

**UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA**  
**FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS**  
**CARRERA PROFESIONAL DE DERECHO**



**TRABAJO DE SUFICIENCIA PROFESIONAL**

**“Marco jurídico de la ciberseguridad en el Perú: diagnóstico y propuestas de fortalecimiento normativo”**

**AUTORES:**

Bach. Flores Castañuedi, Judith  
Bach. Paredes Martinez, Hugo Mitchell

**PARA OPTAR EL TÍTULO PROFESIONAL DE:**

**ABOGADO**

**ASESOR:**

Dr. Vegas Gallo, Edwin Agustín  
ID ORCID: 0000-0002-2566-0115  
DNI: 02771235

**Lima - Perú**

**2025**

## INFORME DE SIMILITUD



### INFORME DE SIMILITUD

N°077-2025-UPCI-FDCP-REHO-T

**A** : **MG. HERMOZA OCHANTE RUBEN EDGAR**  
Decano (e) de la Facultad de Derecho y Ciencias Políticas

**DE** : **MG. HERMOZA OCHANTE, RUBEN EDGAR**  
Docente Operador del Programa Turnitin

**ASUNTO** : Informe de evaluación de Similitud de Trabajo de Suficiencia Profesional:  
**BACHILLER FLORES CASTAÑUEDI, JUDITH**  
**BACHILLER PAREDES MARTINEZ, HUGO MITCHELL**

**FECHA** : Lima, 12 de agosto de 2025.


---

Tengo el agrado de dirigirme a usted con la finalidad de informar lo siguiente:

1. Mediante el uso del programa informático **Turnitin** (con las configuraciones de excluir citas, excluir bibliografía y excluir oraciones con cadenas menores a 20 palabras) se ha analizado el Trabajo de Suficiencia Profesional titulada: “**MARCO JURÍDICO DE LA CIBERSEGURIDAD EN EL PERÚ: DIAGNÓSTICO Y PROPUESTAS DE FORTALECIMIENTO NORMATIVO**”, presentado por los Bachilleres **FLORES CASTAÑUEDI, JUDITH** y **PAREDES MARTINEZ, HUGO MITCHELL**.
2. Los resultados de la evaluación concluyen que el Trabajo de Suficiencia Profesional en mención tiene un **ÍNDICE DE SIMILITUD DE 4%** (cumpliendo con el artículo 35 del Reglamento de Grado de Bachiller y Título Profesional UPCI aprobado con Resolución N° 373-2019-UPCI-R de fecha 22/08/2019).
3. Al término análisis, los Bachilleres en mención **PUEDEN CONTINUAR** su trámite ante la facultad, por lo que el resultado del análisis se adjunta para los efectos consiguientes

Es cuanto hago de conocimiento para los fines que se sirva determinar.

Atentamente,

  
.....  
**MG. HERMOZA OCHANTE, RUBEN EDGAR**  
Universidad Peruana de Ciencias e Informática  
Docente Operador del Programa Turnitin

*Adjunto:*

*\*Resultado de similitud*

## **DEDICATORIA**

En primer lugar, dedicamos este trabajo a Dios todopoderoso, fuente de toda sabiduría y fortaleza, quien nos guió con su luz en los momentos de duda y nos sostuvo con su gracia en medio de las dificultades. Sin Él, nada de esto habría sido posible.

A nuestras familias, quienes, con su apoyo incondicional, paciencia y amor, nos han acompañado en cada paso de este camino académico.

Y a nosotros mismos, por la disciplina, el esfuerzo y la determinación que nos permitieron alcanzar esta meta, convencidos de que este es solo el inicio de una vida profesional guiada por el compromiso y la ética jurídica.

## **AGRADECIMIENTO**

Al Dr. Edwin Agustín Vegas Gallo, Rector de la Universidad Peruana de Ciencias e Informática.

Al Mg. Ruben Edgard Hermoza Ochante, Decano de la Facultad de Derecho y Ciencias Políticas de la Universidad Peruana de Ciencias e Informática.

A nuestros maestros de la Facultad de Derecho de la Universidad Peruana de Ciencias e Informática, quienes con su entrega, compromiso y vocación nos han guiado en este camino de formación profesional.

## DECLARATORIA DE AUTORÍA

<b>Nombres :</b> <i>Judith</i>	<b>Nombres :</b> <i>Hugo Mitchell</i>
<b>Apellidos :</b> <i>Flores Castañuedi</i>	<b>Apellidos :</b> <i>Paredes Martínez</i>
<b>Código :</b> <i>1905000014</i>	<b>Código :</b> <i>1902000020</i>
<b>DNI :</b> <i>10380368</i>	<b>DNI :</b> <i>09585730</i>

Declaramos que somos los autores del trabajo realizado y que es la versión final que hemos entregado a la oficina del Decanato de la Facultad de Derecho y Ciencias Políticas de la Universidad Peruana de Ciencias e Informática.

Asimismo, declaramos que se ha citado debidamente las palabras o ideas de otros autores, refiriendo expresamente el nombre de la obra y página o páginas que nos sirvieron de fuente.

Lima, setiembre del 2025.

## ÍNDICE

CARÁTULA.....	i
INFORME DE SIMILITUD.....	ii
DEDICATORIA.....	iii
AGRADECIMIENTO.....	iv
DECLARATORIA DE AUTORÍA.....	v
ÍNDICE.....	vi
INTRODUCCIÓN.....	8
CAPÍTULO I. Planificación del Trabajo de Suficiencia Profesional.....	10
1.1.    Título del proyecto: Marco jurídico de la ciberseguridad en el Perú: diagnóstico y propuestas.....	10
1.2.    Línea de investigación: Derecho y tecnología.....	10
1.3.    Descripción del problema:.....	10
1.4.    Formulación del problema:.....	12
1.5.    Objetivos:.....	12
1.5.1.    General:.....	12
1.5.2.    Específicos:.....	12
1.6.    Justificación:.....	13
CAPÍTULO II. Marco Teórico.....	15
2.1.    La Ciberdelincuencia y la Ciberseguridad en el Perú.....	15
2.1.1.    Aproximaciones Conceptuales a la Ciberdelincuencia.....	16
2.1.2.    Ciberdelitos desde la Normativa Peruana.....	17
2.1.3.    Ciberseguridad y Ciberdefensa: Un Marco Integral.....	24

2.1.4.	Actores y Vulnerabilidades en la Ciberdelincuencia .....	27
2.1.5.	Respuesta Institucional del Estado Peruano y Gaps Existentes.....	31
2.1.6.	Cooperación Internacional .....	35
2.1.7.	Conclusiones y Necesidades Futuras .....	36
CAPÍTULO III. Desarrollo de Actividades Programadas .....		39
3.1.	Revisión Exhaustiva del Marco Legal Nacional en Ciberseguridad y Ciberdelincuencia.....	39
3.2.	Análisis comparado con legislaciones extranjeras.....	43
3.3.	Estudio de la Respuesta Institucional Peruana Frente a los Delitos Informáticos ...	45
3.4.	Elaboración de Propuestas Normativas .....	49
CAPÍTULO IV. Resultados Obtenidos.....		53
CONCLUSIONES .....		55
RECOMENDACIONES.....		56
REFERENCIAS BIBLIOGRÁFICAS.....		57
ANEXOS .....		59
	Anexo 1. Evidencia de similitud digital .....	60
	Anexo 2. Autorización de publicación en repositorio.....	64

## INTRODUCCIÓN

Vivimos en una época donde lo digital es transversal; la forma cómo nos comunicamos, cómo trabajamos, cómo compramos e incluso cómo funcionan nuestros gobiernos. Esta transformación tan rápida del mundo digital ha cambiado por completo nuestra forma de vivir en sociedad. Y en medio de todo esto, la ciberseguridad se ha vuelto algo fundamental. ¿Por qué? Porque de ella depende que la información que manejamos esté protegida, que nuestras instituciones funcionen con estabilidad y, sobre todo, que nuestros derechos estén resguardados en este nuevo entorno virtual.

En ese sentido, los países tienen hoy un enorme reto: crear leyes claras y eficaces que los ayuden a prevenir, enfrentar y sancionar los ataques cibernéticos, que cada vez son más sofisticados. En el caso del Perú, ya se han dado pasos importantes, como la creación de la Ley N.º 30999, conocida como la Ley de Ciberseguridad, junto con su reglamento. Sin embargo, aún quedan muchos aspectos por mejorar. Existen vacíos legales, poca coordinación entre instituciones y una falta de estándares internacionales que hacen que el sistema aún sea débil frente a las amenazas del ciberespacio.

Por eso, este trabajo de suficiencia profesional busca mirar de cerca cómo está funcionando el marco jurídico actual, identificar sus puntos débiles y plantear propuestas concretas para fortalecerlo. La idea es que contemos con un sistema legal más sólido y moderno, que no solo ayude a proteger mejor nuestra información, sino que también esté en línea con lo que ya vienen haciendo otros países en materia de ciberseguridad.

Este estudio cobra especial importancia porque no se trata solo de actualizar normas por cumplir, sino de preparar al Estado peruano para afrontar los riesgos tecnológicos con

mayor capacidad. Tener una legislación fuerte en ciberseguridad es clave para que las personas confíen en los servicios digitales, para cuidar nuestra soberanía tecnológica y, en última instancia, para avanzar hacia un desarrollo más seguro, justo e inclusivo en este nuevo mundo digital.

Además, es importante recordar que la ciberseguridad no es solo un tema del Estado o de las grandes empresas; es decir, nos toca a todos. Desde la persona que hace una transferencia bancaria desde su celular, hasta los estudiantes que estudian en línea o los pequeños negocios que venden por internet. Todos estamos expuestos, y por eso necesitamos leyes que estén a la altura de los riesgos actuales, que nos protejan de forma efectiva y real.

Mirar hacia afuera también puede ayudarnos. Hay países que ya han recorrido este camino y han desarrollado modelos exitosos que podríamos adaptar a nuestra realidad. Aprender de esas experiencias nos puede ayudar a diseñar una legislación que no solo reaccione ante los problemas, sino que también se adelante a ellos. En ese proceso, el compromiso con la ciudadanía debe ser siempre el eje central.

## **CAPÍTULO I. Planificación del Trabajo de Suficiencia Profesional**

### **1.1. Título del proyecto: Marco jurídico de la ciberseguridad en el Perú: diagnóstico y propuestas**

### **1.2. Línea de investigación: Derecho y tecnología**

### **1.3. Descripción del problema:**

Hoy en día, la tecnología está presente en casi todo lo que hacemos. Desde cómo buscamos información, cómo trabajamos o compramos, hasta cómo nos comunicamos con las instituciones del Estado, todo se ha vuelto digital. Esta transformación ha traído consigo muchos beneficios, es cierto, pero también nos ha expuesto a nuevos peligros. Amenazas como los ciberataques, el robo de datos personales o el sabotaje a sistemas informáticos ya no son situaciones extraordinarias; son riesgos reales que pueden afectarnos en cualquier momento.

