ONTOLOGÍA DEL CIBERDELITO PARA EL DISEÑO DE POLÍTICAS PÚBLICAS EDUCATIVA DE PREVENCIÓN EN BOLIVIA

Ontological Approach to Cybercrime for the Design of Educational Public Prevention Policies in Bolivia

Mullisaca, Choque Carlos
https://orcid.org/0009-0003-6231-6158
cmullisaca2012@gmail.com
UMSA - Docente Informática
La Paz - Bolivia

Chavez Loza, Maria del Pilar
https://orcid.org/0009-0009-7987-7078
pilarchavezloza@gmail.com
UMSA - Docente Ciencias de la Educación
La Paz - Bolivia

Resumen

Este artículo investiga la ontología del ciberdelito como fundamento teórico para el diseño e implementación de políticas públicas educativas orientadas a la prevención del ciberdelito en Bolivia. La expansión del ciberespacio y el creciente uso de las Tecnologías de la Información y la Comunicación (TIC), evidencia un aumento significativo de ciberdelitos como el phishing, ransomware, robo de identidad, acoso en línea y fraude digital, los cuales trascienden fronteras y afectan la seguridad, privacidad e integridad de las personas e instituciones. A partir de un enfoque interdisciplinario —que integra filosofía, derecho, educación y ciencia política—, se analiza la esencia del ciberdelito mediante sus componentes ontológicos: el delito en sí, el medio tecnológico, la víctima y el victimario. La investigación mixta (cualitativo-cuantitativo), se basa en una revisión documental, la aplicación de encuestas a 280 estudiantes de la Universidad Mayor de San Andrés (UMSA) y el análisis segmentado del uso de las TIC mediante el método spline lineal. Los resultados revelan un alto uso

diario de internet entre la población universitaria, junto con una baja comprensión de los conceptos y riesgos asociados al ciberdelito.

Palabras clave: ciberdelito, delito, educación, era digital, ontología, políticas públicas, victimización, vulnerabilidad.

Abstract

This article investigates the ontology of cybercrime as a theoretical foundation for the design and implementation of educational public policies aimed at preventing cybercrime in Bolivia. The expansion of cyberspace and the growing use of Information and Communication Technologies (ICT) reveal a significant increase in cybercrimes such as phishing, ransomware, identity theft, online harassment, and digital fraud, which transcend borders and undermine the security, privacy, and integrity of individuals and institutions. Through an interdisciplinary approach—integrating philosophy, law, education, and political science—the essence of cybercrime is analyzed via its ontological components: the crime itself, technological medium, the victim, and the perpetrator. The mixed-methods research (qualitative-quantitative) is based on a documentary review, the application of surveys to 280 students from the Universidad Mayor de San Andrés (UMSA), and the segmented analysis of ICT use through the linear spline method. The findings reveal high daily internet usage among university students, alongside a low understanding of the concepts and risks associated with cybercrime.

Keywords: cybercrime, crime, education, digital era, ontology, public policies, victimization, vulnerability.

1. Introducción

La ubicuidad de las Tecnologías de la Información y la Comunicación (TIC), junto con la expansión del Internet como red global de interacción, ha transformado profundamente las dinámicas sociales, económicas, políticas, educativas y culturales en particular en el siglo XXI. La evolución tecnológica ha dado origen al ciberespacio, un espacio de comunicación social transnacional y en constante cambio

que ha transformado la vida cotidiana. No obstante, el crecimiento de las tecnologías digitales también ha propiciado la aparición de nuevos ciberdelitos que cruzan fronteras, afectando la seguridad, privacidad e integridad de individuos e instituciones.

La complejidad de delitos como el phishing, el malware, el ransomware, el acoso en línea, la difamación y el fraude exige un abordaje interdisciplinario, filosóficamente y pedagógicamente fundamentado, que permita comprender su naturaleza, los actores involucrados y sus implicaciones éticas y jurídicas. En este contexto, el enfoque ontológico del ciberdelito se presenta como una herramienta teórica esencial para analizar la esencia de este fenómeno digital que involucra al ser humano. Comprender el "ser" del ciberdelito implica desentrañar las estructuras y relaciones que lo constituyen como delito, víctima, medio y perpetrador con el propósito de prevenir su ocurrencia mediante acciones educativas.

