UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

LA EFICACIA DE UNA NORMATIVA ESPECIAL QUE REGULE EL USO DE LA INTELIGENCIA ARTIFICIAL PARA EVITAR CIBER-DELITOS EN EL ECUADOR

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO

AUTORES: WELLINGTON MATEO ANDRADE ARIAS.

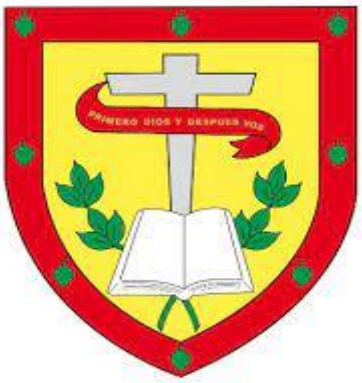
LUIS ALBERTO YURANK TSAMARAINT

DIRECTOR: DR. MARTINEZ ALBORNOZ JUAN PABLO MGS.

CUENCA-ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATOLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADEMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

TÍTULO

LA EFICACIA DE UNA NORMATIVA ESPECIAL QUE REGULE EL USO DE LA INTELIGENCIA ARTIFICIAL PARA EVITAR CIBER-DELITOS EN EL ECUADOR.

TRABAJO DE TITULACION PREVIO A LA OBTENCION DEL TITULO DE ABOGADO.

AUTORES: WELLINGTON MATEO ANDRADE ARIAS.

LUIS ALBERTO YURANK TSAMARAINT.

DIRECTOR: DR. MARTINEZ ALBORNOZ JUAN PABLO.MGS.

CUENCA- ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO

Universidad Católica de Cuenca

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Declaratoria de Autoría y Responsabilidad

Wellington Mateo Andrade Arias portador(a) de la cédula de ciudadanía Nº **0150747368**. Declaro ser el autor de la obra: "**LA EFICACIA DE UNA NORMATIVA ESPECIAL QUE REGULE EL USO DE LA INTELIGENCIA ARTIFICIAL PARA EVITAR CIBER-DELITOS EN EL ECUADOR"**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, **15 de abril de 2021**

F: .....

Wellington Mateo Andrade Arias

C.I. **0150747368**

Universidad Católica de Cuenca

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Declaratoria de Autoría y Responsabilidad

Luis Alberto Yurank Tsamaraint portador de la cédula de ciudadanía Nº **1725573859**. Declaro ser el autor de la obra: **"La eficacia de una normativa especial que regule el uso de la inteligencia artificial para evitar Ciber-Delitos en el Ecuador."**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, **21 de abril de 2025**

F: .....

Luis Alberto Yurank Tsamaraint

C.I. **1725573859**

Universidad Católica de Cuenca

CERTIFICO

Certifico que el presente Trabajo de Investigacion fue desarrollado **por Wellington Mateo Andrade Arias, Luis Alberto Yurank Tsamaraint**, con el Tema: "**La eficacia de una normativa especial que regule el uso de la inteligencia artificial para evitar ciber-delitos en el Ecuador**", bajo mi supervision

Dr. Juan Pablo Martinez Albornoz, Mgs.

tutor

Dedicatoria

La dedicatoria la realizo a mis padres, que han visto mi esfuerzo durante este trayecto que por fin a culminado, a mis hermanos mayores Oscar Andrade y Lenin Andrade, en apoyarme, en darme ánimos para poder culminar mis estudios, a mi hermano Felipe Andrade, que me ha ayudado en los momentos más importantes para poder superarme y lograr este objetivo, y a mis amigos que gracias a sus consejos y apoyo al motivarme en culminar esta etapa, y a mí mismo por haber logrado culminar esta etapa, que no fue fácil, pero al final siempre supe que valdría la pena.

Wellignton Mateo Andrade Arias

A Dios, quién a permitido que durante este largo proceso académico pueda culminar con mis estudios. También, este triunfo es el resultado del apoyo incondicional: de mi compañera y amiga María E. Zambrano; y, de mis hermanos Patricio y Angela, quiénes se han mantenido a mi lado en los momentos más difíciles, siendo la base sobre la cual me he sostenido durante este tiempo, por tanto, este logro también es suyo.

Luis Alberto Yurank Tsamaraint

Agradecimiento

Mi agradecimiento es primero a Dios, y a la virgencita del cisne, que me ha otorgado la salud, paciencia, sabiduría y experiencias para poder haber culminado esta etapa, a mi familia y a mi tutor de tesis al Dr. MGS. MARTINEZ ALBORNOZ JUAN PABLO, agradeciendo por sus enseñanzas sobre el Derecho Informático, cuando fui su estudiante, y gracias a ello ha nacido la idea de esta tesis, y por ultimo a mis amigos que me han acompañado en todo este trayecto.

Wellignton Mateo Andrade arias

Quiero expresar mi más profundo y sincero agradecimiento a mi tutor Dr. Juan Pablo Martínez Albornoz, por la paciencia y, el conocimiento que me ha compartido durante la elaboración del presente trabajo. Asimismo, a todos mis docentes de la Universidad Católica de Cuenca, cuyo conocimiento, dedicación y guía han sido el pilar fundamental en mi preparación profesional. Del mismo modo, agradezco a mi padre y a mi madre por haberme dado la vida y, aunque no estén conmigo, estoy seguro que siempre me acompañan. Agradezco eternamente a todos, por haber sido mi inspiración y por su constante apoyo durante este camino.

Luis Alberto Yurank Tsamaraint

Resumen

En la presente investigación se analizara la necesidad de anexar una normativa especializada para la prevención de los Ciber-Delitos en el Ecuador, la época de la pandemia y la Post-Pandemia el indicie de criminalidad informática ha tenido un aumento considerable, teniendo a los estados como México, Brasil y el Ecuador, como los estados que más han reportado los delitos informáticos, debido a la aparición de nuevas herramientas digitales que han ido tomando un apogeo considerable, no obstante el uso malicioso ha traído consigo aumento de los Ciber-Delitos dentro del Estado ecuatoriano.

Si el Ecuador planea implementar una normativa que regula la Inteligencia Artificial debe ser anexada a la Ley Orgánica de Protección de Datos Personales, este cuerpo legal fue creado en el año 2021, cuya norma regula el tratamiento que se da a la información, sin embargo, en sus ochenta y seis artículos en ninguno menciona regular la inteligencia artificial, tampoco garantiza la prevención de los delitos informáticos.

Palabras clave: *Inteligencia artificial, delitos informáticos, prevención, ciber seguridad, algoritmos, impacto social.*

Abstract

This research examines the need for specialized legislation to prevent cybercrimes in Ecuador. During the pandemic and post-pandemic eras, the rate of cybercrime has increased considerably. Countries such as Mexico, Brazil, and Ecuador have reported the highest number of cybercrimes due to the emergence of new digital tools that have gained considerable popularity. However, the malicious use of technology has led to an increase in cybercrimes within the Ecuadorian state.

If Ecuador plans to implement regulations concerning Artificial Intelligence, it should be incorporated into the Organic Law on Personal Data Protection. This legal body was established in 2021 and is responsible for regulating data processing; however, in its eighty-six articles, none mentions regulating artificial intelligence, nor does it guarantee the prevention of cybercrimes.

Keywords: *Artificial intelligence, cybercrime, prevention, cybersecurity, algorithms, social impact.*

Índice

CONTENIDO

INTRODUCCION

En el Estado ecuatoriano se ha visto la necesidad de implementar una normativa especializada para el regularización de la inteligencia artificial, por el aumento considerable de los delitos informáticos partiendo desde el año dos mil veinte, estos ataques informáticos se deben a la falta de conciencia de las personas en relación a sus publicaciones en las redes sociales y otorgar su información personal a páginas de dudosa existencia, con ello ha sido un método fiable para que los delincuentes informáticos sustraigan la información de la víctima para afectarlas en su patrimonio y otros derechos conexos a la misma.

Esta investigación se puntualiza en como la Ley Orgánica de Protección de Datos Personales, regula o no la inteligencia artificial para la prevención de los Ciber-Delitos dentro de la legislación ecuatoriana debido a que la información ha tomado suma importancia, al momento que se logra el robo de la misma, es por seguro que ocasionara un daño muy grave a la víctima.

Para finalizar esta investigación, se ha podido determinar que, al anexar una normativa especializada para el regularización y control de la Inteligencia Artificial, sería muy beneficioso para el mismo Estado, en diferentes áreas como la educación, salud, en lo social etc. En la seguridad informática su implementación es beneficiosa, por que ayudará a prevenir delitos informáticos y con ello se protege la información, tanto en el sector público como el sector privado y de manera individual para cada ciudadano, ya que la seguridad informática podrá disminuir este tipo de delitos.

CAPÍTULO 1.

Objetivo de aprendizaje: cada objetivo como método de aprendizaje es importante, con ello podemos entender de manera general el derecho informático, y como se puede emplear el uso de la inteligencia artificial para poder evitar el cometimiento de Ciber-Delitos en Ecuador, debido a que su gran desarrollo ha sido determinada como una herramienta necesaria dentro de la sociedad, sin embargo el Estado ecuatoriano no le ha dado la importancia que se debe dar a la inteligencia artificial, con ello se buscaría implementar que se regule su uso y se evitaría el cometimiento de Ciber-delitos, debido a que se está utilizando la propia inteligencia artificial para cometer los delitos informáticos por su falta de normativa para su uso y control por parte del estado.

Examinar de manera legal, doctrinaria y jurisprudencialmente como la falta de norma que debe regular el uso correcto de la inteligencia artificial permite el cometimiento de Ciber-Delitos en Ecuador.

LA SEGURIDAD.

El Ecuador, es un estado libre y soberano, así lo expresa el artículo 1 de la constitución de la república quedando así que, la seguridad interna y externa queda en manos del Estado, para que se pueda garantizar la seguridad el poder legislativo ha creado la norma necesaria para que los cuerpos de seguridad puedan actuar en caso de amenaza en contra de personas nacionales o extranjeras que transitan en el Ecuador, sin embargo esta seguridad solamente radica en lo que sería en un espacio físico, según el autor,

“Michel Foucault: la seguridad es un concepto que nace junto al liberalismo, y se refiere a una forma de gobernar con el objetivo de "[...] garantizar que los individuos o la colectividad estén expuestos lo menos posible a los peligros”. (Luque Juárez, 2024)**.**

Lo que establece el autor en relación a los gobiernos de turno, el Estado debe garantizar la seguridad sin excepción alguna, pero lo complejo en el Ecuador ha sido la prevención de los Ciber-Delitos, otro tipo de delitos que ha ido en aumento así lo establece el medio de comunicación El Mercurio de la ciudad de Cuenca, manifestado lo siguiente:

> Un informe de Panorama de Amenazas 2023, de la empresa de seguridad Kaspersky, reveló que entre agosto de 2022 y agosto de 2023 se reportaron más de 2 millones de ataques cibernéticos en América Latina. Los países en los que se cometieron más delitos informáticos son: Brasil, México, Ecuador. Según un informe de 2021 de la empresa de seguridad informática ESET (2021), en 2020 se registró un aumento del 124 % la cantidad de ataques informáticos en la región. En Ecuador, el número de denuncias de ciberdelitos ha ido en aumento en los últimos años. Según la fiscalía general del Estado en 2019 se registraron 718 denuncias por delitos informáticos. En 2020 se registraron 1.030 denuncias, las cuales aumentaron a 1.851 en 2021 y, en los primeros seis meses del 2022, la policía ya contabilizó 650 nuevas investigaciones en el país.” (Campoverde, Diario El Mercurio, 2024)

Este medio de comunicación a determinado que los países más afectados por los Ciber-delitos, entre ellos se encuentra Ecuador, los casos han ido aumentado esto también se debe a la llegada de la pandemia, con el confinamiento, las personas pasaron más tiempo en sus computadoras o celulares inteligentes y con ello aumentaron de manera gradual los casos de delitos informáticos, añadiendo también que aumentaron con la llegada de la inteligencia artificial.

Para poder entender como los Ciber delitos deben ser prevenidos, debemos partir de conceptos y definiciones de diferentes términos que lo abarcan.

CIBERESPACIO.

La seguridad, al día de hoy con el avance de las tecnologías no únicamente radica en solo espacios físicos, sino también en lo cibernético, gracias al internet y con los avances tecnológicos se abrió un campo amplio para la creación de aplicaciones para poder comunicarse con personas de otros estados, así mismo ha ayudado con la creación de servicios para mejorar la experiencia de los usuarios.