Y el Perú no está ajeno a esta realidad. En los últimos años, hemos visto cómo tanto instituciones públicas como privadas han sido víctimas de ataques cibernéticos que han dejado al descubierto serias fallas en la protección de sus sistemas. Lo más preocupante es que, frente a estos incidentes, la respuesta institucional suele ser débil, desorganizada o simplemente insuficiente. Aunque contamos con una ley específica —la Ley N.º 30999, conocida como la Ley de Ciberseguridad—, su aplicación en la práctica ha sido limitada, y no ha logrado cubrir todos los frentes necesarios.

Uno de los principales desafíos es que no existe una estrategia nacional clara y bien articulada. Las instituciones que deberían liderar la ciberseguridad —como la PCM, el Ministerio del Interior o el Ministerio de Defensa— operan de manera separada, sin una estructura común que integre todo el ciclo de prevención, detección, respuesta y recuperación ante amenazas digitales. Además, muchas de estas entidades enfrentan serias limitaciones en recursos humanos y técnicos, lo cual reduce aún más su capacidad de acción.

A esto se suma que el marco legal actual tiene varios vacíos importantes. Por ejemplo, no hay normas claras para proteger infraestructuras digitales críticas, ni lineamientos que definan el rol de las empresas privadas en la defensa digital del país. Tampoco se ha legislado de forma específica sobre el uso y control del software malicioso (conocido como malware), ni se cuenta con un protocolo nacional unificado para responder ante incidentes cibernéticos. Y, como si fuera poco, el Perú aún no ha suscrito el Convenio de Budapest, que es el principal acuerdo internacional para combatir la ciberdelincuencia y fomentar la cooperación global.

Más allá de lo técnico o legal, la ciberseguridad es también un tema de confianza. Cuando las personas sienten que su información personal no está bien protegida, o que el sistema puede fallar ante un ataque digital, es natural que desconfíen. Y esa desconfianza se traduce en menor uso de servicios digitales, lo que frena el crecimiento y las oportunidades en sectores como la educación, la salud, el comercio y muchos más.

Por eso, no basta con tener leyes bien redactadas: necesitamos que esas leyes se apliquen, se actualicen y se adapten a los cambios constantes del mundo digital. La ciberseguridad es un campo que avanza rápido, y nuestras respuestas deben avanzar al mismo ritmo. Si realmente queremos construir una sociedad digital segura, inclusiva y preparada para

los desafíos del futuro, el Perú necesita con urgencia fortalecer su marco normativo y dotar de mayores capacidades a las instituciones encargadas de velar por nuestra seguridad digital.

#### **1.4. Formulación del problema:**

¿Cuáles son las principales deficiencias del marco jurídico de la ciberseguridad en el Perú y qué propuestas normativas podrían contribuir a su fortalecimiento frente a las amenazas digitales actuales?

#### **1.5. Objetivos:**

##### ***1.5.1. General:***

Analizar el marco jurídico de la ciberseguridad en el Perú para identificar sus deficiencias y formular propuestas normativas.

##### ***1.5.2. Específicos:***

1. Evaluar la Ley N.º 30999 y su reglamento.
2. Identificar vacíos legales en la protección de infraestructuras críticas.
3. Analizar la eficacia de la coordinación interinstitucional.
4. Comparar con marcos jurídicos internacionales.

## **1.6. Justificación:**

Vivimos en una era donde lo digital atraviesa casi todos los aspectos de nuestra vida: desde los trámites con el Estado, hasta cómo hacemos nuestras compras o manejamos nuestra vida personal. En ese contexto, la ciberseguridad se ha vuelto un tema crucial para el desarrollo del país. El constante aumento de ataques informáticos, tanto a entidades públicas como privadas, nos muestra con claridad que el Perú aún no cuenta con un sistema legal lo suficientemente fuerte como para proteger, de forma efectiva, la información y los sistemas que usamos a diario.

Este trabajo nace justamente de esa necesidad: fortalecer el marco jurídico que hoy tenemos en el país. Lo que se busca es identificar dónde están las fallas legales y plantear soluciones que estén alineadas con los estándares internacionales. No se trata solo de tener leyes por cumplir, sino de que estas realmente ayuden al Estado a estar mejor preparado frente a los riesgos digitales. Al mismo tiempo, un sistema legal más sólido contribuirá a resguardar derechos fundamentales como la privacidad, la seguridad y la integridad de la información en un mundo cada vez más digitalizado.

Además, este estudio cobra aún más relevancia en medio del proceso de Transformación Digital que impulsa actualmente el gobierno peruano. En este camino hacia un país más conectado, el marco legal debe avanzar al mismo ritmo que la tecnología. Desde el derecho, podemos y debemos aportar para que esta transición se dé de manera segura, ética y con pleno respeto por los derechos de todas y todos.

También es importante entender que mejorar las leyes sobre ciberseguridad no solo es una forma de defensa frente a los ataques, sino una oportunidad para crear una cultura digital más consciente y responsable. Si logramos establecer reglas claras y mecanismos efectivos de prevención y reacción, ayudamos a que la ciudadanía entienda la importancia de cuidar sus datos y de actuar con responsabilidad en el mundo virtual. Así, construimos un entorno digital donde todos podamos sentirnos más seguros.

Además, apostar por una legislación moderna en este ámbito puede ser un gran impulso para el crecimiento económico del país. Hoy en día, se toman muchas decisiones, desde las más simples hasta las más estratégicas, a través de plataformas digitales. Por eso, tener reglas claras, actualizadas y confiables no solo genera seguridad jurídica, sino también confianza, tanto en la ciudadanía como en quienes quieren invertir o emprender.

Una normativa sólida abre puertas: facilita el desarrollo del comercio electrónico, atrae nuevas oportunidades y ayuda a posicionar al Perú como un país que está listo para enfrentar los desafíos y aprovechar las ventajas del mundo digital. En este sentido, el derecho no se limita a poner límites; también puede ser una herramienta poderosa para impulsar el progreso y construir un futuro más dinámico, inclusivo y seguro para todos.

## **CAPÍTULO II. Marco Teórico.**

### **2.1. La Ciberdelincuencia y la Ciberseguridad en el Perú**

El avance de la tecnología en los últimos años ha cambiado por completo la forma en que vivimos, trabajamos y nos relacionamos. Hoy, gracias al desarrollo digital y a la conectividad a Internet, podemos hacer cosas que antes parecían impensables: estudiar desde casa, comprar con un clic, trabajar a distancia o comunicarnos con personas al otro lado del mundo en segundos.

Pero junto con todos estos beneficios, también han aparecido nuevas amenazas. Y es que, así como la tecnología ha evolucionado para bien, también lo han hecho ciertas formas de delincuencia que ahora operan en el entorno digital. Hablamos de la **ciberdelincuencia**, un fenómeno que cada día se vuelve más sofisticado y que pone en riesgo tanto a personas como a organizaciones.

En este panorama que cambia constantemente, conceptos como **ciberseguridad** y **ciberdefensa** ya no son exclusivos del mundo técnico: se han vuelto piezas clave para proteger lo más valioso. Desde nuestros datos personales hasta la estabilidad de una institución o la seguridad de un país entero, todo puede verse afectado si no se toman las medidas adecuadas.

Por eso, entender y fortalecer estos mecanismos no es solo una cuestión de tecnología, sino de responsabilidad colectiva. Es cuidar lo que hemos construido en este nuevo mundo digital.

### ***2.1.1. Aproximaciones Conceptuales a la Ciberdelincuencia***

Cuando hablamos de **ciberdelincuencia**, también conocida como *ciberdelito* o *cibercrimen*, nos referimos a una serie de acciones ilegales que se cometen usando computadoras, redes o sistemas digitales. Es un término amplio que abarca desde el robo de datos hasta ataques a plataformas o servicios en línea. La Organización de las Naciones Unidas (ONU) la define como cualquier hecho en el que los sistemas informáticos o la información digital son el blanco del delito, o forman parte esencial de cómo se lleva a cabo. Es decir, ya sea que los datos sean lo que se quiere dañar o robar, o que los medios tecnológicos se usen como herramientas para cometer el delito. Por su parte, el investigador Villavicencio (2014) va un poco más allá y explica que la criminalidad informática incluye todas aquellas conductas que buscan vulnerar sistemas de seguridad digital, y que solo pueden ocurrir gracias al uso de la tecnología. Además, señala que las Tecnologías de la Información y la Comunicación (TIC) pueden ser tanto el objetivo del delito, como el medio para cometerlo o incluso el escenario donde ocurre, afectando derechos fundamentales y bienes protegidos por la ley.

Hoy en día, muchos delitos ya no ocurren solo en las calles, sino también detrás de una pantalla. La **ciberdelincuencia** se vale de herramientas que usamos a diario —como computadoras, celulares o redes sociales— para vulnerar derechos tan sensibles como la intimidad, el honor e incluso la libertad sexual. Este fenómeno, que crece cada vez con más fuerza, representa un reto enorme para los gobiernos. No solo se necesita actualizar las leyes, sino también preparar a los profesionales y tomar decisiones urgentes para proteger a las personas y garantizar su bienestar en el mundo digital.

El avance de la ciberdelincuencia es una realidad preocupante. El uso de tecnologías digitales ha crecido a un ritmo acelerado, y con ello también los riesgos. Solo para dar una idea: en 2018, Perú destinó 60 millones de dólares a tecnologías en la nube, y se estimaba que, para 2022, las pérdidas por delitos informáticos en todo el mundo podrían alcanzar los 8 billones de dólares. En nuestra región, América Latina y el Caribe, estos delitos ya generaban costos cercanos a los 575 millones de dólares al año, según datos del Observatorio de Ciberseguridad.

Además, el mundo está cada vez más conectado. Se proyectaba que para 2025 existirían unos 20 mil millones de dispositivos conectados a internet. Esta interconexión masiva hace que seamos más vulnerables. En el caso del Perú, la situación también es alarmante. Según la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional, las denuncias por ciberdelitos se triplicaron en solo cinco años: entre 2015 y 2019 se atendieron más de 10 mil casos, y en 2024 ya se habían reportado más de mil denuncias adicionales. Los delitos más comunes son el fraude informático y los ataques al patrimonio digital, que representan más del 60% del total. Lima Metropolitana —especialmente Lima, Lima Este y Lima Norte— concentra la mayor cantidad de casos.