La ontología, como estudio del ser y la existencia, puede aplicarse al ciberdelito para entender su naturaleza, características, actores y motivaciones. Que ello permita desarrollar políticas públicas efectivas que aborden la creciente amenaza de los ciberdelitos.

El objetivo de este estudio es analizar la relación entre el conocimiento ontológico del ciberdelito y el diseño de políticas educativas públicas, identificando los fundamentos teóricos, normativos y pedagógicos que permitan fortalecer la prevención y la formación ciudadana en el entorno digital boliviano. En la presente investigación se propone establecer una ontología del ciberdelito que sirva como la base de conocimiento para el diseño de políticas públicas, educativas y criminales efectivas en materia de prevención. En consecuencia, la pregunta que guía este estudio es:

¿De qué manera la comprensión ontológica del ciberdelito puede orientar el diseño de políticas educativas públicas orientadas a la prevención en Bolivia?

La sustentación teórica versa sobre la ontología del ciberdelito y su relación con el diseño de políticas educativas públicas de prevención en Bolivia. Se estructura a partir de ejes temáticos interrelacionados:

Ontología del ciberdelito

Blyth, Kovacich y Collmann (2014) definen a la ontología del ciberdelito, como la estructura, los componentes y las relaciones de estos delitos, esencialmente para comprender su naturaleza y las diversas tipologías que ocurren en línea, de la misma forma Aggarwal y Singh (2016), afirman, que se compone de cuatro elementos:

- Delito en sí mismo, que incluye categorías como robo de identidad, piratería informática, acoso en línea, difamación y fraude.
- Medio utilizado, que abarca cualquier dispositivo o sistema empleado (computadora, smartphone, red), cuya identificación es crucial para rastrear a los perpetradores.
- Víctima, que puede ser una persona, organización o institución, y cuya naturaleza influye para determinar la gravedad del delito y el enfoque de las políticas públicas.
- Victimador o perpetrador, es el individuo o grupo que comete el ilícito, y su identificación puede resultar complicada debido al anonimato en Internet.

Estos elementos constituyen la base jurídica para analizar la estructura del ciberdelito y su aplicación dentro del marco penal boliviano. Al trasladar estos principios al entorno digital, se identifican nuevas formas de acción, medios tecnológicos y modalidades de imputación, lo cual exige una revisión continua de la legislación y la educación dentro del marco legal boliviano.

Ciberespacio

La expansión del ciberespacio está directamente ligada al aumento de los ciberdelitos. La comprensión de sus características y las vulnerabilidades que presenta es fundamental para el diseño de

políticas educativas públicas de prevención en Bolivia, ya que permite identificar los puntos de acción necesarios para promover un uso responsable y mitigar los riesgos éticos y sociales que se derivan de esta tecnología en constante evolución.

Políticas Públicas

Según Fischer y Forester (1993), señalan que las políticas públicas (PP) son acciones gubernamentales destinadas a abordar problemas sociales, caracterizadas por su enfoque en el bienestar común, el ejercicio legítimo del poder estatal, la redistribución equitativa de recursos, la definición de problemas públicos y la propuesta de soluciones. Además, estas políticas son interdependientes y dinámicas, adaptándose a los contextos sociales y tecnológicos en constante cambio.

En este sentido, Roxin (2016) y Cano (2017) sostienen que la efectividad de las políticas de seguridad y justicia depende de su articulación con la educación y la participación social. Por ello, las políticas educativas deben integrar la alfabetización digital, la ética tecnológica y la responsabilidad ciudadana como ejes de prevención frente a los ciberdelitos.