El ciberespacio es entendido como un espacio para que las personas puedan navegar en internet, con la creación y mejoramiento de los diferentes softwares.

Para lograr una mejor conectividad es necesario tener el apoyo de infraestructura tecnológica.

DEFINICIÓN DE CIBERNÉTICA.

La cibernética, es la capacidad que tiene las personas en crear los sistemas de computadoras para que este pueda realizar diferentes actividades, como lo son los cálculos matemáticos, no obstante, no solo se queda ahí, con el aumento de las capacidades de los sistemas ha mejorado a tal punto que este pueda pensar por sí mismo conocido como la inteligencia artificial, o ejercer acciones más complejas, pero con menos tiempo.

DIFERENCIA DE LA CIBERNÉTICA Y LA ROBÓTICA.

Cibernética:

> La cibernética es el estudio interdisciplinario de la estructura de los sistemas reguladores. La cibernética está estrechamente vinculada a la teoría de control y a la teoría de sistemas. Tanto en sus orígenes como en su evolución, en la segunda mitad del siglo XX, la cibernética es igualmente aplicable a los sistemas físicos y

> sociales. Los sistemas complejos afectan y luego se adaptan a su ambiente externo. (Enmanuel, 2024)

Robótica:

> La Robótica es una ciencia o rama de la tecnología, que estudia el diseño y construcción de máquinas capaces de desempeñar tareas realizadas por el ser humano o que requieren del uso de inteligencia. Las ciencias y tecnologías de las que deriva podrían ser: el álgebra, los autómatas programables, las máquinas de estados, la mecánica o la informática (Enmanuel, 2024)

La diferencia entre estos dos términos es importante, debido a que la cibernética se dedica a la creación del software, el cerebro de las maquinas como se podría mencionar.

La robótica en cambio se lo puede entender como la construcción de las maquinas, es decir, el cuerpo, o el esqueleto en donde se implementará la cibernética.

RELACIÓN ENTRE LA CIBERNÉTICA Y LA ROBÓTICA.

La cibernética y la robótica tiene un vínculo muy cercano, uno se dedica a la creación de los sistemas, es decir, de su funcionamiento y acciones que podrá ejecutar o también las creación de los algoritmos, en cambio la robótica se dedica al diseño de las maquinas, por ejemplo, se crea un sistema que pueda soldar metales, y con la creación del diseño y modelo adecuado, este podrá ejecutar dicha tarea, en relación con la inteligencia artificial, se relaciona directamente con las dos, debido a que primero se debe crear su software, luego crear un espacio físico para que pueda funcionar, esta herramienta digital es capaz de aprender por sí mismo, entonces podemos determinar que si la inteligencia artificial es utilizada para prevenir los Ciber- delitos, este al tener su propio aprendizaje puede también crear nuevos métodos para la prevención y así evitar que se sigan existiendo más

víctimas que utilizan el mundo digital, pero quien debe regular la inteligencia artificial para que sea utilizado para la prevención de Ciber- Delitos es el mismo Estado ecuatoriano, al no existir una normativa especial para su control, no se puede cumplir con este propósito esto lleva a que se siga afectando la información de los ciudadanos nacionales y extranjeros que residen en el Ecuador.

La inteligencia artificial puede funcionar en diferentes formas o también en los tipos de robots que existen.

TIPOS DE ROBOTS.

> Androides: estos artilugios se parecen y actúan como si fueran seres humanos. Este tipo de robots no existen en la realidad, por lo menos por el momento, sino que son elementos ficcionales. (Enmanuel, 2024)

Los androides, antes era común observarlos en películas de acción, hoy en día con los grandes avances de la tecnología y la robótica, se ha podido incorporar la inteligencia artificial, con el objetivo que simule las actuaciones del ser humano, pero la inteligencia puede ser utilizado también en diferentes ámbitos, en el desarrollo de Ciber- Seguridad, funcionaria correctamente, al estar conectado a la internet, y con ayuda de la capacidad de incorporar grandes cantidades de información podría ser útil en prevenir los Ciber Delitos, al poder identificar a los usuarios con intenciones maliciosas, podría inmediatamente reportar a los agentes de seguridad sobre la posible amenaza a presentarse, además con la implementación del reconocimiento facial sería mucho más fácil identificar a personas que estén con orden de captura.

> Móviles: estos robots cuentan con orugas, ruedas o patas que les permiten desplazarse de acuerdo a la programación a la que fueron sometidos. Estos robots

> cuentan con sistemas de sensores, que son los que captan la información que dichos robots elaboran. (Enmanuel, 2024).

Este tipo de robot, por lo general son incorporados en industrias o en los hogares con funciones únicas y sencillas, no muy complejas, la inteligencia artificial puede ser incorporado en uno de estos robots pero sus funciones físicas serian limitadas, la ventaja aquí es cuando estos robots al estar en un solo espacio físico y al estar conectados al internet en todo momento puede servir como un monitoreo constante si sus dueños o habitantes del hogar están siendo posiblemente víctimas de Ciber-Delitos y con ello podría mejorar la Ciber- Seguridad ya que puede comunicar por vía mensaje al celular o computadora sobre la posible amenaza.

> Industriales: los robots de este tipo pueden ser electrónicos o mecánicos y se los utiliza para la realización de los procesos de manipulación o fabricación automáticos. También se les llama robots industriales a aquellos electrodomésticos que realizan simultáneamente distintas operaciones. (Enmanuel, 2024)

Estos tipos de robots, por lo general son fabricados para una única función, es en crear, armar, desarmar, etc.

En el campo industrial no servirá de mucho integrar la inteligencia artificial, en el ámbito de electrodomésticos si podría ser útil, para compartir información, pero en ciber-seguridad, si es factible aplicarla, ya que al estar conectado a internet podría monitorear constantemente los equipos conectados y con ello podrían evitar los ataques cibernéticos.

> Médicos: bajo esta categoría se incluyen básicamente las prótesis para disminuidos físicos. Estas cuentan con sistemas de mando y se adaptan fácilmente

> al cuerpo. Estos robots lo que hacen es suplantar a aquellos órganos o extremidades, realizando sus funciones y movimientos. (Enmanuel, 2024)

Este tipo de robots, sus funciones en general es otorgar movimientos que fueron limitados, a los seres humanos, pero su equipamiento con diferente software es muy limitado inclusive con la inteligencia artificial.

> Teleoperadores: estos robots son controlados de manera remota por un operador humano. A estos artilugios se los utiliza en situaciones extremas como la desactivación de una bomba o bien, para manipular residuos tóxicos. (Enmanuel, 2024)

La inteligencia artificial puede ser muy beneficioso para este tipo de robots, debido a que, al tener mucho riesgo para una persona en desactivar artefactos explosivos, al aplicarse la inteligencia artificial este funciona inclusive para la recopilación de datos y con ello puede determinar si pertenecen los aparatos explosivos a diferentes organizaciones delictivas, ya que también se han involucrado en temas cibernéticos, como el robo de información.

> Poliarticulados: si bien estos pueden tener de diversas configuraciones, lo que tienen en común estos robots es que son sedentarios. Estos son diseñados para mover sus terminales con limitada libertad y de acuerdo a ciertos sistemas de coordenadas. (Enmanuel, 2024)

Estos tipos de robots, son importantes, ayudan a poder determinar si existe algún Ciber ataque y con ello ubicar de manera más rápida de donde proviene, inclusive, si es programado para rastrear, y prevenir el Ciber- delito, aquí cabe que sean utilizados con la

inteligencia artificial, ya que con ello se podría buscar frenar los ataques cibernéticos inclusive podría encontrar a los responsables del ataque

> Zoomórficos: la locomoción de estos robots imita a la de distintos animales y se los puede dividir en caminadores y no caminadores. Estos últimos están aún muy poco desarrollados mientras que los caminadores sí lo están y resultan útiles para la exploración volcánica y espacial**.** (Enmanuel, 2024)

Estos tipos de robots son más utilizados para recabar información y que puedan acceder donde el ser humano no podría, al implementar la inteligencia artificial podría ayudar a recabar información de animales que puedan estar en peligro de extinción, además a ello, puede servir para tenerlos como rastreadores, es decir, los cazadores ilegales al utilizar terminales para comunicarse, estos robots podrían prevenir la caza ilegal, pero para Ciber-Delitos sería muy limitado.

Los diferentes tipos de robots son utilizados para diversas actividades, cabe mencionar, al aplicar la inteligencia artificial, en algunos robots pueden servir para evitar los Ciber-Delitos, pero otros solamente servirán como meros recolectores de información.

Los tipos de robots son avances sólidas para que la cibernética pueda implementarse en ella, pero hay que recordar que la Ciber seguridad está a manos del Estado ecuatoriano, si no existe una normativa especializada, no se puede garantizar que la información para frenar estos tipos de delitos sea efectivo, la falta de norma especializada en relación a los datos personales y sensibles son importantes pero si el Estado no les da la misma importancia como a otras normas les ha dado, su funcionamiento de seguridad cibernética seria obsoleta.

CIBER-SEGURIDAD.

La Ciber seguridad, es determinante al momento que una persona es víctima de un Ciber ataque, su información se pone en peligro por terceras personas que su único fin es apoderarse de la información y ejecutar acciones que vayan en contra de la persona afectada, la seguridad informática es valioso en estos ataques, gracias a ello se puede tener tranquilidad porque se sabe que su fin es proteger la información de una persona y lo ejecuta por medios de diferentes acciones, con el avance de la tecnología, la inteligencia artificial puede ser implementado para que aumente la seguridad informática.

Esta seguridad dentro de la internet por el ámbito personal queda en manos de los usuarios, no obstante, la seguridad en todo ámbito está en manos del Estado ecuatoriano, al no tener una normativa sólida y especializada dentro de la actual norma que es la Ley Orgánica de Protección de Datos Personales, que regule las nuevas herramientas digitales que existen actualmente como lo es la inteligencia artificial y en un futuro, el Estado no está garantizando la protección de la información de las personas nacionales o extranjeras que residen en el país, la seguridad cibernética necesita apoyo del mismo estado para que este logre frenar el aumento de los ataques cibernéticos, con las lagunas legales que existe, en el Ecuador en relación a la protección de la información no está siendo garantizado que no sea vea vulnerando los derechos de las víctimas.

LA TRAÍDA DE LA INFORMACIÓN.

La triada de la información se compone de 3 términos importantes, los estados deben realizar su protección, la triada es la siguiente:

1. Integridad.
2. Confidencialidad
3. Disponibilidad.

Las personas poseen información muy importante, su característica principales que toda su información es personal, la triada tiene un valor intangible e inalienable, los estados al tener la información personal de cada persona, por ejemplo de su patrimonio, esta información constantemente deben ser trasferidas a otras personas para diferentes finalidades legales, y su protección queda en manos del Estado debido a que si no se regulara su tratamiento existiera muchas inconsistencias en el uso de los datos, en el Ecuador tenemos la "Ley Orgánica de Protección de Datos Personales", cuya norma dio su nacimiento en el año 2021, pero falta mucho camino que el legislador debe entender para poder crear normas que sean cien por ciento efectivas, debido a que, las que se tiene actualmente no han servido en su totalidad en la prevención de los ataques cibernéticos, inclusive no existe norma especializada que regule completamente el uso de la inteligencia artificial, una herramienta que ayuda en diferentes ámbitos, sin embargo para el uso de Ciber delitos ha tenido un avance rápido, en cambio sí en el Ecuador existiese una normativa especializada en el cuerpo legal mencionado para su regularización y prevención de Ciber delitos, sería un avance muy importante pero al no tener norma expresa, el uso de la herramienta digital en el caso de Ecuador quedaría generando más vacíos legales que soluciones.

La triada de la información si no se protege con diferentes normas, esta quedaría en un ámbito de riesgo, debido a que la información que se posee puede afectar a la persona, inclusive si no se regula las herramientas digitales ocasiona un gran riesgo, las normas especializas para regular deben estar anexadas al cuerpo normativo para que logre proteger la información y los datos sensibles y los datos personales, en caso de no existir el regalamiento, no se podría efectivizar un mayor control sobre su uso y los datos podrían ser mal utilizados.