### ***2.1.2. Ciberdelitos desde la Normativa Peruana***

Para que una acción sea considerada un **ciberdelito en el Perú**, no basta con que simplemente cause daño digital; debe estar claramente definida y sancionada en la ley penal. En los últimos años, la legislación peruana ha dado pasos importantes en este campo. Un ejemplo clave es la **Ley N.º 30096**, conocida como la *Ley de delitos informáticos*, que fue promulgada en 2013. Esta norma fue reforzada un año después con la **Ley N.º 30171**, y más adelante, en 2019, con la **Ley N.º 30999**, también llamada *Ley de Ciberdefensa*. Todas estas

leyes tienen un mismo objetivo: prevenir y castigar los delitos cometidos a través del uso de tecnologías de la información y la comunicación, protegiendo tanto los sistemas y datos informáticos como otros derechos fundamentales.

Además, Perú no está solo en esta lucha. Desde 2019, forma parte del **Convenio de Budapest** o *Convenio sobre la Ciberdelincuencia*, un acuerdo internacional que promueve la cooperación entre países para combatir este tipo de delitos. Tanto la legislación nacional como este convenio internacional permiten clasificar los delitos informáticos en diferentes categorías, lo cual ayuda a identificarlos mejor y a enfrentarlos de manera más efectiva.

#### **2.1.2.1. Delitos contra la Confidencialidad, Integridad y Disponibilidad de Datos y Sistemas Informáticos**

En el Perú, la ley contempla diversas formas de ciberdelito y establece sanciones específicas para cada una. Uno de ellos es el **acceso ilícito**, que ocurre cuando una persona entra, sin autorización, a un sistema informático, ya sea en parte o por completo, vulnerando las medidas de seguridad que están allí justamente para evitar eso. No importa si causó daño o no; el simple hecho de ingresar sin permiso ya es un delito y puede ser castigado con una pena de prisión de entre uno y cuatro años, además de una multa económica.

Otro delito es el **atentado contra la integridad de datos**, que se refiere a acciones como borrar, dañar, modificar o hacer inaccesible información digital de forma intencional y sin autorización. La ley no exige que haya un perjuicio concreto para castigar esta conducta. La sanción va de tres a seis años de prisión, más una multa.

También está el **atentado contra la integridad de sistemas informáticos**, que sucede cuando alguien impide que un sistema funcione correctamente, ya sea bloqueándolo, entorpeciendo su uso o paralizando total o parcialmente sus servicios. Este delito puede acarrear penas de prisión similares al anterior, de tres a seis años, además de multa.

Por otro lado, la **interceptación de datos informáticos** se refiere a espiar o captar información digital durante su transmisión, sin que la persona afectada lo sepa, por ejemplo, mensajes privados o archivos en tránsito. Si bien esto ya es grave y se sanciona con tres a seis años de prisión, las penas se vuelven más severas si la información es confidencial o si pone en riesgo temas sensibles como la defensa o la seguridad del país. En esos casos, las penas pueden llegar hasta los diez años.

Finalmente, existe el delito de **abuso de mecanismos y dispositivos informáticos**, que sanciona a quienes crean, venden o incluso simplemente tienen herramientas diseñadas para cometer ciberdelitos. Hablamos de programas maliciosos, contraseñas robadas, códigos de acceso, entre otros. Aunque no se haya cometido aún un ataque, la sola preparación ya es penalizada, con penas de uno a cuatro años de prisión y multa.

#### **2.1.2.2. Delitos Informáticos contra la Indemnidad y Libertad Sexuales**

Uno de los delitos más sensibles que contempla nuestra legislación es el relacionado con las **proposiciones sexuales a niños, niñas y adolescentes a través de medios tecnológicos**. Este delito se comete cuando una persona usa internet, redes sociales, chats u otras plataformas digitales para contactar con un menor de catorce años, con la intención de pedirle material de contenido sexual o proponerle algún tipo de actividad de esa índole. La ley

es clara y firme: esta conducta es sancionada con una pena de prisión que va de cuatro a ocho años, además de la inhabilitación del agresor.

Pero la protección no termina ahí. Si la víctima tiene entre catorce y menos de dieciocho años, y la persona que la contacta utiliza algún tipo de engaño para lograr su propósito, también se considera delito. En este caso, la pena va de tres a seis años de prisión, además de inhabilitación. Lo importante es entender que no se necesita que haya un encuentro físico ni que el contenido sea difundido para que se configure el delito; basta con la intención y el contacto con fines sexuales para que la ley actúe. Este tipo penal busca proteger, por encima de todo, la dignidad, la libertad y la integridad sexual de los menores, reconociendo los riesgos reales que existen en el mundo digital y actuando a tiempo para prevenir daños más graves.

### **2.1.2.3. Delitos Informáticos contra la Intimidad y el Secreto de las Comunicaciones**

Uno de los delitos más delicados en el entorno digital es el **tráfico ilegal de datos**. Este ocurre cuando alguien crea, accede o usa sin autorización una base de datos que contiene información personal o sensible de una persona —sea natural o jurídica—, con el objetivo de venderla, intercambiarla o simplemente aprovecharla para obtener algún beneficio. Esta información puede incluir desde datos familiares y patrimoniales, hasta aspectos laborales o financieros. No importa si causa un daño directo o no; el simple hecho de manipular esa información con fines de lucro es ilegal y puede ser castigado con una pena de entre tres y cinco años de cárcel.

Otro tema importante es la **interferencia telefónica**, que también ha sido incorporado y reforzado dentro del Código Penal. Esta figura sanciona a quienes escuchan o graban conversaciones privadas sin autorización. Si bien ya es grave por sí sola, las penas se vuelven aún más severas cuando la persona que comete el delito es un funcionario público, o cuando la información interceptada es confidencial o pone en riesgo aspectos tan importantes como la defensa o la seguridad nacional. En todos estos casos, la ley busca proteger un derecho fundamental: el de la privacidad, que hoy, más que nunca, se ve amenazado en el mundo digital.

#### **2.1.2.4. Delitos Informáticos contra el Patrimonio**

Uno de los delitos informáticos más comunes y peligrosos en la actualidad es el **fraude informático**. Este delito ocurre cuando alguien usa herramientas tecnológicas —como sistemas, redes o programas— para alterar o manipular datos con el fin de obtener un beneficio personal a costa de otra persona. Puede tratarse, por ejemplo, de clonar información, borrar o cambiar datos, o interferir en el funcionamiento de un sistema informático para engañar y sacar provecho de manera ilegal. En estos casos, la ley peruana establece penas de cárcel que van desde los tres hasta los ocho años, además de una multa económica. La sanción es aún más severa si el daño afecta recursos públicos que están destinados a programas sociales o asistenciales.

A diferencia de la estafa tradicional, en la que se engaña directamente a una persona, el fraude informático se enfoca en manipular sistemas y dispositivos para lograr el mismo objetivo: robar. Como explica Gercke (2014), citado por el Consejo Nacional de Política Criminal, este delito no solo implica engaño, sino también un perjuicio real hacia un tercero, ya sea una persona, una empresa o una institución.

Un ejemplo muy concreto y frecuente de esta práctica es el **carding**. Se trata de una modalidad de estafa en la que los delincuentes obtienen de forma ilegal los datos de una tarjeta bancaria —como el número, el código CVV o la fecha de vencimiento— y los usan para hacer pequeñas compras en línea. Lo hacen así a propósito, para que pasen desapercibidas por los sistemas de seguridad o incluso por el mismo titular de la tarjeta, al menos en un primer momento. Este tipo de fraude, aunque parezca menor, puede escalar rápidamente y dejar a las víctimas con importantes pérdidas económicas.

#### **2.1.2.5. Delitos Informáticos contra la Fe Pública**

La **suplantación de identidad** es un delito que ocurre cuando alguien, usando tecnologías como internet, redes sociales o plataformas digitales, se hace pasar por otra persona —ya sea una persona natural o una empresa— con la intención de causar daño. Ese daño puede ser material, como perder dinero o bienes, o moral, como afectar la reputación, la confianza o la tranquilidad de la víctima. La ley peruana toma muy en serio este tipo de acciones y establece penas de cárcel que van de tres a cinco años si efectivamente se genera un perjuicio.

Lo importante aquí es entender que este delito no solo castiga el acto de suplantar, sino que se enfoca en el **resultado**: el daño causado. Por eso, si alguien intenta suplantar a otra persona pero no logra afectar directamente a la víctima, el hecho no se considera consumado, sino solo como una tentativa. Aun así, sigue siendo grave, porque poner en riesgo la identidad de alguien —ya sea para obtener un beneficio o simplemente para hacer daño— vulnera derechos fundamentales y puede dejar huellas emocionales o económicas difíciles de reparar.

### 2.1.2.6. Agravantes Comunes a los Delitos Informáticos

La **Ley N.º 30096**, que regula los delitos informáticos en el Perú, contempla situaciones especiales en las que la sanción puede ser más severa. Es decir, hay ciertos casos en los que la pena de cárcel no solo se aplica, sino que puede **aumentarse hasta en un tercio** por encima del máximo establecido. Esto ocurre cuando se presentan circunstancias que agravan el delito.

Por ejemplo, cuando **la persona que comete el delito forma parte de una organización criminal**, la ley considera que hay un riesgo mayor, y por eso la sanción también es mayor. Otro caso es cuando **se abusa de un cargo o función** que da acceso a información reservada o datos sensibles. En otras palabras, si alguien usa su posición de confianza para cometer un delito informático, la responsabilidad es más grave.

También se aplica un agravante si **el delito se comete con la intención de obtener un beneficio económico**, salvo que esa intención ya esté considerada en otro tipo penal. Y, finalmente, la ley es especialmente estricta cuando **el ataque compromete servicios esenciales**, como los destinados a la asistencia social, la defensa del país, la seguridad o la soberanía nacional.

Estas agravantes buscan que quienes representen una amenaza mayor para la sociedad reciban una sanción proporcional a la gravedad de sus actos. Porque en el entorno digital, como en cualquier otro, el daño puede ser profundo y, en algunos casos, poner en riesgo a muchos.

### ***2.1.3. Ciberseguridad y Ciberdefensa: Un Marco Integral***

Cuando hablamos de **ciberseguridad** y **ciberdefensa**, es fácil confundirlos, ya que están muy relacionados. Sin embargo, cada uno tiene un enfoque distinto y cumple un rol específico dentro del mundo digital.

Por un lado, la **ciberseguridad** se enfoca en proteger la información y los sistemas tecnológicos que usamos a diario. Es como un escudo que combina herramientas, políticas, buenas prácticas, capacitación y tecnología para evitar que nuestros datos personales o institucionales caigan en manos equivocadas o sufran algún tipo de daño (UIT, 2010, citado en Consejo Nacional de Política Criminal, 2020). El objetivo principal de la ciberseguridad es cuidar tres aspectos clave: la **confidencialidad**, la **integridad** y la **disponibilidad** de la información, lo que comúnmente se conoce como el **modelo CID**.

