UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Regulación del hacking ético: prueba de vulnerabilidad sorpresiva y la exclusión en la subsunción de los delitos de acceso ilícito

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Abogado

AUTORES:

Cuellar Chuquiyuri, Keyla Katherine (orcid.org/0000-0002-5520-7661)

Guerreros Rojas, Mauricio (orcid.org/0000-0002-4122-9376)

ASESOR:

Mg. Colchado Ruiz, Emilio Martin (orcid.org/0000-0003-0462-9757)

LÍNEA DE INVESTIGACIÓN:

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

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la Democracia, Liderazgo y Ciudadanía

LIMA – PERÚ

2023

DEDICATORIA

Keyla Katherine Cuellar Chuquiyuri,
Dedicado a mi adorada madre, por ser mi motivación diaria, mi estímulo y mi orgullo. Gracias por ser mi ejemplo de perseverancia, sacrificio y amor incondicional; también a mi padre por ser mi ángel guardián protector; finalmente a mi esposo y hermana, porque a través de su amor y comprensión me motivaron a seguir adelante.

Mauricio Guerreros Rojas
Dedicado a mi madre, padre y mi abuela.

AGRADECIMIENTO

Keyla Katherine Cuellar Chuquiyuri,
A nuestras familias y amistades, que estuvieron presentes para permitirnos seguir adelante para conseguir nuestros sueños y objetivos en la vida. También un agradecimiento especial al Dr. Emilio Martin Colchado Ruiz, por su invaluable apoyo y guía durante el transcurso del desarrollo de la presente tesis.

Mauricio Guerreros Rojas
A mi madre, padre, mi abuela y amigos por la confianza y apoyo.

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Autenticidad del Asesor

Yo, EMILIO MARTIN COLCHADO RUIZ, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ATE, asesor de Tesis titulada: "Regulación del hacking ético: prueba de vulnerabilidad sorpresiva y la exclusión en la subsunción de los delitos de acceso ilícito", cuyos autores son CUELLAR CHUQUIYURI KEYLA KATHERINE, GUERREROS ROJAS MAURICIO, constato que la investigación tiene un índice de similitud de 15.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 10 de Julio del 2023

Apellidos y Nombres del Asesor:	Firma
EMILIO MARTIN COLCHADO RUIZ **DNI:** 18149033 **ORCID:** 0000-0003-0462-9757	Firmado electrónicamente por: ECOLCHADOR el 24-07-2023 22:01:46

Código documento Trilce: TRI - 0584626

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Originalidad de los Autores

Nosotros, CUELLAR CHUQUIYURI KEYLA KATHERINE, GUERREROS ROJAS MAURICIO estudiantes de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ATE, declaramos bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Regulación del hacking ético: prueba de vulnerabilidad sorpresiva y la exclusión en la subsunción de los delitos de acceso ilícito", es de nuestra autoría, por lo tanto, declaramos que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. Hemos mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

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

Nombres y Apellidos	**Firma**
KEYLA KATHERINE CUELLAR CHUQUIYURI **DNI:** 48484801 **ORCID:** 0000-0002-5520-7661	Firmado electrónicamente por: KCUELLARC el 10-07-2023 08:28:14
MAURICIO GUERREROS ROJAS **DNI:** 75518977 **ORCID:** 0000-0002-4122-9376	Firmado electrónicamente por: GGUERREROSRO el 10-07-2023 08:16:50

Código documento Trilce: TRI - 0584629

INVESTIGA UCV

ÍNDICE DE CONTENIDOS

ÍNDICE DE GRÁFICOS Y FIGURAS

ÍNDICE DE TABLAS

RESUMEN

En la presente investigación titulada “Regulación del hacking ético: prueba de vulnerabilidad sorpresiva y la exclusión en la subsunción de los delitos de acceso ilícito”; en tal sentido, el objetivo general que se tuvo fue determinar si debería regularse el hacking ético para excluirlo del delito de acceso ilícito.

Por otro lado, el tipo de investigación fue básico, y con nivel jurídico – propositivo; asimismo, se tuvo como participantes la DIVINDAT, y los operadores jurídicos del Centro de Lima; y se tuvo 10 participantes. Entre las técnicas que se usaron fue la entrevista y el análisis documental, y como instrumentos guía de entrevista y guía de análisis documental.

De los principales hallazgos se obtuvo que el 100% de los entrevistados afirman que sí, debería regularse el hacking ético incidiendo en la exclusión en la subsunción de los delitos de acceso ilícito; lo cual se contrastó con 25 autores entre artículos científicos y libros.

Finalmente, entre las conclusiones se estableció que no existe en el Perú, una regulación exacta del hacking ético por lo cual existe la posibilidad de procesarse penalmente por el delito de acceso ilícito a hackers grises.

Palabras clave: Hacking ético, hackers, exención, subsunción, exclusión.

ABSTRACT

In the present investigation entitled "Regulation of ethical hacking: surprising vulnerability test and exclusion in the subsumption of crimes of illegal access"; In this sense, the general objective was to determine if ethical hacking should be regulated to exclude it from the crime of illegal access.

On the other hand, the type of investigation was basic, and with a legal - purposeful level; likewise, the population was DIVINDAT, and the legal operators of the Center of Lima; and 10 participants were sampled. Among the techniques that were used was the interview and documentary analysis, and as interview guide instruments and documentary analysis guide.

The main findings it was obtained that 100% of the interviewees affirm that yes, ethical hacking should be regulated, influencing the exclusion in the subsumption of crimes of illegal access; which was contrasted with 25 authors between scientific articles and books.

Finally, among the conclusions it was established that there is no exact regulation of ethical hacking in Peru, for which there is the possibility of criminal prosecution for the crime of illegal access to gray hackers.

Keywords: Ethical hacking, hackers, exemption, subsumption, exclusion.

I. INTRODUCCIÓN

El hacking ético se caracteriza como un nuevo método que busca mejorar la seguridad en los bancos de datos de las empresas a través de pruebas de vulnerabilidad, específicamente en sistemas de protección de datos. Este método podría ser interpretado como una conducta que se subsume en el delito de acceso ilícito, toda vez que las conductas sancionadas en dicho delito son semejantes a las circunstancias que se realiza en el hacking ético, es decir, ambas consisten en el ingreso forzado a un sistema informático de datos, no obstante, la diferencia entre estas recae en la finalidad, pues el acceso ilícito tiene por característica la obtención de beneficios ilícitos y por contrario el hacking ético busca la compensación para mejorar la seguridad de un sistema informático (por medio de la contratación de un servicio). Por ejemplo, esta diferencia se aprecia en el país de Argentina donde el hacking ético se encuentra regulado, identificándose que conductas son reprochables, sin dejar de lado el elemento subjetivo esencial del tipo penal del delito de acceso ilícito, es decir la acción que se ejerce bajo dolo, conforme el artículo segundo del Convenio de Budapest, donde se menciona que la naturaleza del delito de acceso ilícito es “la intención de obtener datos informáticos u otra intención delictiva”. Del mismo modo, según Giménez (2021) la prueba de vulnerabilidad puede representarse como una acción profesional que tiene por motivo principal advertir la vulnerabilidad de la base de datos para evitar el acceso ilícito, o proponer capacitaciones con fines lucrativos con el objetivo de mejorar la seguridad de un sistema informático de protección de datos.

Por otro lado, se advierte que en el Perú no existe una regulación específica sobre el hacking ético o su procedimiento, sin embargo, es menester mencionar que la resolución ministerial N° 004-2016-PCM, que se emitió por la Oficina Nacional de Gobierno Electrónico e Informática de la Presidencia del Consejo de Ministros- ONGEI-PCM, realiza la diferencia del “hacking ético” o pruebas de vulnerabilidad con el delito de acceso ilícito, señalando que las pruebas de vulnerabilidad serán sancionadas penalmente, en las siguientes circunstancias: i) ingresar sin autorización del titular es sancionado como delito

de acceso ilícito, ii) o exceder los límites autorizados.

Al respecto, es relevante acotar que las condiciones impuestas para las pruebas de vulnerabilidad son contradictorias al requisito o la propia naturaleza del hacking ético, ya que no concuerda con los fines y métodos del hacking ético, lo cual advierte Beltrán (2021) al indicar que "(…) el hacking ético es un método por el cual se propone una penetración en la que el evaluador asume el papel de un atacante blanco o legítimo que se sostiene bajo la necesidad de un acto sorpresiva" (p. 32), asimismo, indica que "los métodos son aquellos que se usan con fines de mayor protección que tiene utilidad el hacking ético" (p. 33).

Por tanto, la presente investigación tendrá en cuenta la tipificación actual del acceso ilícito y la necesidad de regular el hacking ético en el Perú, además la disyuntiva sobre la forma que se realiza el hacking ético, y como dicha forma se interpreta indebidamente como una conducta sancionada penalmente por el delito de acceso ilícito.

En este sentido, la formulación del problema, se realizará de la siguiente forma: Problema general: ¿Debería regularse el hacking ético incidiendo en la exclusión en la subsunción de los delitos de acceso ilícito? Problemas específicos: Primer problema específico: ¿La regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito? Segundo problema específico: ¿La regulación de un post registro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito?

Por otro lado, los supuestos en atención a los problemas descritos, serán los siguientes: Supuestos: Supuesto general: Sí, debería regularse el hacking ético incidiendo en la exclusión en la subsunción de los delitos de acceso ilícito. Supuestos Específicos: Primer Supuesto Específico: Si, debería regularse la prueba de vulnerabilidad sorpresiva por hacking ético para excluirlo de la subsunción de los delitos de acceso ilícito. Segundo Supuesto Específico: Sí, debería regularse un post registro como requisitos del hacking ético permite excluirlo de la subsunción de los delitos de acceso ilícito.

Ahora, en cuanto los objetivos que se formularon en razón a los problemas de la investigación, se tienen los siguientes: Objetivos: Objetivo general: Determinar si debería regularse el hacking ético incidiendo en la exclusión en la subsunción de los delitos de acceso ilícito. Objetivos Específicos: Primer Objetivo Específico: Determinar si la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito. Segundo Objetivo Específico: Determinar si la regulación de un post registró como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito.

Finalmente, la justificación o razones por las cuales se realiza la presente investigación, se expone en tres justificaciones, que son las siguientes:

i) Justificación teórica: Esta postura radica bajo el contexto que existe una escasa regulación sobre el hacking ético y las perspectivas para evitar un futuro delito cibernético, ya que existen vacíos legales, por ejemplo, el infringir la no divulgación de los aspectos de vulnerabilidad, entre otros como los requisitos, establecidos en la Resolución ministerial N° 004-2016-PCM, que se emitió por la Oficina Nacional de Gobierno Electrónico e Informática de la Presidencia del Consejo de Ministros- ONGEI-PCM; ii) Justificación práctica: Se busca fortalecer la escasa regulación sobre el hacking ético y las perspectivas para evitar un futuro delito cibernético (acceso ilícito), brindando nuevas formas para fortalecer y promover practicas completamente éticas o controladas; y iii) Justificación metodológica: Permite deslindar y desarrollar nuevas nociones, a fin de generar nuevos estudios referentes a la presente investigación.

II. MARCO TEÓRICO

Se desarrolla los antecedentes internacionales y nacionales, así como las teorías relacionadas con el tema.

En ese sentido, respecto a los **antecedentes internacionales,** podemos señalar a Rincón (2018), en su tesis "*El delito en la cibersociedad y la justicia penal internacional*, que sustento la Universidad Complutense de Madrid, optando el grado de doctor, tuvo como enfoque cualitativo y como objetivo, propone una clara diferencia sobre los delitos informáticos, electrónicos y de las telecomunicaciones en la competencia del Estatuto de Roma. Entre las conclusiones que realizó el autor, se podrá destacar que el uso de las tecnologías y la racionalidad de la ciencia permiten identificar los principales aspectos sobre las diferencias entre delitos informáticos.

Con relación a la conclusión del autor, se podrá destacar que el autor uso de las tecnologías es común que existan fraudes que devienen del uso de los sistemas informáticos, principalmente del acceso ilícito con la finalidad de tener ventaja sobre los métodos comerciales.

Por otro lado, González (2018), en su investigación titulada "*Delincuencia informática: daños informáticos del artículo 264 del Código Penal y propuesta de reforma*", que fue realizada Universidad Complutense de Madrid, y en la cual tuvo como enfoque cualitativo y como objetivo ofrecer una visión general de la delincuencia informática en la actualidad, destacándose entre estos el hacking.

En ese sentido, se destaca entre sus conclusiones que la expansión exponencial de la ciberdelincuencia identificando que existen casos particulares donde se establece factores relevantes sobre el hacking ético y otros tipos de hacking ilícitos.

De la conclusión destacada, se debe tener en cuenta que el aporte a la investigación radica sobre el énfasis que realiza sobre los métodos para mejorar la seguridad cibernética, indicando entre estas el uso del hacking ético o pruebas de vulnerabilidad.

Por otro lado, de las investigaciones nacionales, se debe destacar a Paredes (2013) en su tesis; utilizando el método descriptivo tuvo como objetivo determinar las modalidades en la comisión de delitos cometidos con el uso de sistemas informáticos.

En ese contexto, de las conclusiones se destaca que “las conductas más graves son las intrusiones (hacking) y el acceso y comercialización no autorizados a base de datos son aquellas que se usan mediante el menoscabo de seguridad informática” (p.123), precisando que el delito del hacking se realiza siempre con la finalidad dolosa de comercialización.

En este sentido, Maritza (2022) en su tesis titulada “*Mecanismos de prevención y protección del bien jurídico tutelado frente a la modalidad delictiva phishing en el ordenamiento jurídico penal peruano*”, aplicando el método descriptivo, tuvo como objetivo determinar el bien jurídico tutelado frente la modalidad delictiva phishing.

Es así, que de las conclusiones se destaca que es un supuesto de hacking puro o blanco, donde se verifica si existe un mero acceso de datos o si existe una vulnerabilidad grave que pone en riesgo datos.

A ello se debe agregar que Olivares y Ceras (2021) en su tesis “*Delitos informáticos y la evidencia digital en el proceso peruano del distrito judicial de Junín, 2020”*, aplicó el método descriptivo, tuvo como objetivo determinar si el delito informático evidencia los efectos negativos digitalmente en la comisión de delitos informáticos.

En este contexto, se destaca de las conclusiones de los autores, que los hackers podrían ser referidos como hackers éticos, y estos son contratados por empresas, en cambio, los Crackers son generalmente personas que se introducen a sistemas informáticos remotos con la intención de destruir datos que altera el sistema.

Así también, Infante (2019) en su tesis “*Análisis del delito de hurto de identidad virtual: frente a la seguridad de los sistemas informáticos*”, aplicó el método descriptivo, tuvo como objetivo identificar las modalidades de hurto de

identidad virtual. En este sentido de los principales aspectos que desarrolla el autor es realizar una diferencia entre los hackers blanco, negro, y gris.

En ese sentido, entre las conclusiones se destacó que la División de investigación de delitos de alta tecnología sostienen que es un acto símil a la intrusión como fines de beneficio a personas o centros institucionales, que se denomina en otros países americanos como “criminal hacker”, no obstante, la diferencia con el hacker ético parte de la evaluación de un fin legítimo informal.

Finalmente, de las conclusiones destacadas por los autores Paredes (2013), Olivares y Ceras (2021), Maritza (2022) e Infante (2019), se podrá interpretar como aporte a la investigación, la distinción sobre los tipos de hackers, la repercusión e importancia sobre los métodos de fortalecimiento de los métodos de protección de la base de datos y los sistemas informáticos, así como la forma en la que se investiga los delitos informáticos por la División de investigación de delitos de alta tecnología.

Sobre las teorías relacionadas con el tema, cabe precisar que la regularización del hacking ético, se puede definir como la ruptura de la seguridad informática para mejorar su protección ante cualquier tipo de programa de hackeo que se use para vulnerar cualquier base de datos. En este contexto, cabe mencionar que en el Perú se ratificó la Convención contra la Ciberdelincuencia de Budapest en el año 2013, promulgándose la ley que regula los delitos informáticos (ley N° 30096); sin embargo, se advierte que de los tipos penales que son necesarios de atender, por encontrarse disyuntivas en su práctica, tenemos a los delitos contra datos y sistemas informáticos, siendo uno de los delitos de mayor relevancia el acceso ilícito a la información, que sanciona penalmente las siguientes conductas: i) al sujeto que pese a no tener autorización para el ingreso al sistema informático penetra en la base de datos; ii) o en el caso que excediendo los límites permitidos accede a datos sin autorización. Al respecto, es imprescindible precisar que serán punibles las conductas antes mencionadas, siempre y cuando se efectúe una ruptura de las medidas de seguridad establecidas por la entidad o centro “bancario de datos”.

De lo acotado precedentemente se podrá identificar la controversia de la

investigación que radica en determinar que conductas son sancionables penalmente y como se diferencia el hacking ético con las conductas típicas antes descritas.

De manera que, considerando la controversia descrita, corresponde señalar que el hacking ético se caracteriza como un nuevo método que busca mejorar la seguridad en los bancos de datos de las empresas a través de pruebas de vulnerabilidad, específicamente en sistemas de protección de datos. Este método podría ser interpretado como una conducta que se subsume en el delito de acceso ilícito, toda vez que las conductas sancionadas en dicho delito son semejantes a las circunstancias que se realiza en el hacking ético, es decir, ambas consisten en el ingreso forzado a un sistema informático de datos, no obstante, la diferencia entre estas recae en la finalidad, pues el acceso ilícito tiene por característica la obtención de beneficios ilícitos y por contrario el hacking ético busca la compensación para mejorar la seguridad de un sistema informático (por medio de la contratación de un servicio). Por ejemplo, esta diferencia se aprecia en el país de Argentina, donde el hacking ético se encuentra regulado identificándose que conductas son reprochables, sin dejar de lado el elemento subjetivo esencial del tipo penal del delito de acceso ilícito, es decir la acción que se ejerce bajo dolo, conforme el artículo segundo del Convenio de Budapest, donde se menciona que la naturaleza del delito de acceso ilícito es “la intención de obtener datos informáticos u otra intención delictiva”. Del mismo modo, según Giménez (2021) la prueba de vulnerabilidad puede representarse como una acción profesional que tiene por motivo principal advertir la vulnerabilidad de la base de datos para evitar el acceso ilícito, o proponer capacitaciones con fines lucrativos con el objetivo de mejorar la seguridad de un sistema informático de protección de datos.