El Convenio de Budapest (2001) —primer tratado internacional contra los delitos informáticos— define cuatro categorías principales:

- Ataques contra la información y los sistemas (confidencialidad e integridad de datos).
- Delitos informáticos (fraude y manipulación de información).
- Delitos relacionados con el contenido digital (material ilegal o dañino).
- Infracciones contra la propiedad intelectual.

2. Materiales y Métodos

Con el fin de abordar la problemática planteada, se diseñó una estrategia metodológica compuesta por los siguientes elementos:

2.1. Diseño metodológico

La metodología utilizada fue inductiva, dado que facilitó la generación de categorías a partir de los datos. Asimismo, se enmarca en un tipo de investigación descriptiva y en un diseño metodológico mixto (cuantitativo-cualitativo), lo que permitió abordar de manera integral la complejidad del ciberdelito y acceder a su dimensión ontológica, fundamental para la formulación de políticas educativas de prevención.

2.2. Muestra

La población de estudio estuvo constituida por estudiantes de la Universidad Mayor de San Andrés. La muestra fue no probabilística, de tipo incidental, seleccionada bajo criterios de accesibilidad y representatividad contextual, logrando la participación de 280 estudiantes.

2.3. Técnicas e instrumentos de recolección de datos

Se utilizaron dos técnicas principales: la encuesta y el análisis documental.

- Encuesta: Se aplicó un cuestionario adecuado para entornos universitarios. El instrumento exploró tres dimensiones clave:
    - Frecuencia y modalidades de uso de las Tecnologías de la Información y la Comunicación (TIC).
    - Exposición y experiencias personales relacionadas con riesgos digitales.
    - Nivel de comprensión terminológica sobre el concepto de ciberdelito.
- Análisis documental: Se empleó una matriz de registro mediante fichas bibliográficas para sistematizar normativas legales nacionales e internacionales, además de literatura especializada en ontología, criminalística digital y políticas públicas orientadas a la prevención del cibercrimen.

2.4. Análisis de datos

El procesamiento de la información se estructuró en dos vertientes complementarias:

- Análisis cuantitativo

Se recurrió a técnicas de estadística descriptiva e inferencial. Asimismo, se empleó el método de splines lineales para identificar umbrales de riesgo y modelar relaciones no lineales entre variables como frecuencia de uso de TIC, edad, género y grado de exposición a ciberdelitos.

- Análisis cualitativo

Se aplicó la Teoría Fundamentada (Glaser y Strauss, 1967) con el propósito de identificar categorías que permitan comprender la estructura ontológica del ciberdelito y su vínculo con el ámbito educativo. Este análisis facilitó:

- La identificación de categorías emergentes.
- La comprensión de experiencias subjetivas frente a riesgos digitales.
- La construcción de relaciones conceptuales entre ontología, educación y prevención, esenciales para orientar futuras intervenciones políticas.

3. Resultados

Los resultados nos ayudan a comprender ontológicamente cómo el ciberdelito puede orientar al diseño de políticas educativas públicas orientadas a la prevención en Bolivia.

3.1. Clasificación del ciberdelito

La clasificación de los ciberdelitos permite comprender la naturaleza y características del delito informático, lo que a su vez

facilita la adopción de medidas de sensibilización, prevención e intervención en el diseño de políticas públicas. Esta clasificación se analizó en dos: como medio o instrumento y como fin u objetivo que

La clasificación de los ciberdelitos como medios o instrumentos, permite identificar los diversos tipos de ataques cibernéticos, lo que facilita la comprensión de las amenazas y ataques como ser:

- Fraude en línea: El phishing, pharming y el fraude en subastas en línea.
- Extorsión en línea: Amenazar y extorsionar a personas o empresas, como en el caso del "ransomware" o "secuestro de datos".
- Robo de identidad en línea: Obtener información personal de terceros y utilizarla con fines fraudulentos.
- Tráfico de drogas en línea: Venta y distribución de drogas en línea.
- Delitos financieros en línea: Cometer delitos financieros y de cuello blanco, como la manipulación de acciones y el blanqueo de dinero.

