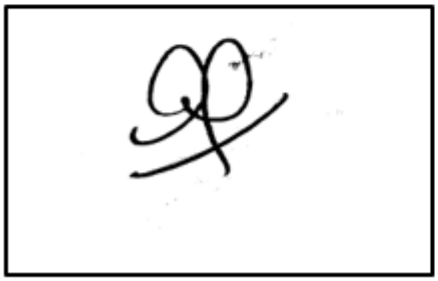
Se me otorga una copia digital del presente documento y solicito sea notificado al siguiente correo electrónico pavalos17@autonoma.edu.pe, a fin de conocer sobre los resultados de la presente investigación.

COMPROMISOS ASUMIDOS POR EL PARTICIPANTE

De estar conforme con las condiciones señaladas, solicitamos consignar si autoriza o no vuestra participación.

AUTORIZACION: (SÍ) (NO)

Asimismo, de permitir la revelación de vuestra identidad, consignar (SÍ) o (NO), colocando vuestra firma en el siguiente recuadro:



AUTORIZACION: (SÍ) (NO)

APELLIDOS Y NOMBRES DEL PARTICIPANTE: Avalos Farfán, Pamela Christie

Figura 7

Consentimiento informado del cuarto entrevistado

DECLARACIÓN DEL PARTICIPANTE

El que firma y autoriza el presente documento, reconoce que la información facilitada en el proceso de ejecución de la presente investigación es estrictamente confidencial y no será usada para ningún otro propósito fuera de los de este estudio sin mi consentimiento. He sido informado de que puedo hacer preguntas sobre la propuesta de investigación en cualquier momento y que puedo retirarme del mismo cuando así lo decida, sin que esto implique responsabilidad para mi persona. De tener preguntas sobre mi participación en este estudio, **puedo contactar al correo electrónico** bhuamanc@autonoma.edu.pe así como al lespinozaf@autonoma.edu.pe

Se me otorga una copia digital del presente documento y solicito sea notificado al siguiente correo electrónico mtovarc@autonoma.edu.pe, a fin de conocer sobre los resultados de la presente investigación.

COMPROMISOS ASUMIDOS POR EL PARTICIPANTE

De estar conforme con las condiciones señaladas, solicitamos consignar si autoriza o no vuestra participación.

AUTORIZACION: (SÍ) (NO)

Asimismo, de permitir la revelación de vuestra identidad, consignar (SÍ) o (NO), colocando vuestra firma en el siguiente recuadro:

AUTORIZACION: (SÍ) (NO)

APELLIDOS Y NOMBRES DEL PARTICIPANTE: Tovar Cerquen, Martín Vicente

Figura 8

Consentimiento informado del quinto entrevistado

DECLARACIÓN DEL PARTICIPANTE

El que firma y autoriza el presente documento, reconoce que la información facilitada en el proceso de ejecución de la presente investigación es estrictamente confidencial y no será usada para ningún otro propósito fuera de los de este estudio sin mi consentimiento. He sido informado de que puedo hacer preguntas sobre la propuesta de investigación en cualquier momento y que puedo retirarme del mismo cuando así lo decida, sin que esto implique responsabilidad para mi persona. De tener preguntas sobre mi participación en este estudio, **puedo contactar al correo electrónico** bhuamanc@autonoma.edu.pe así como al lespinozaf@autonoma.edu.pe

Se me otorga una copia digital del presente documento y solicito sea notificado al siguiente correo electrónico asolorzanom@autonoma.edu.pe, a fin de conocer sobre los resultados de la presente investigación.

COMPROMISOS ASUMIDOS POR EL PARTICIPANTE

De estar conforme con las condiciones señaladas, solicitamos consignar si autoriza o no vuestra participación.

