Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

El ransomware como amenaza digital: Un estudio comparado con la legislación peruana

Ransomware as a digital threat: A comparative study with peruvian legislation

- Recibido: 2025/09/05 - Aprobado: 2025/10/08 - Publicado: 2025/10/23

Orlando Santiago De la Vega Tonato
Universidad Tecnológica Indoamérica, Ambato, Ecuador
odelavega@indoamerica.edu.ec
https://orcid.org/0009-0007-7033-0442

Juan Pablo Santamaria Velasco
Universidad Tecnológica Indoamérica, Ambato, Ecuador
juansantamaria@uti.edu.ec
https://orcid.org/0000-0002-8775-4600

Resumen

El presente artículo tiene como objetivo analizar los vacíos normativos que limitan la protección penal frente al delito de ransomware en Ecuador, a través de una comparación con la legislación penal peruana, con el fin de evaluar cuál de los dos marcos normativos ofrece una mejor respuesta jurídica ante esta amenaza digital. La problemática surge ante el aumento de ataques informáticos mediante software malicioso que encripta información y restringe el acceso a sistemas, afectando gravemente la seguridad de datos tanto públicos como privados. En Ecuador, el artículo 232 del Código Orgánico Integral Penal (COIP) tipifica el ataque a la integridad de sistemas informáticos, mientras que, en Perú, el artículo 4 de la Ley N.º 30096 contempla una figura similar bajo el delito de atentado a la integridad de sistemas informáticos. La metodología utilizada fue de tipo cualitativa, con enfoque descriptivo y analítico, sustentada en el análisis dogmático del tipo penal

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

y la revisión de fuentes doctrinarias, normativas y jurisprudenciales. Los principales hallazgos revelan que la legislación ecuatoriana presenta una mayor amplitud en la descripción típica, permitiendo sancionar tanto la ejecución como las fases preparatorias del ransomware, lo que otorga una ventaja frente a la ley peruana. Sin embargo, Perú fortalece su sistema mediante la adhesión al Convenio de Budapest. Se concluye que el COIP brinda una mejor protección penal sustantiva, aunque Ecuador requiere avanzar en cooperación internacional y armonización normativa. Se recomienda tipificar el ransomware como delito autónomo y ratificar el Convenio de Budapest para una protección integral.

Palabras clave: seguridad digital, legislación comparada, delitos informáticos, Derecho penal, ransomware

Abstract

This article aims to analyze the legal gaps that limit criminal protection against ransomware attacks in Ecuador by comparing Ecuadorian law with Peruvian criminal legislation, to assess which legal framework offers a better response to this digital threat. This issue arises due to the increasing number of cyberattacks using malicious software that encrypts data and restricts access to systems, severely compromising the security of both public and private data. In Ecuador, Article 232 of the Comprehensive Organic Penal Code (COIP) criminalizes attacks on the integrity of computer systems, while in Peru, Article 4 of Law No. 30096 addresses a similar offense, namely, the crime of compromising the integrity of computer systems. The methodology used was qualitative, with a descriptive and analytical approach, based on a doctrinal analysis of the relevant legal provisions and a review of scholarly literature, legal regulations, and case law. The main findings reveal that Ecuadorian legislation offers a broader definition of the offense, allowing for the prosecution of both the execution and preparatory stages of ransomware attacks, thus providing an advantage over Peruvian law. However, Peru strengthens its legal framework by adhering to the Budapest Convention. The conclusion is that the Ecuadorian Comprehensive Organic Penal Code (COIP).provides better substantive criminal protection, although Ecuador needs to improve its international cooperation and regulatory harmonization. It is recommended that Ecuador

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

criminalize ransomware as a standalone offense and ratify the Budapest Convention for comprehensive protection.

Keywords: digital security, comparative legislation, computer crimes, criminal law, ransomware

Introducción

Entre las amenazas digitales más frecuentes y peligrosas que han emergido con el avance de las tecnologías de la información se encuentra el ransomware, una modalidad de ciberataque que consiste en la encriptación maliciosa de archivos o sistemas informáticos con el propósito de exigir un rescate económico generalmente en criptomonedas para devolver el acceso a la información comprometida. (Ávila, 2023). Este tipo de ataque se ha convertido en una herramienta recurrente dentro del ecosistema delictivo digital, empleando técnicas como la ingeniería social y el phishing, aprovechando vulnerabilidades del sistema o la falta de conciencia en ciberseguridad por parte de los usuarios.

En el marco jurídico ecuatoriano, el ransomware no se configura como un delito autónomo, sino que constituye un modus operandi comprendido dentro del tipo penal previsto en el artículo Código Orgánico Integral Penal (COIP, 2014), que sanciona:

> El ataque a la integridad de sistemas informáticos. Esta norma castiga con pena privativa de libertad de tres a cinco años a quien destruya, dañe, borre, deteriore, altere, suspenda, trabe o cause mal funcionamiento o comportamiento no deseado en sistemas de tratamiento de información. (art. 232)

También sanciona a quien desarrolle, distribuya o utilice programas informáticos maliciosos destinados a causar tales efectos. Si estos ataques afectan infraestructura crítica o servicios públicos, la pena se agrava hasta siete años.