Por otro lado, se advierte que en el Perú no existe una regulación específica sobre el hacking ético o su procedimiento, sin embargo, es menester mencionar que la resolución ministerial N° 004-2016-PCM, donde se aprecia que el Consejo de Ministros- ONGEI-PCM, realiza la diferencia del “hacking ético” o pruebas de vulnerabilidad con el delito de acceso ilícito, señalando que las pruebas de vulnerabilidad serán sancionadas penalmente, en las siguientes circunstancias: i) ingresar sin autorización del titular es sancionado como delito

de acceso ilícito, ii) o exceder los límites autorizados.

Al respecto, es relevante acotar que las condiciones impuestas para las pruebas de vulnerabilidad son contradictorias al requisito o la propia naturaleza del hacking ético, ya que no concuerda con los fines y métodos del hacking ético, lo cual advierte Beltrán (2021) al indicar que "(…) el hacking ético es una forma de prueba de penetración, teniendo como naturaleza el fortalecimiento de base de datos y sistemas de acopio" (p. 32), asimismo, indica que el "hacking ético se encuentran libres en el mercado y se pueden aplicar para lograr una mayor protección" (p. 33).

Ahora sobre los aspectos normativos a nivel nacional, se advierte que la Constitución del Perú comprende únicamente de forma general en el artículo 2 los derechos fundamentales, de los cuales se encuentra establecido el secreto y la inviolabilidad de sus comunicaciones y documentos privados; por lo que desde un aspecto general se puede apreciar que la carta magna no permite alguna forma de realizar pruebas de vulnerabilidad.

Sin embargo, es necesario mencionar que los delitos informáticos surgen con el Convenio sobre criminalidad informática de Budapest en el año 2004; y que desde dicha fecha se han aplicado vía tratados la aplicación de normas que busquen promover la seguridad de datos informáticos, así como la lucha sobre la criminalidad informática. Es decir, desde la fecha que se dio este Convenió el Perú ratifico dicho convenio por lo que se aplicaría el control convencional a través del principio de especialidad; y por ende es posible afirmar y sostener que el artículo 2 que regula el acceso ilícito en dicho convenio es aplicable en nuestra legislación.

Cabe precisar que según el Área de asesoría técnica parlamentaria (2020), de la biblioteca del Congreso Nacional de Chile, expone a través del autor Juan Cavada Herrera que "el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático" (p. 5). En tal virtud de podrá deducir que todo acto que quiera sancionarse por la penetración de datos exige que se pruebe la intencionalidad

dolosa o delictiva para lo cual se realiza una conexión por los sistemas informáticos.

Por lo tanto, normativamente no existe una regulación exacta sobre las pruebas de vulnerabilidad, más que el artículo 12 de la ley de delitos informáticos que establece la exención de la responsabilidad en casos de acceso ilícito (y otros delitos) se realice previa autorización por la prueba de vulnerabilidad; es decir existen circunstancias especiales que habilita una excepción; por lo que será necesario evaluar desde un control convencional y especializados que la regulación del hacking ético es contrario a la norma Constitucional.

Finalmente se procede a presentar términos básicos para el entendimiento del presente estudio:

Hacking de caja blanca: Es aquella que se realiza el test con conocimiento completo y previo de la infraestructura que será probada, y es realizado con el apoyo de personal interno.

Hacking de caja gris, parte de un conocimiento parcial del cual no se tiene un completo conocimiento sobre la infraestructura, además suele ser realizada como pentest a través de empresas especializadas.

Hacking de caja negra, es aquella que no se realiza con ningún conocimiento previo de la infraestructura a ser probada, y es la prueba que se realiza con mayor realidad.

Black Hat Hackers, el cual es conocimiento como los sombreros negros que son aquellos profesionales que tienen conocimientos exactos para ingresar a la seguridad de sistemas o computadoras, creando virus con intensiones indebidas, es decir que las actividades que realizan no son éticas.

White Hat Hackers, que son denominados sombreros blanco, que son comúnmente aquellos que realizan hacking ético, y poseen la ética de trabajar bajo una organización disponiendo de sus conocimientos en beneficio y mejora de la seguridad de las empresas.

Grey Hat Hackers, que son aquellos que reconocen ser hackers de sombrero gris, pues poseen una ética semi ambigua porque usan sus conocimientos bajo la práctica similar de los hackers de sombrero negro, pues ingresan a base de datos usando las prácticas de los hackers negros, hallando vulnerabilidad y luego pueden presentarse ante la entidad para su arreglo, es decir se puede lograr atender la vulnerabilidad conociéndose a través de estas prácticas, sin ningún previo acuerdo o contrato como en los casos de hackers de sombreros blancos.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

3.1.1. Tipo de Investigación

Se usó el tipo de investigación **básica**, ya que principalmente la investigación busca generar un nuevo conocimiento, explícitamente la diferencia y regulación del hacking ético en el sistema jurídico penal peruano, donde se encuentra regulado el acceso ilícito como la única forma de penetración a una base de datos (Hernández, Fernández y Baptista, 2014).

Ahora en relación, con dicho tipo de investigación se utilizará el siguiente subtipo:

Jurídico –propositivo:
Se buscó categorizar los requisitos y condiciones para la ejecución de pruebas de vulnerabilidad (hacking ético) a través de un protocolo administrativo aprobado por la ANPD (Autoridad Nacional de Protección de Datos Personales), a fin de que se regule como exención en delito de acceso ilícito que guarda relación a la ley de delitos informáticos. Es decir, que se sancione la conducta de penetrar barreras de seguridad en un sistema informático, salvo los casos que se acredite pruebas de vulnerabilidad. Cabe precisar que el tipo de investigación se caracteriza por la proposición de una modificación normativa (Guamán, Hernández; Yuqui, Llloay, 2021).

3.1.2. Diseño de investigación

Se usó la teoría fundamentada que consiste en el análisis de las características, requisitos y alcances teóricas sobre el hacking ético a fin de identificar una postura; lo cual se corroboró con los instrumentos para establecer una conclusión (Hernández, Fernández y Baptista, 2014).

En este sentido, cabe precisar que se utilizó como fuentes las siguientes:

Fuentes primaria

En la investigación se usó la ley de delitos informáticos, y las 3 sentencias sobre el acceso ilícito que se dio en el Perú en el año 2018 y 2021.

Fuentes secundaria

Se usó la doctrina o textos especializados, explícitamente al autor Magliona (2021) quien expone las condiciones y características del hacking ético.

3.2. Categorías, Subcategorías y matriz de categorización

Tabla N° 1

Categorías, Subcategorías y matriz de categorización

Categorías	Definición Conceptual	Subcategorías	Definición Conceptual
REGULACIÓN DEL HACKING ETICO	El hacking ético es aquella figura técnica que significa prueba de vulnerabilidad de un sistema informático (Beltrán, 2021.	Pruebas de vulnerabilidad sorpresiva	Son aquellas pruebas que tiene la finalidad penetrar una base de datos bajo la aplicación de procedimientos, que pueden ser adoptados de mayor o menor riesgo.
		Post registro para ofrecimiento de servicios	Es un requisito que se exige como condición para comprobar un acto ético con fines de fortalecer la base de datos.
EXCLUSIÓN EN EL DELITO DE ACCESO ILICITO	Son formas de excluir típicamente la conducta sobre un hecho típico (delito regulado) (Beltrán, 2021.	Autorización previa	Es un requisito establecido para la exención de la responsabilidad en casos de acceso ilícito (art. 12° de la Ley de delitos informáticos)
		Exclusión por fin licito	La exclusión o exención es una circunstancia que anulan la responsabilidad bajo la observancia de conductas o requisitos independientes al hecho típico (Beltran, 2021).

3.3. Escenario de estudio

El escenario de estudio serán los juzgados y fiscalías en el Centro de Lima, y la Dirincrip, ubicado en la Av. España en el Cercado de Lima.

3.4. Participantes

Los participantes se conformaron con personal de la División de Delitos de Alta Tecnología de la Unidad – DIRINCRI España, que se encargan de delitos de acceso ilícito en la Av. España en el Cercado de Lima. Además, por los fiscales adjuntos y asistentes en función fiscal de las Fiscalías Corporativa Provincial Penal de Lima (Sede Marte- Centro de Lima) y Jueces en lo penal que tengan subespecialidad en delitos informáticos. Anexo 5)

En tal sentido para la aplicación de los participantes se tomó los siguientes criterios de inclusión y exclusión:

Criterios de inclusión: Para la División de delitos de alta tecnología se tendrá en cuenta a los brigadieres que tengan 2 años en la división de investigación. Asimismo, para los fiscales y jueces se tendrá en cuenta aquellos que tengan mayor de 5 años ejerciendo el cargo.

Criterios de exclusión: Los que no cumplan con los criterios de inclusión.

En virtud a los criterios antes expuestos se presenta la siguiente tabla:

N°	APELLIDOS Y NOMBRES	CARGO
1	MARIA DEL CARMEN PEREYRA ROCA	FISCAL ADJUNTO PROVINCIAL MINISTERIO PUBLICO
2	SALLY VICTORIA SALAZAR TORRES	ASISTENTE EN FUNSION FISCAL
3	JOEL BRAVO YUCRA	ABOGADO EN DERECHO PENAL
4	EDDER JIMENEZ SANCHEZ	ABOGADO EN DERECHO PENAL
5	CESAR ALEJANDRO FRANCO GONZALES	ABOGADO EN DERECHO PENAL
6	DANIEL IGNACIO SANTOS SANTOS	JUEZ TITULAR EN EL JUZGADO ESPECIALIZADO PENAL
7	CRISTIAN DOMINGUEZ MALPARTIDA	ABOGADO EN DERECHO PENAL

8	EDGAR ORLANDO PRADO DE LA CRUZ	INGENIERO EN PERITO DE LA DIVINDAT
9	ANA MARIA GOTUZZO ORTIZ	ABOGADO EN DERECHO PENAL
10	MIGUEL ANGEL VEGAS VACCARO	ABOGADO EN DERECHO PENAL

3.5. Técnicas e instrumentos de recolección de datos

Técnicas

La técnica que se aplicó es la **entrevista,** que según Romero (2018) que permitió recabar información detallada de especialistas en el campo, en relación a cada objetivo, los cuales serán operadores jurídicos de Lima.

Por otro lado, se usó el **análisis documental** que según Romero (2018) permite identificar y localizar cualquier documento, así como conocer su contenido relevante para la investigación relacionado con el hacking ético y su diferencia en el delito de acceso ilícito en la ley de delitos informáticos (Ley N.º 30096).

Instrumento

El instrumento aplicable en el presente estudio serán los siguientes:

Guía de Entrevista: Es un documento por el cual se postuló preguntas específicas, abiertas o cerradas, en relación con los objetivos de estudio y sus categorías.

Descripción del Instrumento: En este sentido, en la presente se usó dos preguntas por cada objetivo.

Guía de análisis documental: Se utilizó una estructura por la cual permitió analizar documentos específicos que tengan relación con la regulación o jurisprudencial respecto al hacking ético y su diferencia o exclusión en la subsunción de los delitos de acceso ilícito.

3.6. Procedimiento

Se aplicaron los instrumentos y ejecutarlo en la DIRINCRI- Aramburu, la

Fiscalía corporativa de Lima Centro, y el Juzgado de Lima- sede Barreto. Luego se procedió a realizar la triangulación de los hallazgos, las teorías y los antecedentes para establecer una postura.

3.7. Rigor científico

Se procedió a entregar los instrumentos para que sean validados por tres expertos los cuales se encuentran en anexos (anexo 3), con lo cual se aprecia que el rigor científico es de 90%.

N°	EXPERTOS	APELLIDOS Y NOMBRES	GRADO	CARGO	%
1	Metodólogo	Martin Emilio Colchado Ruiz	Magister	Docente UCV	95%
2	Abogado	Joel Bravo Yucra	Maestro	Juez en lo penal	95%
3	Abogado	Ada Marina Gotuzzo Ortiz	Maestro	Maestro	95%

3.8. Método de análisis de la información

Los métodos usados fueron:

Método de síntesis:

Se utilizó la síntesis en los datos que se obtengan en las entrevistas y el análisis de documentos de fuentes primarias y secundarias.

Método analítico:

Se utilizó analizando las posturas de los entrevistados y el resumen obtenido de la guía de análisis documental, identificando las principales características sobre el hacking ético, analizando su diferencia con el acceso ilícito.

Método deductivo:

A través de casos particulares que se obtuvo de la guía de análisis documental (jurisprudencia, sentencias u estudios especializados sobre el hacking ético) se abordó los principales elementos para identificar las conductas del hacking ético.

3.9. Aspectos éticos

Se consideró para la elaboración del presente estudio el uso de las normas apa para respetar el derecho de autor, respetando el código de ética; asimismo se cumple con las condiciones y requisitos de la guía de elaboración de tesis, aprobada por la Universidad Cesar Vallejo; así como también se verificó los derechos de autor a través del programa de similitud de antiplagio “turnitin”.

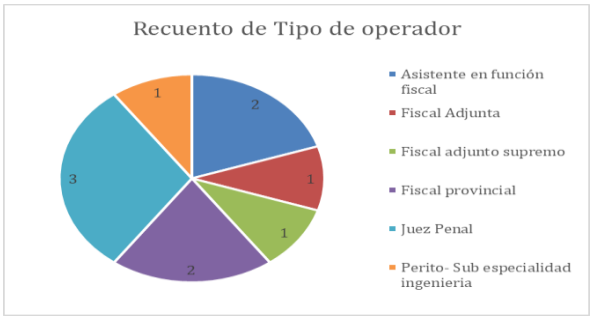
IV. RESULTADOS Y DISCUSIÓN

En el capítulo se presenta en principio el cuadro de participantes, con su tabla y figura respectivo, y luego por cada objetivo específico, se presenta figuras según posturas. Asimismo, de los resultados del análisis documental de artículos tesis y libros analizados para finalmente realizar la discusión pertinente.

Tabla N° 2
Tipo de operador

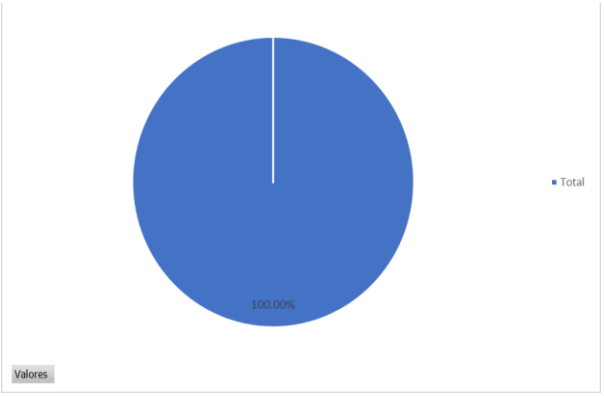
Entrevistados	Recuento de entrevistados por operador
Asistente en función fiscal	**2**
Salazar (2023)	
Santos (2023)	
Fiscal Adjunta	**1**
Pereyra (2023)	
Fiscal adjunto supremo	**1**
Vegas (2023)	
Fiscal provincial	**2**
Gotuzza (2023)	
Prado (2023)	
Juez Penal	**3**
Bravo (2023)	
Franco (2023)	
Jiménez (2023)	
Perito- Sub especialidad ingeniería	**1**
Domínguez (2023)	
Total general	**10**

Figura N° 1.
Tipo de operador



Ahora bien, en cuanto al Objetivo General, que consiste: determinar si debe regularse el hacking ético para excluirlo del delito de acceso ilícito, para tal se obtuvo la siguiente postura:

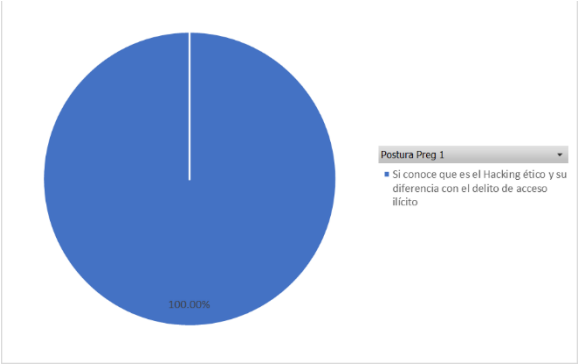
Figura N° 2.
Postura sobre el objetivo general por tipo de operador



Teniendo en cuenta la tabla y figura que antecede, se aprecia que de los 10 entrevistados, el 100% se encuentra de acuerdo que, si debe regularse el hacking ético para excluirlo del delito de acceso ilícito.

Ahora bien, en cuanto a la pregunta N° 1, se obtuvo el siguiente resultado:

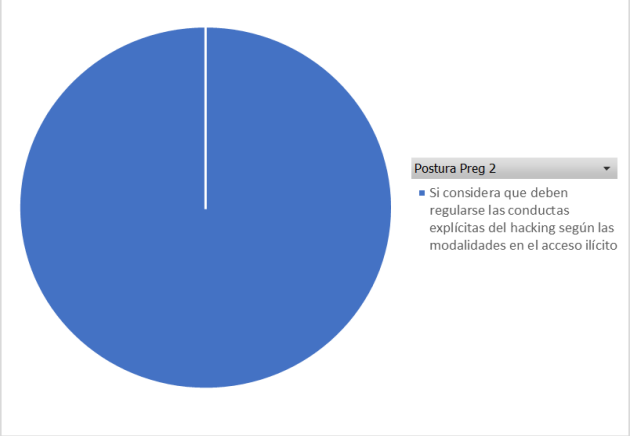
Figura N° 3.
Postura sobre pregunta 1



En este sentido se aprecia que, de la figura con anterioridad, la postura respecto a la pregunta N° 01, es que el 100% de los operadores jurídicos si conocen que es el Hacking ético y su diferencia con el delito de acceso ilícito.