Actualmente el problema dela seguridad cibernética dentro del Ecuador es la falta de norma especializada para poder evitar los Ciber- Delitos, con ello el Estado por medio del poder legislativo a previsto normas que regulen el tratamiento de los datos personales y los datos sensibles, pero con la aparición de nuevas herramientas digitales como lo es la inteligencia artificial, el Estado ecuatoriano debe apoyarse y crear normas que regulen su uso para poder evitar y prevenir los Ciber-Delitos, en Ecuador la falta de norma especializada ha sido un problema grave, con ello se podría evitar los Ciber ataques, pero sin norma que lo regule esta más hecho una fantasía que una realidad.

Una vez que hemos analizado algunos conceptos de Ciber seguridad, es preciso entender que es la inteligencia artificial y porque su desarrollo que ha tenido en los últimos años podría servir para prevenir los Ciber delitos si este sería regulado por el Ecuador.

LA INTELIGENCIA ARTIFICIAL.

La inteligencia artificial no tiene una definición exacta, fue creada por el avance de otras tecnologías como lo es el Big Data, el Internet y el Blockchain.

La inteligencia artificial, es un término que no es nuevo para el día de hoy, este ha sido desde siglos atrás una odisea científica, que las maquinas tengan una inteligencia propia, según el matemático Alan Turning, empezaría su investigación dando como inicio con una simple pregunta, ¿ Pueden pensar las maquinas?, con ello sería el inicio de varias investigaciones, desarrollos, por parte de personas especializadas en informática, robótica y sistemas de la computación en poder crear una maquina capaz de pensar por sí misma, capaz de ejecutar actos sin la intervención del ser humano, con ello su historia ha tenido varios logros, que hasta el día de hoy por su avance ya existe aplicaciones con inteligencia artificial, ayudando en tareas cotidianas a cada persona que pueda tener acceso a ellas, y este acceso es tan sencillo con solo tener un celular inteligente.

La inteligencia artificial en los últimos años ha tenido un avance significativo pero así como se emplea para ser una herramienta digital, también lleva consigo riesgos para sus usuarios, de una manera directa debido a que esta herramienta de la inteligencia artificial al utilizar información, puede también ser modificado para cometer diferentes delitos o Ciber-Delitos, en el caso de Ecuador, las sanciones penales y administrativas, solo la tiene el Código Orgánico Integral Penal, única norma en poder sancionar, si hay normativa que sanciona debe existir un cuerpo normativo para que pueda regular el uso y control, en el Ecuador tenemos a la "**Ley Orgánica de Protección de Datos**", esta normativa es impórtate, aquí es donde se establece como los datos de las personas debe ser tratadas sin generar un perjuicio, pero al ser una normativa nueva, el legislativo no le ha dado la importancia que debe tener, con el avance de las tecnologías, esta normativa también debe ser cambiante, con ello puede la normativa regular uso de plataformas y herramientas digitales que utilicen la información personal o datos sensibles y más en específico, que se regule la inteligencia artificial con una normativa especial y cuya finalidad es evitar o prevenir el cometimiento de Ciber-delitos en el Ecuador.

La prevención de Ciber- Delitos, con el uso de la inteligencia artificial sería una herramienta muy eficaz, esta herramienta digital tiene una relación directa con el Blockchain y el Big Data, para la prevención de los ataques cibernéticos, la inteligencia artificial necesita grandes cantidades de información que debe recopilar, por lo cual el Big Data es una parte esencial, al contener mucha información para ejecutar el reconocimiento, rastreo de los datos maliciosos, rastreo e identificación de donde surgió el ataque, etc.

Sin esto la inteligencia artificial no podría ejecutar bien sus funciones, y en relación al Blockchain, necesita la trasferencia de información de una manera rápida y efectiva caso

contrario si no se puede ejecutar la trasferencia de esta información no cumpliría con la finalidad de la prevención de Ciber-Delitos.

Las instituciones del Estado, al almacenar grandes cantidades de información de los ciudadanos, además al poseer datos muy sensibles que si están puestos al ojo público podría causar un daño muy grave al Ecuador en el ámbito internacional por la falta de control de las herramientas digitales y la sanción de los delitos informáticos y recordemos que el más afectado es el ciudadano, al reservar la información y protegerla, también debe proteger de los ciudadanos ecuatorianos y extranjeros que están residiendo en el país, si no se efectúa una correcta protección, no existiera seguridad informática dentro del Estado, se ha previsto que se ejecute diferentes áreas de protección de la información y con el avance de las tecnologías el uso de la inteligencia artificial para la protección de los datos y la prevención de los Ciber delitos.

CARACTERÍSTICAS DE LA INTELIGENCIA ARTIFICIAL PARA LA PREVENCIÓN DE CIBER DELITOS.

1. **La explicabilidad.**

Esta característica es determínate debido a que forma parte de la esencia de la inteligencia artificial, al poseer la información necesaria la misma herramienta digital podrá realizar lo que sería un aprendizaje autónomo, sin la necesidad de intervenir por parte del ser humano para que este sea programado.

La notificación a la persona sobre cómo va a ser tratada su información es relevante, debido a que la información al poseer datos muy delicados pone en riesgo si estos son mal utilizados o alterados para cometer algún tipo de daño, por lo cual la ciber seguridad ha trabajado en ello para que la información no caiga en personas equivocadas.

La inteligencia artificial para la prevención de Ciber delitos no debe vulnerar derechos reconocidos en la constitución, de ser el caso no se cumpliría la finalidad de prevenir los ataques cibernéticos, la importancia de tener una norma especializada para la regularización de la inteligencia artificial ayudara a que se pueda determinar su uso, el tratamiento de la información y con ello para que trabaje a favor de la ciber seguridad.

2. **La autonomía.**

La autonomía es lo que le caracteriza a la inteligencia artificial, al no depender de la intervención constante del ser humano este puede desarrollar por sí misma métodos que ayuden a la tarea a la que ha sido encargado.

Toda la programación que se necesitare por parte de la inteligencia artificial es importante, gracias a ello, puede aprender por sí misma, la autonomía de la inteligencia artificial no solamente queda limitado a programas o a la nube, si no que este puede inclusive interactuar con las personas, es decir ocasionar menoscabo con los seres humanos, con el avance de la robótica se ha ido observando como la inteligencia artificial puede ser implementada en los Androides, con ello se estaría pasando a otros niveles de la interacción del ser humano con la tecnología, sin embargo en lo que radica en temas de Ciber seguridad, para la prevención de Ciber delitos se ha podido determinar tres maneras de aprendizaje de la inteligencia artificial, son métodos conocido que al ser programados dentro de esta tecnología puede ayudar a que se empiece a desarrollar sus capacidades por cuenta propia sin la necesidad de que el ser humano intervenga en cada paso que este avance.

TIPOS DE INTELIGENCIA ARTIFICIAL.

Durante el desarrollo de la inteligencia artificial, se ha podido determinar dos tipos, el primero conocido como el débil y el segundo conocido como el fuerte.

1.1. **Inteligencia artificial Débil.**

Esta inteligencia artificial es conocida por ejecutar acciones que solamente pueden ser programadas por el ser humano, sus acciones que puede desarrollar son limitadas, debido a que necesita un algoritmo programado.

Las acciones que puede ejecutar son:

- Reconocimiento facial
- Reconocimiento de voz
- Identificación de imágenes y,
- Traducción de voz

Este tipo de inteligencia artificial no posee una capacidad de aprendizaje que analizaremos más adelante, este funciona únicamente con la programación para que ejecute tareas en específico.

Para poder entender este tipo de inteligencia artificial es necesario entender que es un algoritmo informático.

2. **ALGORITMO INFORMÁTICO.**

El algoritmo informático seria pieza esencial para que la inteligencia artificial débil cumpla con sus tareas específicas, debido a que, su programación logre identificar ciertas imágenes, voces, caracteres de personas etc.

Para la prevención de los Ciber-Delitos seria vinculado con el Blockchain y el Big Data, al tener que trasferir de manera rápida la información y al tener que poseer grandes cantidades de información, la inteligencia artificial funcionara correctamente, el Ecuador al poder regularizar la inteligencia artificial puede identificar si esta herramienta está siendo utilizada con finalidad de cometer Ciber- Delitos o delitos, con ello se puede

prevenir diferentes ataques cibernéticos o delitos ejecutados de manera física, para poder regular esta herramienta digital se necesita lo que sería una normativa especializada en el cuerpo legal vigente llamado Ley Orgánica de Protección de Datos Personales, al ser la normativa del tratamiento de la información del Ecuador, es preciso señalar que este sea anexado en el cuerpo legal para que así el Ecuador posea seguridad informática dentro del Estado, y una reducción de los Ciber-Delitos o delitos en general.

2.1. **Características del algoritmo informático.**

Los algoritmos informáticos se los caracteriza por lo siguiente:

- No poseer ambigüedad.
- Para resolver la tarea que se ha encomendado tiene unas secuencias que lo permite hacerlo
- Posee la capacidad de ser ordenado, seguir con el procedimiento para poder llegar al resultado de manera efectiva
- La misma secuencia permite que se obtenga el resultado y sea recibido por sí misma.

2.2. **Tipos de algoritmo informático.**

1. Ordenamiento.

Este tipo de algoritmo al ser de ordenamiento, su dimensión utilitaria es poder ejecutar que las búsquedas sean más eficientes, una vez que se encuentra lo que se busca ayuda a que sea de fácil lectura para las personas y para las mismas maquinas que posee la información recabada.

2. Voraces.

Este tipo de algoritmo, emplea los mejores métodos para que pueda obtenerse los mejores resultados en lo que sea programado. Lo negativo de este algoritmo es cuando al tomar

acciones que den los resultados, no toma como datos las acciones ejecutadas anteriores, es decir, que solamente reconoce la última acción ejecutada, y si cambio, el anterior se perderá, por lo general este algoritmo es utilizado solamente para la optimización.

3. Dinámica.

Este tipo de algoritmo es mucho más efectivo debido a que este realiza una división al trabajo encargado, es decir, lo alterna como tarea principal y sub tareas, una vez que la sub tarea es terminada, el algoritmo puede usar las acciones ejecutadas para terminar la sub tarea para culminar la principal, con ello se realiza un ahorro de recursos.

Los algoritmos son mecanismos que sirven a la inteligencia artificial débil para poder ejecutar las tareas que se han encargado a esta herramienta digital, en el mundo de la Ciber seguridad, este tipo de inteligencia artificial, por su nombre "débil", no genera mucho la atención, no obstante al poder estar siempre con la disposición de grandes cantidades de información (Big Data) puede inclusive mejorar su rendimiento, con ello la prevención de los Ciber-Delitos en el Ecuador sería mucho más sencilla, y puede únicamente quedar en el grado del delito como tentativa, la pena sería menor a la total cuando se consume el delito, pero lo importante de prevenir es que no se vulnere la información, sea datos personal o datos sensibles de las personas.

2.3. Inteligencia artificial Fuerte.

Este tipo de inteligencia artificial es muy diferente al débil, esta inteligencia artificial tiene una particularidad que la hace diferente al otro, su principal característica es que puede aprender por sí mismo, este simulara diferentes actividades del ser humano, como la toma de decisiones importantes, analizar las situaciones, inclusive buscar soluciones para resolver problemas cotidianos del ser humano, en otras palabras buscaría simular las acciones de las personas pero con mejores resultados y en poco tiempo.

Ahora abordaremos los tipos de aprendizaje, para poder entender porque el aprendizaje de la inteligencia artificial es superior a la inteligencia artificial débil, al entender los tipos de aprendizaje se entenderá mucho mejor su diferencia entre las dos inteligencias artificiales:

TIPOS DE APRENDIZAJE DE LA INTELIGENCIA ARTIFICIAL

1. LA NEURONA ARTIFICIAL.

Este tipo de neuronas es utilizado por la inteligencia artificial, su función es similar las actuaciones de las neuronas de los seres humanos, a diferencia con estos, transfieren infracción a una gran velocidad para que este pueda funcionar correctamente, su grado de complejidad consiste cuando tiene que ejecutarse de una forma simultánea pero este podrá aprender por sí mismo con el método ensayo y error con este método ya no es necesario que el ser humano intervenga y que la misma inteligencia artificial pueda ejecutar diferentes métodos de Ciber seguridad para prevenir los Ciber- delitos en Ecuador.

2. APRENDIZAJE AUTOMÁTICO.

El aprendizaje automático, es el más utilizado para ejecutar la inteligencia artificial, funciona como el ser humano, se tiene que aprender para poder ejercer las actividades, en palabras concretas se necesita experiencia para poder ejecutar las diferentes actividades que se le ponga en frente, en este caso, se utilizaría el Big Data para que recopile la información de los Ciber delitos y Ciber seguridad y con ello poder emplear lo necesarios para prevenir los Ciber delitos.