Por otro lado, la **ciberdefensa** tiene un enfoque más estratégico y está vinculada directamente con la seguridad nacional. Es responsabilidad del Estado y, en particular, de sus instituciones de defensa. La **Ley N.º 30999**, que regula este tema en el Perú, la define como la **capacidad militar para responder a amenazas o ataques que ocurren en el ciberespacio y que ponen en riesgo la seguridad del país**. Aquí ya no hablamos solo de proteger datos personales o de empresas, sino de resguardar sistemas críticos como los que controlan el agua, la energía, el transporte o las comunicaciones nacionales.

En este escenario, no podemos esperar a que existan más leyes o estándares para empezar a actuar. **La protección de la información y los sistemas digitales es una responsabilidad compartida**, tanto del sector público como del privado. La prevención, la

preparación y la respuesta ante amenazas deben ser una prioridad hoy, no mañana. Porque en el mundo digital, los ataques pueden ser invisibles, pero sus consecuencias son muy reales.

### **2.1.3.1. Marco de Ciberseguridad en el Estado Peruano**

#### **2.1.3.1.1. Confianza digital y ciberdefensa en el Perú: un compromiso en marcha**

En un mundo cada vez más conectado, **construir confianza en los servicios digitales** es fundamental. Justamente, eso es lo que busca el **Marco de Confianza Digital del Estado Peruano**: que las personas se sientan seguras al interactuar con plataformas digitales, tanto públicas como privadas. Para avanzar en ese camino, desde el año 2020, el **Decreto de Urgencia N.º 007-2020** estableció una medida clave: ahora las entidades del Estado y los proveedores de servicios esenciales —como los del sector financiero, salud, educación, transporte, internet y otros servicios básicos— **están obligados a reportar cualquier incidente de seguridad digital al Centro Nacional de Seguridad Digital**.

Además, si un incidente involucra **datos personales**, también deben colaborar con la **Autoridad Nacional de Protección de Datos Personales**. Aunque aún no se han fijado sanciones concretas en caso de incumplimiento, se ha dado un primer paso importante con la creación del **Registro Nacional de Incidentes de Seguridad Digital**, donde se recopila y gestiona toda esta información a nivel nacional.

El **Centro Nacional de Seguridad Digital** cumple un rol clave en esta tarea. Es el encargado de monitorear y gestionar los incidentes de seguridad digital en todo el país. Su

trabajo incluye **emitir alertas**, proteger la infraestructura crítica y ayudar a que las entidades puedan **responder, recuperarse y aprender de los ataques digitales**. Para eso, cada entidad debe implementar medidas de seguridad que no solo sean técnicas, sino también físicas, organizativas y legales. La idea es garantizar que la información esté siempre protegida: que no se filtre, que no se pierda y que no sea alterada.

Cuando se trata de **datos personales**, la ley va un paso más allá. Exige que las entidades adopten **medidas sólidas de protección**, y establece sanciones altas si no se cumplen. Esto incluye desde capacitaciones periódicas al personal, hasta evaluaciones de riesgos, planes de respuesta frente a incidentes y protocolos de colaboración con terceros que manejan datos sensibles.

#### **2.1.3.1.2. Ciberdefensa: cuando el ciberespacio también es territorio nacional**

Ahora bien, cuando hablamos de proteger al país desde lo digital, entramos en el terreno de la **ciberdefensa**. Esta función está a cargo del **Ministerio de Defensa** y se rige por la **Ley N.º 30999**, que define el marco legal para las operaciones militares en el ciberespacio. Su finalidad es clara: **proteger la soberanía, los intereses del país y los activos críticos nacionales frente a posibles amenazas o ataques digitales** que puedan poner en riesgo la seguridad nacional.

Los encargados de ejecutar estas operaciones son las **Fuerzas Armadas** —el Ejército, la Marina de Guerra y la Fuerza Aérea— bajo la dirección del **Comando Conjunto de las Fuerzas Armadas**. Ellos son los responsables de planificar, coordinar y actuar en el

ciberspacio cuando el país enfrenta una amenaza grave. Para hacerlo, se rigen por las leyes peruanas, la **Constitución**, los tratados internacionales, y por principios como la **legalidad**, la **necesidad** y la **proporcionalidad**, tal como lo establece el artículo 51 de la **Carta de las Naciones Unidas**.

En situaciones donde un ciberataque sobrepasa la capacidad de defensa de las entidades responsables —como los operadores del sector afectado o la Dirección Nacional de Inteligencia—, el **Comando Conjunto de las Fuerzas Armadas** asume la defensa de los activos más sensibles. Estos pueden ser, por ejemplo, redes de energía, sistemas de agua, telecomunicaciones o bases de datos esenciales para el país.

Todo este sistema se articula a través de la **Presidencia del Consejo de Ministros (PCM)**, que mediante la **Secretaría de Gobierno Digital (SeGDi)**, establece los protocolos necesarios para que la respuesta sea rápida, coordinada y efectiva. Esta Secretaría, creada en 2017, no solo dirige el aspecto técnico y normativo de la transformación digital, sino que también impulsa **políticas que hacen posible un país más seguro y moderno en el plano digital**.

#### ***2.1.4. Actores y Vulnerabilidades en la Ciberdelincuencia***

La **ciberdelincuencia** no es solo un delito más que ocurre en internet; es parte de una realidad compleja en la que se cruzan muchas historias. Detrás de cada ataque hay personas afectadas y, muchas veces, delincuentes que operan desde cualquier parte del mundo. Se trata de un entorno cambiante y lleno de desafíos, donde las amenazas a la seguridad pueden

aparecer sin previo aviso y afectar tanto a individuos como a organizaciones. Es un escenario en constante movimiento, donde protegerse se vuelve cada vez más necesario.

#### 2.1.4.1. Víctimas de la Ciberdelincuencia

Aunque no siempre se cuenta con información detallada sobre quiénes son las víctimas de los delitos informáticos, hay ciertos patrones que nos permiten identificar grupos especialmente vulnerables. Por ejemplo, **las personas entre 30 y 44 años** suelen ser las más afectadas por **fraudes bancarios en línea**, con una tasa del 5.8%. Esto puede deberse a que son quienes más realizan transacciones digitales y, por lo tanto, están más expuestas a este tipo de delitos.

También hay otros grupos que enfrentan riesgos muy serios. **Niños, niñas, adolescentes** y personas con poco conocimiento sobre cómo manejar y proteger su información en internet se encuentran en situación de **alto riesgo**. Casos de **suplantación de identidad**, o incluso delitos tan graves como la **pornografía infantil**, siguen circulando en el ciberespacio y afectan profundamente a estos sectores más indefensos.

Pero no solo las personas sufren estos ataques. **Las empresas también son un blanco frecuente**. Según un informe de PWC (2018), **más de la mitad de las empresas peruanas (55%)** ha sido víctima de delitos contra su patrimonio o fraude, y **el ciberdelito es una vía importante** en muchos de estos casos (16%). Las pérdidas económicas no son menores: pueden ir desde **25 mil hasta un millón de dólares**. Entre las técnicas más comunes que usan los atacantes están el **malware (29%)**, el **phishing (24%)** y el **escaneo de redes (7%)**.

Estos datos nos recuerdan que la seguridad digital no es un lujo ni un tema técnico alejado de la vida real. Es una necesidad urgente que debe ser atendida con responsabilidad, educación y acción conjunta.

#### **2.1.4.2. Perpetradores de la Ciberdelincuencia**

El mundo de la ciberdelincuencia es tan diverso como complejo. Si bien no existe un solo perfil de atacante, muchos casos están relacionados con personas que tienen conocimientos avanzados en tecnología. Hablamos, por ejemplo, de **profesionales en ingeniería de sistemas, electrónica, o técnicos en computación** que, en lugar de usar sus habilidades para construir, las emplean para vulnerar sistemas y cometer delitos en el entorno digital.

Lo más preocupante es que, según una encuesta recogida por PWC (2018), **el 75% de los empresarios peruanos creía que los ataques cibernéticos provenían desde dentro de sus propias organizaciones**. Es decir, personas con acceso autorizado que aprovecharon esa confianza para dañar. En cuanto a los atacantes externos, un **50% estaba vinculado con redes de crimen organizado** y un **30% con hackers profesionales**, lo que muestra que, muchas veces, detrás de estos ataques hay estructuras bien organizadas.

En medio de este panorama, el **Ministerio del Interior** lanzó la campaña “**Sé CiberConsciente**”, para informar sobre las técnicas más comunes que usan los ciberdelincuentes. Entre ellas están:

**Phishing:** quizás la más conocida. Consiste en enviar correos o mensajes falsos que imitan a personas o instituciones confiables. El objetivo es que la víctima ingrese sus datos personales o bancarios en páginas fraudulentas.

**Vishing:** parecido al phishing, pero a través de llamadas telefónicas. Se usan números falsos o programas que cambian la voz para obtener información confidencial directamente de la víctima.

**Sim swapping:** aquí, los delincuentes logran duplicar el chip del celular de la víctima. Así, pueden acceder a sus mensajes, códigos de verificación y hasta **ingresar a cuentas bancarias o billeteras digitales.**

**Fake apps o aplicaciones falsas:** simulan ser entidades financieras que ofrecen préstamos fáciles. Piden a la víctima instalar una aplicación (APK), pero en realidad es un programa malicioso que toma el control del celular y puede **robar dinero o incluso contactar a sus conocidos para pedirles transferencias.**

**Ransomware:** este tipo de ataque encripta todos los archivos de un sistema y luego exige un **pago en criptomonedas** a cambio de desbloquearlos. Es como si secuestraran tu información digital y pidieran rescate por ella.

Cada una de estas estrategias busca lo mismo: aprovechar la confianza, la distracción o el desconocimiento de las personas. Por eso, estar informados es nuestra primera línea de defensa. Porque en internet, un clic puede marcar la diferencia entre estar protegidos o convertidos en una nueva víctima.

### ***2.1.5. Respuesta Institucional del Estado Peruano y Gaps Existentes***

El Estado peruano ha venido haciendo esfuerzos para hacerle frente a la **ciberdelincuencia**, y eso es algo que hay que reconocer. Sin embargo, todavía hay **varios retos por superar**. Aún se sienten brechas importantes, sobre todo cuando se trata de **coordinar acciones entre instituciones**, de contar con **personal capacitado** o de disponer de los **recursos logísticos necesarios** para responder de manera rápida y efectiva. Es decir, hay avances, sí, pero todavía queda camino por recorrer para lograr una protección digital realmente sólida y articulada.