A nivel regional, Perú ha adoptado medidas en la lucha contra la ciberdelincuencia mediante la promulgación de la Ley N.º 30096 sobre delitos informáticos, que sanciona conductas como la alteración, interferencia o inutilización de sistemas informáticos. No obstante, en comparación con el ordenamiento jurídico ecuatoriano, dicha normativa presenta un tratamiento más general y

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

menos desarrollado respecto a los presupuestos de tipicidad aplicables a ataques informáticos complejos, como el ransomware. Entonces, el COIP, particularmente a través del artículo 232, ofrece una descripción normativa más precisa y detallada de las conductas que afectan la integridad lógica de los sistemas, lo que lo convierte en un instrumento más eficaz para enfrentar estas amenazas.

En este contexto, el presente artículo académico tiene como finalidad analizar el fenómeno del ransomware como modus operandi dentro del delito de ataque a la integridad de sistemas informáticos en el ordenamiento jurídico ecuatoriano, contrastándolo con la legislación peruana en materia de delitos informáticos. La investigación se orienta a examinar críticamente la capacidad de respuesta del marco legal ecuatoriano frente a este tipo de conductas, considerando la creciente sofisticación de las amenazas digitales. Asimismo, se cuestiona la suficiencia de las disposiciones actuales para enfrentar ataques que afectan principalmente a personas jurídicas, como empresas, bancos e instituciones públicas, generando consecuencias económicas, reputacionales y operativas de gran magnitud.

Este análisis, sustentado en el derecho comparado, pretende aportar a la discusión sobre el fortalecimiento de los mecanismos normativos y judiciales necesarios para combatir eficazmente los delitos informáticos, en especial aquellos que adoptan formas complejas como el ransomware.

Desarrollo

2.1. El ransomware como amenaza digital

El ransomware es un tipo de programa malicioso que bloquea el acceso a los archivos o al sistema de una computadora y exige un pago, generalmente en criptomonedas, para recuperarlos. Su objetivo principal es extorsionar a la víctima a cambio de devolverle el control sobre su información. (Ávila, 2021). El término ransomware proviene del idioma inglés y está formado por las palabras ransom, que significa rescate o secuestro, y ware, una abreviación de software, que se traduce como programa. En español, este concepto también puede interpretarse como programa

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

de secuestro, secuestrador informático o incluso programa de chantaje o chantajista. (Estrada, 2018).

Según Moreno et al. (2020), "el ransomware es un tipo de malware que impide el acceso a la información, cifrando los archivos con algoritmos criptográficos simétricos o asimétricos, solicitando una suma de dinero para recuperar la información cifrada" (p. 40). Esta definición permite comprender cómo el ransomware no solo representa un desafío desde el punto de vista tecnológico, sino también desde el jurídico, ya que su sofisticación convierte a estos ataques en verdaderos instrumentos de coacción digital. Lo relevante no es únicamente la capacidad del software malicioso para cifrar datos, sino el trasfondo extorsivo que plantea nuevas formas de criminalidad digital. Este tipo de amenazas transforma la estructura clásica del delito patrimonial, adaptándola a entornos virtuales donde el control sobre la información es el bien jurídico vulnerado.

Por su parte, Trigo et al. (2017) definen el malware como un conjunto de programas diseñados para dañar o infiltrarse en un sistema informático sin el consentimiento del usuario. Aunque durante mucho tiempo se utilizó el término "virus informático" como sinónimo, el malware abarca una variedad más amplia de amenazas que pueden ser hostiles, intrusivas o molestas. En este contexto, el ransomware se entiende como una forma específica de software malicioso que secuestra un sistema o sus datos, exigiendo un rescate económico para restablecer el acceso.

La historia del ransomware se remonta a finales de los años 80, cuando apareció el primer caso conocido: el troyano AIDS. Este malware fue distribuido a través de disquetes durante una conferencia sobre el SIDA y cifraba únicamente los nombres de los archivos, exigiendo un pago a una cuenta en Panamá para su desbloqueo (Moreno et al., 2020). Aunque en ese entonces se utilizaban algoritmos de cifrado simétricos, su vulnerabilidad los hacía poco eficaces para los ciberdelincuentes, hasta que en 2005 en Rusia comenzaron a emplear algoritmos asimétricos más complejos, marcando un punto de inflexión en la evolución del ransomware.

Estrada (2018) propone que esta evolución puede dividirse en dos grandes etapas: la primera, en la que el ransomware bloqueaba el acceso al sistema operativo hasta que se pagaba un rescate vía SMS; y la segunda, caracterizada por el cifrado de archivos y la exigencia de pagos mediante

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

criptomonedas como el Bitcoin. Este cambio se dio cuando los delincuentes comenzaron a aprovechar el anonimato y la descentralización que ofrecen las criptodivisas, lo cual les permitió operar con menor riesgo de ser rastreados.

Los métodos de propagación del ransomware son variados y cada vez más sofisticados, pero todos tienen en común el aprovechamiento de las vulnerabilidades humanas y técnicas. Uno de los mecanismos más frecuentes es la ingeniería social, mediante la cual los ciberdelincuentes engañan a los usuarios para que ejecuten acciones que comprometan sus sistemas, como descargar archivos maliciosos o acceder a enlaces engañosos. El correo electrónico es una de las vías más comunes, ya que los atacantes suelen enviar mensajes que aparentan ser confiables, como facturas, notificaciones legales o promociones falsas, con archivos adjuntos o enlaces que contienen el malware (Moreno et al., 2020; Trigo et al., 2017).