La clasificación de los ciberdelitos por su fin u objetivo revela motivaciones claras: la búsqueda de ganancias financieras, la identificación de activos valiosos o el daño reputacional de las entidades. Estos fines suelen lograrse a través de diversos métodos o ataques, entre los que se incluyen:

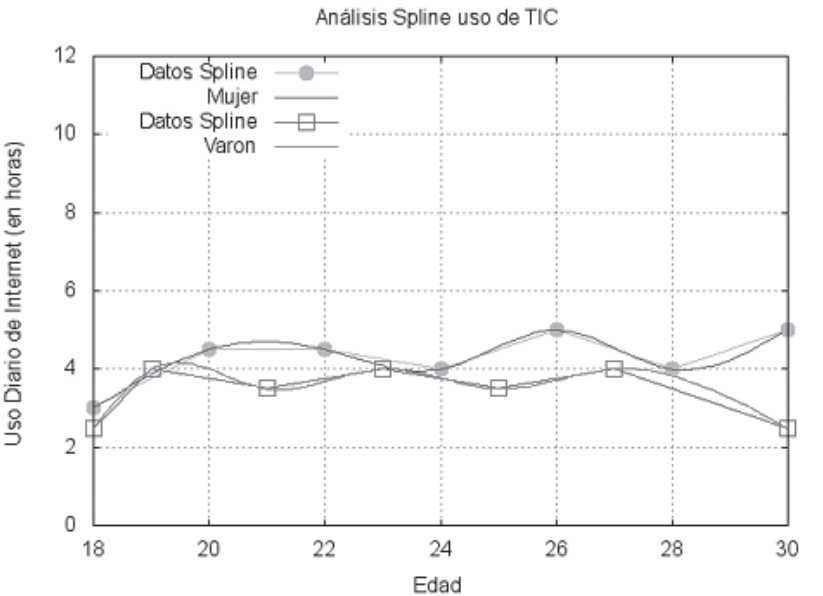
- Hackeo: Acceso no autorizado a sistemas informáticos con el objetivo de obtener información, modificar datos o causar daños.
- Distribución de virus informáticos: Creación y distribución de programas maliciosos con el objetivo de causar daños a sistemas informáticos o robar información.
- Ataques DDoS: Ataque informático que consiste en la sobrecarga intencional de un servidor o sistema para que deje de funcionar.

- Explotación de vulnerabilidades de software: Uso de las debilidades de un sistema informático para obtener acceso no autorizado o causar daños.
- Robo de información confidencial: Obtención no autorizada de información confidencial, como datos personales o de empresas, con el objetivo de utilizarlos para otros delitos o para obtener ganancias financieras.

3.2. Análisis segmentado del uso de las TIC

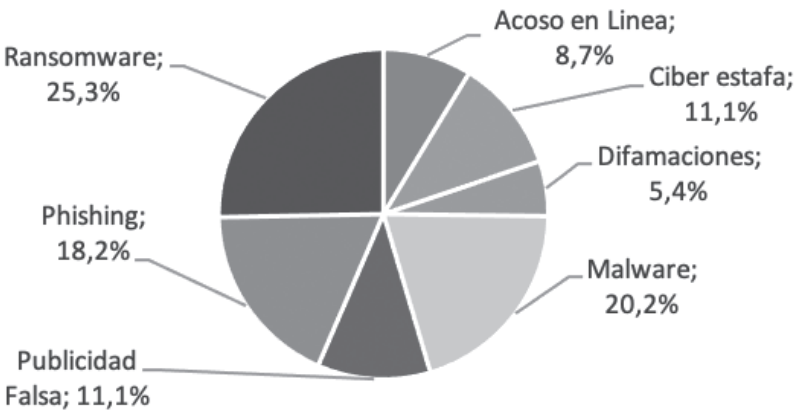
Identificación de umbrales mediante el Método Spline Lineal.

