**UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO**

**FACULTAD CIENCIAS DE LA INGENIERÍA**

**INGENIERÍA EN SOFTWARE**

**TEMA:**

Unidad 1

**MATERIA:**

Investigación Bibliográfica Unidad I

**INTEGRANTES:**

Guaranga Otavalo Ebert Steeven

Mera Carbo Lister Leonardo

**DOCENTE:**

Ing. Guerrero Ulloa Gleiston Ciceron

**QUEVEDO – LOS RÍOS – ECUADOR**

**2023 – 2024**

**Índice**

[Introducción 3](#_Toc153705575)

[Unidad 1 4](#_Toc153705576)

[El derecho y los derechos 4](#_Toc153705577)

[El delito informático 4](#_Toc153705578)

[Impacto de los delitos informáticos 7](#_Toc153705579)

[Estadísticas sobre delitos 8](#_Toc153705580)

[Protección de datos de nivel personal 8](#_Toc153705581)

[Sujetos procesales 8](#_Toc153705582)

[Conclusión 8](#_Toc153705583)

[Bibliografía 8](#_Toc153705584)

# Introducción

La interacción entre "El Derecho" y "Los Derechos" emerge como un pilar esencial para la formación y mantenimiento del orden social y la justicia. "El Derecho" se identifica como un conjunto de normas y principios que regulan las interacciones humanas en las sociedades, encarnando una idea de justicia y orden [1]. Estas normas, que pueden ser impuestas de manera coactiva, son cruciales para la supervivencia y el buen funcionamiento de cualquier sociedad. No obstante, la importancia del derecho trasciende estas funciones básicas, abarcando una misión más profunda y significativa, enfocada en su utilidad práctica y en los elevados objetivos que aspira a alcanzar.

Por otro lado, "Los Derechos" se refieren a las libertades, prerrogativas y protecciones que el sistema jurídico otorga y asegura a los individuos. Estos derechos van desde los derechos humanos universales hasta derechos específicos consagrados en legislaciones nacionales. En un mundo cada vez más digitalizado, surge un nuevo desafío jurídico: el delito informático. Estos crímenes, que incluyen una variedad de acciones ilegales relacionadas con la tecnología de la información, plantean interrogantes significativos sobre la regulación y el control legal [2]. Los delitos informáticos, que pueden ser tanto dolosos como culposos, requieren una atención especial debido a su naturaleza técnica, su rápida ejecución y la dificultad de detección y sanción, resaltando la urgente necesidad de una regulación jurídica internacional en este ámbito [3].

# Unidad 1

## El derecho y los derechos

En el ámbito jurídico, la interacción entre "El Derecho" y "Los Derechos" constituye un eje fundamental en la construcción y mantenimiento del orden social y la justicia. El derecho se define como un conjunto de principios y reglas que reflejan una noción de justicia y orden, regulando las interacciones humanas en todas las sociedades. Este conjunto de normas, que puede ser impuesto de forma coactiva, es fundamental para la supervivencia de cualquier sociedad. La importancia vital del derecho se extiende más allá de esta función básica, comprendiendo una misión más trascendente y profunda, enfocada en su utilidad y en los elevados objetivos que busca alcanzar. Esta perspectiva será analizada y profundizada en secciones posteriores [4].

Por otro lado, "Los Derechos" son las libertades, prerrogativas y protecciones que el sistema jurídico reconoce y garantiza a los individuos, abarcando desde derechos humanos universales hasta derechos específicos consagrados en legislaciones nacionales.

## El delito informático

En el ámbito jurídico actual, caracterizado por la convergencia de las telecomunicaciones y la informática, se abordan frecuentemente cuestiones relacionadas con el uso de la computadora. La respuesta a los diversos problemas que emergen en este entorno puede incluir la regulación de aspectos como los contratos electrónicos, delitos informáticos, valor probatorio de documentos electromagnéticos, internet, comercio electrónico, firmas digitales, protección de datos personales, gestión de bases de datos y la problemática de la piratería [5].



**Figura 1** Delitos informáticos [6]

Los crímenes informáticos, también conocidos como "computer crimes", incluyen una variedad de acciones ilegales que involucran el uso indebido o daño a una computadora y sus accesorios. Esto abarca prácticas como el uso indebido de software, la apropiación o divulgación ilícita de datos, las interferencias en bancos de datos electrónicos ajenos y otras conductas ilegales relacionadas con la informática. Estas actividades delictivas, tipificadas tanto en el Código Penal como en leyes especiales, pueden ser cometidas utilizando sistemas electrónicos de procesamiento de datos, o en contra de ellos, causando daños [7].

Un delito informático se puede definir como cualquier acto o falta cometido intencionalmente por una persona, que resulta en un daño a otros sin que necesariamente el autor obtenga un beneficio directo. Alternativamente, puede tratarse de acciones que proporcionan un beneficio ilícito al autor, aunque no perjudiquen directa o indirectamente a la víctima. Estos actos están tipificados por la ley, ocurren en el entorno informático y son sancionables con penas [5], [7].