Aquí existen dos modelos donde la inteligencia artificial puede ganar experiencia o aprender:

A. Método supervisado.

La inteligencia artificial aprende con la supervisión del ser humano, este le enseña diferentes métodos de aprendizaje para que pueda recabar información sobre cómo debe ejecutarse por sí sola.

B. Método no supervisado.

Este método consiste en dejar por si sola a la inteligencia artificial en que aprenda por su propia cuenta, la inteligencia artificial por su propia cuenta debe entender que acciones son buenas y que acciones son malas, este método es dejar que por sí sola se desarrolle, y con relación a la Ciber seguridad, tendrá en primer plano todo lo que se necesita para que este pueda realizar las tareas de prevención de Ciber delitos.

APRENDIZAJE PROFUNDO.

Este tipo de aprendizaje hace que la inteligencia artificial ejecute grandes cantidades de información, con la ayuda del Big Data y las redes neuronales, con la capacidad de tener la información la inteligencia artificial podría ejecutar diversos métodos de protección de datos y podría inclusive rastrear de manera rápida de donde proviene el atacante que desea obtener de manera ilegal los datos, de diferentes formas podría aprender diversos métodos para cumplir con el objetivo de prevenir los Ciber delitos.

CIBER DELITO.

Hemos podido desarrollar conceptos y análisis de términos que engloba a la inteligencia artificial, cabe mencionar que son los Ciber delitos y la inteligencia artificial lo que buscaría es prevenirlo y así empiece detectar a los responsables de los Ciber ataques.

Definición de Ciber Delito.

La definición de Ciber delito, hablando doctrinariamente no existe una definición concreta, algunos tratadistas han tratado de definir los Ciber delitos.

Los ciber delitos son actos anti jurídicos realizados en el internet, por lo cual, es una persona que está a través de una computadora o un celular inteligente en ejecutar ataques cibernéticos con el único propósito de sustraer la información de la víctima y una vez obtenido la información procede a realizar otros actos que están en contra de la norma jurídica en este caso del Ecuador.

Los delitos informáticos ha sido una nueva forma de amenazar al patrimonio personal de cada persona, añadiendo que ahora lo que se busca a más de afectar el patrimonio de la víctima, es también su imagen, su honor y su intimidad, debido a que los Ciber delitos también van a tratar de poseer los datos sensibles de la víctima y con ello perpetuar diferentes delitos cibernéticos, con el avance del internet los ciber delincuentes han mejorado sus métodos para inducir al engaño y que logran obtener la información, así mismo la ciber seguridad ha tenido avances que han podido frenar estos ciber ataques pero no es su totalidad, cabe mencionar que el internet es un campo abierto y con la llegada de la inteligencia artificial los métodos de los ataques cibernéticos han ido en aumento, con ello la necesidad del Estado ecuatoriano en crear normativa especializada que regule su uso para poder lograr la prevención de los ataques cibernéticos y con ello lograr ubicar a los responsables y que paguen por la conducta antijurídica que realizan por la internet con el uso de las herramientas digitales y dispositivos inteligentes.

Por último, tenemos la Policía Nacional del Ecuador, hace mención a la sustracción de información, para que el ciber delito sea ejecutado de una manera eficaz por el ciber delincuente es necesario que robe primero la información y gracias a ello puede lograr cometer otros diferentes Ciber – Delitos, en el Ecuador no se encuentra tipificado algunos Ciber delitos que provocan un grave daño a nivel personal de la víctima, sea a su patrimonio o directamente a su imagen, con la llegada de la inteligencia artificial los Ciber delitos han sido como renovados, es decir, los ciber delincuentes con las nuevas

tecnologías han ido mejorando sus ataques y con ello la ciber seguridad también se ha tenido que ir adaptando a los nuevos mecanismos empelados por las personas que han estado ejecutado actuaciones con el único fin de generar daño ye n algunos casos este daño no puede ser sancionado por la falta de tipificación de los Ciber- Delitos o por el simple hecho que los atacantes han tendió que usar diferentes métodos de software para borrar su rastreo, por ende cabe aplicar en el Ecuador una normativa especialidad que regule y controle el uso de la inteligencia artificial cuyo fin será la prevención de los Ciber- Delitos.

LOS CIBER- DELITOS MÁS COMUNES EN ECUADOR.

a) **Estafas Cibernéticos.**

La estafa informática se realiza cuando el atacante cibernético induce al error a la víctima y con ello logra beneficiarse económicamente, a diferencia con la estafa común, este tipo de estafa, provoca que la víctima entregue valores económicos con la promesa que se entregue valores más altos.

Existen dos métodos para que se consuma este delito, y son:

Ciber- Delito.	**Explicación del Ciber- Delito.**
Carding	Este Ciber – delito, consiste cuando el atacante ha obtenido la información de las tarjetas de crédito y con ello empieza a generar compras de bienes muebles e inmuebles, sin embargo, el daño más potencial de este ataque cibernético es cuando la información es vendida a otras

	personas con el único fin de afectar a la víctima de una manera gravosa a su patrimonio. El método para robar la información es casi similar al Pishing pero esta consiste en la venta falsa de productos en línea, un ejemplo claro es en el mundo de los videojuegos en línea, las victimas por lo general son los menores de edad, por sacar más ventaja en el juego ingresan a sitios web falsos y otorgan la información de las tarjetas de sus padres o representantes y aquí es donde empieza el problema para las víctimas, sin saber se realizan compras a una magnitud grande que han dejado con deuda impagable, el sistema legal a detectado este Ciber-Delito y con ello ha preservado que en caso de robo o ataque cibernético a las cuentas bancarias, la deuda adquirida no sea cobrada, pero en algunos casos las víctimas no han podido recuperar inclusive su dinero ahorrado.

Pishing.	Este delito consiste en el robo de la información, por lo general se hacen pasar por empresas reconocidas de la ciudad con el único fin de engañar a la víctima y entregue sus datos. Los Ciber delincuentes a más de robar la información, por lo general siempre se acompaña con un software malicioso con el único fin de persuadir a la víctima y que no se percate que su información ha sido robada, con ello genera un estado de intriga y miedo a la víctima, y para concluir los ataques cibernéticos, el delincuente empieza a enviar mensajes extorsivos o simplemente roba el patrimonio de la víctima.

Fuente: Elaboración propia.

b) **Delitos informáticos de daños.**

Ciber- Delito	**Explicación de Ciber- Delitos.**
Pharming	Este tipo de malware es engañar a la víctima pero con páginas de web reales o paginas reales de diferentes empresas, cabe mencionar que al tener un malware

	en su método de ataque ya es considerado dañino, debido a que sustrae la información de la víctima, luego de haber robado la información este empieza a destruir los archivos del computado afectado, generando más daños a la víctima y con ello perjudicando de una manera muy gravosa, cabe mencionar que la información que se roba por parte de los ciber delincuentes pueden ser vendido a terceras personas que pueden generar perjuicios más graves de lo que ya fueron afectados las víctimas.
Ransomware.	Este ataque cibernético es uno de los más agresivos para las víctimas, debido a que este ataque secuestra toda la información de la persona además a ello, bloquea completamente la computadora afectada, y para solucionar este problema la victima debe trasferir un valor económico para que el atacante elimine el virus en la computadora, su riesgo mayor es, para poder realizar el pago para la recuperación de la información y de la computadora se

	necesita acceder a varios enlaces de internet, pero cuyos enlaces solo se lo hace atravesó de la web oscura o Dark Web, aumentado el riesgo de ser nuevamente atacado por otro Ciber-delincuente, como tal este ataque informático es uno de los más peligrosos y agresivos.
Malware.	Los malware consisten en virus que su único fin es robar la información y posterior a ello dejar rastro con la destrucción de la información robada a la víctima, su propagación es muy sencilla, la simple descarga de archivos en internet ya puede ser víctima de cualquier tipo de malware.

Fuente: Elaboración propia.

CIBER DELITOS QUE AFECTAN AL DERECHO A LA INTIMIDAD.

Ciber- Delito	**Explicación del Ciber- Delito**
Ciber-Acoso.	Estés tipo de delitos afectan directamente a los datos sensibles de la víctima, una vez que el atacante ha tomado de manera ilícita sus datos sensibles, este efectúa

	otros tipos de Ciber delitos, en el Ecuador se encuentra tipificado la extorsión sexual, delitos que afectan directamente a la intimidad de la persona y al ser consumado el delito afecta también a la integridad sexual de la víctima, en la definición se hace mención a dos Ciber delitos, cabe mencionar que el Estado ecuatoriano no se encuentran tipificados, lo más cercano que tenemos es al delito mencionado extorsión sexual.

Fuente: Elaboración propia.

TRATAMIENTO DE LA INFORMACIÓN EN EL ECUADOR.

En el Ecuador, existe la Ley Orgánica de Protección de Datos Personales, en el artículo 7 del cuerpo legal mencionado establece lo siguiente:

> Art. 7.- Tratamiento legítimo de datos personas.- El tratamiento será legítimo y lícito si se cumple con alguna de las siguientes condiciones:1) Por consentimiento del titular para el tratamiento de sus datos personales, para una o varias finalidades especificas;2) Que sea realizado por el responsable del tratamiento en cumplimiento de una obligación legal;3) Que sea realizado por el responsable del tratamiento, per orden judicial, debiendo observarse los principios de la presente ley;4) Que el tratamiento de datos personales se sustente en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos

> conferidos al responsable, derivados de una competencia atribuida por una norma con rango de ley, sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta ley y a los criterios de legalidad, proporcionalidad y necesidad;5) Para la ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento de datos personales, encargado del tratamiento de datos personales o por un tercero legalmente habilitado;6) Para proteger intereses vitales, del interesado o de otra persona natural, como su vida, salud o integridad;7) Para tratamiento de datos personales que consten en bases de datos de acceso público; u,8) Para satisfacer un interés legítimo del responsable de tratamiento o de tercero, siempre que no prevalezca el interés o derechos fundamentales de los titulares al amparo de lo dispuesto en esta norma. (Ley Organica de Proteccion de Datos Personales, 2025)

Este articulado establece que, se necesita el consentimiento del titular de los datos o información personal, con el fin de que el titular pueda saber cómo serán tratados sus datos e información.

La persona quien necesite de la información o datos personales de otra persona, deberá notificarla o darle aviso para que acepte o niegue sobre el tratamiento de sus datos que se vayan a usar.

El tratamiento a darse puede ser de diferentes maneras, si la persona que va a utilizar la información de otra, realiza actos que no fueron conectados por el titular, recae a una violación de sus derechos, mas entornados a los datos, intimación y derechos constitucionales como lo son a la imagen, intimidad, honor, etc.

El legislador ha previsto que se realice una separación de los tratamientos de los datos personales con los sensibles, en el artículo 26 tenemos lo siguiente:

> Art. 26.- Tratamiento de datos sensibles. - Queda prohibido el tratamiento de datos personales sensibles salvo que concurra alguna de las siguientes circunstancias: a) El titular haya dado su consentimiento explícito para el tratamiento de sus datos personales, especificándose claramente sus fines.b) El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral y de la seguridad y protección social.c) El tratamiento es necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento.d) El tratamiento se refiere a datos personales que el titular ha hecho manifiestamente públicos. e) El tratamiento se lo realiza por orden de autoridad judicial.f) El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.g) Cuando el tratamiento de los datos de salud se sujete a las disposiciones contenidas en la presente ley. (Ley Organica de Proteccion de Datos Personales, 2025)

Este articulo menciona sobre la importancia de cómo deben ser tratados los datos sensibles, por con la única excepción que necesita autorización judicial, con ello el legislador a previsto que, antes de darle el tratamiento los datos sensibles, el juez debe conocer cómo serán tratados, el juez debe verificar que el tratamiento no vulnere derechos constitucionales.

En los artículos siguientes, hace mención al tratamiento de los datos de personas fallecidas, de salud, datos crediticios.

Este cuerpo legal solamente hace mención al tratamiento de los datos personales y sensibles, pero su tratamiento, por más que se dé el consentimiento del titular o la autorización judicial, no es susceptible que no sea víctima de algún Ciber- delito.