Otro método es la redirección de tráfico, donde el usuario es llevado a sitios web fraudulentos frecuentemente disfrazados de páginas de juegos o software gratuito desde sitios como páginas pornográficas. Al descargar lo que parece ser un programa legítimo, se instala en segundo plano el ransomware. También existen ataques mediante botnets, redes de equipos comprometidos que descargan el malware de manera silenciosa, aprovechando programas aparentemente legítimos como cracks o keygens (Moreno et al., 2020).

Se identifican vulnerabilidades técnicas como las del sistema operativo o de la red. Por ejemplo, si un equipo no está actualizado, los atacantes pueden utilizar exploits para tomar control remoto y cifrar los archivos sin intervención del usuario. En entornos de red, ataques como el man in the middle pueden interceptar la información y manipularla para introducir el ransomware en el sistema de destino (Trigo et al., 2017). Finalmente, también se ha popularizado el modelo Ransomware as a Service (RaaS), donde incluso personas sin conocimientos técnicos pueden lanzar ataques contratando servicios de ransomware en la nube, lo que amplía significativamente el alcance de esta amenaza.

El ransomware se propaga mediante una combinación de engaños, explotación de vulnerabilidades en sistemas operativos y redes. En un entorno digital cada vez más interconectado, esta amenaza ha dejado de ser marginal para convertirse en una de las más

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

peligrosas para la información crítica de usuarios y organizaciones. Tal como señalan Trigo et al. (2017), su crecimiento ha sido semi-exponencial en los últimos años, desde el punto de vista legal, esta modalidad puede encuadrarse dentro del tipo penal de la extorsión, ya que mediante intimidación o suplantación de autoridad se obliga al usuario a entregar bienes, dinero o información que tiene efectos jurídicos. Las consecuencias más comunes de un ataque de ransomware incluyen la pérdida temporal o permanente de información, la interrupción de servicios esenciales y fuertes pérdidas económicas derivadas de la restauración del sistema comprometido.

Como lo menciona Moreno et al. (2020), "el secuestro de los datos o pérdida de información pueden causar una falla de seguridad informática, generando problemas en la integridad y disponibilidad de los datos que pueden implicar sustanciales perjuicios a cualquier organización" (p. 42). Desde una perspectiva jurídica, esta afectación puede también ser comprendida dentro del delito de daño. Según Palazzi (2000), no se requiere que el bien, en este caso, los datos o sistemas quede totalmente destruido o inutilizado para que el delito se configure; basta con que su restauración implique un gasto, esfuerzo o trabajo. Esto puede traducirse, por ejemplo, en la necesidad de recuperar información desde una copia de seguridad o reinstalar sistemas afectados, lo cual representa una pérdida significativa de recursos para la víctima.

2.2. El tratamiento del ransomware en el COIP

El ransomware, encuentra su regulación en el ordenamiento penal ecuatoriano en el artículo 232 del COIP, bajo la figura de ataque a la integridad de sistemas informáticos, y establece lo siguiente:

> La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. (art. 232).

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

Este tipo penal se configura como un delito de resultado, de acción dolosa, cuya estructura típica se centra en la afectación a la integridad lógica de sistemas informáticos y de telecomunicaciones. Desde el punto de vista dogmático, el tipo penal se caracteriza por una pluralidad de verbos rectores, entre los que destacan: destruir, dañar, borrar, deteriorar, alterar, suspender, trabar, causar mal funcionamiento, entre otros. Esta diversidad de verbos permite abarcar una gama amplia de conductas nocivas sobre el entorno digital.

Como sostiene Barbosa (citado en Rosero, 2021), el verbo rector es el núcleo del delito; es el comportamiento humano con la cual se lesiona el derecho de otra persona. En este sentido, el artículo 232 incorpora una enumeración exhaustiva de acciones típicas, lo cual permite capturar jurídicamente diversas formas de ejecución tecnológica, como aquellas empleadas por programas tipo ransomware, que al cifrar archivos y bloquear sistemas, provocan un "comportamiento no deseado", "mal funcionamiento" o incluso la "supresión" de datos informáticos.

Esta característica del tipo penal permite aplicar una interpretación conforme a su naturaleza literal, tal como dispone el artículo 13 del COIP respecto a la interpretación en materia penal, la cual debe ser estricta y ceñida al texto normativo. Así, la figura penal del artículo 232 no requiere una consecuencia material sobre el bien físico, sino sobre el componente lógico de los sistemas computacionales, es decir, su estructura de información, procesamiento y operación.

El artículo 232 no solo contempla conductas consumadas, sino también acciones de carácter preparatorio o de facilitación, al sancionar a quien: "Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo" (COIP, 2014)

Estas conductas constituyen una tipificación anticipada del injusto, en donde el legislador penal busca sancionar la creación y circulación de herramientas diseñadas para dañar sistemas. En este ámbito se inscriben los desarrolladores de ransomware, quienes elaboran software con la finalidad de cifrar información de terceros, ocasionando su inaccesibilidad.