Figura 1. *Uso de TIC*



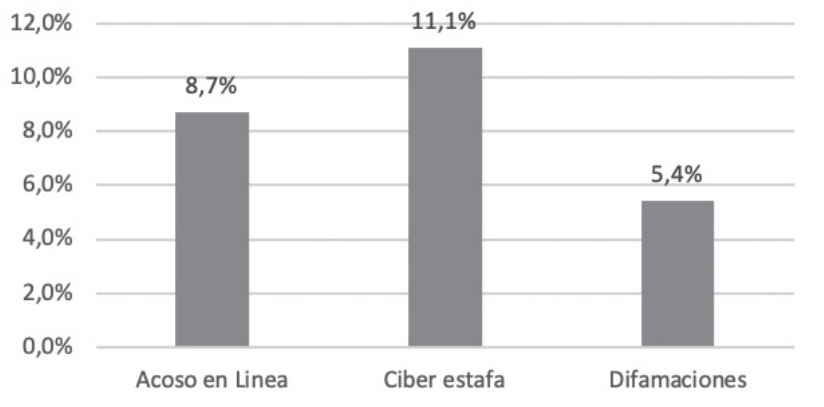
Nota. Esta figura muestra el análisis de los patrones de uso divergentes según el género: mientras que en el género masculino el uso de las TIC disminuye a medida que aumenta la edad, en el género femenino se observa la tendencia contraria, pues las horas de uso tienden a incrementarse con la edad.

Figura 2. *No conoce y no comprende el significado de los términos*



Nota. Esta figura muestra, los resultados que evidencian el porcentaje de desconocimiento y baja comprensión de la terminología sobre ciberdelito.

Figura 3. *Uso de redes sociales/ internet ¿Con qué frecuencia utiliza Internet? (Para redes sociales, noticias, operaciones bancarias, etc.)*



Nota. Esta figura muestra la utilización de Internet: ya sea para redes sociales, consultar noticias, realizar operaciones bancarias u otras actividades, se distribuye de la siguiente manera: el 90.71% de los usuarios accede a Internet diariamente, el 7.14% lo hace una vez a la semana y el 2.14% una vez al mes.

4. Discusión

La discusión de los resultados permite comprender de manera integral cómo la ontología del ciberdelito constituye un fundamento estratégico para orientar el diseño de políticas educativas públicas de prevención en Bolivia.

4.1. Prevención de los ciberdelitos mediante la clasificación.

Los resultados indican que todos los grupos etarios utilizan dispositivos digitales diariamente. No obstante, hay una diferencia notable por género: las mujeres aumentan su uso de TIC a medida que envejecen, mientras que los hombres lo reducen con la edad.

Esta diferencia con enfoque de género, implica que las políticas formativas deben considerar políticas educativas diferenciadas por género, ya que los niveles de exposición determinan también distintos niveles de riesgo frente a los ciberdelitos.

El control preventivo del ciberdelito busca evitar su comisión e incluye principalmente dos estrategias:

- Seguridad Informática: Implica la implementación de medidas técnicas como firewalls, antivirus y sistemas de detección de intrusiones para proteger los sistemas de ataques maliciosos.
- Educación y Concientización: Se enfoca en informar a los usuarios de las TIC sobre los riesgos del ciberdelito y las medidas de seguridad que deben adoptar para protegerse.

Los datos muestran un alto porcentaje de desconocimiento respecto a la terminología técnica vinculada al ciberdelito (phishing, malware, DDoS, ingeniería social, etc.). Este vacío cognitivo revela dos problemas estructurales, como la insuficiente alfabetización digital-crítica en la población universitaria, asimismo, la ausencia de formación sistemática sobre ética digital, seguridad y ciudadanía digital.

Desde la mirada educativa, esta brecha terminológica no es solo un problema de vocabulario, sino de comprensión ontológica del fenómeno. Si los estudiantes desconocen la "naturaleza del ser" del ciberdelito —sus elementos constitutivos, actores, medios y fines—, no pueden reconocer riesgos, anticiparse a ellos ni actuar de forma responsable.