Ahora bien, en cuanto a la pregunta N° 2, se tuvo la siguiente postura:

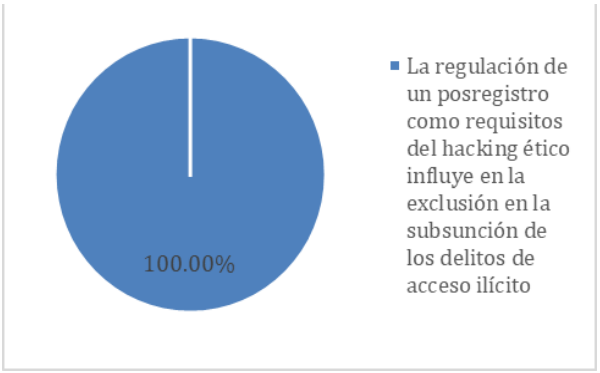
Figura N° 4.
Postura sobre pregunta 2



En este sentido de la figura que antecede se aprecia que, el 100% de los entrevistados respecto a la pregunta N° 2, refirieron que si considera que deben regularse las conductas explícitas del hacking según las modalidades en el acceso ilícito.

Ahora bien, respecto al Objetivo Específico 1, que consiste en determinar si la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito, se obtuvo la siguiente postura:

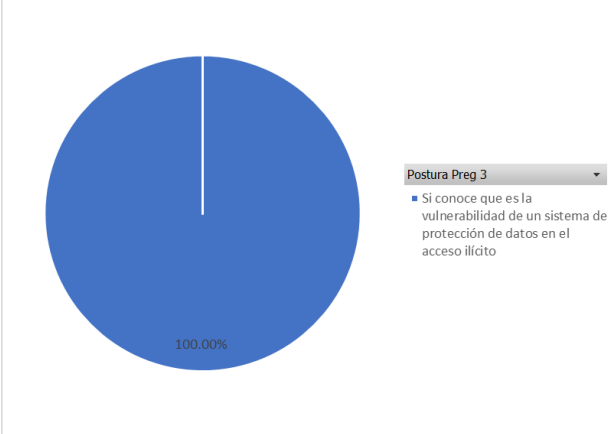
Figura N° 5
Postura sobre el objetivo específico 1 por tipo de operador



Teniendo en cuenta la tabla y figura que antecede, se aprecia que de los 10 entrevistados, el 100% se encuentra de acuerdo que, la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito.

Ahora bien, en cuanto a la pregunta N° 3, se obtuvo el siguiente resultado:

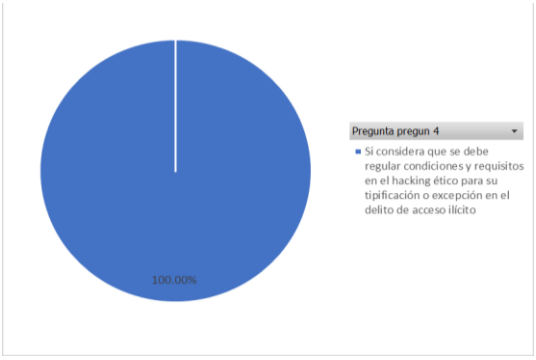
Figura N° 6.
Postura sobre pregunta 3



En este sentido se aprecia que, de la figura con anterioridad, la postura respecto a la pregunta N° 03, es que el 100% de los operadores jurídicos si considera que se debe regular condiciones y requisitos en el hacking ético para su tipificación o excepción en el delito de acceso ilícito.

Ahora bien, en cuanto a la pregunta N° 4, se tuvo la siguiente postura:

Figura N° 7.
Postura sobre pregunta 4

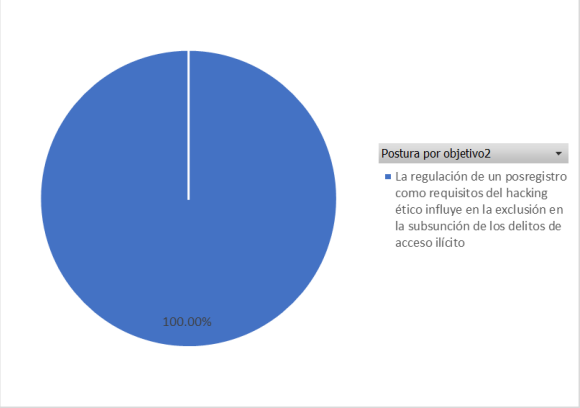


En este sentido de la figura que antecede se aprecia que, el 100% de los entrevistados respecto a la pregunta N° 4, refirieron que si considera que deben regularse las conductas explícitas del hacking según las modalidades en el acceso ilícito.

Ahora bien, respecto al Objetivo Específico 2, determinar si la regulación de un post registro como requisitos del hacking ético influye en la exclusión en la

subsunción de los delitos de acceso ilícito. En este sentido se obtuvo el siguiente resultado:

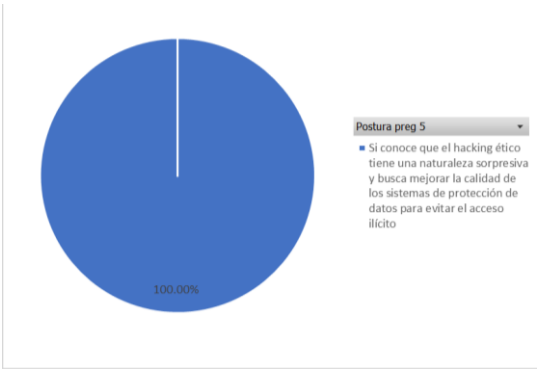
Figura N° 8.
Postura sobre el objetivo específico 2 por entrevistado



Teniendo en cuenta la tabla y figura que antecede, se aprecia que de los 10 entrevistados, el 100% se encuentra de acuerdo que, la regulación de un post registro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito.

Ahora bien, en cuanto a la pregunta N° 05, se obtuvo el siguiente resultado:

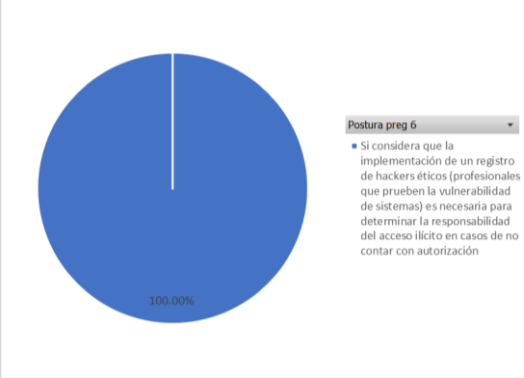
Figura N° 9.
Postura sobre pregunta 5



En este sentido se aprecia que, de la figura con anterioridad, la postura respecto a la pregunta N° 5, es que el 100% de los operadores jurídicos sí conocen que el hacking ético tiene una naturaleza sorpresiva y busca mejorar la calidad de los sistemas de protección de datos para evitar el acceso ilícito.

Ahora bien, en cuanto a la pregunta N° 6, se tuvo la siguiente postura:

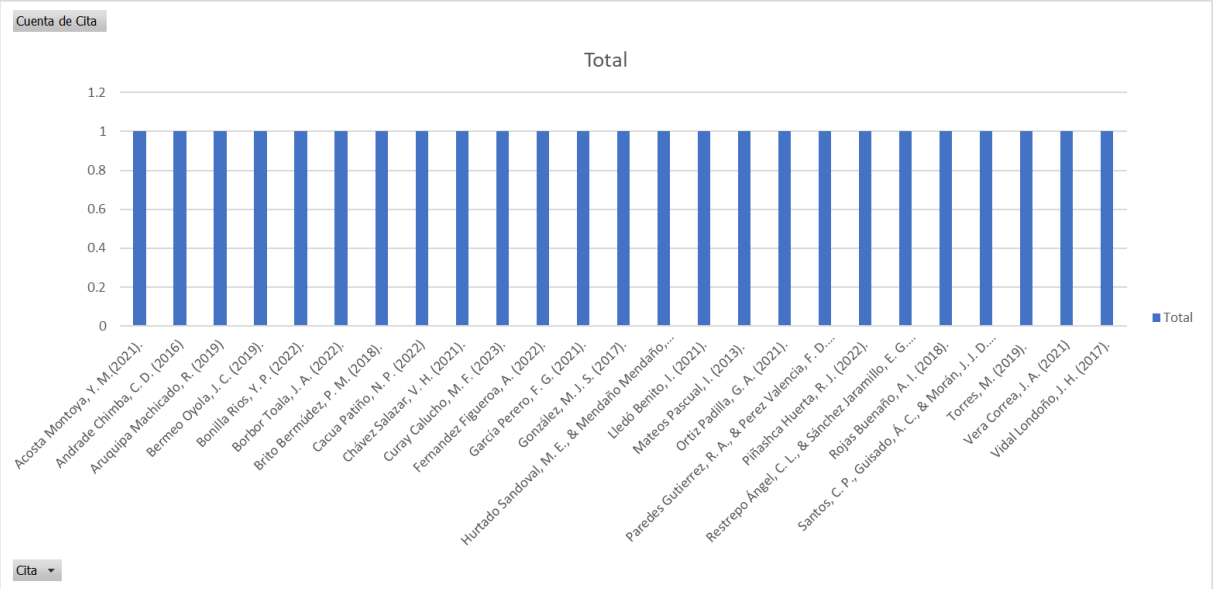
Figura N° 10
Postura sobre pregunta 6



En este sentido de la figura que antecede se aprecia que, el 100% de los entrevistados respecto a la pregunta N° 6, refirieron que si considera que deben regularse las conductas explícitas del hacking según las modalidades en el acceso ilícito.

De los resultados del análisis documental según posturas, se tiene que, de los documentos analizados, se precisa que constaron de artículos científicos y libros que fueron realizados por 25 autores, que se muestran a continuación:

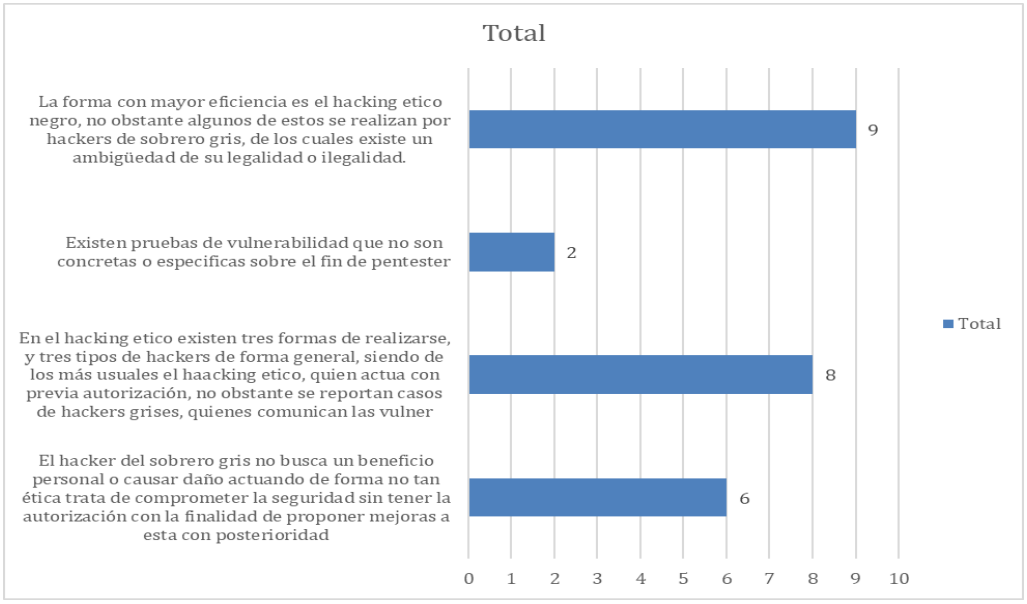
Figura N° 11
Posturas del análisis documental



Ahora bien, teniendo en cuenta los artículos y libros analizados, se presentan las posturas que se identificaron de dichos documentos, que constan en los siguientes:

En relación al objetivo general, se tuvo el siguiente resultado (ver tabla N° 6, anexo 3)

Figura N° 12
Postura sobre el análisis documental según objetivo general



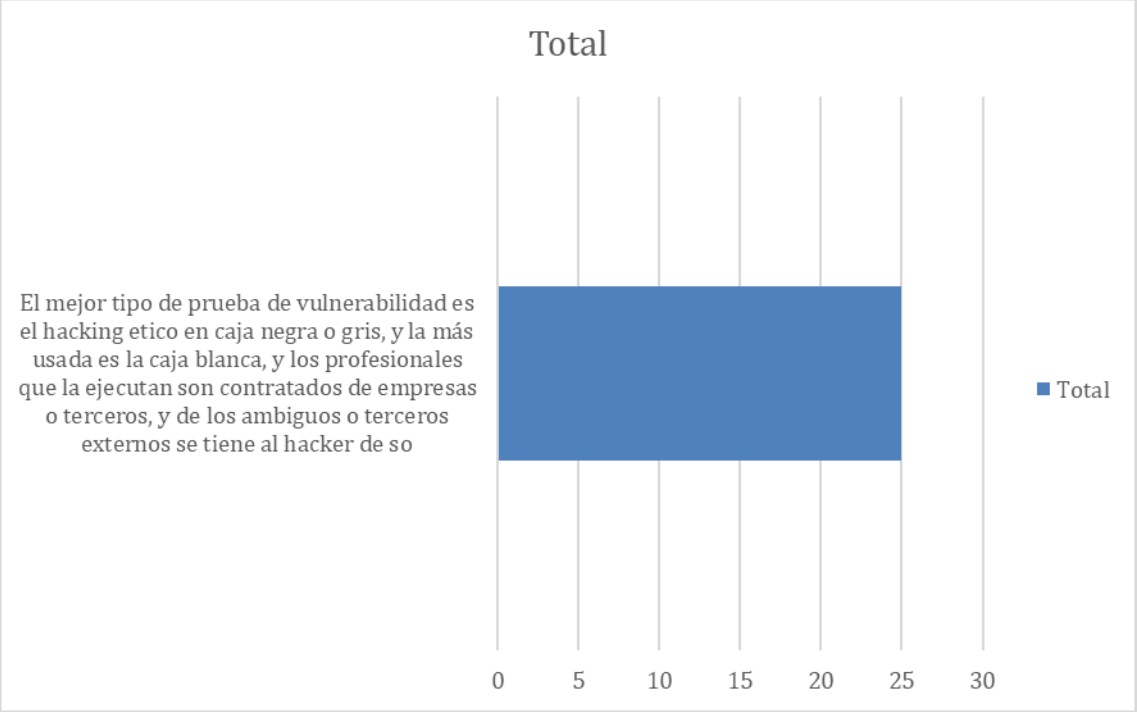
En este sentido de la figura que antecede se aprecia que, los autores Acosta Montoya (2021), Brito Bermúdez (2018), García Perero (2021), González (2017), Restrepo Ángel & Sánchez Jaramillo (2018) y Torres, M. (2019), señalaron que el hacker del sobrero gris no busca un beneficio personal o causar daño actuando de forma no tan ética trata de comprometer la seguridad sin tener la autorización con la finalidad de proponer mejoras a esta con posterioridad; asimismo, los autores Aruquipa Machicado (2019), Bonilla Rios (2022), Cacua Patiño (2022), Curay Calucho (2023), Fernández Figueroa (2022), Hurtado Sandoval & Mendaño (2016), Mateos Pascual (2013) y Rojas Buenaño (2018), señalaron que en el hacking ético existen tres formas de realizarse, y tres tipos de hackers de forma general, siendo de los más usuales el hacking ético, quien actúa con previa autorización, no obstante, se reportan casos de hackers grises, quienes comunican las vulnerabilidades con fines de obtener asesorías personales o practicar sus métodos. Por otro lado, los

autores Santos, Guisado & Morán (2017) y Vidal Londoño (2017) señalan que existen pruebas de vulnerabilidad que no son concretas o específicas sobre el fin de pentester.

Finalmente, los autores Andrade Chimba (2016), Bermeo Oyola (2019), Borbor Toala (2022), Chávez Salazar (2021), Lledó Benito (2021), Ortiz Padilla (2021), Paredes Gutierrez & Perez Valencia (2022), Piñashca Huerta (2022) y Vera Correa (2021), señalaron que la forma con mayor eficiencia es el hacking ético negro, no obstante, algunos de estos se realizan por hackers de sobrero gris, de los cuales existe una ambigüedad de su legalidad o ilegalidad.

Por otro lado, en cuanto a las posturas identificadas en relación al primer objetivo específico se tienen los siguientes:

Figura N° 13
Postura sobre el análisis documental según objetivo específico 1

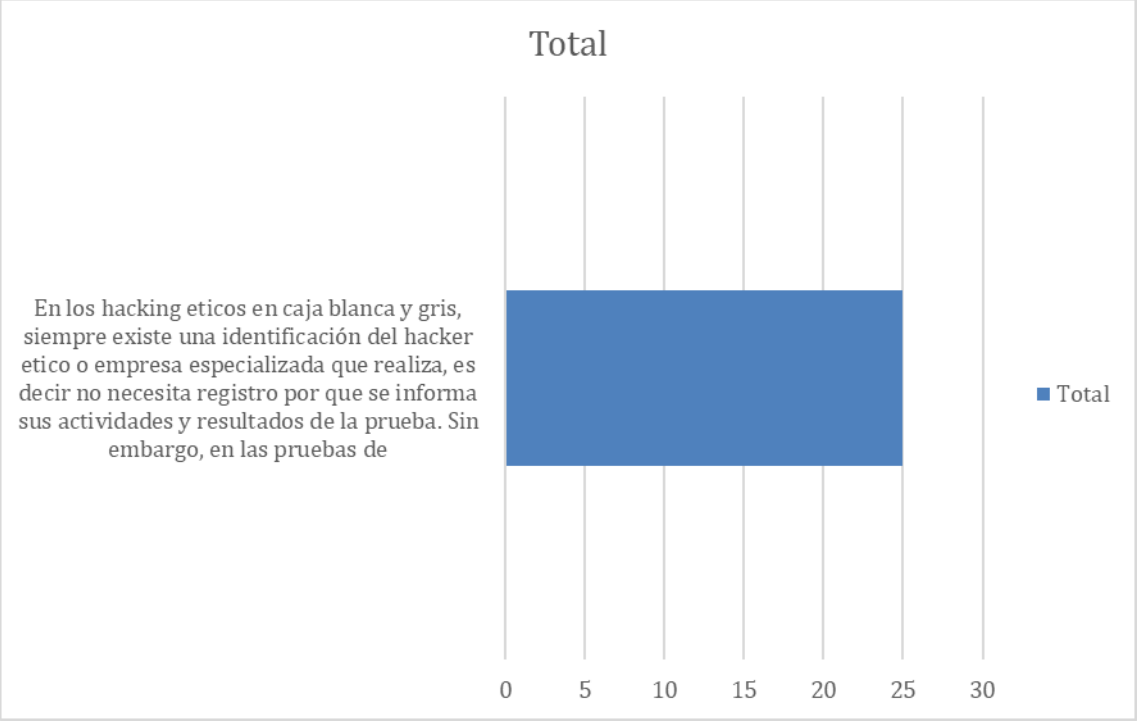


En este sentido de la figura que antecede se aprecia que, los autores Acosta Montoya (2021), Brito Bermúdez (2018), García Perero (2021), González

(2017), Restrepo Ángel & Sánchez Jaramillo (2018), Torres, M. (2019), Aruquipa Machicado (2019), Bonilla Rios (2022), Cacua Patiño (2022), Curay Calucho (2023), Fernández Figueroa (2022), Hurtado Sandoval & Mendaño Mendaño (2016), Mateos Pascual (2013), Rojas Buenaño (2018), Santos, Guisado & Morán (2017) y Vidal Londoño (2017), Andrade Chimba (2016), Bermeo Oyola (2019), Borbor Toala (2022), Chávez Salazar (2021), Lledó Benito (2021), Ortiz Padilla (2021), Paredes Gutiérrez & Pérez Valencia (2022), Piñashca Huerta (2022) y Vera Correa (2021), señalaron que el mejor tipo de prueba de vulnerabilidad es el hacking ético en caja negra o gris, y la más usada es la caja blanca, y los profesionales que la ejecutan son contratados de empresas o terceros, y de los ambiguos o terceros externos se tiene al hacker de sombrero gris, que su ética es ambigua, pero produce una mayor simulación a la realidad.