Este enfoque legislativo reconoce una tendencia moderna en derecho penal: la intervención punitiva sobre las fases previas del delito, especialmente en materia informática, donde la

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

trazabilidad y el daño pueden ser difusos. Como explica Saltos Salgado (2021), los delitos informáticos afectan un nuevo interés social cuyo reconocimiento legislativo urge, diferenciando así entre delitos computacionales como nuevas formas comisivas de delitos y delitos informáticos, aquellos que afectan el novísimo del bien jurídico penal propuesto. Desde esta óptica, el artículo 232 cumple una función doble: sanciona la consumación del ataque y, al mismo tiempo, penaliza su estructuración técnica y logística, incluso antes de que se materialice el daño.

Este tipo penal en cuestión tiene como objeto de tutela la integridad de los sistemas de información y comunicación, lo cual incluye su estructura operativa, lógica y funcional. De acuerdo con Carrión (2020), el bien jurídico protegido a que se refiere el contenido de cada tipo penal es el elemento o aspecto que en la codificación moderna sirve para agrupar los delitos. Así, el artículo 232 se ubica dentro del título dedicado a los delitos contra la seguridad de los sistemas informáticos, protegiendo bienes como la disponibilidad, integridad y confiabilidad de datos digitales.

En el caso del ransomware, al cifrar archivos y alterar la capacidad operativa del sistema, se afecta de forma directa la disponibilidad y funcionalidad de los datos, en términos de interrupción del acceso y control de estos por parte del titular legítimo. Esta afectación encaja de manera plena con el núcleo de protección del artículo 232, cuya finalidad es preservar el orden funcional del ecosistema digital.

Es importante señalar que, este tipo penal también protege bienes inmateriales, como la confidencialidad de la información o el control legítimo sobre la infraestructura tecnológica, lo cual lo diferencia de los delitos patrimoniales clásicos. En este contexto, el derecho penal informático evoluciona hacia la tutela de nuevos bienes jurídicos digitales, producto de la transformación tecnológica y de las necesidades actuales del Estado y la sociedad.

El artículo 232 también contempla un agravante cualificado cuando el ataque recae sobre bienes informáticos destinados a la prestación de un servicio público o vinculados con la seguridad ciudadana: “Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.” (COIP, 2014)

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

Este inciso refleja una política penal diferenciada, basada en la mayor peligrosidad social del ataque cuando sus consecuencias pueden afectar el interés público o la seguridad colectiva. Así, por ejemplo, si un programa como el ransomware llega a comprometer los sistemas de una institución hospitalaria, policial, financiera o educativa estatal, se activa este rango agravado.

Esta disposición coincide con lo señalado por Alvarado (2020), quien indica que los organismos de seguridad y defensa deben actuar en respuesta a esa situación de amenaza a la seguridad interna y externa, y establecer las respectivas políticas, regulaciones y estrategias para cuidar la privacidad de las personas y la información, servicios e infraestructura sensible del Estado. En este sentido, la norma penal no solo sanciona el daño individual, sino que refuerza su función de protección institucional, orientada a garantizar la continuidad y seguridad del Estado digital.

Como sujeto activo de este delito esta "la persona", lo que significa que puede ser cometido por cualquier individuo sin requerimientos de una cualidad especial. No se trata de un delito de sujeto activo calificado. Como explica el COIP en los artículos 190 y siguientes, este tipo de redacción implica que tanto personas naturales como jurídicas pueden ser responsables en calidad de autor, coautor o cómplice, en función del grado de intervención en el hecho.

De acuerdo con esto, el sujeto pasivo del delito es quien resulta perjudicado por la afectación informática. En el caso del ransomware, este puede ser una persona natural, una entidad pública, una empresa privada o incluso organismos del Estado, conforme a la definición amplia del tipo penal.

2.3. Tratamiento del ransomware en la legislación peruana

En el marco del derecho penal peruano, el delito de atentado a la integridad de sistemas informáticos (AISI), tipificado en el artículo 4 de la Ley N.º 30096 o Ley de Delitos Informáticos establece lo siguiente:

> El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa (Ley N.º 30096, 2013, art. 4).

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

Este tipo penal se caracteriza por proteger la integridad, el acceso y la funcionalidad de los sistemas informáticos como bienes jurídicos, reconociendo su relevancia no solo patrimonial, sino también operativa dentro de entornos empresariales, públicos y personales. Aunque la norma no menciona expresamente el delito de ransomware, la redacción amplia de los verbos rectores "inutiliza", "impide el acceso", "entorpece" o "imposibilita" permite considerar que esta modalidad delictiva puede encuadrarse dentro del AISI.

De la Mata y Hernández (2009) afirman que el delito de AISI no se agota en una simple afectación patrimonial, sino que se configura como un delito pluriofensivo, ya que los daños ocasionados pueden extenderse al normal desarrollo de actividades empresariales o incluso afectar el servicio público. Estos autores sostienen que las consecuencias económicas principales y más graves no se limitan a la pérdida del valor económico de los datos afectados, sino que se expanden al perjuicio para, por ejemplo, la actividad empresarial que se esté llevando a cabo. Este análisis permite comprender que, en un caso de ransomware, los daños no se limitan al software, sino que generan afectaciones en cascada a intereses jurídicos más amplios.