#### **2.1.5.1. Instituciones y Servicios de Respuesta**

En el Perú, distintas instituciones públicas están asumiendo un rol activo para enfrentar los crecientes desafíos de la **ciberdelincuencia**, aunque todavía hay mucho por mejorar para lograr una respuesta articulada y eficaz.

La **Policía Nacional del Perú (PNP)**, por ejemplo, cuenta desde el año 2005 con una unidad especializada: la **División de Investigación de Delitos de Alta Tecnología (DIVINDAT)**. Esta área se dedica exclusivamente a investigar delitos informáticos y realiza análisis forense de computadoras, celulares y otros dispositivos. Sin embargo, **solo hay dos oficinas en todo el país** —una en Lima y otra en Arequipa—, lo que limita bastante su capacidad de acción, especialmente fuera de estas regiones. En 2019, DIVINDAT tenía aproximadamente **150 efectivos en Lima y 23 en Arequipa**, pero solo **70 estaban debidamente capacitados** en ciberdelitos. Sin duda, ese número es bajo para la magnitud del problema.

Por el lado del **Ministerio Público**, si bien aún no existen fiscalías especializadas en ciberdelincuencia en todo el país, **en 2020 se dio un paso importante** al crear una **Fiscalía Especializada en Ciberdelincuencia** mediante una comisión especial. Además, la **Unidad de Cooperación Judicial Internacional y de Extradiciones** viene gestionando solicitudes de colaboración con otros países, especialmente desde que el Perú ratificó el **Convenio de Budapest**, que promueve justamente este tipo de cooperación internacional.

En cuanto al **Poder Judicial**, aún no existen **juzgados penales especializados** en delitos informáticos. Por ahora, estos casos se ven en los juzgados penales comunes o mixtos, lo que puede dificultar una respuesta ágil o especializada.

Desde la **Presidencia del Consejo de Ministros (PCM)** también se vienen impulsando acciones importantes. La **Secretaría de Gobierno Digital (SeGDí)**, por ejemplo, lidera los procesos de innovación tecnológica en el Estado y coordina la transformación digital a nivel nacional. Además, trabaja con el **Ministerio de Educación** para incorporar temas de **ciberseguridad y ciberdefensa** en los currículos educativos, lo cual es clave para formar a futuras generaciones más preparadas frente a los riesgos digitales.

Otra unidad clave de la PCM es el **PECERT**, el equipo responsable de coordinar la prevención, atención y respuesta ante incidentes de ciberseguridad en el sector público. Este grupo también desarrolla estrategias para mejorar la seguridad de la información en las entidades del Estado.

Finalmente, la **Superintendencia de Banca, Seguros y AFP (SBS)** también cumple un rol muy importante. A través de la **Resolución SBS N.º 504-2021**, exige a las entidades

bajo su regulación que **reporten los incidentes de seguridad** de la información tanto al **Comité de Riesgos** como a otras entidades del gobierno. Además, ha establecido un sistema de **multas** para los concesionarios de telecomunicaciones que no cumplan con facilitar información clave como la geolocalización o la intervención de comunicaciones, cuando sea requerida legalmente.

#### **2.1.5.2. Desafíos y Brechas Identificadas**

##### **2.1.5.2.1. Brechas que el Estado aún debe cerrar frente a la ciberdelincuencia**

Aunque el Estado peruano ha venido tomando acciones importantes para enfrentar la ciberdelincuencia, las fuentes revelan que aún **existen brechas serias** que deben atenderse si queremos construir una verdadera respuesta eficaz y oportuna.

**Falta de articulación entre instituciones:** Uno de los problemas más visibles es la **falta de coordinación** entre la Policía Nacional, las fiscalías y el Poder Judicial. Cada uno maneja su información por separado, lo que complica mucho el trabajo en equipo y ralentiza la prevención, investigación y sanción de los delitos informáticos. Es urgente que estas entidades puedan **compartir información de forma más fluida**, sin duplicar esfuerzos, y que sus sistemas estén preparados para **interoperar** entre sí. Además, sus propios reglamentos deberían considerar con más claridad cómo proteger datos y sistemas, y cómo actuar ante los distintos tipos de delitos digitales.

**Dificultades para acceder a información clave en las investigaciones:** Las empresas que proveen servicios digitales no siempre cuentan con mecanismos eficientes para mantener actualizados los datos de titularidad de las direcciones IP. Además, cuando las autoridades solicitan esa información, muchas veces hay **demoras importantes**. También, acceder a registros protegidos —como las comunicaciones o los datos bancarios— implica una orden judicial, lo que, aunque comprensible por temas legales, **retrasa los procesos**. Por eso, se necesita una normativa que permita a las autoridades competentes **acceder a esta información con mayor agilidad**, sin comprometer los derechos de los ciudadanos.

**Débil formación especializada en ciberdelitos:** Otro aspecto preocupante es la **falta de personal capacitado**. Tanto en las fiscalías como en los juzgados, aún hay vacíos de conocimiento sobre cómo se cometen los delitos informáticos y cómo deben abordarse legalmente. Las escuelas de formación de la Policía no cuentan con laboratorios ni recursos suficientes, y el número de agentes especializados en la DIVINDAT es **muy limitado** para la cantidad de casos que se presentan. Tampoco hay un grupo consolidado de **peritos informáticos** en el Ministerio Público a nivel nacional, ni suficientes fiscales formados en el impacto de las TIC en el crimen y en la cooperación internacional. Es fundamental **invertir en capacitación especializada**, incluso con estudios en el extranjero, para estar realmente preparados.

**Limitaciones logísticas y de infraestructura:** Más allá del personal, muchas entidades no cuentan con las **herramientas adecuadas para investigar**. Se necesita software actualizado, equipos forenses, laboratorios bien implementados y espacios de trabajo adecuados. También es clave contar con **manuales estandarizados** que guíen la cooperación internacional. Pero nada de esto será posible si no se asigna **un presupuesto suficiente** para

fortalecer la infraestructura y extenderla a más regiones del país, especialmente a las fiscalías provinciales.

**Falta de cultura preventiva y conciencia ciudadana:** Finalmente, uno de los aspectos más descuidados es la **prevención**. Muchas personas no saben cómo se cometen los delitos digitales, ni qué señales deben identificar para no caer en ellos. Y aunque no denunciar sigue siendo algo común, esto solo alimenta el problema. Es urgente trabajar en una estrategia de comunicación masiva, generar alianzas entre el Estado y el sector privado, y **formar ciudadanos más conscientes y preparados**. Porque la ciberseguridad no es solo tarea del Estado: es un compromiso compartido.

#### ***2.1.6. Cooperación Internacional***

El Perú no está solo en la lucha contra la **ciberdelincuencia**. Forma parte de **acuerdos internacionales clave** que han ayudado a mejorar nuestra legislación y fortalecer la cooperación con otros países. Gracias a ello, se han dado pasos importantes para enfrentar de manera conjunta los delitos que ocurren en el entorno digital, donde las fronteras físicas ya no son una barrera.

Uno de los acuerdos más importantes es el **Convenio de Budapest**, que el Perú ratificó en el año 2019. Este tratado permite que **jueces y fiscales puedan solicitar asistencia internacional** cuando se trata de investigar delitos informáticos. Lo valioso de este convenio es que conecta al Perú con países como **Estados Unidos, Italia, España, Japón, Canadá, Argentina, Chile y Colombia**, entre muchos otros, facilitando una **cooperación penal rápida y efectiva**. Además, contempla la existencia de una **Red 24/7**, que permite solicitar de manera

urgente la **preservación de datos digitales** o la **obtención de pruebas electrónicas** necesarias para una investigación.

Además, desde 2014, el Perú también forma parte del **Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Cibercriminalidad**, lo que refuerza aún más sus lazos de colaboración en este ámbito con otros países de la región.

Sin embargo, a pesar de contar con estos marcos internacionales, todavía existen **brechas en nuestras normas y capacidades operativas**. A las autoridades les sigue costando acceder a la información de manera oportuna, lo que dificulta el avance de las investigaciones y, muchas veces, permite que los responsables queden impunes. Por eso, es urgente seguir **mejorando nuestras leyes** y fomentar el **intercambio de información con los países miembros del Convenio de Budapest**. Esto permitiría cerrar los vacíos legales que hoy son aprovechados por los ciberdelincuentes, especialmente cuando actúan desde fuera del país o en zonas grises de la legislación internacional.

En resumen, si bien hemos avanzado, aún hay mucho por hacer. Cooperar con otros países no es solo una estrategia legal, sino una necesidad real frente a un delito que no entiende de fronteras.

### ***2.1.7. Conclusiones y Necesidades Futuras***

La **cibercriminalidad** se ha convertido en un problema cada vez más visible y preocupante en el Perú. Su impacto no es solo digital; afecta directamente el **patrimonio, la**

**seguridad y la tranquilidad de las personas.** Y aunque se han dado pasos importantes, como el desarrollo de leyes y la creación de instituciones especializadas como la **DIVINDAT** o las iniciativas del **Ministerio Público**, aún enfrentamos **retos muy grandes**.

Uno de los principales desafíos está en **cómo se coordinan las instituciones entre sí**, pero también en la falta de **personal especializado** y de los **recursos técnicos necesarios** para actuar con rapidez y precisión. La verdad es que la **cibercriminalidad avanza muy rápido**, y muchas veces el Estado **no logra adaptarse con la misma velocidad**. A esto se suma que, como sociedad, todavía **nos falta una cultura de prevención** frente a los riesgos digitales. Todo esto deja claro que **es urgente pasar de las intenciones a la acción** y aplicar medidas concretas.

Según la información disponible, hay algunas **prioridades clave** que el Estado peruano —en alianza con el sector privado— debería atender sin demora:

Primero, **unificar y estandarizar la información sobre delitos informáticos** en todo el país. Esto ayudaría mucho a las investigaciones y al seguimiento de los casos.

Segundo, es momento de impulsar la **aprobación de una Ley de Ciberseguridad moderna y funcional**, que integre a todos los actores del Estado y potencie la colaboración con el sector privado.

También es fundamental **fortalecer las capacidades humanas y logísticas** de quienes están en la primera línea de investigación, sanción y prevención. Esto incluye **crear más**

**unidades especializadas, capacitar continuamente al personal y dotarlos de tecnología actualizada.**

No podemos dejar de lado la **educación y la sensibilización ciudadana**. Lanzar campañas informativas y educativas sobre cómo prevenir los ciberdelitos es vital para que las personas estén más alerta y protegidas.

Finalmente, es indispensable **mejorar los mecanismos de cooperación internacional**. Muchos de estos delitos cruzan fronteras, y para enfrentarlos necesitamos trabajar de la mano con otros países.

Avanzar hacia una **ciberseguridad sólida y confiable en el Perú** es un desafío que no se resuelve de un día para otro. Pero con compromiso, inversión y una visión conjunta entre Estado, empresas y ciudadanía, podemos construir **un entorno digital más seguro, responsable y resiliente para todas y todos**.