Finalmente, en cuanto a las posturas identificadas en relación al primer objetivo específico se tienen los siguientes:

Figura N° 14
Postura sobre el análisis documental según objetivo específico 2



En este sentido de la figura que antecede se aprecia que, los autores Acosta Montoya (2021), Brito Bermúdez (2018), García Perero (2021), González

(2017), Restrepo Ángel & Sánchez Jaramillo (2018), Torres, M. (2019), Aruquipa Machicado (2019), Bonilla Ríos (2022), Cacua Patiño (2022), Curay Calucho (2023), Fernández Figueroa (2022), Hurtado Sandoval & Mendaño Mendaño (2016), Mateos Pascual (2013), Rojas Buenaño (2018), Santos, Guisado & Morán (2017) y Vidal Londoño (2017), Andrade Chimba (2016), Bermeo Oyola (2019), Borbor Tóala (2022), Chávez Salazar (2021), Lledó Benito (2021), Ortiz Padilla (2021), Paredes Gutiérrez & Pérez Valencia (2022), Piñashca Huerta (2022) y Vera Correa (2021), señalaron que en los hacking éticos en caja blanca y gris, siempre existe una identificación del hacker ético o empresa especializada que realiza, es decir no necesita registro por que se informa sus actividades y resultados de la prueba. Sin embargo, en las pruebas de terceros externos, que se reportan no se cuenta con un registro y comúnmente solo se conoce los resultados, sin procedimiento y posterior al ataque el hacker profesional (hacker gris) pone en conocimiento para realizar pruebas de vulnerabilidad o solo realiza pruebas con fines de mejorar sus capacidades y con el fin de mejorar la seguridad de las empresas.

Discusión objetivo general:

Teniéndose los resultados de las entrevistas y el análisis documental que constan de artículos y libros sobre el hacking ético, se procede a realizar la discusión para lo cual se aplica la triangulación considerando los hallazgos, los antecedentes de investigación, la teoría o dogmática y la postura de los autores en relación a cada objetivo.

En este sentido, se procede a realizar el análisis respecto al objetivo general: “Determinar si debe regularse el hacking ético para excluirlo del delito de acceso ilícito”, para lo cual se analiza, lo siguiente:

En cuanto a las posturas de los entrevistados cabe precisar que de los 10 operadores precisaron que, si debe regularse el hacking ético, para lo cual Bravo, Franco y Jiménez (2023) hacen alusión que el hacking ético es una novedad que, si bien se encuentra establecido como una exclusión de la responsabilidad sobre el acceso ilícito, ello no evita que sean procesados casos sobre el hacking ético, hasta en los casos de hacking ético blanco al

inició de la regulación del delito de acceso ilícito. En este sentido agrega Prado (2023), que una de las deficiencias normativas en cuento a la regulación es la falta de subclasificación sobre los tipos de hacking y hackers, con lo cual se evitaría realizar una investigación innecesaria que finalmente no cumplirá con determinarse el fin doloso (acceso ilícito con fines de penetración y beneficio).

En este sentido cabe del análisis documental se pudo apreciar que nivel nacional e internacional no se ha regulado diferencias en cuanto al hacking ético y el acceso ilícito, así como tampoco se realizó una clasificación del hacking ético o los sujetos que realizan dicha actividad en los sistemas normativos de España, Colombia, Ecuador, y otros países; sin embargo, en Italia se hace una exclusión sobre las pruebas de vulnerabilidad, señalando Torres (2019) que para establecer la responsabilidad penal por el uso de inteligencias artificiales que realizan pruebas de vulnerabilidad deberá considerarse los aspectos de su programación y el profesional técnico que realiza dicha programación. En tal contexto, de las principales posturas de los autores, entre estos Acosta Montoya (2021), Brito Bermúdez (2018), García Perero (2021), González (2017), Restrepo Ángel & Sánchez Jaramillo (2018), se puede interpretar que existe una ambigüedad sobre que prueba de vulnerabilidad de hacking ético es la más idónea para garantizar la seguridad en bases de datos, y a su vez que los profesionales que comúnmente son contratados para dichas pruebas son los hackers éticos o blancos, y que a diferencia de este en algunos casos e contratan con posterioridad a hackers grises.

Ante ello, es preciso señalar Denegri (2017) quien en su investigación identifica que el test de vulnerabilidad o penetration testing, pentesting, son aquellas pruebas de vulnerabilidad los cuales tiene por finalidad la identificación y exploración de vulnerabilidades, amenazas o riesgos que puedan presentarse, ya sea en aplicación de software, de la web de una organización o redes.

En este sentido, Álvarez y Hevia (2020), agregan que estas pruebas tienen como naturaleza esencial el acto sorpresivo que simula un ataque, de forma análoga, y por tanto, argumenta que las pruebas se utilizan como

simulaciones de actos hostiles contra el objeto, que en este caso será una base de datos, precisando que las pruebas de vulnerabilidad se realizan por profesionales que cuentan con certificaciones e incluso metodologías para llevar a cabo es decir un procedimiento, que debe estar avalado por una institución.

Asimismo, exponen que el hacking ético se subdivide por tres formas, que son:

- De caja blanca: Es aquella que se realiza el test con conocimiento completo y previo de la infraestructura que será probada, y es realizado con el apoyo de personal interno.
- De caja gris, parte de un conocimiento parcial del cual no se tiene un completo conocimiento sobre la infraestructura, además suele ser realizada como pentest a través de empresas especializadas.
- De caja negra, es aquella que no se realiza con ningún conocimiento previo de la infraestructura a ser probada, y es la prueba que se realiza con mayor realidad.

Sin embargo, cabe destacar lo señalado por Vera Correa (2021), quien señala que los hacking éticos con mayor eficiencia traen en muchas ocasiones la llegada de hackers profesionales con una ambigua ética; y por tanto únicamente debería considerarse los hackers blancos quienes realizan sus actividades con comunicación, métodos y autorización.

Al respecto desde nuestra opinión, podemos señalar que en Perú actualmente no existen normas que regulen el hacking ético, y únicamente en la Ley de delitos informáticos se expone en el artículo 12°, la exclusión en los casos de que se cuenten con autorización, es decir en los casos donde se realice el hacking de caja blanca (donde existe una baja eficiencia pues no se simula el peligro de un ataque real). En esta línea la Oficina Nacional de Gobierno Electrónico e Informática de la Presidencia del Consejo de Ministros (ONGEI-PCM), realiza una exposición sobre el hacking ético indicando que la única forma por la cual se ejercería pruebas de vulnerabilidad es a través de una previa autorización. Sin embargo, ante la creciente evaluación de formas

de penetración surge la necesidad imperiosa de realizar prácticas que emulen con mayor eficacia las pruebas de vulnerabilidad a un ataque real, es decir que se apliquen pruebas de vulnerabilidad que simulen un real ataque con la finalidad de establecer los riesgos altos, bajos y regulares de la seguridad en un almacenamiento de datos, para lo cual se concuerda con las posturas de los entrevistados y de los autores quienes exponen que desde un aspecto de eficacia y de fortalecimiento a la seguridad de bases informáticas se debe regular y promover pruebas de mayor eficacia, por lo que no solo se podría utilizar el hacking en caja blanca, sino el gris o hasta el negro, y preferentemente se posibilite al hacker gris las prácticas de hacking ético.

Al respecto analizando el derecho constitucional sobre el derecho a la privacidad establecido en el literal 10 del artículo 2° de la referida carta magna; se puede denotar que en comparación a los tratados internacionales y la noción que todo derecho no es absoluto, así como la aplicación de un control convencional de las normas por especialidad, en el Perú no existe norma explicita que prohíba o establezca la imposibilidad de proceder a realizar pruebas de vulnerabilidad con mayor eficiencia y que logren su cometido que es promover el fortalecimiento de la integridad de la seguridad de bases de datos, conforme el artículo 1° de la Ley de delitos informáticos; por lo que en consonancia a la convención de Budapest, así como en congruencia a las prácticas jurisprudenciales expuestas por la AMAG (2016) en el Manual Auto Instructivo del Curos “delitos informáticos) es necesario una debida regulación sobre todos los tipos de hacking y los sujetos activos.

En tal sentido ante lo expuesto, podemos identificar que claramente en el Perú no se encuentra regulado de forma expresa el hacking ético, lo cual conforme a los entrevistados genera un innecesario procesamiento de casos a hackers blancos a grises, que realizan las pruebas de vulnerabilidad con fines de proteger y fortalecer la seguridad de los almacenes de datos; por lo que en este sentido, podemos sostener que debería regularse el hacking ético con lo cual será necesario recomendar la exclusión o exención de la responsabilidad por el delito de acceso ilícito.

Discusión objetivo específico 1

Por otro lado, respecto al primer objetivo específico que consiste en “Determinar si la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito”. Se analiza lo siguiente:

En cuanto a los hallazgos del primer objetivo específico, se tiene que los 10 entrevistados indicaron que se encuentran de acuerdo sobre la calidad sorpresiva de la prueba de vulnerabilidad en el hacking ético; asimismo, entre estos, Salazar (2023), preciso que las formas que se subdivide o clasifica el hacking ético y los hackers, y que en la actualidad no se encuentran reguladas generando un desconocimiento sobre necesidad previa de la autorización como único elemento para la eximir de la responsabilidad penal por el acceso ilícito. A ello Vegas (2023) de forma extensa identifica que la finalidad dolosa del acceso ilícito parte de la Convención de Budapest, y que la falta de exactitud en la regulación de las formas de realizar las pruebas de vulnerabilidad con fines de insertar políticas de fortalecimiento en contra del acceso ilícito generan una regulación defectuosa, ya que actualmente la ley de delitos informáticos no comprende las formas de hacking ético en caja blanca, gris y negra, posibles requisitos para posibilitar su aplicación en el sistema jurídico peruano.

En este sentido, cabe precisar que de acuerdo a las posturas en conjunto analizadas que constan en 25 artículos y libros, se puede destacar a Morales (2018), quien indica que no todos los hacking éticos necesitan una previa autorización, y además que existen enfoques de aplicación y tipos de hackers. Entre estos, distingue a los siguientes:

Black Hat Hackers, el cual es conocimiento como los sombreros negros que son aquellos profesionales que tienen conocimientos exactos para ingresar a la seguridad de sistemas o computadoras, creando virus con intensiones indebidas, es decir que las actividades que realizan no son éticas.

White Hat Hackers, que son denominados sombreros blanco, que son comúnmente aquellos que realizan hacking ético, y poseen la ética de trabajar bajo una organización disponiendo de sus conocimientos en beneficio y mejora de la seguridad de las empresas.

Grey Hat Hackers, que son aquellos que reconocen ser hackers de sombrero gris, pues poseen una ética semi ambigua porque usan sus conocimientos bajo la práctica similar de los hackers de sombrero negro, pues ingresan a base de datos usando las prácticas de los hackers negros, hallando vulnerabilidad y luego pueden presentarse ante la entidad para su arreglo, es decir se puede lograr atender la vulnerabilidad conociéndose a través de estas prácticas, sin ningún previo acuerdo o contrato como en los casos de hackers de sombreros blancos.

En este sentido, de los antecedentes de investigación Corredor (2019) establece que las formas de penetración permiten una distinción clara entre las pruebas de vulnerabilidad, no solo con aquellas prácticas de vulnerabilidad que cuentan con autorización (caja blanca y hacking blanco) sino que pretenden incentivar la práctica de simulaciones con la mayor realidad posible para que se logre la promoción de prácticas de fortalecimiento sobre la seguridad de almacenes de datos, con la finalidad que tengan mínimos márgenes de error.

En tal sentido en nuestra condición de autores, podemos sostener que la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético no se encuentra debidamente regulada, pues la naturaleza sorpresiva no se logra con la pruebas de vulnerabilidad en caja blanca, y por ende es necesario aplicar simulaciones para las pruebas de vulnerabilidad que tengan mayor eficacia, para lo cual se debería regular los tipos de hacking ético y especificar que sujetos podrían realizar pruebas de vulnerabilidad y que medidas deberían adoptarse para evitar que se apertura investigaciones por delitos de acceso ilícito.

Discusión objetivo específico 2

Finalmente, en cuanto al segundo objetivo específico que es “Determinar si la regulación de un post registro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito”; se analiza, lo siguiente:

Respecto a los hallazgos encontrados de la guía de entrevistas se precisa que los 10 entrevistados afirman que es necesario reglamentar un post registros para la práctica de pruebas de vulnerabilidad, obviándose claramente aquellos que cuentan con autorización (hacking en caja blanca que se realizan por hackers blancos), es decir solo aplicado a los hacking éticos en caja gris y negra que se realicen por hackers grises, ello a fin de incentivarse la práctica de simulaciones con la mayor realidad posible de ataques cibernéticos.

En este sentido, de los documentos analizados antes descritos, se destaca a García (2021) quien refiere sobre los hackers de sobrero gris, que, si bien violan principios o estándares éticos, no realizan la penetración o prueba de prueba de vulnerabilidad con intenciones maliciosas, sino por contrario tiene la intención de generar pruebas por el bien común.

Al respecto, de los antecedentes se destaca Domínguez (2023) quien identifica que la regulación de pruebas de vulnerabilidad con mayor flexibilidad ética permitiría promover a futuro la conversión de profesionales de alta tecnología con debida certificación, y con ello se pueden realizar pruebas con mayor realidad y eficacia, ya que no siempre los hackers grises ejercen pruebas de vulnerabilidad con la finalidad de generar sesgos en la seguridad y obtener beneficios, sino con él a fan de probar la seguridad de datos informáticos y comunicar los riesgos de seguridad en la base de datos.

En este sentido, Gonzales (2018), describe en general que el hacking ético, tiene la finalidad de ejercer de forma metódica pruebas de vulnerabilidad en almacenes de datos identificando riesgos en la seguridad para el ingreso, para ello se usan virus u otras estrategias, y no siempre deben ser aplicados por hackers blancos (aunque es lo usualmente realizado), sino que existe la posibilidad de autorización para los grey hackers, toda vez que comúnmente los profesionales que ejercen hacking ético, lo hacen bajo el método de caja negra, lo cual tiende a ser cuestionado por su ética, ya que resulta ambigua al realizar pruebas sin conocimiento de la entidad titular del almacén de datos, y con ello produce que se cuestionado, sin embargo dicha prueba reproduce con la mayor eficiencia un ataque a la seguridad de datos.

En este sentido, cabe precisar según Jeimy y Cano (2021) la definición sobre el hacking ético la cual que comprende tres formas de ejercerse, en caja blanca (con autorización y apoyo interno- cuenta con una tasa mínima de eficacia), el negro (que no cuenta con autorización y no cuenta con datos de la empresa o apoyo- emula la realidad y tiene una máxima eficacia), y el gris (que se realiza sin autorización y con posterior regularización, al llegar a una acuerdo con la entidad sobre sus conocimientos en la penetración lograda).

En el orden de ideas el autor Neif (2016), cuestiona el ejercicio de las pruebas con hackers negros, señalando que los hacking éticos que se ejercen por hackers negros o crackers no resultan los más idóneos, siendo riesgosos al ser demasiado ambiguo su ética o los resultados, por lo que a fin de lograr la emulación más cercana al riesgo de la penetración se debería considerar los hacking éticos en caja gris que se realizan por hacker blancos o greys.

Al respecto es preciso señalar que con anterioridad se han declarado circunstancias especiales de exención de responsabilidad que afectan derechos fundamentales, como lo es el caso de Ana Estrada, por lo tanto también es posible desde un aspecto constitucional establecer formas sorpresivas para realizar pruebas de vulnerabilidad, estableciendo una exención sobre pruebas sorpresivas, claro está sin dejar de lado como se establece por la AMAG (2016) la observancia del nexo de causalidad que muestra intención dolosa, y en ese sentido la mejor manera sería regular el hacking ético promoviendo todos los tipos que se busquen primero incentivar pruebas de vulnerabilidad con mayor realismo; y por ende se llamen a los hacker gris a realizar pruebas de vulnerabilidad permitiendo que estos promuevan prácticas de fortalecimiento a la integridad de sistemas informáticos, para lo cual se debe tener en cuenta que según la AMAG (2016) para establecer prácticas de vulnerabilidad que sean sorpresivas en los casos del hacking ético deben promoverse formas de detectar la acción dolosa que es brindar la facilidad de acceso al software, es decir a través del uso de virus que dejen registro de sus actividades.