Desde el punto de vista de la tipicidad objetiva, el delito de AISI es común y no exige una cualidad especial en el sujeto activo, lo que resulta adecuado frente a fenómenos como el ransomware, donde los autores pueden ser agentes individuales o colectivos, muchas veces ajenos a estructuras formales delictivas. Como señalan Carrillo Díaz y Montenegro Dávila (2018), se trata de un delito común, ya que "no requiere en el agente una calidad especial, un conocimiento o título especial [...] o la calidad de posición de garante de los sistemas informáticos involucrados" (p. 55). Esta amplitud facilita la persecución penal del delito sin necesidad de probar conocimientos técnicos especializados en el autor, lo cual es funcional frente a modalidades como el ransomware, que pueden ser perpetradas incluso mediante herramientas disponibles en la web.

El sujeto pasivo suele definirse como el propietario, posesionario o usufructuario legítimo del sistema informático objeto de la agresión. Esta caracterización, aunque válida, resulta insuficiente frente a fenómenos como el ransomware, en los que los efectos del delito pueden extenderse más allá del titular del sistema. Es entonces que, el delito de ransomware adquiere un carácter pluriofensivo, pues si bien ataca un bien mueble específico (el sistema informático), las

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

consecuencias trascienden hacia los intereses de múltiples personas naturales o jurídicas, lo que exige una interpretación amplia del sujeto pasivo en función del daño efectivo. Esta visión dinámica y contextualizada fortalece la protección penal frente a modalidades complejas del cibercrimen.

Respecto a la tipicidad subjetiva, la norma peruana exige expresamente dolo directo. Se requiere que el agente actúe "deliberada e ilegítimamente", lo que excluye toda forma de culpa. Como subrayan los mismos autores, "la exigencia de una acción deliberada resalta innecesariamente la exigencia de una conducta dolosa" (Carrillo Díaz & Montenegro Dávila, 2018, p. 56). En el caso del ransomware, este requisito se cumple sin dificultad, ya que la instalación de malware con fines extorsivos supone una acción intencional, consciente y planificada.

En cuanto a la condición objetiva de punibilidad, el delito solo se configura si el sistema informático se encuentra en funcionamiento al momento del ataque. Señalan que, si el dispositivo no presta servicios o no se encuentra operativo, el delito puede considerarse imposible o dar lugar a una tentativa inidónea. Esto podría representar una limitación para la persecución penal de ciertos casos de ransomware en los que el ataque se produce antes de que el sistema entre en funcionamiento. Sin embargo, una interpretación más amplia del riesgo creado por el ataque podría justificar su sanción como tentativa.

En materia de delitos informáticos, el principal instrumento internacional es el Convenio sobre la Ciberdelincuencia, conocido como Convenio de Budapest, aprobado por el Comité de Ministros del Consejo de Europa en su 109.ª reunión, el 8 de noviembre de 2001, y abierto a la firma el 23 de noviembre del mismo año en la ciudad de Budapest, durante la Conferencia Internacional sobre Ciberdelincuencia. Este tratado persigue tres objetivos fundamentales: armonizar las legislaciones penales nacionales en materia de delitos informáticos, establecer mecanismos eficaces de investigación, y facilitar la cooperación internacional entre los Estados parte (Comité de Ministros del Consejo de Europa, 2001). El Perú se adhirió formalmente al Convenio mediante la Resolución Legislativa N.º 30913, del 12 de febrero de 2019, ratificada posteriormente a través del Decreto Supremo N.º 010-2019-RE, del 9 de marzo del mismo año, entrando en vigor el 1 de diciembre de 2019 (Elías Puelles, 2023).

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

En este marco, el artículo 5 del Convenio adquiere especial relevancia para el tratamiento penal del ransomware, al abordar expresamente las conductas que afectan la integridad de los sistemas informáticos. Bajo el título "Ataques a la integridad del sistema", dicho artículo establece lo siguiente:

> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos (Convenio de Budapest, 2001, art. 5).

Aquí se describe con claridad las conductas típicas que constituyen un ataque a la integridad de un sistema informático, y que son plenamente compatibles con las características técnicas del ransomware, cuyo modus operandi consiste precisamente en introducir un software malicioso para inutilizar, bloquear o cifrar el acceso a sistemas o archivos. La mención explícita a acciones como la transmisión o alteración de datos permite considerar que el ransomware debe ser objeto de criminalización directa dentro del marco nacional.

La incorporación de Perú al Convenio no solo significa un alineamiento con estándares internacionales, sino también una oportunidad para evaluar la coherencia y suficiencia de la legislación interna, especialmente considerando las observaciones doctrinarias respecto a las limitaciones de la Ley N.º 30096 frente a nuevas formas de cibercriminalidad. Como advierte Elías Puelles (2023), la adhesión al Convenio de Budapest no se agota en la suscripción formal, sino que exige del Estado una acción normativa sostenida y técnica, que permita adecuar permanentemente su legislación penal y procesal frente a fenómenos como el ransomware. Por tanto, el Convenio representa tanto un instrumento de protección penal sustantiva como un marco procesal e institucional de cooperación internacional, cuya eficacia dependerá del compromiso del Estado en su aplicación normativa, judicial y operativa.