4.2. La clasificación del ciberdelito como herramienta pedagógica y política

La clasificación de los ciberdelitos constituye una herramienta esencial no sólo para su identificación, sino también para su prevención. La prevención efectiva, sin embargo, requiere una combinación de medidas técnicas y estratégicas, así como el mantenimiento constante de la información sobre las últimas técnicas y tendencias de ciberdelitos para enfrentar las amenazas de:

- Phishing: Evitar hacer clic en enlaces desconocidos o sospechosos en correos electrónicos y mensajes de texto. No revele información personal o financiera a fuentes no confiables.
- Malware: Mantener actualizado el software de seguridad y antimalware. No descargar software de fuentes no confiables.
- Hacking: Crear contraseñas seguras y cambiar regularmente sus contraseñas. No comparta su información de inicio de sesión con nadie.
- Ransomware: Mantener actualizado su software de seguridad y antimalware. Realizar copias de seguridad regulares de los archivos importantes en un dispositivo externo o en la nube.
- DDoS: Proteger la red con firewalls y medidas de seguridad adicionales.
- Ingeniería social: Ser escéptico ante las solicitudes inesperadas de información personal o financiera. Asegúrese de verificar la identidad de las personas con las que está hablando antes de compartir información.

- Robo de identidad: Mantener seguro la información personal y financiera. No revelar información a fuentes no confiables y monitoree su actividad financiera regularmente para detectar posibles fraudes.

4.3. Control correctivo del ciberdelito

El control correctivo del ciberdelito se centra en la detección y sanción de los autores de delitos informáticos una vez que estos han ocurrido, e incluye las siguientes estrategias clave:

- Investigación y Persecución Penal: Requiere la participación de expertos en informática forense para la recuperación y análisis de evidencia digital (Taylor y Fritsch, 2015). En Bolivia, existen leyes específicas que sancionan estos delitos con penas de prisión.
- Cooperación Internacional: Es fundamental dado que el ciberdelito trasciende fronteras. Esto implica acuerdos de extradición e intercambio de información para la identificación de los culpables y la ejecución de investigaciones conjuntas. Bolivia ha suscrito acuerdos en esta materia con países como Brasil, Argentina y Estados Unidos.

La combinación de controles preventivos (seguridad informática, educación) y correctivos (investigación, persecución y cooperación internacional) es esencial para proteger la seguridad y privacidad en la era digital en Bolivia.

El enfoque ontológico permite comprender el ciberdelito no solo como una conducta ilegal, sino como un fenómeno social que emerge de interacciones humanas, tecnológicas y culturales.

4.4. Políticas públicas para abordar los ciberdelitos

El ciberdelito representa un desafío creciente en Bolivia, impactando significativamente la economía, la privacidad y la seguridad ciudadana. Para hacer frente a esta problemática, el país ha implementado un marco legal y de políticas públicas que comprende:

- Constitución Política del Estado (CPE,2009): Reconoce la importancia de las TIC, obliga al Estado a incorporar nuevas tecnologías (Art. 103) y garantiza el derecho de acceso a la información (Art. 106) y la seguridad en su uso.
- Código Penal (Ley N° 1768, 1997): Sanciona conductas específicas como la manipulación informática y el uso indebido de datos informáticos (Arts. 363 bis y ter).
- Ley de Telecomunicaciones (Ley N° 164, 2011): Regula el sector, garantiza el acceso universal a los servicios (Art. 5) y establece la protección de los derechos de los usuarios y la privacidad. Esta ley creó la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT).
- Centro de Gestión de Incidentes Informáticos (CGII): Creado en 2015 bajo la AGETIC, esta entidad es responsable de prevenir, detectar y responder a incidentes de seguridad informática, además de promover la cultura de ciberseguridad a nivel nacional.