## **CAPÍTULO III. Desarrollo de Actividades Programadas**

La elaboración de este trabajo de suficiencia profesional fue un camino trazado con cuidado, paso a paso. Desde el inicio, todo estuvo enfocado en alcanzar un propósito muy claro: **analizar a fondo el estado de la ciberseguridad en el Perú**, con una mirada crítica pero también constructiva.

Cada actividad, cada revisión y cada reflexión formaron parte de un proceso cuidadosamente planificado, pensado no solo para entender la situación actual, sino también para **proponer ideas concretas que puedan mejorarla**. Este no fue solo un ejercicio académico, sino una oportunidad para aportar desde el derecho a un tema que nos toca a todos en nuestra vida diaria: cómo protegernos en un entorno digital que crece y cambia constantemente.

### **3.1. Revisión Exhaustiva del Marco Legal Nacional en Ciberseguridad y Ciberdelincuencia**

La primera gran tarea de este trabajo fue **revisar a fondo las leyes que rigen la ciberseguridad y la lucha contra los delitos informáticos en el Perú**. Esta etapa fue clave, porque permitió construir una base sólida de conocimiento que ayudara a entender cómo está regulado hoy este tema tan importante, y hasta qué punto esas normas están respondiendo o no a los desafíos del entorno digital.

Durante esta revisión, se analizaron diversas normas que tienen impacto directo en la materia. Algunas de las más relevantes fueron:

Entre las normas más importantes que se revisaron está la **Ley N.º 30999**, conocida como la *Ley de Ciberdefensa*. Esta ley, junto con su reglamento, es uno de los principales marcos legales que tenemos en el país sobre el tema. Sin embargo, al analizarla con detenimiento, quedó claro que **su aplicación en la práctica ha sido bastante limitada**. Aunque la intención es buena, **aún no logra cubrir todos los aspectos necesarios para enfrentar los desafíos actuales** del entorno digital.

También se analizó la **Ley N.º 30096**, la *Ley de Delitos Informáticos*, que fue promulgada en 2013 y posteriormente reforzada por la **Ley N.º 30171** en 2014. Estas normas fueron pensadas para **prevenir y sancionar los delitos cometidos a través de herramientas tecnológicas**, como el acceso indebido a sistemas o el robo de datos. Buscan proteger tanto la información como los derechos fundamentales de las personas, algo cada vez más necesario en un mundo tan conectado.

Por último, se revisó el **Decreto de Urgencia N.º 007-2020**, una norma que marcó un paso importante porque estableció la **obligación de reportar incidentes de seguridad digital**. Esta medida aplica tanto para las entidades del Estado como para los proveedores de servicios esenciales, quienes deben informar cualquier incidente al **Centro Nacional de Seguridad Digital**. Si bien esta norma representa un avance, todavía hay mucho por hacer para garantizar su cumplimiento efectivo y que estas alertas se conviertan en una herramienta real de prevención y respuesta.

Después de esta primera revisión, fue posible identificar con bastante claridad **una serie de vacíos y desafíos** que presenta el marco legal actual en materia de ciberseguridad. Lo que se observó es que, si bien existen normas importantes, **estas no terminan de responder de forma**

**efectiva a la complejidad ni a la dimensión real de los riesgos digitales** que enfrentamos hoy.

En otras palabras, las amenazas avanzan más rápido que las leyes. Y eso deja al país en una situación de vulnerabilidad. Entre los puntos más preocupantes que salieron a la luz, destacan los siguientes:

**Falta de un enfoque integral:** Aunque la Ley N.º 30999 y su reglamento son avances importantes, lo cierto es que **no logran conectar de manera efectiva todas las etapas necesarias frente a un ciberataque**. Hoy más que nunca se necesita una estrategia que integre prevención, respuesta inmediata y recuperación, y eso todavía no está bien definido en la ley.

**Vacíos legales y normas que aún faltan:** Hay temas urgentes que simplemente no están regulados. Por ejemplo, **no existen normas claras para proteger las infraestructuras digitales críticas del país**, como los sistemas de energía, salud o telecomunicaciones. Además, **no se ha definido qué papel deberían asumir las empresas privadas** en la defensa cibernética nacional. Y a pesar de que el uso de software malicioso (como los conocidos malware) es una amenaza común, **no hay una ley que regule específicamente su control o sanción**.

**Obligaciones poco claras y sin consecuencias definidas:** Uno de los grandes problemas es que **no se exige de forma contundente el reporte de incidentes cibernéticos**, ni hay sanciones reales para quienes incumplen medidas básicas de seguridad digital. Si bien el Decreto de Urgencia N.º 007-2020 obliga a reportar incidentes, lo cierto es que **todavía no existen sanciones claras** si esa obligación no se cumple.

**Falta de coordinación y alineamiento internacional:** El sistema actual **todavía se percibe como débil**, en parte porque las instituciones no trabajan de forma coordinada y, además, **el Perú aún no se ha alineado plenamente con los estándares internacionales en la materia**. Esto nos deja un paso atrás en un mundo donde la cooperación global en ciberseguridad es cada vez más importante.

**Dificultades para poner en práctica lo que está en el papel:** Aunque las leyes existen, **su aplicación real sigue siendo limitada**. Las instituciones que lideran este tema —como la PCM, el Ministerio del Interior y el Ministerio de Defensa— **trabajan de forma aislada**, sin una estructura común que unifique esfuerzos y permita una respuesta integrada frente a amenazas digitales. En la práctica, eso significa que **las respuestas pueden ser lentas, fragmentadas o poco efectivas**.

Este primer diagnóstico fue clave para tener una visión clara del problema legal que enfrentamos. Gracias a él, se pudo definir con precisión por qué **urge reforzar la legislación en ciberseguridad en el Perú**. Y es que hoy, lo digital atraviesa prácticamente todo lo que hacemos: cómo nos comunicamos, trabajamos, compramos o incluso cómo nos relacionamos con el Estado. En ese contexto, **la ciberseguridad no es solo un tema técnico, sino una necesidad real para proteger nuestra información, el funcionamiento de nuestras instituciones y nuestros derechos en el entorno virtual**.

### 3.2. Análisis comparado con legislaciones extranjeras

Después de revisar la normativa peruana, el siguiente paso fue mirar hacia afuera. ¿Qué están haciendo otros países? ¿Qué podríamos aprender de sus experiencias? Así surgió la segunda etapa: un análisis comparativo con **otros marcos legales más avanzados**, pero en contextos parecidos al nuestro.

Se eligieron tres países como referencia:

**España**

**Chile**

**México**

Todos ellos han dado pasos importantes en el desarrollo de políticas públicas de ciberseguridad. Y aunque sus realidades son distintas en algunos aspectos, comparten ciertos desafíos con el Perú, lo que los convierte en **buenos modelos para observar, aprender y adaptar soluciones** que funcionen en nuestro propio entorno.

Al comparar estos modelos internacionales, fue posible identificar **buenas prácticas y enfoques concretos que realmente funcionan**. Muchas de estas ideas podrían adaptarse al contexto peruano y servir de base para construir **una legislación más sólida, actual y efectiva** en materia de ciberseguridad.

Entre los aprendizajes más valiosos que surgieron de este análisis comparado, destacan los siguientes puntos clave:

**Centros Nacionales de Ciberseguridad:** Una de las prácticas más destacables en países como España, Chile y México es que cuentan con **centros nacionales dedicados exclusivamente a coordinar todo lo relacionado con la ciberseguridad**. Estos centros funcionan como el corazón del sistema de defensa digital, articulando acciones, gestionando incidentes y promoviendo la prevención. En el caso del Perú, **aún no tenemos un ente rector que cumpla plenamente ese rol**, lo que dificulta tener una respuesta rápida y coordinada frente a las amenazas. La ausencia de una autoridad clara, con poder de decisión y acción, termina generando vacíos y respuestas fragmentadas.

**Leyes claras para proteger infraestructuras críticas:** Otro punto importante es que estos países han desarrollado **marcos legales específicos para identificar y proteger sus infraestructuras digitales más sensibles**, como redes eléctricas, sistemas de salud, transporte o comunicaciones. En cambio, en el Perú, **no contamos todavía con una normativa que defina qué se considera infraestructura crítica ni cómo debe protegerse**, lo que nos deja expuestos frente a posibles ataques en sectores fundamentales para el país.

**Sistemas de reporte obligatorio con respaldo legal real:** También se observó que en estos países **existen mecanismos formales para reportar incidentes de seguridad digital**, y lo más importante: **están respaldados por leyes que incluyen sanciones claras si no se cumplen**. Si bien en el Perú ya existe el Decreto de Urgencia N.º 007-2020, que establece la obligación de reportar incidentes al Centro Nacional de Seguridad Digital, **aún falta que se definan las consecuencias concretas en caso de incumplimiento**. Sin un marco sancionador, la norma pierde fuerza y no se garantiza que todas las entidades la tomen con la seriedad que merece.

Este análisis comparativo dejó algo muy claro: **sí es posible construir leyes modernas y eficaces** que realmente funcionen frente a los retos del mundo digital. Los ejemplos de otros países nos muestran caminos viables, soluciones concretas y enfoques que podríamos adaptar a nuestra realidad.

Esto refuerza la idea de que **las propuestas de reforma legal para el Perú no solo son necesarias, sino perfectamente alcanzables**. Mirar lo que han hecho otras naciones no significa copiar, sino aprender y adelantarnos a los riesgos. Tener esta mirada externa nos permite **ir un paso adelante**, en lugar de esperar a que los problemas se agraven para recién actuar.

### **3.3. Estudio de la Respuesta Institucional Peruana Frente a los Delitos Informáticos**

La tercera actividad planteada en este trabajo se enfocó en **analizar de forma crítica cómo está respondiendo el Estado peruano ante los delitos informáticos**. Para tener una mirada completa y realista, se revisaron informes oficiales de distintas entidades públicas que tienen un rol clave en esta tarea.

Este análisis permitió conocer **qué capacidades tienen actualmente estas instituciones**, pero también visibilizar sus limitaciones, aquellas que dificultan una respuesta rápida y efectiva frente a las amenazas digitales. Entre las entidades evaluadas se encuentran:

Ministerio del Interior.

Ministerio Público.

Poder Judicial.

Policía Nacional del Perú (PNP).

Presidencia del Consejo de Ministros (PCM).

Al revisar toda esta información, quedó en evidencia que **el Estado peruano todavía enfrenta serias limitaciones operativas** que dificultan dar una respuesta efectiva y a tiempo frente a los delitos informáticos. Aunque hay esfuerzos importantes, **aún existen brechas que es necesario cerrar con urgencia** si queremos estar realmente preparados para enfrentar las amenazas del ciberespacio.