AUTORIZACION: (SÍ) (NO)

Asimismo, de permitir la revelación de vuestra identidad, consignar (SÍ) o (NO), colocando vuestra firma en el siguiente recuadro:

AUTORIZACION: (SÍ) (NO)

APELLIDOS Y NOMBRES DEL PARTICIPANTE: Solorzano Maguiña, Alexander Adolfo

(Anexo 6): Preguntas de la entrevista

Tabla 9

Preguntas de la entrevista

Variable	Dimensiones	Preguntas
Secreto Empresarial	**Propiedad Intelectual**	¿Cómo afecta el espionaje empresarial a la protección de la propiedad intelectual en las empresas de Lima?
		¿Qué papel cree que debe desempeñar INDECOPI en la prevención del espionaje empresarial para proteger la propiedad intelectual?
	Información Confidencial	¿Cuáles son las principales vulnerabilidades en la protección de la información confidencial que han observado en las empresas de Lima?
		¿Qué sistemas informáticos y/o software recomienda implementar para fortalecer la seguridad de la información confidencial frente al espionaje empresarial?
Espionaje Empresarial	**Acceso Ilícito**	¿Considera que Indecopi sanciona eficazmente a las personas y/o empresas que acceden ilícitamente a información empresarial confidencial?
		¿Cuáles son las modalidades más utilizadas para acceder ilícitamente a información empresarial confidencial de las empresas de Lima?
	Competencia Desleal	¿Qué incentivos económicos se podrían implementar para que las empresas no compitan deslealmente mediante actos de espionaje empresarial?
		¿Cuáles son los principales retos que enfrentan las empresas en Lima para proteger sus secretos empresariales frente al espionaje empresarial?

(Anexo 7): Transcripción de las preguntas de la entrevista

Tabla 10

Transcripción de la primera pregunta

Entrevistado	¿Cómo afecta el espionaje empresarial a la protección de la propiedad intelectual en las empresas de Lima?
Dr. Gerardo Manuel Aybar Izaguirre	Si bien todas las libertades en la Comisión Política del Perú se ha establecido que existe una libertad de empresa, al mismo tiempo la protección o el garantizar la propiedad intelectual es importante aquí en el Perú, en la legislación peruana. Bueno, definitivamente un espionaje, las empresas son afectadas económicamente porque puede dañar su reputación y puede generar un perjuicio económico a la empresa.
Dr. Moises Huaman Picchuaman	Bueno en principio el tema de la protección de la información que puedan generar las empresas definitivamente les va afectar de manera directa toda vez que las empresas en general desarrollan información, actividades y procesos con el único propósito de alcanzar mayor productividad. El prejuicio que van a tener es económico ya que a estas empresas les ha tomado tiempo implementar estos secretos y deben cuidarlos.
Dra. Pamela Avalos Farfan	Afecta a las empresas causando daños económicos, daños a la reputación de una empresa y pérdida de la información.
Dr. Martin Vicente Tovar Cerquen	Bueno definitivamente este tema del espionaje tiene una debilidad legal en todo sentido y vemos los resultados en los expedientes del órgano fiscalizador y mayor responsable como es Indecopi creo que ahí viene el problema. El segundo problema es que no se atiende las necesidades de aquellos que tenemos empresas es la afectación empresarial. Por ejemplo el tema del espionaje definitivamente hoy la tecnología ha avanzado bastante que no solo es el uso del beneficio empresarial sino también es un uso indebido por los que conforman la empresa y que aquellos no se les hace firmar ciertos protocolos esa información perjudica a las empresas.
Dr. Alexander Solorzano Maguiña	Lo afecta negativamente a las empresas. Porque al conocer la producción, al conocer las formas de comercialización, publicidad de una empresa, va a hacer que el competidor utilice más recursos para poder rebajar a su competidor y para esto estas empresas hacen este espionaje contratando otras empresas que se dedican a eso, a hacer el espionaje, utilizando también medios electrónicos, como el hackeo, como los hackers, para obtener información del competidor.