¿LAS SANCIONES QUE ESTABLECE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EVITA LOS CIBER-DELITOS?

En la normativa vigente, desde el articulado 67 al 74, únicamente menciona las sanciones, administrativas para servidores públicos y privados, refiriéndose únicamente cuando, existe el mal tratamiento de la información personal y sensible de cada persona que ha otorgado su consentimiento para entregar la información, sin embargo, para prevenir los Ciber- Delitos en el Ecuador no se encuentra positivado, con ello las sanciones y medidas correctivas que está establecido en el cuerpo legal no es suficiente para la prevención de los Ciber- Delitos en Ecuador.

La inteligencia artificial es una herramienta digital que puede servir para la prevención de los Ciber-Delitos, con la programación y los algoritmos correctos y necesarios se vuelven una pieza fundamental para la prevención y protección de la información de cada persona, y la misma ayudaría a identificar a los posibles responsables del ataque informático.

La falta de normativa para la regularización de la inteligencia artificial ha provocado lagunas legales que al momento de encontrar a los responsables, es prácticamente nula, por lo cual, al no regular una herramienta eficaz como lo es la inteligencia artificial, el Ecuador seguirá siendo un Estado en donde no se compromete en evitar el cometimiento de Ciber-Delitos, inclusive tampoco tipifica delitos informáticos, que en caso que una

persona sea víctima es muy gravosa de manera personal, poniendo en riesgo la información.

CAPÍTULO 2.

Objetivo de aprendizaje:

En este capítulo se realizará el análisis de los bienes jurídicos protegidos que son vulnerados en los delitos informáticos, y realizaremos un breve análisis de cada uno de ellos debido a la gran importancia que tienen ya que, la víctima del Ciber-Delito al tratarse de sus datos sean personales o sensibles, ocasiona un gran perjuicio ya que no solo va a afectar a un solo derecho, sino que estos están conexos con otros.

En el capítulo uno hemos realizado el análisis de conceptos en materia de seguridad, ciber seguridad y de la normativa vigente que es la Ley Orgánica de Protección de Datos Personales, para poder determinar la necesidad de la creación de una normativa especial que regule la inteligencia artificial para la prevención de Ciber-Delitos, en este capítulo es preciso hablar sobre el bien jurídico protegido y que normativa actual que se encuentra en el Código Orgánico integral Penal, sanciona y garantiza la protección del bien jurídico en el ámbito de la informática.

EL BIEN JURÍDICO PROTEGIDO.

El bien jurídico protegido dentro del campo del derecho es importante, en cualquier momentos si existe alguna vulneración este ocasiona un grave daño a nivel personal, en el campo del derecho informático no es la excepción, la inteligencia artificial con su gran avance se ha tenido que ir vinculando con el derecho penal, debido a que la conducta penalmente relevante no queda solo con actos meramente físicos o verbales, sino también se expande por medio del uso de las herramientas digitales como la inteligencia artificial.

Los ciber delincuentes necesitan primero recopilar la información y lo realizan por medio de los ataques cibernéticos al logran su cometido, con la información sustraída abre más el campo de acciones de los ciber delincuentes, con el único fin de generar daños al patrimonio de la víctima, y con ello se ve afectado el bien jurídico protegido.

En el Ecuador, el derecho penal protege el bien jurídico, esto se lo puede entender la forma en la que el Estado va a garantizar la protección los derechos de los ciudadanos que posee, por ejemplo la vida, la libertad, la propiedad privada entre otros, en esta investigación nos centraremos únicamente al bien jurídico protegido que son vulnerados a las víctimas en los Ciber- Delitos, la información que es sustraída, alterada o modificada para provocar robo de patrimonio o afectar a la imagen de la persona a nivel personal es muy gravoso.

El bien jurídico protegido es importante y valioso debido a que son derechos intangibles e inalienables, con ello el Estado ecuatoriano debe garantizar su protección y evitar que terceras personas vulneren estos derechos.

La necesidad de tipificar los delitos es para proteger el bien jurídico, con ello es fácil observar que, si no hay delito, no hay sanción, a ello no hay la protección y seguridad que debe otorga el Estado en relación a la información de cada persona, esto nos hace entender que, se necesita de la norma para garantizar la protección de los derechos de la persona en relación a la información.

Para poder analizar y entender cuál es el bien jurídico protegido en estos Ciber-Delitos debemos recapitular primero todos los delitos informáticos tipificados en el Ecuador.

Delitos informáticos tipificados en el Código Orgánico Integral Penal.

En el Código Orgánico Integral Penal, es necesario hacer una recapitulación de los delitos informáticos, y estos son:

Art. 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.- La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años**.** (Codigo Organico Integral Penal, 2025)

Art. 178.- Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley. (Codigo Organico Integral Penal, 2025)

Art. 186.-Estafa.- (Reformado por el Art. 2 de la Ley s/n, R.O. 598-3S, 30-IX 2015; y por el Art. 42 de la Ley s/n, R.O. 107-S, 24-XII-2019).- La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años. La pena máxima se aplicará a la persona que: 1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario. 2. Defraude mediante el uso de dispositivos

electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares. 3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica. 4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento. 5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor. 6. (Agregado por el Art. 41 de la Ley s/n, R.O. 107-S, 24-XII-2019). - A través de una compañía de origen ficticio, induzca a error a otra persona, con el fin de realizar un acto que perjudique su patrimonio o el de un tercero. La persona que perjudique a más de dos personas o el monto de su perjuicio sea igual o mayor a cincuenta salarios básicos unificados del trabajador en general será sancionada con pena privativa de libertad de siete a diez años. La estafa cometida a través de una institución del Sistema Financiero Nacional, de la economía popular y solidaria que realicen intermediación financiera mediante el empleo de fondos privados, públicos o de la Seguridad Social, será sancionada con pena privativa de libertad de siete a diez años. La persona que emita boletos o entradas para eventos en escenarios públicos o de concentración masiva por sobre el número del aforo autorizado por la autoridad pública competente, será sancionada con pena privativa de libertad de treinta a noventa días. Si se determina responsabilidad penal de una persona jurídica, será sancionada con multa de cien a doscientos salarios básicos unificados del trabajador en general**.** (Codigo Organico Integral Penal, 2025)

Art. 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la

transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes (Codigo Organico Integral Penal, 2025)

Art. 191.- Reprogramación o modificación de información de equipos terminales móviles. - La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años. Art. 192.- Intercambio, comercialización o compra de información de equipos terminales móviles. - La persona que intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años. Art. 193.- Reemplazo de identificación de terminales móviles. - La persona que reemplace las etiquetas de fabricación de los terminales móviles que contienen información de identificación de dichos equipos y coloque en su lugar otras etiquetas con información de identificación falsa o diferente a la original, será sancionada con pena privativa de libertad de uno a tres años**.**Art. 194.- Comercialización ilícita de terminales móviles. - La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de

telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. Art. 195.- Infraestructura ilícita. - La persona que posea infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil, será sancionada con pena privativa de libertad de uno a tres años. No constituye delito, la apertura de bandas para operación de los equipos terminales móviles (Codigo Organico Integral Penal, 2025)

Art. 229.- Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años**.** (Codigo Organico Integral Penal, 2025)

Art. 230.- Interceptación ilegal de datos. - (Sustituido por el Art. 12 de la Ley s/n R.O. 526- 4S, 30-VIII-2021). - Será sancionada con pena privativa de libertad de tres a cinco años: 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma, contenido digital en su origen, destino o en el interior de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales. 2. La persona que ilegítimamente diseñe, desarrolle, ejecute, produzca, programe o envíe contenido digital, códigos de accesos o contraseñas, certificados de

seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente al que quiere acceder. 3. La persona que posea, venda, distribuya o, de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos, dispositivos electrónicos, programas u otros contenidos digitales destinados a causar lo descrito en el número anterior. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos, o programas o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior**.** Art. 231.- Transferencia electrónica de activo patrimonial. - La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona**.** (Codigo Organico Integral Penal, 2025)

Art. 232.- Ataque a la integridad de sistemas informáticos.- (Sustituido por el Art. 13 de la Ley s/n R.O. 526-4S, 30-VIII-2021).- La persona que destruya, dañe,

borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseado, o suprima total o parcialmente contenido digital, sistemas informáticos, sistemas de tecnologías de la información y comunicación, dispositivos electrónicos o infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general, con el propósito de obstaculizar de forma grave, deliberada e ilegítima el funcionamiento de un sistema informático, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos, programas o sistemas informáticos maliciosos o destinados a causar los efectos señalados en el primer inciso de este artículo. 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**.** (Codigo Organico Integral Penal, 2025)

Art. 233.- Delitos contra la información pública reservada legalmente. - La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de

> mayor gravedad**.**Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. (Sustituido por el Art. 14 de la Ley s/n R.O. 526-4S, 30-VIII-2021). - 1. La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho sobre dicho sistema, será sancionada con la pena privativa de la libertad de tres a cinco años. 2. Si la persona que accede al sistema lo hace para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a las o los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años**.** En el Código Orgánico Integral Penal se encurta tipificado en un total de 15 Ciber-Delitos, lamentablemente hay delitos que todavía no se encuentran tipificados, estos delitos lo mencionamos en el capítulo uno, delitos cibernéticos que de igual manera afectan a la información de la víctima y a otros derechos conexos, con ello se puede denotar los vacíos legales en relación a la protección del bien jurídico de las víctimas, al no tener tipificado el delito informático su protección queda en manos de los ciber delincuentes que lograron sustraer la información. Una vez que hemos analizado conceptos del bien jurídico protegido, determinaremos cuales son los bienes jurídicos que son afectados cuando una persona es víctima de este tipoi de delitos. (Codigo Organico Integral Penal, 2025)

LOS BIENES JURÍDICOS PROTEGIDOS AFECTADOS POR LOS CIBER-DELITOS.

El ámbito del derecho penal es proteger el bien jurídico de cada persona sea individualmente o colectivamente, en el campo del derecho informático no es la

excepción, debido a que también existe el bien jurídico que de igual manera al ser afectado provoca un daño grave a la víctima, todo esto cometido por los Ciber delincuentes, de tal manera que el derecho penal se ve involucrado en la protección del bien jurídico protegido pero en el ámbito informático, a continuación analizaremos cuales son el bien jurídico protegido afectados por los Ciber-Delitos:

La información.

En el derecho informático la información se lo podría considerar el bien jurídico protegido más afectado en general, la información es entendía como el conjunto de datos que forma parte de la persona natural o jurídica, en el campo del derecho existe los derechos tangibles e intangibles, por lo cual el Estado debe brindar la protección de estos derechos, pero con la información hay que darle un trato diferente, al ser intangible este no podrá ser tratado como los tangibles, pero su protección es esencial con las conductas penalmente relevantes para poder ser sujeto de sanción, su protección es vital.

La información al ser el bien jurídico protegido que es considerado el más vulnerado a nivel general, también existen otros que se vinculan a la información y tenemos los siguientes bienes jurídicos protegidos afectados de igual manera por los Ciber-Delitos:

El patrimonio.

El patrimonio es un derecho que también se encuentra sujeto a vulneraciones, como se especifica en la cita, no es necesario que el patrimonio solamente forme parte de lo tangible, si no también existe patrimonio intangible como los derechos de autor, también el dinero digital, etc.

Al tratarse del patrimonio, es susceptible a que su información sea borrada o sustraída por lo cual el Estado ecuatoriano debe velar por la Ciber seguridad de cada persona, sea individual o colectivamente, al ser el patrimonio sujeto de vulneración se debe tener más

cuidado al momento de entregar la información en páginas de dudosa existencia o simplemente no entregar a terceras personas.

La intimidad, reserva, y confidencialidad de los datos.

La intimidad.

El derecho a la intimidad es una parte esencial de cada persona, como expresa el autor, la intimidad ayuda al desarrollo de la persona, en los Ciber-Delitos, la vulneración de la intimidad es dañino para la víctima, al divulgar información sensible genera daños en el ámbito social, en lo personal inclusive puede generar problemas psicológicos.

En el Ecuador ya se encuentra establecido una sanción para quien vulnere el derecho a la intimidad, sin embargo esta investigación trata de establecer la necesidad de crear una normativa especializa que regule la inteligencia artificial para prevenir los Ciber-Delitos, con ello, no cumple lo que se ha expresado en el capítulo uno que es, antes de la sanción debe haber una prevención, por lo cual al prevenir los Ciber-Delitos, el índice de robo de datos sensibles bajaría a unas cifra considerable, siempre y cuando exista la norma positivada, caso contrario solo se podría establecer la sanción, pero en delitos informáticos encontrar a los responsables ya es una tarea muy difícil de ejecutar.