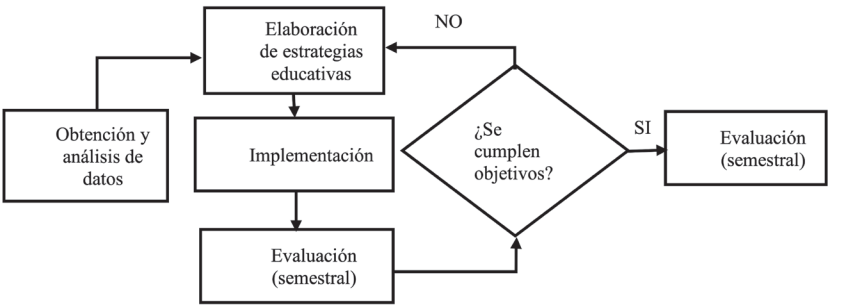
Por tanto, Bolivia requiere una política pública educativa que incorpore, como la formación a docentes y estudiantes en responsabilidades ético-digitales; de la misma forma elaborar protocolos institucionales de protección y respuesta, por último, buscar la participación activa de universidades, ATT, ADSIB, AGETIC y sociedad civil.

5. Conclusión

Los hallazgos de la investigación permiten concluir que la ontología del ciberdelito constituye una herramienta teórica esencial para comprender y afrontar de manera estratégica los riesgos digitales que enfrenta la sociedad boliviana. La interpretación de los datos evidencia que la prevención del ciberdelito no puede limitarse a soluciones tecnológicas o jurídicas; por el contrario, debe sustentarse en políticas educativas públicas que sean sistemáticos, críticos y éticamente orientados, capaces de transformar la manera en que la población se relaciona con el ciberespacio.

Una ontología clara facilita la identificación de tipos de ciberdelitos y mejora la colaboración entre expertos, siendo crucial para el diseño de políticas que equilibren la privacidad y la seguridad. Aunque Bolivia ha avanzado con leyes, debe seguir trabajando en la prevención y el combate de estos delitos para garantizar la seguridad y estabilidad nacional.

Figura 4. *Propuesta de diseño de una política educativa pública contra el ciberdelito*



Referencias

Aggarwal, D., Singh, R. (2016). Cyber Crime and Its Impacts on Society. 140.https://doi:10.5120/ijca2016909068

Arancibia Clavel, C. (2020). Derecho penal boliviano: Editorial Verbo Jurídico.

Asamblea Legislativa Plurinacional de Bolivia. (2009). Constitución Política del Estado de Bolivia.

Asamblea Legislativa Plurinacional de Bolivia. (2011). Ley N.º 164 de Telecomunicaciones.

Asamblea Legislativa Plurinacional de Bolivia. (2018). Código Penal (Ley N.º 1768).

Bacigalupo, E. (2019). Derecho penal: Parte general. Hammurabi.

Blyth, A., Kovacich, G. (2014). Information Assurance: Surviving in the Information Environment. Springer Science & Business Media

Cano, J. (2017). Políticas de seguridad: Prevención del delito y disuasión. Ediciones Política Pública.

Decreto Supremo 2514. (2015). Creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación. Estado Plurinacional de Bolivia.

Floridi, L. (2014). The fourth revolution: How the infosphere is reshaping human reality. Oxford University Press.

García, J. (2018). Políticas públicas de seguridad. En G. Martínez (Ed.), Seguridad ciudadana: Retos y perspectivas (pp. 55–70). Editorial Universidad de Lima.

Glaser, B. G., Strauss, A.L. (1967). The Discovery of Grounded Theory: Strategies for Qualitative Research. Ed. Routledge

Lévy, P. (1999). Cibercultura: La cultura de la sociedad digital. Anthropos.

Roxin, C. (2016). Derecho penal: Parte general. Civitas.

Schneier, B.(2013). A Declaration of the Independence of Cyberspace, Cyber Security, and Trust. Harvard Kennedy School

Taylor, R. W., Fritsch, E. J. (2015). Digital crime and digital terrorism. Prentice Hall.

Turkle, S. (1995). Life on the screen: Identity in the age of the Internet. Simon Schuster.

Zaffaroni, E. (2013). Manual de derecho penal: Parte general. Ediar.

Fecha de recepción: 27 de octubre de 2025
Fecha de aceptación: 28 de noviembre de 2025