Tabla 11

Transcripción de la segunda pregunta

Entrevistado	¿Qué papel cree que debe desempeñar INDECOPI en la prevención del espionaje empresarial para proteger la propiedad intelectual?
Dr. Gerardo Manuel Aybar Izagirre	Indecopi debe cumplir el mandato establecido por la Comisión Política del Perú y al mismo tiempo, por lo cual su finalidad que fue creado para hacer las acciones administrativas necesarias para poder sancionar a las empresas que hayan incurrido en espionaje y que estén afectando a otras empresas a través de un perjuicio económico con este robo o pérdida de información.
Dr. Moises Huaman Picchuaman	La propiedad intelectual es protegida por Indecopi hay formas donde Indecopi puede inscribir secretos industriales, secretos comerciales y en este caso información trascendental respecto a las empresas o al manejo de información que puedan tener las empresas . Ahora qué papel cumplen el de supervisar, sancionar a las empresas que incumplen con estas normativas que están vigentes y tienen alcance nacional y de protección a todas las empresas y entes que tienen bajo su regulación.
Dra. Pamela Avalos Farfan	Indecopi debe sancionar a las empresas o personas que vulneren derechos de propiedad intelectual ya que es el organismo regulador a cargo de ella.
Dr. Martin Vicente Tovar Cerquen	Simplemente evaluar lo que hoy en dia trae consigo las sentencias que emite Indecopi hay mucha vulnerabilidad para aquellas personas que son trabajadores de las empresas entonces creo que aquí el trabajo de Indecopi es primero existir una correlación normativa que deba emitir el Estado en materia penal que hay una divergencia el tema que no se toca es de sanción no muy comprometido ya que dejan a Indecopi en un desamparo total de esa manera por eso es que no se da una sanción clara.
Dr. Alexander Solorzano Maguiña	El espionaje empresarial está considerado como una infracción que obviamente va a merecer una sanción. Entonces, lo que tiene que hacer Indecopi solamente es cumplir con su función. Función, sancionar, verificar cuáles son las empresas que realizan espionaje y sancionar. No solamente la empresa que realiza espionaje, sino la que contrata a esas empresas para el espionaje.

Tabla 12

Transcripción de la tercera pregunta

Entrevistado	¿Cuáles son las principales vulnerabilidades en la protección de la información confidencial que han observado en las empresas de Lima?
Dr. Gerardo Manuel Aybar Izagirre	Quizás hay una debilidad desde el punto de vista del ámbito legal, porque los funcionarios no tienen acuerdos de confidencialidad firmados de manera correcta y al mismo tiempo no suscriben dentro de su contrato de trabajo también ciertas penalidades o al mismo tiempo decirles a ellos que van a recibir sanciones en el ámbito penal o civil o económico ante una transgresión de la confidencialidad de la información de la empresa.
Dr. Moises Huaman Picchuaman	En general ahora con el auge de la digitalización nosotros estamos teniendo acceso a información de manera digital. Las empresas también guardan la información en carpetas digitales, archivos digitales en servidores. Por ende están expuestos a piratas informáticos incluso también a la seguridad jurídica entre la empresa y los empleados. Deben usar diversas herramientas para poder controlar este riesgo y así mismo de manera legal.
Dra. Pamela Avalos Farfan	Falta de acuerdos de confidencialidad, pocas penalidades de incumplimiento, sistemas electrónicos.
Dr. Martin Vicente Tovar Cerquen	Principalmente sería el espionaje empresarial si hablamos de contratos atípicos hoy en dia se ve muchos enlaces empresariales en el dia a dia hay cláusulas de confidencialidad para los trabajadores, los actos atípicos de sabotaje empresarial, las ventajas competitivas para cierto sector que produce este tipo de sabotaje podríamos llamar el patrimonio de las personas jurídicas del sector privado.
Dr. Alexander Solorzano Maguiña	A ver, las principales vulnerabilidades. Que las empresas que son objeto de espionaje no toman las medidas de seguridad no tienen conciencia no tienen conciencia de que pueden ser objeto de espionaje entonces dentro de las políticas empresariales hay muchas empresas que no toman conciencia para ellos es más no tienen conciencia de que pueden ser objeto de espionaje básicamente Básicamente eso sería.