Lo preocupante es que esas brechas se traducen, en la práctica, en respuestas que muchas veces resultan **débiles, poco coordinadas o simplemente insuficientes**. A continuación, te comparto los principales puntos que reflejan esta realidad:

**Falta de coordinación entre instituciones:** Uno de los problemas más evidentes es que **las entidades responsables no están trabajando de forma articulada**. La Policía Nacional, el Ministerio Público y el Poder Judicial tienen funciones que, en vez de complementarse, muchas veces se superponen o no se conectan bien. Cada uno maneja su información por separado, lo que complica el trabajo en equipo, **ralentiza las investigaciones** y crea vacíos en la respuesta a los incidentes. Hoy por hoy, **no existe una estructura clara ni un ente que lidere y unifique los esfuerzos frente a los delitos informáticos**.

**Falta de personal capacitado y especializado:** Este es otro punto crítico. Aunque hay profesionales comprometidos, **la cantidad de personas realmente preparadas para enfrentar delitos cibernéticos aún es muy baja**.

Por ejemplo, la DIVINDAT de la Policía Nacional —que se creó en 2005 para investigar este tipo de delitos— solo tiene oficinas en Lima y Arequipa. Y de todo su personal, apenas unos 70 agentes contaban con capacitación especializada en 2019.

En el Ministerio Público, si bien en 2020 se creó una Fiscalía Especializada en Cibercriminalidad, **todavía no hay suficientes fiscales ni peritos informáticos a nivel nacional.**

El Poder Judicial, por su parte, **no cuenta con juzgados especializados en delitos digitales**, lo que limita una atención oportuna y eficaz.

Incluso las escuelas de formación policial **no disponen de laboratorios ni herramientas necesarias** para entrenar adecuadamente a su personal en este tipo de investigaciones.

**Falta de herramientas tecnológicas y logística adecuada:** Muchas de las instituciones que enfrentan estos delitos **no tienen acceso a software actualizado, ni a equipos forenses ni laboratorios bien implementados.** Esto afecta directamente la calidad de las investigaciones. Además, **no hay manuales estandarizados para cooperar con organismos internacionales**, y el presupuesto destinado a fortalecer estas capacidades suele ser insuficiente o no se prioriza como debería.

**Dificultades para obtener información clave:** Uno de los grandes obstáculos en las investigaciones es el **acceso lento o limitado a datos sensibles**, como la titularidad de una dirección IP. Las empresas proveedoras de servicios digitales no siempre entregan la

información con la rapidez necesaria, y en muchos casos se requiere una orden judicial para acceder a registros protegidos como comunicaciones o datos bancarios. Este proceso, aunque legalmente justificado, **puede tomar tiempo valioso que los ciberdelincuentes aprovechan.**

**Falta de cultura preventiva y poca conciencia ciudadana:** Tal vez uno de los aspectos más olvidados es la prevención. **Muchas personas aún no saben cómo protegerse en el entorno digital ni qué hacer si son víctimas de un delito informático.** Esto no solo aumenta el riesgo, sino que también contribuye a la baja tasa de denuncias, lo que a su vez **hace que el problema crezca en silencio.** Es necesario promover una cultura digital más responsable y ofrecer herramientas sencillas para que todos puedan navegar con mayor seguridad.

A pesar de todos estos desafíos, también es justo **reconocer que hay esfuerzos valiosos en marcha.** Por ejemplo, el **Centro Nacional de Seguridad Digital**, liderado por la **Secretaría de Gobierno Digital (SeGDí)** de la PCM, cumple un rol fundamental al encargarse de monitorear y gestionar los incidentes de seguridad digital que ocurren en el país.

Otro actor importante es la **Superintendencia de Banca, Seguros y AFP (SBS)**, que ha dado pasos firmes al exigir que las entidades bajo su supervisión reporten cualquier incidente de ciberseguridad. Además, ha establecido sanciones claras cuando no se entrega información clave, lo que ayuda a **reforzar la responsabilidad de las instituciones** frente a estos temas.

### 3.4. Elaboración de Propuestas Normativas

La última etapa de este trabajo de suficiencia profesional estuvo dedicada a **plantear propuestas concretas que ayuden a mejorar nuestro sistema legal en materia de ciberseguridad**. Después de todo el análisis realizado, quedó claro que el Perú necesita dar pasos firmes para fortalecer tanto su marco normativo como la forma en que gestiona la seguridad digital a nivel institucional.

Estas propuestas nacen directamente de lo que se identificó a lo largo del estudio: **vacíos legales, debilidades operativas y una respuesta todavía limitada frente a las amenazas del ciberespacio**. La intención no es solo llenar esos vacíos, sino **construir un sistema legal más sólido, moderno y preparado para lo que viene**.

En esencia, lo que se busca es que el Estado tenga herramientas reales y bien definidas para **responder con mayor eficacia a los riesgos digitales**, y al mismo tiempo, garantizar que los derechos de las personas —como la privacidad, la seguridad de su información o el acceso confiable a servicios digitales— **estén bien protegidos en este nuevo entorno virtual**.

Las principales propuestas normativas incluyen:

**Reformar la Ley N.º 30999:** Una de las primeras propuestas es actualizar esta ley clave para que sea mucho más clara y funcional. Se sugiere incorporar definiciones específicas sobre qué debe hacer cada institución, cómo deben actuar ante un incidente, qué presupuesto se necesita y cómo se deben reportar los ciberataques. La idea es **darle mayor fuerza y claridad al**

**sistema legal**, para que no quede solo en el papel, sino que pueda aplicarse de manera real y efectiva.

**Crear un ente rector especializado en ciberseguridad:** Hoy en día, uno de los principales problemas es que no hay una entidad que realmente lidere y articule todo el ecosistema digital. Por eso, se plantea la creación de **una institución con autonomía técnica y operativa**, que no solo coordine a las demás, sino que **lidere con visión y estrategia todo lo relacionado con la seguridad digital del país**. Esto permitiría superar la actual fragmentación institucional.

**Implementar un Sistema Nacional de Ciberseguridad funcional:** No basta con tener normas; también se necesita un sistema que funcione. Por eso, se propone poner en marcha **un sistema operativo real, con un centro de operaciones (SOC), protocolos de acción rápida, una plataforma para compartir información entre entidades y equipos humanos bien capacitados**. Todo esto permitiría detectar y responder a incidentes digitales de forma ágil y coordinada.

**Aprobar una ley para proteger infraestructuras críticas digitales:** Existen sectores —como la salud, la energía, el transporte o las comunicaciones— que son especialmente sensibles ante cualquier ataque cibernético. Por eso, se propone **una ley que identifique claramente cuáles son esas infraestructuras clave, que establezca estándares mínimos de seguridad y que determine obligaciones concretas para quienes las gestionan**, tanto desde el sector público como el privado.

**Ratificar el Convenio de Budapest sobre ciberdelincuencia:** Aunque el Perú ya ha dado algunos pasos en este sentido, **aún no ha ratificado oficialmente el Convenio de Budapest**,

que es el principal tratado internacional en esta materia. Esta ratificación permitiría **fortalecer la cooperación con otros países**, agilizar la asistencia técnica y mejorar la capacidad del Estado para perseguir delitos informáticos que muchas veces cruzan fronteras. No ratificarlo, en cambio, **nos deja aislados frente a redes criminales que sí operan globalmente**.

**Fortalecer las capacidades humanas y logísticas:** Para que todo lo anterior funcione, se necesita personal capacitado y recursos adecuados. Por eso, se propone **crear más unidades especializadas, ofrecer formación continua a nivel nacional (e incluso internacional), y dotar a las instituciones de tecnología de punta**, desde software especializado hasta laboratorios forenses digitales bien equipados.

**Fomentar la educación y sensibilización ciudadana:** Finalmente, y no menos importante, está el componente social. La ciudadanía debe ser parte activa en la prevención. Por eso, se plantea **desarrollar campañas informativas y educativas a gran escala**, que ayuden a las personas a reconocer riesgos, a protegerse y a actuar de forma responsable en el entorno digital. Porque una sociedad informada es una sociedad más segura.

En pocas palabras, todo este proceso de trabajo, desde la planificación hasta la ejecución de cada actividad, permitió **realizar un análisis completo y con propuestas reales**. Al revisar la legislación nacional, aprender de lo que están haciendo otros países y mirar de forma crítica cómo están funcionando nuestras instituciones, fue posible **detectar con claridad cuáles son los puntos débiles de nuestro sistema jurídico en ciberseguridad**.

Y lo más importante: no se quedó solo en el diagnóstico. Se propusieron **soluciones concretas y viables** para reforzar ese sistema y adaptarlo a los desafíos digitales que enfrentamos hoy. Este enfoque, que une lo local con lo global, lo técnico con lo humano, **busca preparar al**

**Estado peruano para enfrentar los riesgos tecnológicos con mayor solidez, construyendo paso a paso un entorno digital más seguro, justo e inclusivo para todos.**

## **CAPÍTULO IV. Resultados Obtenidos**

El panorama de la ciberseguridad en el Perú revela una realidad preocupante, marcada por una estructura normativa e institucional que aún no logra dar respuesta a los desafíos del mundo digital contemporáneo. A pesar de contar con un marco jurídico base, la Ley N.º 30999 y su reglamento, este resulta insuficiente para enfrentar la complejidad y magnitud de las amenazas cibernéticas actuales. La ley carece de un enfoque integral: no articula de manera efectiva las etapas clave de prevención, respuesta y recuperación ante incidentes, ni establece obligaciones específicas como el reporte obligatorio de ataques, ni sanciones proporcionales para quienes incumplan con las medidas de seguridad exigidas.

Esta fragilidad legal se ve agravada por una fragmentación institucional profunda. Las funciones de ciberseguridad están dispersas entre múltiples entidades como la Presidencia del Consejo de Ministros (PCM), el Ministerio de Defensa, el Ministerio del Interior y OSIPTEL, lo que genera vacíos funcionales, superposiciones de competencias y una ausencia total de una estructura jerárquica clara. Sin un ente rector con autoridad normativa y operativa, el Estado peruano se encuentra incapacitado para coordinar una respuesta unificada y eficaz frente a los incidentes cibernéticos, dejando al país expuesto a vulnerabilidades sistémicas.

Además, el Perú carece de un sistema nacional de ciberseguridad funcional y plenamente operativo. No existe un centro de operaciones dedicado, ni líneas de coordinación permanentes, ni un presupuesto asignado con prioridad estratégica. Esta falta de una estrategia nacional vinculante limita drásticamente la capacidad del Estado para defender sectores críticos como energía, salud, finanzas o transporte y la infraestructura digital básica del país ante ciberataques cada vez más sofisticados.