En este sentido, podemos sostener que el hacking ético blanco no

resulta ser un acto típico en la ley de delitos informáticos, ya que actualmente las practicas se ciñen en el ejercicio del hacking en caja blanca (es decir con previa autorización), no obstante, cuando se realizan prácticas en caja gris es donde se produce el cuestionamiento de la ilicitud, por cuanto es ambigua la finalidad del hacker (excluyendo a los black y crakers), es decir se cuestiona que la finalidad del hacker que realiza el hacking ético sea para fortalecer las seguridad en almacenes de datos, por tanto, lo que debería promoverse es establecer formas por las cuales se logren identificar a los hackers grey a fin de evitar dicho cuestionamiento produciendo una base de datos que obligue a todo hacker gris a realizar el registro de sus actividades bajo apercibimiento de ser investigado como autor del delito de acceso ilícito.

V. CONCLUSIONES

No existe en el Perú una regulación exacta del hacking ético por lo cual existe la posibilidad de procesarse penalmente por el delito de acceso ilícito a hackers grises por realizar pruebas de vulnerabilidad en caja blanca, gris o negra, lo cual incentiva a que se realicen pruebas de menor eficacia y con ello se incumpla con la finalidad de la ley de delitos informáticos que es combatir la ciberdelincuencia.

En la ley de delitos informáticos no se comprende la posibilidad de ejercer pruebas de vulnerabilidad sorpresiva, es decir se produce una posible tipificación del hacking ético gris o negro realizado por los hackers de sombrero gris, por lo cual será necesario identificar las formas por las cuales podrían generarse dichas pruebas por los hackers grises, a fin de promover mejores prácticas de fortalecimiento contra la ciberdelincuencia, y a su vez incentivar que los hackers grises se conviertan en blancos.

Se debería reglamentar un post registro como requisito del hacking ético (para los hackers grises) como requisito de la exención de la responsabilidad penal en los casos que se inicie una investigación por el delito de acceso ilícito, explícitamente en el art. 12 de la ley de delitos informáticos, para lo cual se puede generar la obligación de que los profesionales de alta ingeniería que realicen pruebas de vulnerabilidad cuenten con certificaciones o por lo menos realicen el registro de sus actividades y métodos para la penetración de datos de forma anónima con el registro de IP, bajo responsabilidad de que se presuma actos ilícitos ante el ejercicio de pruebas de vulnerabilidad.

VI. RECOMENDACIONES

Se recomienda a la DIVINDAT que realice un informe sobre los tipos de hacking ético y los profesionales que puedan realizarlo, remitiéndose a la Escuela del Ministerio Público para que remita una propuesta vía lege ferenda proponiéndose al Congreso la modificación de la Ley de Delitos Informáticos.

Se encomiende a la Presidencia del Consejo de Ministros - PCM que se reconozca a través de una directiva las practicas del hacking ético, considerando dejar sin efecto la resolución ministerial N° 004-2016-PCM, y permitir pruebas de vulnerabilidad sorpresiva, es decir que permita y reconozca el hacking ético desde el blanco al negro, y que estos puedan ser realizados por los hackers de sombrero blanco y gris, con la finalidad de dotar mayor exigencia en las pruebas de vulnerabilidad para que emulen riesgos reales de un ataque cibernético.

Se recomiende a través de la Comisión del Congreso la modificación del art. 12° de la Ley de delitos informáticos, de la siguiente forma:

> ***Segundo párrafo***
> "(…)
> *En el caso de realizar la conducta descrita en el artículo 2, se deberá considerar que para el hacking ético blanco, gris o negro, que se realice por un hacker gris será exento de responsabilidad al contar con autorización previa o haber realizado un post registro durante las 48 horas siguientes al hackeo, estableciendo el detalle de sus actividades y métodos aplicados por el profesional técnico que realiza pruebas de vulnerabilidad, a fin de mejorar y promover la protección de sistemas informáticos.*

REFERENCIAS

Acosta, Y. M. (2022). *Proposal for security and vulnerability analysis with Ethical hacking techniques in a controlled environment for the Company Nostradamus SA SONES*. https://repository.unad.edu.co/handle/10596/42681

Andrade, C.D. (2016). *Implementation of web security tools in an internet sales store developed in Prestashop* (Bachelor's thesis, Quito: Universidad de las Américas, 2016). https://dspace.udla.edu.ec/handle/33000/6483

Aruquipa, R. (2019). *Forensic audit on cloned cards case: Banco Unión (Doctoral dissertation, Universidad Mayor de San Andres. Faculty of Economic Sciences*. Public Accounting Career. Institute of Research in Accounting, Financial and Audit Sciences. Postgraduate Unit). https://repositorio.umsa.bo/handle/123456789/20998

Beltran, P. (2021). *Aplicación de Hacking ético para gestionar la prevención de ataques a la red de comunicación de Inversiones Mayito – Agente BCP* [Maestría en ingeniería de sistemas con mención en tecnologías informáticas]. Lima, Perú. UCV. Repositorio. Downloads/Beltrán_CPO-SD.pdf

Bermeo, J. C. Implementation of ethical Hacking for the detection and evaluation of network vulnerabilities in the company Complex del Perú SAC-Tumbes; 2017. http://repositorio.uladech.edu.pe/handle/20.500.13032/10391

Bonilla Rios, Y. P. (2021). Technical legal and management skills for blue team and red team. *Reviwe teams*. https://repository.unad.edu.co/handle/10596/51782

Borbor, J.A. (2022). *Study of computer security to the servers of a transport cooperative in the province of Santa Elena* (Bachelor's thesis, La

Libertad: Universidad Estatal Península de Santa Elena. 2022). https://repositorio.upse.edu.ec/handle/46000/8645

Brito, P. M. (2018). Diagnóstico de Ethical Hacking para la Universidad Politécnica Salesiana. https://openaccess.uoc.edu/handle/10609/81272

Cacua, N. P. Technical, legal and management skills for Blue Team and Red Team teams. https://repository.unad.edu.co/handle/10596/51810

Carvajal, V. E. (2022). *Hacktivismo de anonymous en el Ecuador: análisis realista de las estrategias y consecuencias de los actores no estatales transnacionales en el modelo ecuatoriano de Ciberseguridad (2011-2020)* (Bachelor's thesis, PUCE-Quito). http://repositorio.puce.edu.ec/handle/22000/20370

Chávez, V.H. (2021). Ethical Hacking Methodology to improve the computer security of the technological infrastructure in the provincial Gad of Napo (Master's thesis). https://dspace.uniandes.edu.ec/handle/123456789/13713

Crespo, A. (2007). El muestreo en la investigación cualitativa. *Revista nure*. http://www.sc.ehu.es/plwlumuj/ebalECTS/praktikak/muestreo.pdf

Curay, M.F. (2023). *Vulnerability analysis of domestic wireless networks using Pentesting in Tungurahua* (Bachelor's thesis, Technical University of Ambato. Faculty of Systems, Electronic and Industrial Engineering. Information Technology Career). http://repositorio.uta.edu.ec/handle/123456789/38304

Fernández, A. Capacidades técnicas, legales y de gestión para equipos blue team y red team. https://repository.unad.edu.co/handle/10596/51812

Fernández Miranda, H. A. (2019). *Análisis de la seguridad del sitio web del Ministerio del Trabajo aplicando pruebas de Pentesting en la sede principal de la ciudad de Bogotá*. Revista de la Universidad de Bogotá. https://repository.unad.edu.co/handle/10596/27059

García, F.G. (2021). *Analysis and implementation of ethical hacking techniques and tools for Cybersecurity* (Bachelor's thesis, La Libertad: Península de Santa Elena State University, 2021). https://repositorio.upse.edu.ec/handle/46000/5917

Giménez, V. (2021). *Hacking y ciberdelito*. Valencia, España: Universidad Politecnica de Valencia. https://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf

Giménez, V. (2021). *Hacking y ciberdelito*. Valencia, España: Universidad Politécnica de Valencia. https://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf

Giménez, V. (2021). *Hacking y ciberdelito*. Valencia, España: Universidad Politecnica de Valencia. https://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf

González, J. A. (2018). *Delincuencia informática: daños informáticos del artículo 264 del Código Penal y propuesta de reforma*. (Tesis Doctoral, Universidad Complutense de Madrid). https://eprints.ucm.es/23826/

González, M.J.S. (2017). Legal regulation of robotics and artificial intelligence: challenges for the future. *Legal Review of the University of León*, 4(4), 25-50. https://pdfs.semanticscholar.org/ea29/4cbf53fd151134f1d949382dc89d8af120ab.pdf

Grant, J., 2019. Hackeo Ético: Guía complete para principiantes para aprender y comprender el concepto de hacking ético (Libro En Español/Ethical Hacking Spanish Book Versión). S.l.: Independently Published. ISBN 978-1-71105-900-6.

Hurtado, M.E., & Mendaño Mendaño, L.A. (2016). Implementation of ethical hacking techniques for the discovery and evaluation of vulnerabilities in the network of a State portfolio (Bachelor's thesis, Quito, 2016.). http://bibdigital.epn.edu.ec/handle/15000/16836

Infante, B. (2019). *Análisis del delito de hurto de identidad virtual: frente a la seguridad de los sistemas informáticos* (pregrado). Repositorio UNP. https://repositorio.unp.edu.pe/bitstream/handle/20.500.12676/2524/DECP-INF-GUE-2019.pdf?sequence=1&isAllowed=y

Lledó, I. (2021). Visión del derecho penal en relación con la robótica, IA y la ciberdelincuencia. *Visión del derecho penal en relación con la robótica, IA y la ciberdelincuencia*, 149-196. https://www.torrossa.com/gs/resourceProxy?an=5085251&publisher=FZ1825

Maritza, E. (2022). *Mecanismos de prevención y protección del bien jurídico tutelado frente a la modalidad delictiva phishing en el ordenamiento jurídico penal peruano*. Repositorio UIGV. http://webcache.googleusercontent.com/search?q=cache:eEWLNkoZJXsJ:repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/6595/TESIS_ESPARTA%2520CENTENO.pdf%3Fsequence%3D1&cd=6&hl=es-419&ct=clnk&gl=pe

Mateos, I. (2013). *Cybercrime: technological development and persecution*. Lima https://oa.upm.es/id/eprint/22176

Meditaciones postmodernas sobre el castigo. https://dialnet.unirioja.es/descarga/articulo/3311815.pdf

Olivares, B y Ceras M. (2021). *Delitos informáticos y la evidencia digital en el proceso peruano del distrito judicial de Junín, 2020* (pregrado). Repositorio Universidad de los andes. https://repositorio.upla.edu.pe/bitstream/handle/20.500.12848/2690/TESIS%20en%20formato%20PDF.pdf?sequence=1&isAllowed=y

Ortiz, G.A. (2021). Analysis of techniques for ethical hacking-pentesting tests on websites. https://dspace.ucacue.edu.ec/handle/ucacue/12756

Paredes, R. A., & Pérez Valencia, F. D. (2022). Controles del centro de seguridad de internet para la defensa cibernética que minimizan las vulnerabilidades. https://repositorio.usil.edu.pe/items/068ba270-5773-

4dc3-8ba8-3c359c3055bb/full

Paredes, J. (2013). *De los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, en el período 2009-2010* (tesis posgrado). Repositorio UNMSM. https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/10314/Paredes_pj.pdf?sequence=3&isAllowed=y

Piñashca, R.J. (2022). Evaluation of ethical hacking techniques to analyze the computer security of the district municipality of Los Olivos, Lima. https://repositorio.uss.edu.pe/handle/20.500.12802/9377

Protección legal para la búsqueda y notificación de vulnerabilidades. https://www.scielo.cl/scielo.php?pid=S0719-25842020000200001&script=sci_abstract

Restrepo, C. L., & Sánchez Jaramillo, E. G. (2018) Análisis de los resultados de Ethical Hacking para el control de vulnerabilidades de la base de datos Tao esquema Servicios de la Alcaldía de Ibagué. https://repository.unad.edu.co/handle/10596/18786

Rincón, R. J. (2018). *El delito en la cibersociedad y la justicia penal internacional*. Madrid: (Tesis Doctoral, Universidad Complutense de Madrid). https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/74705/Palacios_CEF-SD.pdf?sequence=4&isAllowed=y

Rincón, R. J. (2018). *El delito en la cibersociedad y la justicia penal internacional*. Madrid: (Tesis Doctoral, Universidad Complutense de Madrid). https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/74705/Palacios_CEF-SD.pdf?sequence=4&isAllowed=y

Rojas, A. I. (2018). Ethical hacking to analyze and evaluate information security in the infrastructure of the Plasticaucho Industrial SA Company (Bachelor's thesis, Technical University of Ambato. Faculty of Systems, Electronic and Industrial Engineering. Engineering Degree in Computer

and Information Systems). http://repositorio.uta.edu.ec/handle/123456789/28102

Santos, C. P., Guisado, Á. C., & Morán, J. J. D. (2017). The phenomenon of cybercrime in Spain: The proposal of the Nebrija University in the training of personnel for the prevention and treatment of cybercrime. Police and public safety magazine, 237-270. https://www.camjol.info/index.php/RPSP/article/view/4312

Vera, J.A. (2021). *Application of pentesting techniques to determine vulnerabilities in the lan network of the csednet company in Santo Domingo* (Bachelor's thesis, Riobamba National University of Chimborazo). http://dspace.unach.edu.ec/handle/51000/7481

Vidal, J.H. (2017). A new experience in ethical hacking security. https://repository.unimilitar.edu.co/handle/10654/15838

Vilca, G. (2018). *LOS HACKERS: "DELITO INFORMATICO FRENTE AL CODIGO PENAL PERUANO*" [tesis pregrado]. Repositorio UNASAM. Huaraz. http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2496/T033_47272593_T.pdf?sequence=1&isAllowed=y

Zapata, J. (2019). Uso de tecnologías de pruebas de penetración para validación de seguridad de aplicaciones web basado en el top 10 de vulnerabilidades de OWASP. *Revista UNAD*. https://repository.unad.edu.co/handle/10596/28466

Guamán, K; Hernández, E; Yuqui, C; Llloay, S. (2021). La investigación jurídica: objeto, paradigma, método, alcance y tipos. *Revista Conrado, 17(S2), 169-178.* https://conrado.ucf.edu.cu/index.php/conrado/article/download/2006/1964/#:~:text=Los%20Tipos%20de%20Investigaci%C3%B3n%20Jur%C3%ADdica,Investigaci%C3%B3n%20e%20Investigaci%C3%B3n%20Argumentativa.

ANEXOS

Anexo 1.- Matriz de consistencia

Anexo 2.- Guía de entrevista / Ficha de análisis documental

Anexo 3.- Validación de expertos

Anexo 4.- Tablas de resultados de las entrevistas y el análisis documental

Anexo 5.- Evidencia de entrevistas

ANEXOS

ANEXO 01-
Matriz de Consistencia

Regulación del hacking ético: prueba de vulnerabilidad sorpresiva y la exclusión en la subsunción de los delitos de acceso ilícito

PROBLEMAS	OBJETIVOS	SUPUESTOS	CATEGORÍAS	DEFINICIÓN CONCEPTUAL	SUB CATEGORÍAS	DEFINICIÓN CONCEPTUAL	METODOLOGÍA
PG: ¿Debería regularse el hacking ético incidiendo en la exclusión en la subsunción de los delitos de acceso ilícito?	**OB:** Determinar si debería regularse el hacking ético para excluirlo del delito de acceso ilícito.	**SG:** Sí, debería regularse el hacking ético incidiendo en la exclusión en la subsunción de los delitos de acceso ilícito.	REGULACIÓN DEL HACKING ETICO	El hacking ético es una prueba de vulnerabilidad que tiene la finalidad de realizar ataques simulados con fines de reforzar la seguridad en las bases de datos, que no se encuentran expresamente regulados en la norma.	Pruebas de vulnerabilidad sorpresiva	Son aquellas pruebas que tiene la finalidad penetrar una base de datos bajo la aplicación de procedimientos, que pueden ser adoptados de mayor o menor riesgo.	**Enfoque de investigación**: Cualitativo **Tipo de investigación:** Básica
					Post registro para ofrecimiento de servicios	Es un requisito que se exige como condición para comprobar un acto ético con fines de fortalecer la base de datos.	Nivel Jurídico propositivo

PE1: ¿La regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito?	**OE1:** Determinar si la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito.	**SE1:** Si, debería regularse la prueba de vulnerabilidad sorpresiva por hacking ético para excluirlo de la subsunción de los delitos de acceso ilícito.	EXCLUSIÓN EN EL DELITO DE ACCESO ILICITO	La exclusión o exención son conductas que típicamente representan un acto ilícito; sin embargo, existen circunstancias especiales que condicionan su responsabilidad bajo la observación de requisitos, en el acceso ilícito en la fecha es que se cuente con una previa autorización	Autorización previa	Es un requisito previo para la exención regulado en el art. 12 de la ley de delitos informáticos	**Escenario:** Ministerio Público de Lima (sede Abancay) y el Juzgado Penales Liquidadores de Lima. **Diseño de investigación:** Teoría fundamentada **Participantes:** 10
PE2: ¿La regulación de un post registro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito?	**OE2:** Determinar si la regulación de un post registro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito	**SE2:** Sí, debería regularse un post registro como requisitos del hacking ético permite excluirlo de la subsunción de los delitos de acceso ilícito			Exclusión por fin licito	La exclusión o exención es una circunstancia que anulan la responsabilidad bajo la observancia de conductas o requisitos independientes al hecho típico.	**Técnicas** • Entrevista y análisis documental **Instrumento** • Guía de entrevista • Guía de análisis documental **Métodos** • Método de síntesis • Método analítico • Método deductivo

ANEXO 2-
Instrumentos de recolección de datos

GUÍA DE ENTREVISTA

El presente instrumento pretende recopilar su opinión respecto a la "Regulación del hacking ético: prueba de vulnerabilidad sorpresiva y la exclusión en la subsunción de los delitos de acceso ilícito**"**

Para lo cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales.

Entrevistado (Nombre, apellido, edad)**:**
Máximo Grado académico:
Cargo:
Institución:

Fecha_____ Hora_____ Lugar_____

Determinar si debería regularse el hacking ético para excluirlo del delito de acceso ilícito

OBJETIVO GENERAL

1.¿Conoce que es el Hacking ético y su diferencia con el delito de acceso ilícito?