Tabla 13

Transcripción de la cuarta pregunta

Entrevistado	¿Qué sistemas informáticos y/o software recomienda implementar para fortalecer la seguridad de la información confidencial frente al espionaje empresarial?
Dr. Gerardo Manuel Aybar Izagirre	Se debe hacer todo, se debe comprar todos los software y todos los equipos tecnológicos necesarios que vayan en contra de en este caso los virus, los malware y todo lo que al final puede hacer ataques cibernéticos a la empresa que se pueda vulnerar este tipo de información y pueda generar un perjuicio económico a la sociedad.
Dr. Moises Huaman Picchuaman	Son específicos no sabría precisar pero lo que sí es necesario son los acuerdos que se firman entre el empleador y el empleado que son los famosos acuerdos de confidencialidad cuando tu entras a trabajar en una empresa en donde van a manejar información sensible tú te comprometes a cuidar ese tipo de información confidencial. Ahora a nivel digital está prohibido por reglamento llevar usb a las empresas donde manejan este tipo de información. La información sensible que pueda tener la empresa no se van a quedar con la protección única de la norma o la protección por parte de las autoridades en este caso Indecopi sino también las empresas van a implementar herramientas y mecanismos de seguridad. A nivel legal las empresas van a obligar a firmar contratos donde uno se comprometa a no difundir ningún tipo de información.
Dr. Pamela Avalos Farfan	Que se instalen dispositivos informáticos, webcam, micrófonos para de esa manera evitar pérdida de información sensible. Prohibir la impresión de documentos confidenciales.
Dr. Martin Vicente Tovar Cerquen	Creo que podemos recabar mucho lo que hoy nos deja la inteligencia artificial hoyo en día no hay software que pueda darle una mayor tranquilidad al ámbito empresarial pero sí podríamos recurrir a ciertos mecanismos al uso de la inteligencia artificial que viene trabajando en otros países donde quizás tienen vulnerabilidad pero no en gran escala entonces considero que con el avance de la tecnología podríamos tratar de recurrir a software fortalecidos para que puedan establecerse mayor seguridad en las empresas.
Dr. Alexander Solorzano Maguiña	La verdad es que no sabría responderle. En todo caso, esa pregunta tendría que hacerse a un informático. Porque lo que sí recomiendo es que los sistemas informáticos se pongan candados. Ahora, ¿cómo lo hacen? Es un informático, lo tiene que decir.

Tabla 14

Transcripción de la quinta pregunta

Entrevistado	¿Considera que Indecopi sanciona eficazmente a las personas y/o empresas que acceden ilícitamente a información empresarial confidencial?
Dr. Gerardo Manuel Aybar Izagirre	Yo creo que Indecopi no tiene ahorita la capacidad para sancionar a esas empresas que incurren en espionaje, ellos andan más concentrados en sancionar a las grandes empresas, en ver cosas que de repente podría afectar económicamente a las sociedades en el país y a nuestro desarrollo económico.
Dr. Moises Huaman Picchuaman	Si, en tanto sea acreditado, aprobado es un proceso de investigación y luego sanción. Ahora como todo procedimiento tiene sus etapas va a ver el derecho a la defensa y en el momento oportuno en cuanto se llegue a la sanción. Si he tenido conocimiento que las multas son bastantes altas y porque el Estado como política tiene la protección de las empresas si alguien está atentando contra una empresa está atentando en decencia con el propósito del Estado.
Dra. Pamela Avalos Farfan	Indecopi a través de sus multas busca sancionar estas conductas, pero considero que no todas las empresas denuncian estos actos ilícitos.
Dr.Martin Vicente Tovar Cerquen	Definitivamente no, en las lecturas que he tenido con respecto a Indecopi hay una vulnerabilidad para aquellas personas que utilizan de manera ilegal la información tan importante que tienen las personas jurídicas. No hay una eficaz labor por parte de Indecopi hacia las personas que vulneran la información sensible de las empresas.
Dr. Alexander Solorzano Maguiña	Quien debe sancionar y reprimir estas conductas desleales es Indecopi, pero Indecopi no funciona, en mi concepto no funciona.