2.4. Comparación con Ecuador

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

El tratamiento jurídico del ransomware en Ecuador y Perú presenta similitudes relevantes, aunque también diferencias sustantivas en cuanto a técnica legislativa, capacidad preventiva y articulación con estándares internacionales. En primer lugar, ambos ordenamientos jurídicos no tipifican expresamente el ransomware como delito autónomo. Sin embargo, sus legislaciones permiten encuadrar esta modalidad delictiva dentro de tipos penales más amplios. En el caso ecuatoriano, el COIP lo aborda en el artículo 232, bajo la figura de ataque a la integridad de sistemas informáticos. Este artículo contiene una lista amplia de verbos rectores, como destruir, dañar, trabar, alterar, causar mal funcionamiento o generar un comportamiento no deseado, lo cual permite incluir en su ámbito de protección los efectos generados por programas tipo ransomware, que cifran archivos y bloquean el acceso legítimo a los sistemas. En Perú, el artículo 4 de la Ley N.º 30096 sobre delitos informáticos tipifica el atentado a la integridad de sistemas informáticos, sancionando a quien inutilice o impida el funcionamiento de estos sistemas. Aunque no menciona directamente al ransomware, la redacción también permite su inclusión mediante interpretación extensiva.

Una diferencia importante entre ambos países radica en el enfoque preventivo de su legislación penal. Mientras en Ecuador se penalizan no solo las conductas consumadas, sino también las acciones preparatorias vinculadas al desarrollo y distribución de programas maliciosos lo que incluye a los creadores y difusores de ransomware, en Perú la norma penal sanciona únicamente la acción de inutilizar o afectar el sistema, sin contemplar la preparación o facilitación del delito. Esta diferencia demuestra que la legislación ecuatoriana adopta un modelo de intervención anticipada frente a amenazas informáticas, con mayor capacidad de prevención y control penal frente al ciclo completo de la conducta delictiva. Esta anticipación legislativa es coherente con la tendencia moderna del derecho penal a sancionar etapas previas del delito, particularmente en el ámbito de los delitos informáticos, donde la trazabilidad del daño es difusa.

Respecto al bien jurídico protegido, ambos sistemas legales buscan garantizar la integridad, disponibilidad y funcionalidad de los sistemas informáticos. En Ecuador, además de proteger el componente lógico de los sistemas, se reconoce la afectación a bienes inmateriales como la confidencialidad de la información y el control legítimo sobre la infraestructura digital. En el caso

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

peruano, la doctrina ha señalado que el atentado a la integridad de sistemas informáticos tiene un carácter pluriofensivo, ya que los efectos del delito pueden extenderse más allá del titular del sistema y afectar intereses empresariales, institucionales o de servicio público. Esta visión permite interpretar el ransomware no solo como un delito contra la propiedad digital, sino también como una amenaza al normal desarrollo de actividades esenciales para la sociedad.

Una diferencia destacable es la inclusión de agravantes. El artículo 232 del COIP ecuatoriano establece una pena mayor (de cinco a siete años) cuando el ataque recae sobre sistemas destinados a la prestación de servicios públicos o relacionados con la seguridad ciudadana. Esta agravante cualificada fortalece la protección penal de infraestructuras críticas como hospitales, instituciones financieras, organismos de seguridad o servicios estatales. Por el contrario, la legislación peruana no prevé agravantes específicas cuando la conducta afecta este tipo de sistemas, lo que representa una limitación frente a los crecientes ataques dirigidos a entidades de alto valor estratégico. En este aspecto, Ecuador se posiciona con una política penal diferenciada, capaz de responder con mayor severidad ante delitos informáticos de alto impacto social.

En cuanto a la alineación con estándares internacionales, Perú presenta una ventaja clara frente a Ecuador. El Estado peruano se adhirió formalmente al Convenio de Budapest en 2019, lo que le permite participar en mecanismos de cooperación jurídica internacional, recibir asistencia técnica y actualizar permanentemente su legislación penal frente a nuevas formas de ciberdelincuencia. El artículo 5 de dicho tratado establece la obligación de los Estados parte de tipificar como delito la obstaculización grave e ilegítima del funcionamiento de sistemas informáticos, incluyendo conductas como la transmisión, deterioro o supresión de datos, que encajan con el modus operandi del ransomware. Esta adhesión permite a Perú incorporar principios uniformes de derecho penal sustantivo y procesal en la lucha contra el cibercrimen. En contraste, Ecuador no ha suscrito ni ratificado el Convenio de Budapest, lo que limita su capacidad de cooperación internacional y lo mantiene relativamente aislado en el ámbito global de la ciberseguridad jurídica.

Tanto Ecuador como Perú cuentan con herramientas normativas que permiten sancionar el ransomware, aunque lo hacen desde enfoques distintos. Ecuador adopta una posición legislativa más robusta en términos de prevención anticipada y protección de infraestructuras críticas,

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

mientras que Perú se alinea más firmemente con los marcos internacionales al haber ratificado el Convenio de Budapest. A pesar de estas fortalezas, ambos países comparten una deuda normativa pendiente: la tipificación expresa del ransomware como delito autónomo, lo cual permitiría una mejor sistematización de su tratamiento penal, mayor claridad para los operadores jurídicos y la adopción de políticas públicas especializadas en materia de ciberseguridad. Finalmente, una propuesta de mejora legislativa debería incluir, en ambos países, el fortalecimiento de capacidades técnicas investigativas, la articulación con agencias internacionales de cooperación y el desarrollo de una estrategia penal integral frente al cibercrimen contemporáneo.