En contraste, el análisis comparado con países como España, Chile y México muestra un camino diferente: estos Estados han avanzado significativamente en la implementación de políticas públicas respaldadas por normativas específicas para proteger sus infraestructuras críticas, han creado centros nacionales de ciberseguridad y han impuesto obligaciones legales claras, como el reporte de incidentes. Estas experiencias ofrecen lineamientos valiosos que el Perú podría adoptar para diseñar una legislación más robusta y adaptada a sus necesidades.

Finalmente, el Perú enfrenta una limitación adicional en el ámbito internacional: aún no ha ratificado el Convenio de Budapest sobre Ciberdelincuencia. Esta omisión representa un obstáculo serio para la cooperación judicial internacional, restringiendo la capacidad del país para integrarse a redes globales de colaboración, intercambio de información y asistencia técnica en la lucha contra la ciberdelincuencia transnacional. Sin esta herramienta, el Perú queda rezagado en la arena global de la seguridad digital, perdiendo oportunidades clave para fortalecer su defensa cibernética desde una perspectiva colectiva y multilateral.

## CONCLUSIONES

- El marco jurídico de la ciberseguridad en el Perú, representado principalmente por la Ley N.º 30999 y su reglamento, resulta insuficiente para enfrentar los desafíos del entorno digital actual, debido a su carácter general y a la falta de disposiciones específicas que garanticen una protección integral de los sistemas críticos nacionales.
- La debilidad institucional y la falta de coordinación efectiva entre los distintos organismos estatales encargados de la ciberseguridad dificultan una respuesta unificada y eficiente ante amenazas cibernéticas, lo que expone al país a riesgos significativos en materia de defensa digital y protección de datos.
- La ausencia de un sistema nacional de ciberseguridad plenamente funcional, con infraestructura operativa, liderazgo institucional y financiamiento adecuado, limita seriamente la capacidad del Estado peruano para prevenir, detectar y mitigar incidentes de seguridad en el ciberespacio.
- El análisis de las normativas en España, Chile y México muestra que incorporar reportes obligatorios, protección de infraestructuras críticas y centros nacionales de ciberseguridad permite crear leyes modernas y efectivas, modelo útil para la reforma legal en el Perú.
- La falta de adhesión del Perú a instrumentos internacionales como el Convenio de Budapest debilita su posición en el escenario global de la ciberseguridad, limitando la cooperación judicial y técnica internacional, elemento crucial para hacer frente a delitos cibernéticos de carácter transnacional.

## RECOMENDACIONES

- Reformar la Ley N.º 30999, incorporando disposiciones claras sobre funciones específicas, protocolos de actuación ante incidentes, asignación presupuestaria y mecanismos obligatorios de reporte de ciberataques, con el fin de robustecer el sistema normativo y hacerlo más eficaz frente a las amenazas digitales.
- Establecer un ente rector especializado en ciberseguridad, con autonomía técnica y capacidad operativa, que centralice la gobernanza del ecosistema digital, articule la acción entre instituciones y ejerza liderazgo estratégico en la implementación de políticas de seguridad cibernética.
- Implementar un Sistema Nacional de Ciberseguridad, con un centro de operaciones de seguridad (SOC), protocolos de respuesta rápida, una plataforma de información compartida y recursos humanos capacitados, que permita monitorear y responder a incidentes de forma oportuna y coordinada.
- Elaborar una ley sobre la protección de infraestructuras críticas digitales, que identifique los sectores prioritarios, defina estándares mínimos de seguridad, y establezca obligaciones específicas para operadores públicos y privados en la gestión de riesgos cibernéticos.
- Ratificar el Convenio de Budapest sobre Ciberdelincuencia, con el objetivo de fortalecer la cooperación internacional, acceder a mecanismos de asistencia técnica y judicial transfronteriza, y armonizar la legislación penal nacional con los estándares internacionales en la lucha contra los delitos informáticos.

## REFERENCIAS BIBLIOGRÁFICAS

Centro de Noticias del Congreso. (2025, 31 de marzo). De interés nacional la creación del Comité de alto nivel de ciberseguridad del Estado peruano. Comunicaciones - Congreso.

Consejo Nacional de Política Criminal. (2020, diciembre). Diagnóstico situacional multisectorial sobre la ciberdelincuencia en el Perú. Ministerio de Justicia y Derechos Humanos, Observatorio Nacional de Política Criminal.

García, V. (2019). ¿Cómo está avanzando la ciberseguridad en el Perú? Breve aproximación al marco normativo. *Actualidad Jurídica Uría Menéndez*, 52, 176–179.

Ley N° 30096, Ley de Delitos Informáticos. (2013, 22 de octubre). *El Peruano*.

Ley N° 30999, Ley de Ciberdefensa. (2019, 26 de agosto). *El Peruano*.

Ministerio del Interior. (2025, 4 de marzo). ¡Sé CiberConsciente! Mininter presenta campaña para combatir y prevenir la ciberdelincuencia. *Noticias*.

Ministerio Público Fiscalía de la Nación. (2020, 15 de septiembre). “Convenio sobre la Ciberdelincuencia” permite a jueces y fiscales realizar requerimientos de cooperación internacional. *Gobierno del Perú*.

Presidencia del Consejo de Ministros. (2024, 12 de diciembre). Perú en el Índice Global de Ciberseguridad 2024: retos y oportunidades. Informes y publicaciones.

Revoredo, A. (2024, 22 de julio). Responsabilidades y obligaciones relacionadas con ciberseguridad en la legislación peruana. Revoredo.pe.  
<https://revoredo.pe/responsabilidades-y-obligaciones-relacionadas-con-ciberseguridad-en-la-legislacion-peruana/>

## **ANEXOS**

## Anexo 1. Evidencia de similitud digital



# Paredes Martinez, H & Flores Castañuedi, J

## “Marco jurídico de la ciberseguridad en el Perú: diagnóstico y propuestas de fortalecimiento normativo”

Titulos

REVISION 2025

Universidad Peruana de Ciencias e Informatica

### Detalles del documento

Identificador de la entrega

trn:oid::1:3340309844

Fecha de entrega

15 sep 2025, 11:39 a.m. GMT-5

Fecha de descarga

15 sep 2025, 11:53 a.m. GMT-5

Nombre del archivo

Trabajo\_Suficiencia\_Profesional\_2\_Derecho.docx

Tamaño del archivo

3.6 MB

52 páginas

11.775 palabras

64.633 caracteres






## 4% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

### Filtrado desde el informe

- ▶ Bibliografía
- ▶ Texto citado

### Fuentes principales

- 4%  Fuentes de Internet
- 1%  Publicaciones
- 2%  Trabajos entregados (trabajos del estudiante)

### Marcas de integridad

#### N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

## Fuentes principales

- 4% Fuentes de Internet
- 1% Publicaciones
- 2% Trabajos entregados (trabajos del estudiante)

## Fuentes principales

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1	Internet	
	hdl.handle.net	<1%
2	Internet	
	www.scribd.com	<1%
3	Trabajos del estudiante	
	Universidad Privada Antenor Orrego 2025	<1%
4	Internet	
	risti.xyz	<1%
5	Internet	
	repositorio.unan.edu.ni	<1%
6	Internet	
	www.gob.pe	<1%
7	Internet	
	repositorio.upcl.edu.pe	<1%
8	Internet	
	repositorio.ulasamericas.edu.pe	<1%
9	Internet	
	www.urla.com	<1%
10	Internet	
	app.ldlpol.com	<1%
11	Trabajos del estudiante	
	Universidad Internacional de la Rioja	<1%

**12** Trabajos del estudiante

Universidad Peruana de Ciencias e Informática

<1%

## Anexo 2. Autorización de publicación en repositorio



### FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

#### 1.- DATOS DEL AUTOR

Apellidos y Nombres: FLORES CASTAÑUEDI JUDITH  
DNI: 10380368 Correo electrónico: yuyipress13573@gmail.com  
Domicilio: CONDOMINIO GENA MZ. A LT. 6, COMAS  
Teléfono fijo: 936859649 Teléfono celular: 936859649

#### 2.- IDENTIFICACIÓN DEL TRABAJO DE SUFICIENCIA PROFESIONAL O TESIS

Facultad / Carrera: DERECHO Y CIENCIAS POLÍTICAS / DERECHO

Tipo: Trabajo de Suficiencia Profesional (X) Tesis ( )

Título del Trabajo de Suficiencia Profesional / Tesis:

"MARCO JURÍDICO DE LA CIBERSEGURIDAD EN EL PERÚ: DIAGNÓSTICO Y PROPUESTAS DE FORTALECIMIENTO NORMATIVO"

#### 3.- OBTENER:

Título Profesional

#### 4. AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

Por la presente declaro que el documento indicado en el ítem 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencias e Informática para publicar la versión electrónica en su Repositorio Institucional (<http://repositorio.upci.edu.pe>), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art23 y Art.33.

Autorizo la publicación de mi tesis (marque con una X):

Sí, autorizo el depósito y publicación total.

No, autorizo el depósito ni su publicación.

Como constancia firmo el presente documento en la ciudad de Lima, a los

15 días del mes de AGOSTO de 202 5.

FIRMA



HUELLA

## FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

### 1.- DATOS DEL AUTOR

Apellidos y Nombres: PAREDES MARTINEZ HUGO MITCHELL

DNI: 09585730 Correo electrónico: hmitchellpm@gmail.com

Domicilio: CALLE EL VELERO 150, DPTO. 502, URB. INGENIEROS LA CASTELLANA, SANTIAGO DE SURCO

Teléfono fijo: 942721163 Teléfono celular: 942721163

### 2.- IDENTIFICACIÓN DEL TRABAJO DE SUFICIENCIA PROFESIONAL O TESIS

Facultad / Carrera: DERECHO Y CIENCIAS POLÍTICAS / DERECHO

Tipo: Trabajo de Suficiencia Profesional (X) Tesis ( )

Título del Trabajo de Suficiencia Profesional / Tesis:

"MARCO JURÍDICO DE LA CIBERSEGURIDAD EN EL PERÚ: DIAGNÓSTICO Y  
PROPUESTAS DE FORTALECIMIENTO NORMATIVO"

### 3.- OBTENER:

Título Profesional

### 4. AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

Por la presente declaro que el documento indicado en el ítem 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencias e Informática para publicar la versión electrónica en su Repositorio Institucional (<http://repositorio.upci.edu.pe>), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art23 y Art.33.

Autorizo la publicación de mi tesis (marque con una X):

Sí, autorizo el depósito y publicación total.

No, autorizo el depósito ni su publicación.

Como constancia firmo el presente documento en la ciudad de Lima, a los

15 días del mes de AGOSTO de 2025.

  
FIRMA



HUELLA