Tabla 15

Transcripción de la sexta pregunta

Entrevistado	¿Cuáles son las modalidades más utilizadas para acceder ilícitamente a información empresarial confidencial de las empresas de Lima?
Dr.Gerardo Manuel Aybar Izagirre	Hoy en día lo estamos viendo a través de los hackers con venta de información ilegal en los mercados, en los mercados, podemos decir mercados negros donde venden información como data de las empresas como por ejemplo en el centro de Lima en Wilson y al mismo tiempo a través también de la transgresión de los acuerdos de confidencialidad que tienen los trabajadores.
Dr. Moises Huaman Picchuaman	Como le dije es a través de un hacker de información si la empresa está con temas informáticos que van a manejar su información sensible. La otra forma es la compra de información de manera ilícita, base de datos que a veces son extraídas de distintas empresas pagan por esa información. Las empresas invierten mucho en la producción de conocimiento, métodos y por ende también se preocupan en cautelar este tipo de información.
Dra. Pamela Avalos Farfan	Vulneración de convenios o acuerdos de confidencialidad, robo de información a través de hackers, entre otros.
Dr. Martin Vicente Tovar Cerquen	La información secreta que se tiene hablando de estos contratos atípicos. Eso también lo vemos en el ámbito público cuando hablamos de contratación del estado utilizan en la modalidad de espionaje ilícitamente está sancionada y al parecer también utilizan diferentes tipos de estrategias porque nosotros tenemos un vacío de tipo penal del espionaje corporativo por allí viene el problema. Cuales son, divulgación de fórmulas industriales, entre otras que establecen ciertas desventajas desleales.
Dr. Alexander Solorzano Maguiña	Espionaje en forma material. ¿Por qué? Porque ellos ingresan una persona ahí en la empresa para que recabe la información.contacten con alguien del competidor, alguien que trabaja en la empresa para que le den información. Dos, y el hackeo, pues, el hackeo a través de los hackers. Pero más es la modalidad, es penetrando en esas empresas, haciendo relaciones, cualquier persona ahí, un administrador, un contador, algo que le dé la información de la empresa

Tabla 16

Transcripción de la séptima pregunta

Entrevistado	¿Qué incentivos económicos se podrían implementar para que las empresas no compitan deslealmente mediante actos de espionaje empresarial?
Dr. Gerardo Manuel Aybar Izagirre	Yo pienso que de repente el tema de incentivos económicos, incentivos económicos al mismo tiempo deberían ser un tema básico de una sanción económica o que al final esto pueda cargar multas y un registro de sociedades que incurren en estos actos que son desleales, para que así las otras empresas o proveedores puedan de repente revisar y puedan verificar.
Dr. Moises Huaman Picchuaman	Bueno incentivos como tal no tanto, podríamos considerar un incentivo negativo digamos indecopi haciendo más duras las sanciones que se puedan establecer aquellas empresas que incurran en este tipo de actos pero incentivos como tal no. Sería interesante que se tenga y se promueva la protección de información en las empresas. Hay sanciones que pueden llegar hasta el ámbito penal ojo que no descarta esa posibilidad también.
Da. Pamela Avalos Farfan	Mayores sanciones para que de esa manera disminuyan estos actos de conductas anticompetitivas en las empresas.
Dr. Martin Vicente Tovar Cerquen	Existen incentivos económicos esto viene en el ámbito administrativo cuando un trabajador ve que su jefe está haciendo algo ilícito y el da aviso el estado lo recompensa existe una ley que avala pero eso es para combatir en el sector público no es para el sector privado ley que favorece económicamente nadie lo ejercita porque nadie quiere perder un trabajo en el ámbito público. Pero si deben existir incentivos para el ámbito privado de esa manera pueden disminuir los casos sobre el espionaje empresarial.
Dr. Alexander Solorzano Maguiña	A ver, no hay una política del Estado para reprimir la competencia desleal referente al espionaje, no hay. Indecopi no cumple con su función, Indecopi debería hacer un seguimiento y sancionar. Y conozco pocos casos, casi no conozco casos de empresas que han contratado espías y que han sido sancionadas. Obviamente, la empresa que se siente afectada por el espionaje hace la denuncia de copia y tendría que hacer un procedimiento sancionador contra esa empresa. Pero no conozco casos, no hay muchos casos de eso. Pero sin embargo, es una realidad que se presenta.