Discusión

Diversos autores han contribuido a la comprensión jurídica del ransomware desde diferentes enfoques, lo que permite construir una visión más completa sobre esta modalidad delictiva y su tratamiento legal en los sistemas penales de Ecuador y Perú. En primer lugar, la conceptualización dogmática del delito informático propuesta por Barbosa resulta esencial para entender el núcleo del tipo penal previsto en el artículo 232 del COIP. Barbosa señala que el verbo rector es el eje del delito, pues representa el comportamiento humano que lesiona un bien jurídico. Esta afirmación cobra especial importancia en el análisis del ransomware, ya que el artículo 232 incluye una variedad de verbos rectores como dañar, trabar, alterar o causar mal funcionamiento, que permiten subsumir en su contenido las conductas propias de los ataques cibernéticos mediante este tipo de software malicioso.

Asimismo, Saltos, Robalino y Pazmiño (2021) aportan una distinción teórica relevante al separar los delitos computacionales como formas de comisión novedosas de los delitos informáticos como afectaciones a un nuevo bien jurídico penal: la integridad digital. Este planteamiento justifica la necesidad de que el derecho penal reconozca nuevas esferas de tutela ante la evolución tecnológica. A la luz de esta perspectiva, el ransomware debe ser considerado no simplemente como un medio de comisión de delitos clásicos, sino como una forma autónoma de afectación a la estructura lógica, funcional y operativa de los sistemas digitales.

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

Por otro lado, Alvarado (2020) resalta el deber del Estado de adoptar medidas estratégicas y regulatorias para proteger los sistemas e infraestructuras sensibles. Este enfoque institucional se conecta con la agravante prevista en el artículo 232 del COIP cuando el ataque informático recae sobre bienes vinculados a servicios públicos o a la seguridad ciudadana. Alvarado sostiene que estas amenazas requieren una respuesta articulada entre la política criminal y la política pública, lo cual se traduce en normas penales más severas para ataques que comprometan la estabilidad de funciones esenciales del Estado. Su aporte justifica jurídicamente la necesidad de distinguir el nivel de afectación social del ransomware dependiendo del blanco del ataque.

En el contexto peruano, autores como Carrillo Díaz y Montenegro Dávila (2018) afirman que el delito de atentado a la integridad de sistemas informáticos, previsto en la Ley N.º 30096, es un delito común que no exige una cualidad especial en el autor. Esta idea es valiosa en el tratamiento del ransomware, ya que facilita su persecución penal sin necesidad de probar conocimientos técnicos especializados en el sujeto activo. El enfoque de estos autores amplía el espectro de posibles responsables, y facilita la labor probatoria del Estado al momento de imputar responsabilidades por ataques digitales.

A su vez, De la Mata y Hernández (2009) defienden la tesis de que este tipo de delitos son pluriofensivos, es decir, que sus efectos trascienden el daño directo sobre los sistemas informáticos. Esto es especialmente relevante en los ataques de ransomware, cuyos efectos pueden paralizar operaciones empresariales, comprometer servicios públicos e incluso afectar derechos fundamentales. Este enfoque justifica que los delitos informáticos deban analizarse no solo desde la perspectiva del daño patrimonial o técnico, sino también desde sus consecuencias sociales, jurídicas y económicas más amplias.

Elías Puelles (2023) realiza un aporte fundamental al destacar la importancia de la adhesión al Convenio de Budapest no como una acción formal, sino como un compromiso sustantivo que obliga a los Estados a actualizar sus marcos legales y fortalecer su cooperación internacional en la lucha contra el cibercrimen. Por lo cual, su análisis es especialmente valioso para el caso ecuatoriano, donde la falta de adhesión al Convenio limita las capacidades institucionales para actuar frente a fenómenos como el ransomware. El autor propone una interpretación activa de los

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

compromisos internacionales, entendiendo que la efectividad del derecho penal en el ámbito digital requiere una armonización normativa y un esfuerzo sostenido de adecuación técnica.

Conclusiones

El análisis comparado del tratamiento legal del ransomware en las legislaciones penales de Ecuador y Perú permite identificar avances y deficiencias en la respuesta jurídica frente a esta modalidad delictiva. En el caso ecuatoriano, el artículo 232 del COIP ofrece una tipificación amplia y técnicamente adecuada para sancionar este tipo de ataques, al contemplar una pluralidad de verbos rectores que permiten incluir dentro de su alcance conductas como el cifrado, bloqueo o inutilización de datos que caracteriza al ransomware. Asimismo, se destaca su enfoque anticipado, al penalizar no solo la ejecución del daño sino también actos preparatorios como la creación o distribución de programas maliciosos, lo cual constituye una ventaja relevante en términos de prevención penal.