_____
_____
_____
_____.

2.¿Considera que deben regularse las conductas explícitas del hacking según las modalidades en el acceso ilícito?

_____
_____
_____
_____.

Determinar si la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito

OBJETIVO ESPECÍFICO 1

3.¿Conoce que es la vulnerabilidad de un sistema de protección de datos en el acceso ilícito?

_____
_____
_____
_____

4.¿Considera que se debe regular condiciones y requisitos en el hacking ético para su tipificación o excepción en el delito de acceso ilícito?

_____
_____
_____
_____

Determinar si la regulación de un post registro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito

OBJETIVO ESPECÍFICO 2

5.¿Conoce que el hacking ético tiene una naturaleza sorpresiva y busca mejorar la calidad de los sistemas de protección de datos para evitar el acceso ilícito?

_____
_____
_____
_____

6. ¿Considera que la implementación de un registro de hackers éticos (profesionales que prueben la vulnerabilidad de sistemas) es necesaria para determinar la responsabilidad del acceso ilícito en casos de no contar con autorización?

_____

_____

_____

_____

FIRMA	SELLO

Ficha de análisis documental

I. Objetivo General, y Objetivos Específicos 1 y 2

Determinar si debería regularse el hacking ético para excluirlo del delito de acceso ilícito

II. Análisis

Cita	
País	
Referencia	
Aporte:	
Postura al objetivo:	

Determinar si la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito

I. Análisis

Cita	
País	
Referencia	
Aporte:	
Postura al objetivo:	

Determinar si la regulación de un post registro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito

I. Análisis

Cita	
País	
Referencia	
Aporte:	
Postura al objetivo:	

ANEXO 3-
Validación de expertos

GUÍA DE ENTREVISTA

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 4 VALIDACIÓN DE EXPERTO Y CONFIABILIDAD

VALIDACIÓN DE INSTRUMENTO (GUÍA DE ENCUESTA)

I. DATOS GENERALES

1.1. Apellidos y Nombres: Joel Bravo Yucra

1.2. Cargo e institución: Abogada Independiente – Juez en lo Penal – grado Maestro

1.3. Nombre del instrumento motivo de evaluación: Guía de entrevista

1.4. Autor (a) de Instrumento: Cuellar Chuquiyuri, Keyla Katherine y Guerreros Rojas, Mauricio

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE				ACEPTABLE		
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.												X	
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.												X	
4. ORGANIZACIÓN	Existe una organización lógica.												X	
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales												X	
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.												X	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												X	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos												X	
9. METODOLOGÌA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.												X	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												**X**	

III. OPINIÓN DE APLICABILIDAD x

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

IV. PROMEDIO DE VALORACIÓN: 95%

Lima, 26 de abril del 2023

PODER JUDICIAL DEL PERÚ

FIRMA DEL EXPERTO INFORMANTE

JOEL BRAVO YUCRA
DNI. 41599455
ESPECIALISTA LEGAL
SEPTIMO JUZGADO PENAL LIQUIDADOR
CORTE SUPERIOR DE JUSTICIA DEL CALLAO

PERÚ | Ministerio de Educación | Superintendencia Nacional de Educación Superior Universitaria | Dirección de Documentación e Información Universitaria y Registro de Grados y Títulos

REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

Graduado	Grado o Título	Institución
BRAVO YUCRA, JOEL **DNI 41592855**	**BACHILLER EN DERECHO Y CIENCIAS POLITICAS** **Fecha de diploma:** 08/07/2009 Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	UNIVERSIDAD INCA GARCILASO DE LA VEGA ASOCIACIÓN CIVIL ***PERU***
BRAVO YUCRA, JOEL **DNI 41592855**	**ABOGADO** **Fecha de diploma: 24/12/2009** Modalidad de estudios: -	UNIVERSIDAD INCA GARCILASO DE LA VEGA ASOCIACIÓN CIVIL ***PERU***

UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÒN DE INSTRUMENTO (GUÌA DE ENCUESTA)

I. DATOS GENERALES

1.1. Apellidos y Nombres: Ada Marina Gotuzzo Ortiz

1.2. Cargo e institución: Fiscal Provincial – Ministerio Público – grado Maestra en lo penal

Nombre del instrumento motivo de evaluación: Guía de entrevista

1.3. Autor(A) de Instrumento: Cuellar Chuquiyuri, Keyla Katherine y Guerreros Rojas, Mauricio

II. ASPECTOS DE VALIDACIÒN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.												x	
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Esta adecuado a los objetivos y las necesidades reales de la investigación.												X	
4. ORGANIZACIÓN	Existe una organización lógica.												X	
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales												X	
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.												X	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												X	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos												X	
9. METODOLOGÌA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.												x	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												X	

III. OPINIÓN DE APLICABILIDAD x

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

si
---5%---

IV. PROMEDIO DE VALORACIÓN:

95%

Ada Marina Gotuzzo Ortiz
Fiscal Provincial
2º Fiscalía Provincial Penal Corporativa
de Chosica - 1º Despacho

Lima,26 de abril del 2023

PERÚ | Ministerio de Educación | Superintendencia Nacional de Educación Superior Universitaria | Dirección de Documentación e Información Universitaria y Registro de Grados y Títulos

REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

Graduado	Grado o Título	Institución
GOTUZZO ORTIZ, ADA MARINA **DNI 07654995**	**ABOGADO** **Fecha de diploma: 24/05/1990** Modalidad de estudios: -	UNIVERSIDAD NACIONAL FEDERICO VILLARREAL ***PERU***
GOTUZZO ORTIZ, ADA MARINA **DNI 07654995**	**BACHILLER EN DERECHO** **Fecha de diploma: 18/05/1989** Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	UNIVERSIDAD NACIONAL FEDERICO VILLARREAL ***PERU***

VALIDACIÓN DE INSTRUMENTO

I. **DATOS GENERALES**

I.1. Apellidos y Nombres: Colchado Ruiz, Emilio Martin

I.2. Cargo e institución donde labora: Docente de investigación – Magister en Derecho

I.3. Nombre del instrumento motivo de evaluación: Guía de entrevista

I.4. Autor(A) del instrumento: Cuellar Chuquiyuri, Keyla Katherine y Guerreros Rojas, Mauricio

II. **ASPECTOS DE VALIDACIÓN**

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Está formulado con lenguaje comprensible.												X	
2. OBJETIVIDAD	Está adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Está adecuado a los objetivos y las necesidades reales de la investigación.												X	
4. ORGANIZACIÓN	Existe una organización lógica.												X	
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales												X	
6. INTENCIONALIDAD	Está adecuado para valorar las categorías.												X	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												X	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos												X	
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.												X	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												X	

III. **OPINIÓN DE APLICABILIDAD**

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

IV. **PROMEDIO DE VALORACIÓN:** 95%

Lima, 29 de abril de 2023.

INFORMANTE

FIRMA DEL EXPERTO

DNI 18149033 Telf.: 919630575

PERÚ | Ministerio de Educación | Superintendencia Nacional de Educación Superior Universitaria | Dirección de Documentación e Información Universitaria y Registro de Grados y Títulos

REGISTRO NACIONAL DE GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

Graduado	Grado o Título	Institución
COLCHADO RUIZ, EMILIO MARTIN **DNI 18149033**	**MAGISTER EN ADMINISTRACION ESTRATEGICA DE EMPRESAS** **Fecha de diploma: 05/11/2014** Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ ***PERU***
COLCHADO RUIZ, EMILIO MARTIN **DNI 18149033**	**BACHILLER EN DERECHO** **Fecha de diploma: 09/05/1998** Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	UNIVERSIDAD PRIVADA ANTENOR ORREGO ***PERU***
COLCHADO RUIZ, EMILIO MARTIN **DNI 18149033**	**ABOGADO** **Fecha de diploma: 10/03/2000** Modalidad de estudios: -	UNIVERSIDAD PRIVADA ANTENOR ORREGO ***PERU***

ANEXO 4 -
Tablas de resultados de las entrevistas y el análisis documental

Tabla N° 3

Postura sobre el objetivo general por entrevistado

Postura por objetivo general: Pregunta N° 1 y 2	Cuenta de Postura por objetivo general
Si debe regularse el hacking ético para excluirlo del delito de acceso ilícito	**10**
Bravo (2023)	**1**
Si, sobre el delito de acceso ilícito, no obstante, sobre el hacking ético lo conozco a grandes rasgos	1
Si, a fin de esclarecer de forma concreta la norma debería evaluarse su beneficio o su innecesaria regulación, finalmente a la fecha se cuenta con excepciones explicitas en la ley, que, si bien no producen o exponen el hacking ético como prueba de vulnerabilidad, tampoco cierra su oportunidad de sostenerse como inimputabilidad o como acto atípico.	1
Domínguez (2023)	**1**
Si, de forma concreta la primera cuenta con un fin ilícito, y a segunda tiene un fin técnico y de rendimiento para el fortalecimiento de las bases de datos.	1
Si.	1
Franco (2023)	**1**
Sí de forma general se entiende como aquellas pruebas que tienen como bases políticas de mejoramiento a la seguridad sistemas de datos partiendo del concepto que en la actualidad se regula excepciones concretas al acceso ilícito nombrándose las pruebas de vulnerabilidad.	1
Sí ya que en la fecha se viene presentando diversas formas de acceso a base de datos entre estas el hacking ético lo cual ha producido incógnitas en razón a la subclasificación de la misma.	1
Gotuzza (2023)	**1**
Si.	1
Si.	1
Jiménez (2023)	**1**
Si es una modalidad por la cual un sujeto especializado en alta tecnología realiza pruebas de vulnerabilidad es decir la penetración en base de datos a fin de identificar cuáles son los elementos que muestran mayor vulnerabilidad en el sistema del software.	1
Sí ya que en la actualidad aún se encuentra en desarrollo la tipificación del acceso ilícito un claro ejemplo es el hacking ético y sus clasificaciones que pueden ser el hacking gris el negro y el blanco de los cuales el gris y el blanco pertenecen a los límites de la licitud en cuanto a las actividades de vulnerabilidad por lo que la simple exclusión que actualmente se prevé en la norma específica de los delitos informáticos no engloba la tipicidad o atipicidad de dichas clasificaciones.	1
Pereyra (2023)	**1**
Si, el Hacking ético en el Perú no distingue los tipos de hacker, ya que	1

es muy distinto hablar del hacker blanco y gris que el negro. Además, en la actualidad la mayor controversia es en relación al hacker gris el cual puede infringir alguna ley o precepto ético, pero no actúan con la malicia que caracteriza al hacker de sombrero negro, es decir la diferencia entre el acceso ilícito es la finalidad del acto, el cual en algunas ocasiones genera disyuntivas en su aplicación, ya que en uno se cuenta con datos específicos de la penetración y en otros solo de la base general de datos que será el objetivo.	
Si, atendiendo la necesidad de subclasificar los tipos de hacking e identificar claramente cuando pueden ser excluido el hacking ético ante una denuncia por acceso ilícito, toda vez que la exclusión que se encuentra en la ley de delitos informáticos, no distingue el hacking blanco (donde se cuenta con previa autorización) con el hacking ético gris y el acceso ilícito, ya que puede teñirse como un acto presumiblemente ilícito, por lo que debería establecerse igual que lo conciliadores, ingenieros que se encuentren previamente registrado en una base de datos para realizar pruebas de vulnerabilidad para el fortalecimiento de pruebas de vulnerabilidad sorpresiva.	1
Prado (2023)	**1**
Si.	1
Si.	1
Salazar (2023)	**1**
Si, principalmente es el dolo sobre el acto invasivo al sistema de seguridad que guarda datos de relevancia para la entidad en el acceso ilícito.	1
Si, dado que ya han pasado más de 4 años desde la dación de la norma y hasta la fecha no se han producido cambios sobre el hacking (acceso ilícito), ello evidencia que en el sistema peruano no se ha venido desarrollando nuevos conceptos como el hacking ético, siendo este una herramienta para fortalecer las políticas contra el acceso ilícito.	1
Santos (2023)	**1**
Si.	1
Si.	1
Vegas (2023)	**1**
Si, de forma concreta la primera tiene por finalidad verificar los riesgos en la seguridad de una base de datos, y la segunda es un delito que engloba la penetración dolosa a una base de datos con fines de aprovechamiento o beneficio.	1
Si, considerando la complejidad del hacking ético y las diversas modalidades del acceso ilícito.	1
Total general	**10**

Tabla N° 4

Postura sobre el objetivo específico 1 por entrevistado

Postura por objetivo general: Pregunta N° 3 y 4	**Recuento Postura por objetivo1**
La regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito.	**10**
Bravo (2023)	**1**

Si, representa el grado de seguridad de una base de datos.	1
Si a fin de evitar la formulación de procesos de forma innecesario para lo cual debería incluir un registro de actividades sobre las prácticas del hacking ético.	1
Domínguez (2023)	**1**
Si, es el nivel de riesgo que tiene una base de datos.	1
Si para evitar la inseguridad en caso se alegue el uso de hacking ético.	1
Franco (2023)	**1**
Sí es una forma de medir la actividad en relación a la posible vulneración de un sistema informático siendo esta modalidad comúnmente aplicada a través de la previa autorización lo cual es contradictorio a la propia naturaleza del hacking ético.	1
Sí ya que evitaría las contradicciones constantes sobre el acto de magnético y el acceso ilícito principalmente sobre las subclasificaciones como es el hacking ético gris.	1
Gotuzza (2023)	**1**
Si.	1
Si.	1
Jiménez (2023)	**1**
Sí es el medio o grado por el cual se identifica aspectos o elementos de riesgo dentro de un sistema de seguridad que comprende datos relevancia para la entidad correspondiente.	1
Sí ya que en la actualidad el artículo 12 de la ley de delitos informáticos establece la exclusión del acceso ilícito mediante pruebas de vulnerabilidad cuando únicamente se tiene la autorización por lo que dicho contexto no concuerda con todas las formas de vulnerabilidad y pruebas de vulnerabilidad que son ejercidas en la actualidad.	1
Pereyra (2023)	**1**
Si, la vulnerabilidad, es el grado potencial para que un acto de penetración se realice sobre un sistema de seguridad de datos relevantes para una entidad, dependiendo de los datos es el grado de afectación a la entidad.	1
Si, ya que actualmente se encuentra regulado una excepción que consiste en la previa autorización para el acceso de datos, no obstante, existen comunidades de informáticos y peritos que cuestionan la finalidad sobre el acceso ilícito el cual cosiste en probar la vulnerabilidad con fines comerciales o testeo, es decir para vender sus servicios a la entidad (promoción agresiva) o la publicación de vulnerabilidad con el fin que la entidad corrija sus vulnerabilidades en el sistema de seguridad.	1
Prado (2023)	**1**
Si.	1
Si.	1
Salazar (2023)	**1**
Si, concretamente se hace referencia al grado de penetración o potencial afectación a una base de datos que pertenece a una entidad, principalmente las afectadas son base de datos de centros bancarios o empresas tercerías.	1
Si, principalmente para el hacking ético que se denomina como gris, pues existen casos donde se formula cargos contra un imputado a sabiendas que no se generó bajo un acto doloso, siendo finalmente absuelto o sobreseído por ausencia de pruebas concretas que demuestren el fin ilícito (beneficio) del acceso.	1

Santos (2023)	**1**
Si, es el grado o nivel de riesgo en la base de datos de una empresa o institución.	1
Si, ya que la actual exclusión que es la autorización, no engloba su naturaleza sorpresiva.	1
Vegas (2023)	**1**
Si.	1
Si, a fin de evitar complicaciones o desgaste del Estado para tratar de determinar la existencia del fin doloso en el acceso ilícito, por lo que a manera practica fijar requisitos o condiciones para la práctica de hacking ético sorpresivo permitiría identificar estas conductas bajo sanción de ser denunciados por declaración falsa en un proceso judicial.	1
Total general	**10**

Tabla N° 5

Postura sobre el objetivo específico 2 por entrevistado

Postura por objetivo general: Pregunta N° 5 y 6	**Recuento de Postura por objetivo2**
La regulación de un post registro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito	**10**
Bravo (2023)	**1**
Si, sobre el delito de acceso ilícito, no obstante, sobre el hacking ético lo conozco a grandes rasgos	1
Si, a fin de esclarecer de forma concreta la norma debería evaluarse su beneficio o su innecesaria regulación, finalmente a la fecha se cuenta con excepciones explicitas en la ley, que, si bien no producen o exponen el hacking ético como prueba de vulnerabilidad, tampoco cierra su oportunidad de sostenerse como inimputabilidad o como acto atípico.	1
Domínguez (2023)	**1**
Si, de forma concreta la primera cuenta con un fin ilícito, y a segunda tiene un fin técnico y de rendimiento para el fortalecimiento de las bases de datos.	1
Si.	1
Franco (2023)	**1**
Sí de forma general se entiende como aquellas pruebas que tienen como bases políticas de mejoramiento a la seguridad sistemas de datos partiendo del concepto que en la actualidad se regula excepciones concretas al acceso ilícito nombrándose las pruebas de vulnerabilidad.	1
Sí ya que en la fecha se viene presentando diversas formas de acceso a base de datos entre estas el hacking ético lo cual ha producido incógnitas en razón a la subclasificación de la misma.	1
Gotuzza (2023)	**1**
Si.	1
Si.	1
Jiménez (2023)	**1**
Si es una modalidad por la cual un sujeto especializado en alta tecnología realiza pruebas de vulnerabilidad es decir la penetración en base de datos a fin de identificar cuáles son los elementos que muestran mayor vulnerabilidad en el sistema del software.	1