Téllez Valdés describe los delitos informáticos como acciones ilícitas en las que las computadoras se utilizan como herramienta o son el objetivo. Estas pueden ser conductas tipificadas, ilegales y realizadas con culpa, donde las computadoras también se utilizan como herramienta o son el objetivo [7].

Además, el avance tecnológico complica la detección de estos delitos. La falta de seguridad en los sistemas y la reticencia a denunciar por temor a dañar la imagen pública o por otros motivos, contribuyen a la impunidad en este ámbito.



**Figura 2** La tecnología y la ley [8]

Estas acciones delictivas, clasificadas como de "cuello blanco", se caracterizan por ser cometidas generalmente por individuos con conocimientos específicos. Frecuentemente se llevan a cabo en contextos laborales, aprovechando las oportunidades que surgen en el entorno tecnológico y económico. Estos delitos suelen causar pérdidas económicas significativas a las víctimas y, en muchos casos, generan beneficios sustanciales para quienes los perpetran.

* La comisión de estos delitos se facilita por la rapidez con la que pueden ejecutarse, a menudo en fracciones de segundo y sin necesidad de presencia física del delincuente. A pesar de su frecuencia, las denuncias son escasas, en parte debido a la insuficiente regulación jurídica a nivel internacional. Son especialmente comunes y sofisticados en el sector militar y presentan desafíos significativos para su comprobación debido a su naturaleza técnica.
* Mayoritariamente, estos delitos son cometidos con intención (dolosos), aunque también existen muchos casos que resultan de negligencia o imprudencia (culposos), y en ocasiones su resultado supera la intención original (preterintencionales). Además, ofrecen facilidades para su comisión por parte de menores de edad, aprovechando su tiempo libre.
* La proliferación creciente de estas acciones delictivas subraya la necesidad urgente de una regulación jurídica a nivel internacional. Hasta el momento, estos ilícitos siguen siendo mayormente impunes ante la ley.

En las últimas décadas, el Ecuador ha sufrido profundas transformaciones económicas, sociales y políticas. La Constitución del 2008, aprobada en las urnas, impone obligaciones inaplazables y urgentes como la revisión del sistema jurídico para cumplir con el imperativo de justicia y certidumbre [9].

El artículo 190 del Código Orgánico Integral Penal tipifica los delitos informáticos, definiéndolos como aquellos actos que utilizan sistemas informáticos, redes electrónicas o de telecomunicaciones para facilitar la adquisición no autorizada de bienes ajenos o para realizar transferencias no consentidas de bienes, valores o derechos, causando perjuicio a la persona afectada o a terceros. Esta definición incluye acciones como alterar, manipular o modificar el funcionamiento de redes electrónicas, programas informáticos, sistemas de telemática y equipos terminales de telecomunicaciones. Quienes cometan estos actos enfrentarán una pena privativa de libertad que oscila entre uno y tres años [9].

## Impacto de los delitos informáticos

El avance de las tecnologías de la información y comunicación en distintos sectores sociales no siempre ha resultado ser beneficioso. Si bien estas tecnologías han contribuido a mejorar la calidad de vida de las personas, también han surgido conductas dañinas que desafían la capacidad del sistema jurídico actual para regularlas adecuadamente. Existe un debate continuo entre el uso legítimo y el abuso de las actividades informáticas en la sociedad contemporánea. En algunos casos, resulta complicado encuadrar estas conductas dentro de las normativas penales tradicionales, debido a la imposibilidad de aplicar analogías bajo el principio de legalidad. En el derecho penal, es necesario que la conducta se ajuste precisamente a la norma penal para que se considere como un delito sujeto a investigación y sanción. Además, estas conductas abarcan una amplia gama de crímenes o delitos, que pueden llevarse a cabo en distintos países y en diferentes momentos [10].

Los ciberataques tienen consecuencias adversas en la economía de un país. Defenderse contra los delitos informáticos representa un desafío tanto para individuos como para organizaciones. Los criminales cibernéticos emplean técnicas cada vez más sofisticadas, lo que contribuye al incremento de estos delitos por diversos motivos. Además, se reconoce la importancia de profundizar en el análisis de casos relacionados con este tipo de crimen y la necesidad de estar debidamente preparados para enfrentarlos [11]. Si un ataque informático tiene éxito en una organización gubernamental el impacto es económico por pérdida de tiempo, es social por la desatención a los ciudadanos, es político por la imagen del gobierno de turno.

**Pérdidas económicas:** el ciberdelito puede tener un impacto financiero en empresas e individuos. Esto incluye lavado de dinero, fraude financiero y perturbación de negocios.

**Costos de recuperación y protección:** las organizaciones suelen gastar grandes sumas de dinero para recuperarse de los ciberataques y mejorar sus sistemas de seguridad para prevenir futuros ataques.

**Vulnerabilidad de datos confidenciales:** los ataques cibernéticos pueden comprometer datos personales y confidenciales, lo que lleva a una violación de la confidencialidad y de la información confidencial.