Por su parte, la legislación peruana, a través del artículo 4 de la Ley N.º 30096, si bien también permite sancionar el ransomware de forma indirecta, presenta limitaciones en su alcance preventivo, al no contemplar fases preparatorias del delito ni establecer agravantes específicas cuando los ataques afectan servicios públicos o infraestructuras críticas. No obstante, su adhesión al Convenio de Budapest fortalece la articulación de su derecho penal con los estándares internacionales, facilitando la cooperación entre Estados y el desarrollo progresivo de su marco jurídico frente a los delitos informáticos.

En función de estos elementos, se concluye que, en términos de estructura normativa y capacidad de respuesta penal inmediata, la legislación ecuatoriana brinda una mayor protección frente al ransomware, al tipificar de forma más detallada las conductas y prever mecanismos anticipados de sanción. Sin embargo, en lo que respecta a la cooperación internacional, armonización legislativa y actualización normativa frente al cibercrimen transnacional, el modelo peruano presenta una ventaja, al haber ratificado el Convenio de Budapest.

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

Aunque Ecuador dispone de un tipo penal técnicamente sólido, enfrenta aún desafíos importantes, especialmente en materia de cooperación internacional, institucionalidad investigativa y reforma legislativa integral. En consecuencia, se recomienda una futura tipificación expresa del ransomware como delito autónomo y la adhesión del Estado ecuatoriano al Convenio de Budapest, como medidas necesarias para cerrar los vacíos normativos y fortalecer la protección jurídica frente a una de las amenazas digitales más graves de la actualidad.

El COIP establece una agravante cualificada (pena de 5 a 7 años) cuando los ataques afectan sistemas vinculados a servicios públicos o seguridad ciudadana. Esta diferenciación punitiva, ausente en la legislación peruana, refleja una política criminal más sofisticada que reconoce el mayor impacto social de los ataques contra infraestructuras estratégicas del Estado.

Tanto Ecuador como Perú requieren avances normativos: la tipificación autónoma del ransomware como delito específico, el fortalecimiento de capacidades técnicas investigativas y, en el caso ecuatoriano, la adhesión urgente al Convenio de Budapest. Solo mediante una estrategia integral que combine protección penal sustantiva, cooperación internacional y desarrollo institucional, ambos países podrán enfrentar eficazmente esta amenaza digital transnacional.

Referencias

Alvarado, J. (2020). Coordinación de Investigación, Desarrollo Tecnológico e Investigación. Revista Científica Artistas, 75.
Rosero Altamirano, M. (2021). Recuperado el 23 de Septiembre de 2023, de http://dspace.unach.edu.ec/bitstream/51000/8033/1/5.-TESIS%20ABIGAIL%20ROSERO-DER.pdf

Ávila, S. F. (2021). Evolución e impacto del ransomware en América Latina desde el año 2015. [Monografía]. Repositorio Institucional UNAD. Recuperado de: https://repository.unad.edu.co/handle/10596/42667

Ávila Niño, F. Y. (2023). Ransomware, una amenaza latente en Latinoamérica. InterSedes, 24(49), 92-119

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171

Carrillo Díaz, C. F., & Montenegro Dávila, A. N. (2018). La criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos. Obtenido de: https://hdl.handle.net/20.500.12802/4514

Carrión, F. (02 de Septiembre de 2020). Crónica. Recuperado el 04 de Agosto de 2023, de Crónica: https://cronica.com.ec/2020/09/02/el-bien-juridico-protegido/

Código Orgánico Integral Penal. (2014). Registro Oficial Suplemento 180 de 10 de febrero de 2014. Quito, Ecuador.

Comité de Ministros del Consejo de Europa (2001) Informe Explicativo del Convenio sobre la Ciber-delincuencia. https://rm.coe.int/16802fa403

De la Mata, N y Hernández L. (2009). El delito de daños informáticos: una tipificación defectuosa. Estudios Penales y Criminológicos, n.° 29, Santiago de Compostela.

Elías Puelles, R. N. (2023). El delito de hacking o acceso ilícito a sistemas informáticos. THEMIS Revista De Derecho, (83), 413-433. https://doi.org/10.18800/themis.202301.023

Estrada Cola, C. (2018). Estudio sobre el malware Ransomware. Universitat Oberta de Catalunya (UOC). Recuperado de: http://hdl.handle.net/10609/89025

Huerta Morán, E. (2024). La falta de tipificación del ransomware y su incidencia en la desprotección de la persona jurídica. [Tesis de pregrado, Universidad Nacional de Chimborazo]. Repositorio UNACH.

Moreno, J., Rodríguez, C., & Leguias, I. (2020). Revisión sobre propagación de ransomware en sistemas operativos Windows. *I+ D Tecnológico*, *16*(1), 39-45.

Saltos, M., Robalino, J., & Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. Scielo

Trigo, S., Castellote, M., Podestá, A., Ruiz de Angeli, G., Lamperti, S., & Constanzo, B. (2017). Ransomware: seguridad, investigación y tareas forenses. Recuperado de: http://redi.ufasta.edu.ar:8082/jspui/handle/123456789/1595

Período Julio - Diciembre 2025
Vol. 2 No. 2, pp 19 - 39
redarevista@gmail.com
ISSN: 3028-8959 DOI: https://doi.org/10.69583/reda.v2n2.2025.171