Reserva.

La reserva consiste en que la información no es catalogada para acceso público, es decir, es la información que ciertas personas pueden poseer, siempre y cuando el titular de la misma los autorice, esta información para los Ciber delincuentes es muy deseado debido a que saben el potencial riesgo de su exposición a l público y con ello para poder afectar a la persona solicitan mediante sus ataques recompensas económicas para que las personas paguen por ella para que se devuelva la información, lamentablemente este tipo

de recuperación de la información no garantiza que el atacante lo siga poseyendo, existe circunstancias cuando se ha realizado los pagos pero de igual manera la información sale a dominio público.

Este derecho va ligado también con la intimidad y la confidencialidad de los datos, como se explicó su publicación a dominio público es muy dañina y a pesar de realizar los pagos a los ciber delincuentes no es una garantía que la información pase a manos de terceros y con ello generar lo que sería el perjuicio a la víctima.

Seguridad en el Tráfico Jurídico.

Los negocios que son susceptibles a derecho, con el avance de las tecnologías se ha presentado que los contratos ya no son necesarios la presencia de las partes para la firma del contrato o negocio, al existir la firma electrónica ha facilitado los negocios de diferentes distancias, sin embargo al ser información que posee datos de las partes contratantes o negociadores se considera delicados, el ciber delincuente al momento de poseer la información por medio de un ataque cibernético, existe el riesgo que la información sustraída sea vendida a terceras personas.

La propiedad.

La propiedad en el ámbito del derecho se lo puede entender como los bienes muebles e inmuebles y los tangibles y los no tangibles, reconocidos en el Código Civil del Ecuador, al tratarse de la información se lo considera intangible por lo cual, el derecho a estimado su protección por medio de la acción punitiva del Estado, sin embargo, el Ecuador al no poseer delitos ignoranticos tipificados, existe el riesgo de la vulneración de los derechos informáticos de cada persona.

Los bienes jurídicos protegidos son valiosos e importantes para cada persona, su vulneración es dañina para la víctima.

La vulneración de un derecho informático esta concadenada con otros derechos, la vulneración de un solo derecho acarrea la vulneración de otros derechos reconocidos constitucionalmente.

La implementación de una normativa especializada en el cuerpo legal, Ley Orgánica de Protección de Datos Personales, es necesaria para poder regular de la inteligencia artificial y con ello poder prevenir los Ciber- Delitos en el Ecuador, recordemos que si no hay delitos tipificados la prevención será mejor que la sanción, y al evitar que se consuma el delito se protege de mejor manera la información y con ello se lograría incluso una ciber seguridad eficiente y eficaz.

CAPÍTULO 3.

Objetivo de aprendizaje:

En este capítulo vamos analizar un cuerpo legal internacional promulgado y aprobado por la Unión Europea, sobre la regularización de la inteligencia artificial, esta herramienta digital ha tenido un desarrollo muy fuerte y con ello nace la necesidad de regularla para evitar que se vulnere derechos de los usuarios, y con ello garantizar su protección.

Analizaremos la legislación chilena debido a que posee un proyecto de ley que fue aprobado y se encuentra en pleno desarrollo, de igual manera con la Unión Europea, es en base al regalamiento de la inteligencia artificial, con la finalidad de poder aumentar la Ciber seguridad en el Estado de Chile y con ello disminuir los ataques informáticos.

Se realizaría el análisis comparativo con la legislación ecuatoriana.

LEGISLACIÓN COMPARADA.

Unión Europea.

La Unión Europea en la pasada fecha, 13 de Marzo del año 2024, entro en vigencia la ley de la inteligencia artificial, cuyo promotor y aprobación fue la Unión Europea, los Estados miembros dio el primer paso en regular la inteligencia artificial debido a que su desarrollo se lo ha visto de una manera acelerada, por lo cual se tuvo la necesidad de plantear diferentes limitaciones en su desarrollo y también en el ámbito de la Ciber seguridad, se planteó acciones cuyo uso únicamente debe ser el adecuado y se adecuo la norma que identifique a las personas que utilicen la inteligencia artificial para cometer ciber delitos y con ello, cada Estado deberá tipificar las sanciones correspondientes.

Las limitaciones que se ha establecido en la ley de la unión europea son en relación al riesgo, lo ha establecido de la siguiente manera: alto, mediano, bajo e inaceptable.

Al platear las limitaciones a la inteligencia artificial ya se está formando a esta herramienta en que sea utilizado de una manera ética y moralmente correcto, al regular ayuda a prevenir que esta herramienta digital sea utilizado para el cometimiento de los ciber delitos, un ejemplo claro que tenemos de un ciber delito con uso de inteligencia artificial es el Deep Fake, usa la fotografía de una persona y se puede crear videos de índole sexual afectando varios bienes jurídicos que hemos hablando en el anterior capitulo, con la normativa ya vigente esto es imposible de hacer, debido a que este sistema informático lo que se busca es que respete los derechos fundamentales y no los vulnere.

La unión europea al tener regulado esta herramienta digital, ayuda a que ciertos delitos informáticos que empleen la inteligencia artificial no sean ejecutados, dando como resultado una disminución de este tipo de delitos, cabe mencionar que su uso de esta herramienta digital por cualquier persona ya sería controlado y quien pretenda darle un

uso ilegal a la misma se podrá identificar al pretendiente del delito y que los estados miembros determine las sanciones correspondientes.

Distinción de la Normativa Ecuatoriana frente a la ley de inteligencia artificial de la Unión Europea.

En el Ecuador tenemos la Ley Orgánica de Protección de Datos Personales, cuya finalidad de la normativa se encuentra en su artículo 1.

La finalidad del cuerpo legal es en garantizar el ejercicio de los datos personales y su información, que en artículos más siguientes mencionan sobre que tratamiento deben darse y como este si se incurre que a la persona que se ha otorgado la información mal utilizo o vulnero derechos al ciudadano acarreara una responsabilidad y la normativa provee algunas sanciones que se pueden ejecutar en contra del responsable y en caso de incurrir a un delito debemos remitirnos al Código Orgánico Integral Penal.

Esta normativa únicamente menciona sobre el tratamiento de los datos personales, sin embargo en sus ochenta y tres artículos en ninguno de ellos menciona sobre la regularización de la inteligencia artificial, lamentablemente en el Ecuador al no tener normativa expresa sobre su uso, desarrollo y control, se tiene la facilidad de crear diferentes contenidos que vulnere los derechos de los ciudadanos en el ámbito informático y con ello se abre las puertas a los Ciber- Delincuentes en crear otros métodos para atacar a la información.

Si al existir un control de la inteligencia artificial en el Ecuador, este a más de prevenir que se use esta hermetizan digital para cometer Ciber-Delitos, podría ser utilizado para la prevención de otros tipos de delitos sea en lo informático como en lo físico.

El Ecuador no cuenta con normativa que regule esta inteligencia artificial, a diferencia que la Unión Europea, sus estados miembros al crear una normativa nueva, este de inmediato se implementa en cada Estado.

En el siguiente capítulo hablaremos sobre como la implementación de la inteligencia artificial en seguridad es efectivo, esto ocurrió en la ciudad de Cuenca, esta información la profundizaremos en el síguete capitulo, sobre cómo afectaría en el entorno social su implementación.

Legislación Chilena.

En la legislación de chile, desde el año 2023, se presentó un proyecto de ley que tiene como finalidad la creación de una normativa para la regularización de la inteligencia artificial, la normativa se denomina

"POLÍTICA NACIONAL DE CIBERSEGURIDAD 2023-2028" (Biblioteca del Congreso Nacional, 2023).

Esta normativa publica que se encuentra en creación hasta el año 2028, el Estado de Chile ha empezado a establecer las bases de la regularización de esta herramienta digital en el continente latino americano, teniendo como referencia la ley aprobada por la Unión Europea, con bases de esta normativa que es nueva, se ha planteado cinco objetivos que se pretende cumplir con la creación de esta normativa y son:

Infraestructura resiliente: El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad y de desastres socioambientales, bajo una perspectiva de gestión de riesgos. (Biblioteca del Congreso Nacional, 2023)

Este objetivo que se plantea, es la adaptación de las diversidades que se puede presentar en este caso seria, las situaciones en relación a la ciber seguridad, por lo cual, con la creación de la normativa se permite determinar que en caso de un ciber ataque, se analice y se actué de una manera correcta para poder minimizar los daños informáticos que pudo haber ocasionado el ataque y con ello lograr realizar las investigaciones para que este pueda identificar a los responsables, cabe mencionar que la cooperación internacional seria pieza clave debido a que ciertos delitos informáticos son cometidos en otros estados, y al lograrse identificar al ciber delincuente, se contiene con el debido proceso para determinar la responsabilidad.

Derechos de las personas: El Estado protegerá y promoverá la protección de los derechos de las personas en Internet, a través del fortalecimiento de la institucionalidad existente en materia de ciberseguridad; y de la generación, adopción, y promoción de los mecanismos y las herramientas tecnológicas necesarias para que cada persona pueda integrarse a la sociedad y desarrollarse y expresarse plenamente. (Biblioteca del Congreso Nacional, 2023)

La protección de los derechos reconocidos en la constitución quedan en manos del Estado, en el capítulo uno se habló sobre la responsabilidad que tiene el Estado en relación a la seguridad y la ciber seguridad, el estado chileno lo que lograra es intensificar la protección en la red o el internet para cada usuario, y al otorga a las diferentes instituciones públicas mejoraría la ciber seguridad, y con ello brindaría a los ciudadanos la protección de sus derechos y que puedan navegar y ejercer sus derechos en las redes sociales como la libre expresión sin tener alguna afectación negativa en sus derechos constitucionales.

Cultura de ciberseguridad: Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas, responsabilidad en el manejo de tecnologías digitales, y

promoción y garantía de los derechos de las personas. (Biblioteca del Congreso Nacional, 2023)

El Estado de Chile, para poder garantizar la prevención de los Ciber-Delitos en su Estado, no solo provee que se implementa el uso de herramientas digitales, sino que también, el conocimiento en las aulas y en las persona que por general utilizan la internet, deben tener en cuenta los riesgo que puede existir al momento de otorga su información a diferentes páginas de internet o aplicaciones móviles, por lo cual crear conciencia en la prevención de los Ciber-Delitos con el único fin de evitar más víctimas en este tipo de delitos.

> Coordinación nacional e internacional: El Estado creará una gobernanza pública para coordinar las acciones necesarias en ciberseguridad. Los organismos públicos y privados crearán, en conjunto, instancias de cooperación con el propósito de comunicar y difundir sus actividades en ciberseguridad, evitar la duplicación de trabajo y pérdida de recursos, y hacer eficientes los esfuerzos en esta área.

En el ámbito internacional, el Estado se coordinará con países, organismos, instituciones y otros actores internacionales para permitir a nuestro país enfrentar de mejor manera las actividades maliciosas e incidentes en el ciberespacio. (Biblioteca del Congreso Nacional, 2023)

Se mencionó en el punto uno, la cooperación internacional es importante al momento de prevenir y sancionar este tipo de delitos, con el apoyo internacional aumenta las actuaciones de manera eficaz para prevenir que se siga vulnerado los bienes jurídicos protegidos, y con ello aumentando la Ciber seguridad del Estado, en caso de lograr identificar a los responsables, con la ayuda internacional se lograría inclusive que el responsable sea sancionado.

La inteligencia artificial jugaría un papel importante al momento de prevenir los delitos ignoranticos, y con la cooperación internacional se lograría que por medio del uso del Big

Data y el Blockchain se logre en manera constante la actualización de los diferentes delitos informáticos y con ello prevenir que se vuelva a repetir estos delitos.

> Fomento a la industria y la investigación científica: El país promoverá el desarrollo de una industria de la ciberseguridad, que proteja a las personas y las organizaciones y que sirva a sus objetivos estratégicos. Para ello, fomentará la focalización de la investigación científica aplicada en temas de ciberseguridad, acorde a las necesidades del país. (Biblioteca del Congreso Nacional, 2023)

La investigación es parte esencial del desarrollo informático, las instituciones públicas y privadas al tener en conjunto una normativa que logre aportar a su estudio y desarrollo es una fuente fiable y la Ciber seguridad aumentaría en el país latino americano, con este proyecto de ley en progreso hasta su entrada en vigencia que es el año 2028, tendrá mayor capacidad de regular la inteligencia artificial y proteger los bienes jurídicos de cada ciudadano que este residiendo en Chile y otorgar una seguridad en la internet a cada usuario.