Sí ya que en la actualidad aún se encuentra en desarrollo la tipificación del acceso ilícito un claro ejemplo es el hacking ético y sus clasificaciones que pueden ser el hacking gris el negro y el blanco de los cuales el gris y el blanco pertenecen a los límites de la licitud en cuanto a las actividades de vulnerabilidad por lo que la simple exclusión que actualmente se prevé en la norma específica de los delitos informáticos no engloba la tipicidad o atipicidad de dichas clasificaciones.	1
Pereyra (2023)	**1**
Si, se diferencia entre el acceso ilícito es la finalidad del acto, el cual en algunas ocasiones genera disyuntivas en su aplicación, ya que en uno se cuenta con datos específicos de la penetración y en otros solo de la base general de datos que será el objetivo.	1
Si, atendiendo la necesidad de subclasificar los tipos de hacking e identificar claramente cuando pueden ser excluido el hacking ético ante una denuncia por acceso ilícito, toda vez que la exclusión que se encuentra en la ley de delitos informáticos, no distingue el hacking blanco (donde se cuenta con previa autorización) con el hacking ético gris y el acceso ilícito, ya que puede teñirse como un acto presumiblemente ilícito, por lo que debería establecerse igual que lo conciliadores, ingenieros que se encuentren previamente registrado en una base de datos para realizar pruebas de vulnerabilidad para el fortalecimiento de pruebas de vulnerabilidad sorpresiva.	1
Prado (2023)	**1**
Si.	1
Si.	1
Salazar (2023)	**1**
Si, principalmente es el dolo sobre el acto invasivo al sistema de seguridad que guarda datos de relevancia para la entidad en el acceso ilícito.	1
Si, dado que ya han pasado más de 4 años desde la dación de la norma y hasta la fecha no se han producido cambios sobre el hacking (acceso ilícito), ello evidencia que en el sistema peruano no se ha venido desarrollando nuevos conceptos como el hacking ético, siendo este una herramienta para fortalecer las políticas contra el acceso ilícito.	1
Santos (2023)	**1**
Si.	1
Si.	1
Vegas (2023)	**1**
Si, de forma concreta la primera tiene por finalidad verificar los riesgos en la seguridad de una base de datos, y la segunda es un delito que engloba la penetración dolosa a una base de datos con fines de aprovechamiento o beneficio.	1
Si, considerando la complejidad del hacking ético y las diversas modalidades del acceso ilícito.	1
Total general	**10**

Tabla N° 6

Postura del objetivo general

Posturas	**Recuento**

El hacker del sobrero gris no busca un beneficio personal o causar daño actuando de forma no tan ética trata de comprometer la seguridad sin tener la autorización con la finalidad de proponer mejoras a esta con posterioridad	**6**
Acosta Montoya, Y. M.(2021). Brito Bermúdez, P. M. (2018). García Perero, F. G. (2021). González, M. J. S. (2017). Restrepo Ángel, C. L., & Sánchez Jaramillo, E. G. (2018). Torres, M. (2019). **En el hacking ético existen tres formas de realizarse, y tres tipos de hackers de forma general, siendo de los más usuales el hacking ético, quien actúa con previa autorización, no obstante, se reportan casos de hackers grises, quienes comunican las vulnerabilidades con fines de obtener asesorías personales o practicar sus métodos.**	**8**
Aruquipa Machicado, R. (2019) Bonilla Rios, Y. P. (2022). Cacua Patiño, N. P. (2022) Curay Calucho, M. F. (2023). Fernandez Figueroa, A. (2022). Hurtado Sandoval, M. E., & Mendaño Mendaño, L. A. (2016). Mateos Pascual, I. (2013). Rojas Buenaño, A. I. (2018). **Existen pruebas de vulnerabilidad que no son concretas o específicas sobre el fin de pentester**	**2**
Santos, C. P., Guisado, Á. C., & Morán, J. J. D. (2017). Vidal Londoño, J. H. (2017). **La forma con mayor eficiencia es el hacking ético negro, no obstante, algunos de estos se realizan por hackers de sobrero gris, de los cuales existe una ambigüedad de su legalidad o ilegalidad.**	**9**
Andrade Chimba, C. D. (2016) Bermeo Oyola, J. C. (2019). Borbor Tóala, J. A. (2022). Chávez Salazar, V. H. (2021). Lledó Benito, I. (2021). Ortiz Padilla, G. A. (2021). Paredes Gutiérrez, R. A., & Pérez Valencia, F. D. (2022). Piñashca Huerta, R. J. (2022). Vera Correa, J. A. (2021)	
Total general	**25**

Tabla N° 7
Postura del primer objetivo específico

Postura del primer objetivo específico	Recuento
El mejor tipo de prueba de vulnerabilidad es el hacking ético en caja negra o gris, y la más usada es la caja blanca, y los profesionales que la ejecutan son contratados de empresas o terceros, y de los ambiguos o terceros externos se tiene al hacker de sombrero gris, que su ética es ambigua, pero produce una mayor simulación a la realidad	**25**
Acosta Montoya, Y. M. (2021).	
Andrade Chimba, C. D. (2016)	
Aruquipa Machicado, R. (2019)	
Bermeo Oyola, J. C. (2019).	
Bonilla Rios, Y. P. (2022).	
Borbor Tóala, J. A. (2022).	
Brito Bermúdez, P. M. (2018).	
Cacua Patiño, N. P. (2022)	
Chávez Salazar, V. H. (2021).	
Curay Calucho, M. F. (2023).	
Fernández Figueroa, A. (2022).	
García Perero, F. G. (2021).	
González, M. J. S. (2017).	
Hurtado Sandoval, M. E., & Mendaño Mendaño, L. A. (2016).	
Lledó Benito, I. (2021).	
Mateos Pascual, I. (2013).	
Ortiz Padilla, G. A. (2021).	
Paredes Gutiérrez, R. A., & Pérez Valencia, F. D. (2022).	
Piñashca Huerta, R. J. (2022).	
Restrepo Ángel, C. L., & Sánchez Jaramillo, E. G. (2018).	
Rojas Buenaño, A. I. (2018).	
Santos, C. P., Guisado, Á. C., & Morán, J. J. D. (2017).	
Torres, M. (2019).	
Vera Correa, J. A. (2021)	
Vidal Londoño, J. H. (2017).	
Total general	**25**

Tabla N° 8
Postura del primer objetivo específico

Postura del segundo objetivo específico	Recuento
En los hacking éticos en caja blanca y gris, siempre existe una identificación del hacker ético o empresa especializada que realiza, es decir no necesita registro por que se informa sus actividades y resultados de la prueba. Sin embargo, en las pruebas de terceros externos, que se reportan no se cuenta con un registro y comúnmente solo se conoce los resultados, sin procedimiento y posterior al ataque el hacker profesional (hacker gris) pone en conocimiento para realizar pruebas de vulnerabilidad o solo realiza pruebas con fines de mejorar sus capacidades y con el fin de mejorar la seguridad de la empresa.	**25**
Acosta Montoya, Y. M. (2021).	1
Andrade Chimba, C. D. (2016)	1
Aruquipa Machicado, R. (2019)	1
Bermeo Oyola, J. C. (2019).	1
Bonilla Ríos, Y. P. (2022).	1
Borbor Tóala, J. A. (2022).	1
Brito Bermúdez, P. M. (2018).	1
Cacua Patiño, N. P. (2022)	1
Chávez Salazar, V. H. (2021).	1
Curay Calucho, M. F. (2023).	1
Fernández Figueroa, A. (2022).	1
García Perero, F. G. (2021).	1
González, M. J. S. (2017).	1
Hurtado Sandoval, M. E., & Mendaño Mendaño, L. A. (2016).	1
Lledó Benito, I. (2021).	1
Mateos Pascual, I. (2013).	1
Ortiz Padilla, G. A. (2021).	1
Paredes Gutiérrez, R. A., & Pérez Valencia, F. D. (2022).	1
Piñashca Huerta, R. J. (2022).	1
Restrepo Ángel, C. L., & Sánchez Jaramillo, E. G. (2018).	1
Rojas Buenaño, A. I. (2018).	1
Santos, C. P., Guisado, Á. C., & Morán, J. J. D. (2017).	1
Torres, M. (2019).	1
Vera Correa, J. A. (2021)	1
Vidal Londoño, J. H. (2017).	1
Total general	**25**

Anexo 5 –
Evidencia de entrevistas

ANEXO 2: Instrumentos de recolección de datos

GUÍA DE ENTREVISTA

El presente instrumento pretende recopilar su opinión respecto a la "Regulación del hacking ético: prueba de vulnerabilidad sorpresiva y la exclusión en la subsunción de los delitos de acceso ilícito**"**

Para lo cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales.

Entrevistado (Nombre y apellido)**:** María del Carmen Pereyra Roca
Máximo Grado académico: Titulada – Egresada de Maestría
Cargo: Fiscal Adjunta Provincial
Institución: Ministerio Público

Fecha 03/05/23 Hora__12:00_ Lugar Campo Marte- Ministerio Público

Determinar si debe regularse el hacking ético para excluirlo del delito de acceso ilícito

OBJETIVO GENERAL

1. ¿Conoce que es el Hacking ético y su diferencia con el delito de acceso ilícito?

   El Hacking ético en el Perú no distingue los tipos de hacker, ya que es muy distinto hablar del hacker blanco y gris que el negro. Además, en la actualidad la mayor controversia es en relación al hacker gris el cual puede infringir alguna ley o precepto ético, pero no actúan con la malicia que caracteriza al hacker de sombrero negro, es decir la diferencia entre el acceso ilícito es la finalidad del acto, el cual en algunas ocasiones genera disyuntivas en su aplicación, ya que en uno se cuenta con datos específicos de la penetración y en otros solo de la base general de datos que será el objetivo.

2. ¿Considera que deben regularse las conductas explícitas del hacking según las modalidades en el acceso ilícito?

Si, atendiendo la necesidad de subclasificar los tipos de hacking e identificar claramente cuando pueden ser excluido el hacking ético ante una denuncia por acceso ilícito, toda vez que la exclusión que se encuentra en la ley de delitos informáticos, no distingue el hacking blanco (donde se cuenta con previa autorización) con el hacking ético gris y el acceso ilícito, ya que puede teñirse como un acto presumiblemente ilícito, por lo que debería establecerse igual que lo conciliadores, ingenieros que se encuentren previamente registrado en una base de datos para realizar pruebas de vulnerabilidad para el fortalecimiento de pruebas de vulnerabilidad sorpresiva.

OBJETIVO ESPECÍFICO 1

Determinar si la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito.

3. ¿Conoce que es la vulnerabilidad de un sistema de protección de datos en el acceso ilícito?

Si, la vulnerabilidad, es el grado potencial para que un acto de penetración se realice sobre un sistema de seguridad de datos relevantes para una entidad, dependiendo de los datos es el grado de afectación a la entidad.

4. ¿Considera que se debe regular condiciones y requisitos en el hacking ético para su tipificación o excepción en el delito de acceso ilícito?

Actualmente se encuentra regulado una excepción que consiste en la previa autorización para el acceso de datos, no obstante, existen comunidades de informáticos y peritos que cuestionan la finalidad sobre el acceso ilícito el cual cosiste en probar la vulnerabilidad con fines comerciales o testeo, es decir para vender sus servicios a la entidad

(promoción agresiva) o la publicación de vulnerabilidad con el fin que la entidad corrija sus vulnerabilidades en el sistema de seguridad.

OBJETIVO ESPECÍFICO 2

Determinar si la regulación de un posregistro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito

5. ¿Conoce que el hacking ético tiene una naturaleza sorpresiva y busca mejorar la calidad de los sistemas de protección de datos para evitar el acceso ilícito?

Propiamente el hacking ético ha venido cambiando pues ahora el hacking blanco se cuenta con una autorización previa, y que la diferencia al acceso ilícito, es que dicha prueba se conoce por la entidad, no obstante ello no impide de que pueda ser aplicada sobre distintos host o bases Myps que se encuentren dentro de la base de datos, es decir no impide de que pueda ejercer una penetración sorpresiva sobre otros datos con el previo conocimiento del gerente en jefe en el momento, o con posterioridad, lo cual conlleva a la siguiente figura denominada hacking gris.

6. ¿Considera que la implementación de un registro de hackers éticos (profesionales que prueben la vulnerabilidad de sistemas) es necesaria para determinar la responsabilidad del acceso ilícito en casos de no contar con autorización?

Si, permitiría que el hacking ético (gris) sea ejercido sin temor a represalia, conllevando a las empresas a la inversión de ciberseguridad sobre la base de datos, más aún si hasta la fecha sigue creciendo los delitos de accesos ilícitos en bancos u otras entidades._____

Firma

María del Carmen Pereyra Roca
Fiscal Adjunta Provincial
de la 26° FPPL

ANEXO 2: Instrumentos de recolección de datos

GUÍA DE ENTREVISTA

El presente instrumento pretende recopilar su opinión respecto a la "Regulación del hacking ético: prueba de vulnerabilidad sorpresiva y la exclusión en la subsunción de los delitos de acceso ilícito"

Para lo cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales.

Entrevistado (Nombre y apellido)**:** Sally Victoria Salazar Torres
Máximo Grado académico: Titulada
Cargo: Fiscal Adjunta Provincial
Institución: Ministerio Público

Fecha 03/05/23 Hora__16:00_ Lugar Campo Marte- Ministerio Público

Determinar si debe regularse el hacking ético para excluirlo del delito de acceso ilícito

OBJETIVO GENERAL

1. ¿Conoce que es el Hacking ético y su diferencia con el delito de acceso ilícito?

   Si, principalmente es el dolo sobre el acto invasivo al sistema de seguridad que guarda datos de relevancia para la entidad en el acceso ilícito.

2. ¿Considera que deben regularse las conductas explícitas del hacking según las modalidades en el acceso ilícito?

   Si, dado que ya han pasado más de 4 años desde la dación de la norma y hasta la fecha no se han producido cambios sobre el hacking (acceso ilícito), ello evidencia que en el sistema peruano no se ha venido desarrollando nuevos conceptos como el hacking ético, siendo este una herramienta para fortalecer las políticas contra el acceso ilícito.

OBJETIVO ESPECÍFICO 1

Determinar si la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito.

3. ¿Conoce que es la vulnerabilidad de un sistema de protección de datos en el acceso ilícito?

_Si, concretamente se hace referencia al grado de penetración o potencial afectación a una base de datos que pertenece a una entidad, principalmente las afectadas son base de datos de centros bancarios o empresas tercerías.

4. ¿Considera que se debe regular condiciones y requisitos en el hacking ético para su tipificación o excepción en el delito de acceso ilícito?

_Si, principalmente para el hacking ético que se denomina como gris, pues existen casos donde se formula cargos contra un imputado a sabiendas que no se generó bajo un acto doloso, siendo finalmente absuelto o sobreseído por ausencia de pruebas concretas que demuestren el fin ilícito (beneficio) del acceso.

OBJETIVO ESPECÍFICO 2

Determinar si la regulación de un posregistro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito

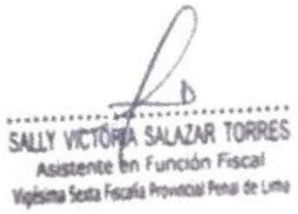
5. ¿Conoce que el hacking ético tiene una naturaleza sorpresiva y busca mejorar la calidad de los sistemas de protección de datos para evitar el acceso ilícito?

_Si principalmente los test de vulnerabilidad tienen la finalidad de generar mayor reforzamiento sobre las pruebas de vulnerabilidad contratadas por las mismas entidades, pues en otros países se regula el hacking ético bajo una base de datos o la concertación posterior de los datos adquiridos

y las vulnerabilidades, es decir que entre las partes puede existir un consenso que finalmente en el proceso no se considera al ser un delito que se afectan bienes indisponibles (datos personales).

6. ¿Considera que la implementación de un registro de hackers éticos (profesionales que prueben la vulnerabilidad de sistemas) es necesaria para determinar la responsabilidad del acceso ilícito en casos de no contar con autorización?

__Si, ya que procesalmente nos permitirá establecer ante la ausencia en dicho registro que su actividad de se presume y corrobora como un acto con fines ilícitos tentativos, es decir que no se llegaron a concertar.



Firma

ANEXO 2: Instrumentos de recolección de datos

GUÍA DE ENTREVISTA

El presente instrumento pretende recopilar su opinión respecto a la "Regulación del hacking ético: prueba de vulnerabilidad sorpresiva y la exclusión en la subsunción de los delitos de acceso ilícito"

Para lo cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales.

Entrevistado: Yoel Bravo Yucra
Máximo Grado académico: Maestros en Derecho Penal
Cargo: Juez Penal
Institución: Séptimo Juzgado del Penal Liquidador

Fecha 19 de mayo de 2023 Hora 8:30 pm Lugar: presencial

Determinar si debe regularse el hacking ético para excluirlo del delito de acceso ilícito

OBJETIVO GENERAL

1. ¿Conoce que es el Hacking ético y su diferencia con el delito de acceso ilícito?

   _Si, sobre el delito de acceso ilícito, no obstante, sobre el hacking ético lo conozco a grandes rasgos.

2. ¿Considera que deben regularse las conductas explícitas del hacking según las modalidades en el acceso ilícito?

   _A fin de esclarecer de forma concreta la norma debería evaluarse su beneficio o su innecesaria regulación, finalmente a la fecha se cuenta con excepciones explicitas en la ley, que, si bien no producen o exponen el hacking ético como prueba de vulnerabilidad, tampoco cierra su oportunidad de sostenerse como inimputabilidad o como acto atípico.

OBJETIVO ESPECÍFICO 1

Determinar si la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito.

3. ¿Conoce que es la vulnerabilidad de un sistema de protección de datos en el acceso ilícito?

_Si, conforme a los peritos de la DIVINDAT representar el grado de seguridad de una base de datos.

4. ¿Considera que se debe regular condiciones y requisitos en el hacking ético para su tipificación o excepción en el delito de acceso ilícito?

__Si a fin de evitar la formulación de procesos de forma innecesario para lo cual debería incluir un registro de actividades sobre las prácticas del hacking ético.

OBJETIVO ESPECÍFICO 2

Determinar si la regulación de un posregistro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito

5. ¿Conoce que el hacking ético tiene una naturaleza sorpresiva y busca mejorar la calidad de los sistemas de protección de datos para evitar el acceso ilícito?

Particularmente sus características y elementos no son de mi entero conocimiento, pero tengo entendido que las condiciones sorpresivas son propias para las pruebas de vulnerabilidad.

6. ¿Considera que la implementación de un registro de hackers éticos (profesionales que prueben la vulnerabilidad de sistemas) es necesaria para determinar la responsabilidad del acceso ilícito en casos de no contar con autorización?

Si, de acuerdo a lo que menciono con anterioridad.