**Degradación de la confianza:** el ciberdelito puede socavar la confianza de los ciudadanos en las instituciones digitales, afectando así al comercio electrónico y las transacciones en línea.

**Amenazas a la seguridad nacional:** ciberataques contra infraestructuras críticas para la seguridad nacional.

**Desafíos legales y regulatorios:** La naturaleza cada vez mayor del delito cibernético pone a prueba las leyes existentes, lo que requiere una actualización y adaptación constantes para combatir eficazmente las actividades delictivas.

**Innovación en respuesta a los ataques:** el cibercrimen está impulsando el desarrollo de nuevas tecnologías de seguridad y estrategias de defensa más sólidas.

**El auge de las tácticas de cibercrimen:** a medida que avanza la tecnología, también ha aumentado el número de ciberdelincuentes que utilizan métodos más sofisticados para cometer delitos.

## Estadísticas sobre delitos en el ecuador

A medida que la tecnología avanza, el ciberdelito en Ecuador ha experimentado un notable incremento en los últimos años [12]. En el trabajo investigativo de Ron et al.[12]presenta estadísticas y análisis detallados sobre los delitos informáticos.

Antes de dar a conocer las estadísticas presentados en los años anteriores, es necesario conocer los delitos más comunes usados en el Ecuador por los ciberdelincuentes. En la tabla 1, se presenta los delitos más comunes y la respectiva sanción en el articulo respectivo presentado por el COIP [13]:

Tabla 1: Delitos más comunes y su sanción en el artículo respectivo

|  |  |  |
| --- | --- | --- |
| Descripción | Articulo | Sanción (años en prisión) |
| Pornografía infantil | 103 | 13 a 16 |
| Violación del derecho a la intimidad | 178 | 1 a 3 |
| Revelación ilegal de información de bases de datos | 229 | 1 a 3 |
| Interceptación de comunicaciones | 476 | 3 a 5 |
| Ataque a la integridad de sistemas informáticos | 232 | 3 a 5 |
| Delitos contra la información pública reservada legalmente | 233 | 3 a 5 |
| Acceso no consentido a un sistema informático, telemático o de telecomunicaciones | 234 | 3 a 5 |

En la Figura 3 se muestra la variación en el número y porcentaje de delitos informáticos por provincia entre los años 2015 y 2016 [12]:

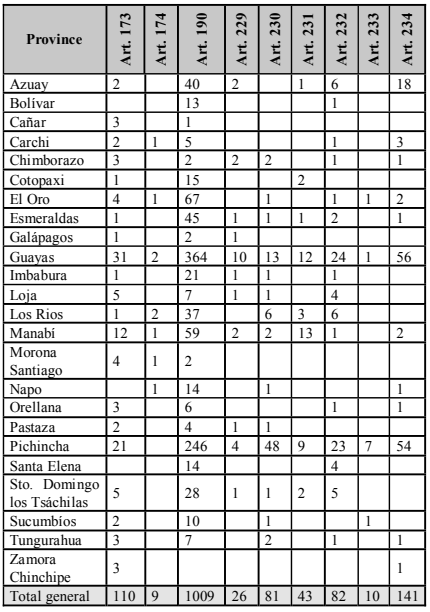


Figura 3: Delitos informáticos por provincia

En base a estas estadísticas, Se observó que el mayor número de delitos ocurrió en las provincias de Guayas y Pichincha, siendo estas las más pobladas y con mayor desarrollo tecnológico de Ecuador. Se documentó una disminución en la ocurrencia de delitos informáticos en general, y en particular aquellos referidos a delitos financieros (artículos 190, 186 y 231)

Por otro lado, en el trabajo de Aparicio [14] proporciona un análisis detallado de los delitos informáticos en Ecuador en los años 2017, 2018, 2018 enfocándose en el marco legal establecido por el COIP. La Figura 4 presenta una representación gráfica de los delitos más frecuentes ocurridos durante esos tres años.

Gráfico

Descripción generada automáticamente

Figura 4: Delitos informáticos en los años 2017, 2018, 2019

Dado el gráfico de barras, se detalla un aumento en las denuncias de 2017 a 2019 para los delitos de acceso no consentido a sistemas informáticos (Art. 234), interceptación ilegal de datos (Art. 230), ataque a la integridad de sistemas informáticos (Art. 232), y revelación ilegal de bases de datos (Art. 229). Las estadísticas muestran un crecimiento notable en los casos reportados para el Artículo 234 en 2019 en comparación con años anteriores.

## Protección de datos de nivel personal

La protección de datos personales a nivel personal es un derecho fundamental que permite a los individuos controlar, disponer y decidir sobre sus datos personales. Este derecho busca proteger la privacidad, la intimidad y asegurar la transparencia en el tratamiento de datos personales, garantizando que estos sean correctos y solo accesibles para fines específicos [15].

## Sujetos procesales

# Conclusión

# Bibliografía