La ley que se encuentra en progreso en la legislación chilena estableció algunos principios principales que se deben seguir con estricta observancia, los principios son los siguientes:

> a) intervención y supervisión humana; b) solidez y seguridad técnica; c) privacidad y gobernanza de datos; d) transparencia y explicabilidad; e) diversidad, no discriminación y equidad; f) bienestar social y medioambiental; g) rendición de cuentas y responsabilidad; *h*) Protección de los derechos de los consumidores**.** (IAPP, 2024)

Los principios que recoge el proyecto de ley, en su literal d, en el capítulo 1 ya se habló sobre la explicabilidad, la intervención humana dentro del desarrollo de la inteligencia artificial y el respeto de estos principios son fundamentales para que se logre optimizar

su desarrollo y que este pueda ejecutarse de una manera correcta sin existir vulneraciones a los derechos reconocidos constitucionalmente.

Sistemas de la inteligencia artificial clasificadas.

El proyecto de ley que se encuentra en desarrollo, de igual manera con la ley de la inteligencia artificial de la Unión Europea, ha clasificado los sistemas de la inteligencia artificial y son a continuación:

> Sistemas de IA de riesgo inaceptable: aquellos sistemas de IA incompatibles con el respeto y garantía de los derechos fundamentales de las personas, por lo que su introducción en el mercado o puesta en servicio se encuentra prohibida. Algunos ejemplos son: sistemas de manipulación subliminal; aquellos que explotan vulnerabilidades de las personas para generar comportamientos dañinos; aquellos de categorización biométrica de personas basadas en datos personales sensibles; aquellos sistemas de calificación social genérica; aquellos sistemas de identificación biométrica remota en espacios de acceso público en tiempo real; aquellos sistemas de extracción no selectiva de imágenes faciales; y los sistemas de evaluación de los estados emocionales de una persona. (IAPP, 2024)

> Sistemas de IA de alto riesgo: aquellos sistemas de IA autónomos o componentes de seguridad de productos que puedan afectar negativamente a la salud y la seguridad de las personas, sus derechos fundamentales o el medio ambiente, así como los derechos de los consumidores, especialmente si fallan o se utilizan de forma impropia. Estos sistemas son permitidos cumpliendo las reglas contenidas en el artículo 8º del proyecto, así como otras obligaciones de seguimiento posterior a su comercialización. (IAPP, 2024)

> Sistemas de IA de riesgo limitado: aquellos sistemas de IA que presentan riesgos no significativos de manipulación, engaño o error, producto de su interacción con personas naturales. Se permite su comercialización, en cuanto cumpla con obligación de transparencia en sistema de IA contenida en el artículo 12º, que indica que se informe de manera clara, inteligible y oportuna a las personas naturales expuestas a un sistema de IA que están interactuando con esta tecnología. (IAPP, 2024)

Sistemas de IA sin riesgo evidente: todos los demás sistemas de IA que no entran en las categorías mencionadas anteriormente (IAPP, 2024)

La clasificación de la inteligencia artificial es necesaria, para poder determinar que acciones son y no son correctas ante el uso de esta herramienta digital, como se mencionó en párrafos anteriores, la inteligencia artificial en uso de los Ciber-Delitos ha tomado fuerza, la necesidad de prevenirlos es beneficiosa, la finalidad de la prevención es que no se vulnere los derechos y en caso de existir la vulneración se debe sancionarlo.

La regularización de la inteligencia artificial en el Estado de Chile, y al mismo tiempo de la Unión Europea es considerado un desafío debido a que no es sencillo regular una herramienta digital en poco tiempo, la normativa al plantear los riesgos y principios a seguir es un paso más para que la inteligencia artificial empiece a funcionar a favor de los ciudadanos sin incurrir a la vulneración de los derechos de los usuarios, es decir que la información que vaya a poseer esta herramienta digital, deben ser tratadas de una manera adecuada sin perjuicio a los derechos de la persona que otorgo su información , la complejidad de efectuar el control de la inteligencia artificia es en la respuesta de crear los algoritmos necesarios para que este pueda funcionar acorde a la norma creada, es

decir, que su regularización debe ser sostenible y que brinde la seguridad necesaria para que este funcione acorde a la norma que se está trabajando en la legislación chilena.

El desarrollo de una normativa que regule la inteligencia artificial es el primer paso para poder combatir los Ciber-Delitos, en la época de la pandemia provocado por el coronavirus del año 2020, se provocó el confinamiento de las personas en casa, por lo cual aumento el uso de aplicaciones móviles y el uso masivo de la red, sin embargo aquella época para los Ciber-Delincuentes fue una mina de oro por así llamarlo debido a que muchas personas fueron víctimas de los ataques informáticos y con la llegada de la inteligencia artificial aumentaron otros delitos informáticos que inclusive afectaron a persona a nivel internacional, como el delito de Deep Fake.

La necesidad de la creación de regular la inteligencia artificial es poner un freno a estos ataques informáticos y con ello mismo emplear esta hermetizan digital para la prevención de la misma, por lo cual, Chile ya ha empezado a dar los primeros pasos en Ciber seguridad en América Latina.

Diferencia legislativa del Estado de Chile frente a la legislación del Ecuador.

El Estado chileno ha previsto un proyecto de ley que ha empezado su desarrollo y continuación hasta el año 2028, con el único fin de regular la nueva herramienta digital que ha tomado fuerza, la inteligencia artificial.

Este proyecto previste varios beneficios tanto en la seguridad, Ciber seguridad para los usuarios de la red y que, al implementar el desarrollo de la inteligencia artificial, se garantiza que no sea utilizado para fines ilícitos.

El Ecuador ha realizado la presentación de un proyecto de ley, sin embargo la asamblea nacional no ha tratado de darle forma ni discusión a la ley que fue presentada en el año 2024, lamentablemente en el Ecuador no se ha dado la importancia al derecho de la

información de los ciudadanos, a pesar que tiene quince delitos informáticos, no es suficiente para proteger los bienes jurídicos protegidos, incluso en la norma de la Ley Orgánica de Protección de Datos Personales no se visualiza la regulación y prevención de Ciber-Delitos, al solo tener el tratamiento de la información, este no garantiza su total protección, cabe añadir que el Ecuador posee la garantía jurisdiccional del Habeas Data, inclusive su dimensión utilitaria no es suficiente para la protección de la información.

CAPÍTULO 4

Objetivo de aprendizaje:

En este capítulo analizaremos el impacto social que tiene Ecuador en relación a la implementación de la inteligencia artificial para la Ciber seguridad, debido a la falta de aplicación o inexistencia de normativa especializada que regule esta herramienta digital.

LA IMPLEMENTACIÓN DE LA INTELIGENCIA ARTIFICIAL EN EL ECUADOR PARA LA PREVENCIÓN DE LOS CIBER-DELITOS.

La necesidad implementar la inteligencia artificial en la legislación ecuatoriana se ve vinculado con el cuerpo legal “Ley Orgánica de Protección de Datos Personales”.

En el Ecuador, la normativa que se relaciona con la protección de la información es la normativa mencionada, sin embargo, no ha cumplido con su finalidad, en proteger en toda manera la informático de las personas, la ley enmarca únicamente trata sobre el tratamiento de los datos personales y los datos sensibles, y la norma establece sanciones a las personas naturales o jurídicas que se le ha otorgado la información, por su mal uso, no tratar la información como se supo conocer a la persona interesada, etc.

En sus ochenta y seis articulados no se expresa ninguna norma en regular la inteligencia artificial, por lo cual ha dejado vacíos legales desde su promulgación en el año 2021.

la necesidad de implementar el uso de la inteligencia artificial en el Ecuador seria ventajoso para el Estado, como en el ámbito empresarial, aumentaría la productividad y toma de decisiones de las empresas, para una mejor eficacia, inclusive en el sector público como en la educación mejoraría los métodos de enseñanzas para que los niños y adolescentes logren una mejor atención y desarrollo en sus capacidades cognitivas, además se podría mejorar las condiciones educativas de los estudiantes discapacitados.

En el Estado ecuatoriano se vendría muy ventajoso su aplicación en diferentes áreas sea en lo público como en lo privado, pero en relación a la seguridad y Ciber seguridad existiere una mejor aplicación de métodos de prevención, identificación de los presuntos responsables y su sanción, recordemos que en capitulo uno se habló que la seguridad sea en los espacios físicos y en el Ciber espacio queda en manos del propio Estado por medio del poder legislativo con la creación de las normas ayudaría a que se desarrolle diferentes mecanismos de protección a los ciudadanos y a los derechos reconocidos constitucionalmente, aquí estamos hablando de las garantías materiales e inmateriales.

Garantías Constitucionales.

Para poder entender la diferencia entre estas dos garantías debemos primero saber que se entiende como garantía constitucional:

> Conjunto de normas en la Constitución que aseguran el disfrute y libre ejercicio de los derechos humanos. En general son todos aquellos medios que permiten hacer efectivo un derecho. Ejemplo: El amparo es una de las garantías que se tienen para hacer efectivos los derechos constitucionales (Acceso a la Justicia, 2024)

Las garantías constitucionales será como un mecanismo para que las personas que se encuentran dentro de un Estado, gocen de sus derechos sin que estos se vean limitados, por lo cual se crea lo que sería las garantías jurisdiccionales con ello ayudan a proteger los derechos y que no sean vulnerados, sin embargo existe ocasiones en la que los derechos son vulnerados por lo cual la norma estima acciones dentro de la justicia para que sean reparados, las garantías jurisdiccionales reconocidas en el Ecuador son:

- Acción de Protección
- Acción Extraordinaria de Protección
- Habeas Corpus
- Habeas Data
- Acceso a la Información Publica
- Medidas Cautelares
- Acción de Incumplimiento
- Acción por Incumplimiento
- Acción Extraordinaria de Protección en Contra de Decisiones de la Justicia indígena.

Todas estas garantías se encuentran reconocidas en la Constitución, y en la ley de garantías jurisdiccionales y control constitucional.

Garantías Materiales e Inmateriales.

Este tipo de garantías son reconocidas en la constitución y estas tienen una función vinculada una con otra.

Garantías Inmateriales.

Este tipo de garantías son las que se encuentran plasmadas en la normativa o los cuerpos legales, en relación con la ciber seguridad y protección de la información, es necesario

tener positividad la norma para poder otorgar diferentes acciones o competencias a las instituciones públicas para que estas puedan ejercerlas y poder garantizar a los ciudadanos una mejor respuesta ante las diferentes situaciones que puedan presentarse.

Para la prevención de los Ciber-Delitos, es necesario que la norma sea plasmada para que pueda las garantías materiales ejecutarse.

Garantías Materiales.

Este tipo de garantías se ejecuta después de la positivización de las normas, esto quiere decir que, para poder que las instituciones del Estado, puedan crear métodos de Ciber seguridad y la implementación de la Inteligencia Artificial, se debe tener primero la norma positivizada y para poder ejecutarlas se crea los espacios físicos para poder aplicar lo que la norma está establecida, ejerciendo completamente sus competencias y atribuciones que otorga la norma.

Las instituciones para la prevención y sanción, pueden ser atribuidas a:

- Fiscalía General del Estado.
- Policía Nacional
- Policía Judicial.
- Centros Forenses
- Centro de Investigación Especializado.
- Grupo de Operaciones Especiales.
- Fuerzas Armadas
- Fuerzas Navales.
- Poder Judicial.

Estas instituciones del estado son las que podrían intervenir directamente para que se pueda ejercer e implementar la inteligencia artificial para la prevención de los Ciber-

Delitos, ya que el Estado no solamente debe proteger la información de los ciudadanos que residen en el País, también podrían hacerlo para evitar los delitos informáticos terroristas que se puedan ejecutar en control del mismo Estado.

Entonces la implementación de la herrerita digital sería beneficioso para el Ecuador.

El Ecuador y los Ciber-delitos.

En el capítulo uno se mencionó cuáles son los delitos no tipificados en la legislación ecuatoriana, un ejemplo a ello tenemos el Deep Fake, delito cibernético que emplea el uso de la inteligencia artificial, con este tipo de delito no solo afecta a la persona en su información, también se afecta derechos como la imagen, honor, privacidad, etc.