Firma

ANEXO 2: Instrumentos de recolección de datos

GUÍA DE ENTREVISTA

El presente instrumento pretende recopilar su opinión respecto a la "Regulación del hacking ético: prueba de vulnerabilidad sorpresiva y la exclusión en la subsunción de los delitos de acceso ilícito**"**

Para lo cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales.

Entrevistado (Nombre y apellido)**: Edder Jiménez Sánchez**
Máximo Grado académico: Maestro en derecho penal
Cargo: Juez
Institución: Poder Judicial

Fecha 16 de mayo de 2023 Hora: 6:10 pm Lugar: presencial

Determinar si debe regularse el hacking ético para excluirlo del delito de acceso ilícito

OBJETIVO GENERAL

1. ¿Conoce que es el Hacking ético y su diferencia con el delito de acceso ilícito?

   _Si es una modalidad por la cual un sujeto especializado en alta tecnología realiza pruebas de vulnerabilidad es decir la penetración en base de datos a fin de identificar cuáles son los elementos que muestran mayor vulnerabilidad en el sistema del software.

2. ¿Considera que deben regularse las conductas explícitas del hacking según las modalidades en el acceso ilícito?

   __sí ya que en la actualidad aún se encuentra en desarrollo la tipificación del acceso ilícito un claro ejemplo es el hacking ético y sus clasificaciones que pueden ser el hacking gris el negro y el blanco de los cuales el gris y el blanco pertenecen a los límites de la licitud en cuanto a las actividades de vulnerabilidad por lo que la simple exclusión que actualmente se prevé

en la norma específica de los delitos informáticos no engloba la tipicidad o atipicidad de dichas clasificaciones.

OBJETIVO ESPECÍFICO 1

Determinar si la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito.

3. ¿Conoce que es la vulnerabilidad de un sistema de protección de datos en el acceso ilícito?

_sí es el medio o grado por el cual se identifica aspectos o elementos de riesgo dentro de un sistema de seguridad que comprende datos relevancia para la entidad correspondiente.

4. ¿Considera que se debe regular condiciones y requisitos en el hacking ético para su tipificación o excepción en el delito de acceso ilícito?

__sí ya que en la actualidad el artículo 12 de la ley de delitos informáticos establece la exclusión del acceso ilícito mediante pruebas de vulnerabilidad cuando únicamente se tiene la autorización por lo que dicho contexto no concuerda con todas las formas de vulnerabilidad y pruebas de vulnerabilidad que son ejercidas en la actualidad.

OBJETIVO ESPECÍFICO 2

Determinar si la regulación de un posregistro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito

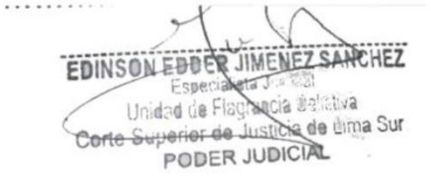
5. ¿Conoce que el hacking ético tiene una naturaleza sorpresiva y busca mejorar la calidad de los sistemas de protección de datos para evitar el acceso ilícito?

_principalmente se tiene en cuenta que en la actualidad las pruebas de vulnerabilidad son parte del fortalecimiento de los sistemas de seguridad que guardan datos por lo que la aplicación y la promoción de dichas

pruebas se vulnerabilidad deben ser cada vez más eficientes y efectivas en este contexto es de suma relevancia que se generen nuevos métodos que busquen la perfección o mayor eficiencia en la protección es decir a través de los métodos de las pruebas de vulnerabilidad con una condición sorpresiva.

6. ¿Considera que la implementación de un registro de hackers éticos (profesionales que prueben la vulnerabilidad de sistemas) es necesaria para determinar la responsabilidad del acceso ilícito en casos de no contar con autorización?

-Sí ya que sería un método tanto para prevenir la comisión del delito de acceso ilícito mediante el hacking ético negro hoy los métodos como el craqueo lo cual a su vez permitirá aplicar el hacking ético bajo su verdadera naturaleza la cual es una condición sorpresiva y finalmente permitirá en actividad procesal establecer una prueba sobre el acto de acceso pues al no registrar sus actividades conlleva a la conclusión de que efectivamente se cometió el acceso ilícito con fines de obtener un beneficio.



Firma

ANEXO 2: Instrumentos de recolección de datos

GUÍA DE ENTREVISTA

El presente instrumento pretende recopilar su opinión respecto a la "Regulación del hacking ético: prueba de vulnerabilidad sorpresiva y la exclusión en la subsunción de los delitos de acceso ilícito"

Para lo cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales.

Entrevistado: Cesar Alejandro Franco Gonzales
Cargo: Juez Titular
Institución: Juzgado Especializado Penal

Fecha 19 de mayo de 2023 Hora: 17:00 pm Lugar: Juzgado

Determinar si debe regularse el hacking ético para excluirlo del delito de acceso ilícito

OBJETIVO GENERAL

1. ¿Conoce que es el Hacking ético y su diferencia con el delito de acceso ilícito?

   Sí de forma general se entiende como aquellas pruebas que tienen como bases políticas de mejoramiento a la seguridad sistemas de datos partiendo del concepto que en la actualidad se regula excepciones concretas al acceso ilícito nombrándose las pruebas de vulnerabilidad.

2. ¿Considera que deben regularse las conductas explícitas del hacking según las modalidades en el acceso ilícito?

   _sí ya que en la fecha se viene presentando diversas formas de acceso a base de datos entre estas el hacking ético lo cual ha producido incógnitas en razón a la subclasificación de la misma.

OBJETIVO ESPECÍFICO 1

Determinar si la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito.

3. ¿Conoce que es la vulnerabilidad de un sistema de protección de datos en el acceso ilícito?

__sí es una forma de medir la actividad en relación a la posible vulneración de un sistema informático siendo esta modalidad comúnmente aplicada a través de la previa autorización lo cual es contradictorio a la propia naturaleza del hacking ético.

4. ¿Considera que se debe regular condiciones y requisitos en el hacking ético para su tipificación o excepción en el delito de acceso ilícito?

__sí ya que evitaría las contradicciones constantes sobre el acto de magnético y el acceso ilícito principalmente sobre las subclasificaciones como es el hacking ético gris.

OBJETIVO ESPECÍFICO 2

Determinar si la regulación de un posregistro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito

5. ¿Conoce que el hacking ético tiene una naturaleza sorpresiva y busca mejorar la calidad de los sistemas de protección de datos para evitar el acceso ilícito?

_sí ya que la propia naturaleza de las pruebas de vulnerabilidad desde un principio tiene una actividad sorpresiva lo cual en nuestra legislación es contraria.

6. ¿Considera que la implementación de un registro de hackers éticos (profesionales que prueben la vulnerabilidad de sistemas) es necesaria para determinar la responsabilidad del acceso ilícito en casos de no contar con autorización?

_ sí ya queda la fecha no existen métodos por los cuales se establezcan de forma concreta cuando se realizan pruebas de vulnerabilidad por lo que aplicar un registro previo o posterior permitiría identificar el fin que tienen con dicha penetración es decir si es un acceso ilícito o una prueba de vulnerabilidad.

Firma

ANEXO 2: Instrumentos de recolección de datos

GUÍA DE ENTREVISTA

El presente instrumento pretende recopilar su opinión respecto a la "Regulación del hacking ético: prueba de vulnerabilidad sorpresiva y la exclusión en la subsunción de los delitos de acceso ilícito"

Para lo cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales.

Entrevistado (Nombre y apellido)**:** Daniel Ignacio Santos Santos
Máximo Grado académico: Egresado de Maestría
Cargo: Asistente en función fiscal
Institución: Ministerio Público

Fecha_25 de mayo de 2023 Hora_18:00 Lugar_ Despacho Fiscal

OBJETIVO GENERAL

Determinar si debe regularse el hacking ético para excluirlo del delito de acceso ilícito

1. ¿Conoce que es el Hacking ético y su diferencia con el delito de acceso ilícito?

   _Si.

2. ¿Considera que deben regularse las conductas explícitas del hacking según las modalidades en el acceso ilícito?

   __Si.

OBJETIVO ESPECÍFICO 1

Determinar si la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito.

3. ¿Conoce que es la vulnerabilidad de un sistema de protección de datos en el acceso ilícito?

   _Si, es el grado o nivel de riesgo en la base de datos de una empresa o institución.

4. ¿Considera que se debe regular condiciones y requisitos en el hacking ético para su tipificación o excepción en el delito de acceso ilícito?

   __Si, ya que la actual exclusión que es la autorización, no engloba su naturaleza sorpresiva.

OBJETIVO ESPECÍFICO 2

Determinar si la regulación de un posregistro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito

5. ¿Conoce que el hacking ético tiene una naturaleza sorpresiva y busca mejorar la calidad de los sistemas de protección de datos para evitar el acceso ilícito?

   _Si.

6. ¿Considera que la implementación de un registro de hackers éticos (profesionales que prueben la vulnerabilidad de sistemas) es necesaria para determinar la responsabilidad del acceso ilícito en casos de no contar con autorización?

   Si, a través del registro podrá considerarse todo hacking ético, sea con autorización (en la que se excedió de los limites) o sin ella que es un acceso ilícito, es decir permitirá corroborar o enervar la responsabilidad en acceso a bases de datos.

Firma

ANEXO 2: Instrumentos de recolección de datos

GUÍA DE ENTREVISTA

El presente instrumento pretende recopilar su opinión respecto a la "Regulación del hacking ético: prueba de vulnerabilidad sorpresiva y la exclusión en la subsunción de los delitos de acceso ilícito"

Para lo cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales.

Entrevistado (Nombre y apellido)**:** Miguel Ángel Vegas Vaccaro
Máximo Grado académico: Doctor en Derecho Penal
Cargo: Fiscal Adjunto Supremo
Institución: Ministerio Público

Fecha_25 de mayo de 2023 Hora_17:00 Lugar Sede Abancay

OBJETIVO GENERAL

Determinar si debe regularse el hacking ético para excluirlo del delito de acceso ilícito

1. ¿Conoce que es el Hacking ético y su diferencia con el delito de acceso ilícito?

   _Si, de forma concreta la primera tiene por finalidad verificar los riesgos en la seguridad de una base de datos, y la segunda es un delito que engloba la penetración dolosa a una base de datos con fines de aprovechamiento o beneficio.

2. ¿Considera que deben regularse las conductas explícitas del hacking según las modalidades en el acceso ilícito?

   _Si, considerando la complejidad del hacking ético y las diversas modalidades del acceso ilícito.

OBJETIVO ESPECÍFICO 1

Determinar si la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito.

3. ¿Conoce que es la vulnerabilidad de un sistema de protección de datos en el acceso ilícito?

   _Si.

4. ¿Considera que se debe regular condiciones y requisitos en el hacking ético para su tipificación o excepción en el delito de acceso ilícito?

   _Si, a fin de evitar complicaciones o desgaste del Estado para tratar de determinar la existencia del fin doloso en el acceso ilícito, por lo que a manera practica fijar requisitos o condiciones para la práctica de hacking ético sorpresivo permitiría identificar estas conductas bajo sanción de ser denunciados por declaración falsa en un proceso judicial.

OBJETIVO ESPECÍFICO 2

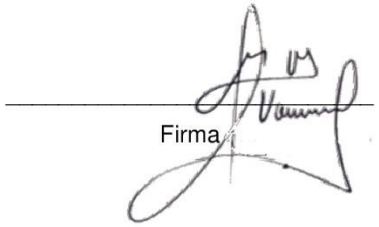
Determinar si la regulación de un posregistro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito

5. ¿Conoce que el hacking ético tiene una naturaleza sorpresiva y busca mejorar la calidad de los sistemas de protección de datos para evitar el acceso ilícito?

   _Si.

6. ¿Considera que la implementación de un registro de hackers éticos (profesionales que prueben la vulnerabilidad de sistemas) es necesaria para determinar la responsabilidad del acceso ilícito en casos de no contar con autorización?

   __Si, en concordancia a mi anterior respuesta.



Firma

ANEXO 2: Instrumentos de recolección de datos

GUÍA DE ENTREVISTA

El presente instrumento pretende recopilar su opinión respecto a la "Regulación del hacking ético: prueba de vulnerabilidad sorpresiva y la exclusión en la subsunción de los delitos de acceso ilícito"

Para lo cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales.

Entrevistado (Nombre y apellido)**:** Cristian Domínguez Malpartida
Máximo Grado académico: Ingeniero
Cargo: Perito en DIVINDAT
Institución: PNP

Fecha 25 de mayo de 2023 Hora 20:00 Lugar_ Aramburu

OBJETIVO GENERAL

Determinar si debe regularse el hacking ético para excluirlo del delito de acceso ilícito

1. ¿Conoce que es el Hacking ético y su diferencia con el delito de acceso ilícito?

   _Si, de forma concreta la primera cuenta con un fin ilícito, y a segunda tiene un fin técnico y de rendimiento para el fortalecimiento de las bases de datos.

2. ¿Considera que deben regularse las conductas explícitas del hacking según las modalidades en el acceso ilícito?

   __Si.

OBJETIVO ESPECÍFICO 1

Determinar si la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito.

3. ¿Conoce que es la vulnerabilidad de un sistema de protección de datos en el acceso ilícito?

_Si, es el nivel de riesgo que tiene una base de datos.

4. ¿Considera que se debe regular condiciones y requisitos en el hacking ético para su tipificación o excepción en el delito de acceso ilícito?

_Si para evitar la inseguridad en caso se alegue el uso de hacking ético.

OBJETIVO ESPECÍFICO 2

Determinar si la regulación de un posregistro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito

5. ¿Conoce que el hacking ético tiene una naturaleza sorpresiva y busca mejorar la calidad de los sistemas de protección de datos para evitar el acceso ilícito?

_Si, ya que desde un principio las pruebas de vulnerabilidad tienen una función que cosiste en la protección y fortalecimiento de una base de datos, por lo que, la empresa de datos, como son pequeñas empresas, bancos de empeño u otros podrá ser beneficiados por el permiso posterior para que pueda solicitar

6. ¿Considera que la implementación de un registro de hackers éticos (profesionales que prueben la vulnerabilidad de sistemas) es necesaria para determinar la responsabilidad del acceso ilícito en casos de no contar con autorización?

__Si, así podrá evitarse la necesidad de realizar pruebas complementarias para identificar el autor y quien realizo la conducta del acceso ilícito, para lo cual se puede implementar la obligación de contar con certificación de Ethical Hacking and Countermeasures v12

DOMÍNGUEZ MALPARTIDA CRISTIAN JAVIER
INGENIERO CIVIL
Reg. CIP N° 130747

ANEXO 2: Instrumentos de recolección de datos

GUÍA DE ENTREVISTA

El presente instrumento pretende recopilar su opinión respecto a la "Regulación del hacking ético: prueba de vulnerabilidad sorpresiva y la exclusión en la subsunción de los delitos de acceso ilícito"

Para lo cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales.

Entrevistado (Nombre y apellido)**:** Edgar Orlando Prado De La Cruz
Máximo Grado académico: Magister en penal
Cargo: fiscal provincial
Institución: Ministerio público

Fecha 26 de mayo de 2023 Hora 20:00 Lugar_ Aramburu

OBJETIVO GENERAL

Determinar si debe regularse el hacking ético para excluirlo del delito de acceso ilícito

1. ¿Conoce que es el Hacking ético y su diferencia con el delito de acceso ilícito?

   _Si.

2. ¿Considera que deben regularse las conductas explícitas del hacking según las modalidades en el acceso ilícito?

   __Si.

OBJETIVO ESPECÍFICO 1

Determinar si la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito.

3. ¿Conoce que es la vulnerabilidad de un sistema de protección de datos en el acceso ilícito?

_Si.

4. ¿Considera que se debe regular condiciones y requisitos en el hacking ético para su tipificación o excepción en el delito de acceso ilícito?

_Si.

OBJETIVO ESPECÍFICO 2

Determinar si la regulación de un posregistro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito

5. ¿Conoce que el hacking ético tiene una naturaleza sorpresiva y busca mejorar la calidad de los sistemas de protección de datos para evitar el acceso ilícito?

_Si.

6. ¿Considera que la implementación de un registro de hackers éticos (profesionales que prueben la vulnerabilidad de sistemas) es necesaria para determinar la responsabilidad del acceso ilícito en casos de no contar con autorización?

__Si.

ANEXO 2: Instrumentos de recolección de datos

GUÍA DE ENTREVISTA

El presente instrumento pretende recopilar su opinión respecto a la "Regulación del hacking ético: prueba de vulnerabilidad sorpresiva y la exclusión en la subsunción de los delitos de acceso ilícito"

Para lo cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales.

Entrevistado (Nombre y apellido)**:** Ana Marina Gotuzzo Ortiz
Máximo Grado académico: Magister en penal
Cargo: Fiscal provincial
Institución: Ministerio público

Fecha 26 de mayo de 2023 Hora 22:00 Lugar_ Hogar

OBJETIVO GENERAL

Determinar si debe regularse el hacking ético para excluirlo del delito de acceso ilícito

7. ¿Conoce que es el Hacking ético y su diferencia con el delito de acceso ilícito?

_Si.

8. ¿Considera que deben regularse las conductas explícitas del hacking según las modalidades en el acceso ilícito?

__Si.

OBJETIVO ESPECÍFICO 1

Determinar si la regulación de la prueba de vulnerabilidad sorpresiva por hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito.

9. ¿Conoce que es la vulnerabilidad de un sistema de protección de datos en el acceso ilícito?

_Si.

10. ¿Considera que se debe regular condiciones y requisitos en el hacking ético para su tipificación o excepción en el delito de acceso ilícito?

_Si.

OBJETIVO ESPECÍFICO 2

Determinar si la regulación de un posregistro como requisitos del hacking ético influye en la exclusión en la subsunción de los delitos de acceso ilícito

11. ¿Conoce que el hacking ético tiene una naturaleza sorpresiva y busca mejorar la calidad de los sistemas de protección de datos para evitar el acceso ilícito?

_Si.

12. ¿Considera que la implementación de un registro de hackers éticos (profesionales que prueben la vulnerabilidad de sistemas) es necesaria para determinar la responsabilidad del acceso ilícito en casos de no contar con autorización?

__Si.

Ada Marina Gotuzzo Ortiz
Fiscal Provincial
2ª Fiscalía Provincial Penal Corporativa
de Chosica - 1º Despacho