Figura 17

Transcripción de la octava pregunta

Entrevistado	¿Cuáles son los principales retos que enfrentan las empresas en Lima para proteger sus secretos empresariales frente al espionaje empresarial?
Dr. Gerardo Manuel Aybar Izagirre	Pienso que deberían tener una correcta política de protección de los datos de la empresa, los datos personales de sus clientes, al mismo tiempo una mejor custodia de ello, de repente comprar software o implementación de sistemas en la nube que les permita tener todo ello bajo una protección, inclusive encriptado, para que al final no se afecte su vulneración y se vean afectados económicamente. O su reputación de la empresa frente a estos actos.
Dr. Moises Huaman Picchuaman	Como les dije un poco está relacionado esto a la seguridad que puedan tener seguridad como tipo digital prohibiendo o instalando sistemas que sea difícil el acceso a esta información por agentes externos ahora esto a nivel digital. Ahora a nivel legal un factor importante es este contrato a veces de exclusividad que es diferente. Los trabajadores manejan la información por lo tanto se obligan a mantener la información en esa posición para la empresa. Se ve reflejado en las normas de conducta o en los reglamentos establecidos. Es de acuerdo a las empresas a que rubro se dedican y cada uno tiene sus políticas y medidas de protección que puedan resguardar bien su información confidencial.
Dra Pamela Avalos Farfan	La firma de acuerdos de confidencialidad que otorguen la mayor protección a las partes, mejores políticas de tratamiento de datos, entre otros.
Dr. Martin Vicente Tovar Cerquen	Hay que sacar cálculos porque hay que ver las cosas desde un punto de vista cuantitativo y cualitativo no se tiene un registro por ejemplo de las pérdidas económicas de una empresa definitivamente pasan por alto pero si se tiene las incidencias que se pueden ver por Indecopi de los resultados que emiten mediante los expedientes. Trabajar en conjunto para que se pueda establecer normas que sancionen penalmente.
Dr. Alexander Solorzano Maguiña	Lo primero, las empresas tienen que tomar conciencia de que pueden ser penetradas y recabar información de su know-how, de su producción, de su personal, de sus políticas de inversiones. ¿Por qué se produce el espionaje? Porque muchas empresas quieren saber cómo está trabajando su competidor. Es como una guerra. Si en una guerra, tú por inteligencia, y el espionaje es inteligencia,y el espionaje es inteligencia tú ves que el enemigo tiene mil efectivos tú cuántos cuántos efectivos tú le pones para destrozar esos mil cinco mil diez mil si yo sé que tienen si tienen este caso la mente metralletas que es lo que yo tengo que poner tanques puestos tanques para eliminar el espionaje es inteligencia es inteligencia importante inteligencia de primera mano entonces las empresas tienen que tomar conciencia de que están en una guerra, en una guerra comercial, y que tienen que cerrar, primero, fidelizar a su gente, que su gente no los traicione, porque a veces por dinero la gente vende información. Acuerdos de confidencialidad. Incluso celebrar acuerdos de confidencialidad, muy bien, fidelizar a su gente.