Otro ejemplo de ataque informático con uso de inteligencia artificial es la suplantación de identidad.

El Ecuador cuenta con quince delitos informáticos tipificados, pero su tipificación no es suficiente para frenar o disminuir el porcentaje de delitos que han sido denunciados, en relación a esto nace la necesidad de crear una normativa especialidad anexada a la **ley orgánica de protección de datos personales**, para que tanto las instituciones públicas como privadas se apoyen entre sí y desarrollen diferentes mecanismos de prevención de los ciber delitos, en el capítulo tres mencionamos a la legislación chilena, realizaron la aceptación de un proyecto de ley que inicio en el año 2023 y su promulgación finalizara en el año 2028, con esta normativa ya se emplea diferentes principios a seguir, que acciones son correctas y cuales no en relación al uso dela inteligencia , por lo cual ya se está trabajando en un cuerpo legal que ayude al desarrollo en ciber seguridad para el estado chileno.

En relación al Estado ecuatoriano frente a la protección de los datos no ha sido tomado con verdadera relevancia o importancia, debido a que los problemas internos del estado

como la crisis política no han permitido que el legislativo trabaje en actualizar la normativa para la prevención de los ciber delitos.

Impacto social en el Ecuador frente al uso de la inteligencia artificial.

La inteligencia artificial en el aspecto de la ciber seguridad, brindaría una ayuda sumamente importante, esta herramienta digital ha empezado a tener fuerza dentro de la seguridad.

Ciudad de Cuenca y la Implementación de la Inteligencia artificial para la prevención de delitos.

La ciudad de Cuenca provincia del Azuay, el alcalde de la ciudad ha renovado el centro de seguridad ciudanía y con ello se ha empleado las cámaras con inteligencia artificial, su función que posee estas cámaras es tener la capacidad de realizar identificación facial de las personas, con ello se facilita identificar a las persona que poseen orden de captura por diferentes delitos o boletas de apremio en caso de estar adeudando pensiones alimenticias, la municipalidad a entregado un espacio a la inteligencia artificial para la seguridad en la ciudad de Cuenca.

Ahora bien, si se puede empelar la inteligencia artificial para la seguridad en las calles, también se puede implementar para la seguridad cibernética, para lo cual se necesita una norma especializada.

Una vez positivizado la normativa necesaria para que se empiece a desarrollar los algoritmos para que la inteligencia artificial empiece a ejecutar la protección de los usuarios del internet y con ello que se proteja sus derechos informáticos, recordemos que la vulneración de la información acarrea la vulneración de otros derechos.

El Ciber-Delito y su detección.

En el capítulo uno se recopilo conceptos necesarios para entender lo que es son los Ciber-Delitos, con el paso del tiempo su aumento ha sido de gran riesgo para que este para la seguridad, afectado en el patrimonio de las personas, y otros derechos relacionados con la información.

La necesidad de proteger la información ante estos ataques, se ha planteado primero la seguridad individual de cada persona, por ejemplo que sus dispositivos electrónicos como las computadoras, celulares inteligentes, tablets y otros dispositivos que necesiten el uso de la internet, tengan instalados por mínimo un antivirus y actualizado a las últimas versiones que otorgue la empresa, también que las personas tengan conciencia sobre las diferentes publicaciones que pueden ejercer en las diferentes aplicaciones móviles o programas y sobre la información que vayan a otorgar a otras personas.

De ahí, que es el primer paso para que una persona no sea víctima de un ataque informático, sin embargo, las actuaciones de seguridad tienen un papel crucial, estas instituciones sea del ámbito público o privado, realizan las investigaciones necesarias en caso de presentar un delito informático.

Lamentablemente la delincuencia informática ha tenido un avance exponencial, gracias al desarrollo de las nuevas tecnologías, las instituciones de seguridad han tenido que desarrollar otros mecanismos de seguridad para que estos tipos de delitos no continúen, por ejemplo, la hermetizan actual más innovadora es la inteligencia artificial.

En Ecuador, la seguridad cibernética no ha sido tema principal dentro del poder legislativo, a diferencia de la Unión Europea, existen diferentes uniones, y normativas que han determinado una lucha constante y que hacen frente a los ataques cibernéticos, uno de ellos se denomina Estrategia 2020-2025, donde los estados miembros se unen para

poder crear normativa y mecanismos para frenar los ataques informáticos y con ello lograr que se disminuya los porcentajes de este tipo de delitos en cada estado miembro.

La unión europea en base a las diferentes estrategias ha planteado cuatro pilares fundamentales que son:

El primer pilar, hace referencia a la lucha contra el terrorismo y el crimen organizado; el segundo pilar, hace referencia al futuro del entorno de la seguridad, dentro de este pilar encontraremos pasos para la protección de la infraestructura critica, espacios públicos y ciberseguridad. El tercer pilar, se refiere a crear un ecosistema de seguridad rígido y fuerte. El cuarto pilar hace referencia a hacer frente a la evolución de las amenazas, específicamente aquellas que ocurren en el ámbito cibernético (Legidos, 2024)

La Unión Europea ha prestado mayor importancia para la lucha de los delitos informáticos, al haber ejercido diferentes ámbitos de protección para la informática ha tenido con finalidad evitarlos, el más grave que se ha presentado de este tipo de delitos es el Ciber terrorismo, este tipo de delito es el más gravoso para un Estado por lo cual si prevención en que sea ejecutado es de suma importancia.

En el año 2025 ha tomado también relevancia el factor patrimonial de cada persona, además la moneda electrónica o las cripto monedas, el delincuente lo que busca es apropiarse de este dinero, de ahí su necesidad de protegerlos de diferentes ataques, además a ello contiene información como el domicilio, datos personales, un método conocido para su protección es por medio del cifrado extremo a extremo y con ello para poder acceder a la información es por medio de una llave especial.

La Inteligencia artificial y su relación con la Ciber Seguridad.

La inteligencia artificial ha sido la herramienta digital que ha tenido avances muy rápidos en su desarrollo, en el ámbito de la seguridad informáticos podrá ser clave esencial para

la prevención de este tipo de delitos, cabe mencionar que, al tener regular la inteligencia artificial por medio de una normativa, su desarrollo en cada legislación sería más efectivo, debido a que si se programa a la inteligencia artificial para la prevención de los Ciber-Delitos, tendría como resultado más ventajas en la seguridad dentro del Ecuador.

La inteligencia artificial, dentro de su desarrollo debería emplearse lo que sería la identificación de ciertos patrones o en algunos casos los bucles, esto se debe a que los delincuentes informáticos por lo general ejecutan ciertas acciones muy similares con otras, de este modo la inteligencia artificial podría detectar el posible delito que se vaya a cometer.

En la ciber seguridad, por lo general se usa los antivirus dentro de los sistemas pero al aplicarlo con la inteligencia artificial este podría desarrollar nuevos mecanismos de prevención de los Ciber-Delitos, debido a que este al aprender por sí mismo puede generar nuevos métodos de predicción de un ataque o crear la facilidad de identificarlos mucho más rápido, con ayuda del Big Data, al poseer grandes cantidades de información puede asimilar los métodos ya existentes para la protección de los datos, pero con el aprendizaje automatizado que es lo que le caracteriza a esta herramienta digital, puede empelar nuevas formas y adaptarse a las diferentes situaciones a presentarse para la protección de la información.

Análisis de la vulnerabilidad de los sistemas.

En el párrafo anterior se mencionó que al poder tener a su disposición grandes cantidades de información, ayudaría a la detección de los diferentes malware para prevenir que se ejecuten en los sistemas, además, la inteligencia artificial podría ayudar a solucionar temas de seguridad que para el ser humano podría no percatarse, nos referimos a que la inteligencia artificial con ayuda del Blockchain puede analizar grandes cantidades de

información en poco tiempo por lo cual, puede determinar si en la seguridad implementada en el sistema existe alguna vulnerabilidad, con ello automáticamente podría trabajar para poder cerrar estas brechas que para el delincuente informático le resultaría beneficioso.

Disminución de los ataques e identificación del modus operandi.

La inteligencia artificial al poseer grandes cantidades de información , poder detectar los patrones de ataques o bucles de los sistemas y del delincuente informático, con ello esta herramienta digital ayuda a determinar de una manera más sencilla cuando es y cuando no es un ataque informático y al poder registrar todos los avances y análisis que realizara para la seguridad, los Ciber-Delincuentes tendrían por obligación cambiar sus métodos de ataques a la información, y gracias a la inteligencia artificial empezaría a cortar los modus operandi hasta tal punto que la seguridad informática este tres pasos más adelante que el agresor o delincuente cibernético, debido que, al cortar los métodos de ataques se encontrarían muy limitados las posibilidades de otro ataque inclusive a gran escala y con ello la inteligencia artificial podría mejorar sus métodos de detección de donde se produjo el ataque.

El uso de la información personal y sensible.

El anexo de la normativa especializada de la regularización de la inteligencia artificial permitiría que el tratamiento de la información sea más eficiente, seguro y confiable para el propietario o titular de la información, al tener regulado la inteligencia artificial.

El uso de la inteligencia artificial puede garantizar que la información que ha otorgado el titular no sea sujeto a vulneraciones de sus derechos, evitando así que se sustraigan la información, y que se cometan otros tipos de delitos.

Las prohibiciones que hemos analizado en el capítulo tres, en la Unión Europea, la inteligencia artificia debe respetar los derechos de cada persona, con ello se lograra garantizar una correcta aplicación de esta herramienta digital y con ello mejorar la seguridad informática de la población ecuatoriana y que su información sea protegida en todo ámbito sea en el sector público o privado

CONCLUSIONES.

En el mundo digital los derechos han sido vulnerando de diferentes formas, en el internet el uso de antivirus no ha garantizado una protección total ante diferentes ataques cibernéticos, cuyo objetivo principal de estos ataques es apoderarse de la información y al poseer el conjunto de los datos personales y los datos sensibles, generar pánico en las victimas y que estos se vean obligados a cumplir con las diferentes exigencias de los delincuentes informáticos para poder recuperar su información.

Con el apogeo que ha empezado a tener la inteligencia artificial ya sea en el ámbito estudiantil, medico, personal, etc. La inteligencia artificial ha tenido que ser regulada para que no sea empelada para la vulneración del bien jurídico protegido en el aspecto del derecho informático , por lo cual cabe la necesidad de regularla, en la Unión Europea, en el año pasado dio el primer paso en regularla en una normativa que a cada Estado miembro debe acogerse e implementar en su legislación respectiva y posterior a ello el Estado de Chile, con la aprobación de un proyecto de ley que tendrá como finalizado en el año 2028, su promulgación para la ciber seguridad en el Estado chileno ha tenido mayor fuerza e importancia para que las nuevas herramientas digitales que empiezan aparecer en el mundo sean a favor de la población y no que sea en contra, con estos regimientos se ha logrado minimizar su uso para cometer delitos informáticos, con la norma aprobada en la Unión Europea es el primer paso para que su desarrollo e investigación y aplicación no sea malicioso si no ventajoso.

La inteligencia artificial para su aplicación se ha relacionado con la robótica, debido a que este puede considerarse el cuerpo del sistema, hemos analizado los tipos de robots, y en cada uno se ha planteado la posibilidad de aplicar la inteligencia artificial y en otros casos no, debido a que solamente pueden ejercer un rol de recolección de información , por lo cual, en los sistemas de seguridad que posee el Ecuador, será mucho más factible su aplicación en torno a la seguridad informática, recordemos que todo aspecto de seguridad le corresponde al Estado por medio de normativa e instituciones públicas.

El impacto que podría tener la inteligencia artificial en el Ecuador es muy beneficioso, en el aspecto empresarial, laboral, medico, educativo, artesanal, elaboración de producto entre otros.

En la seguridad informática es necesario para el Ecuador empiece a fortalecer la protección de la seguridad debido a que, los ataques informáticos durante la pandemia y la época post-pandemia a abierto las brechas a los Ciber- Delincuentes en el Ecuador para cometer diferentes tipos de delitos, sea suplantación de identidad, delitos que afecten a la intimidad, al patrimonio, de ahí la necesidad de fortalecer los sistemas de la seguridad cibernética para que estos tipos de delitos tengan una disminución considerable y que el Estado promueva normativas para la protección, de la información.

El Estado ecuatoriano, si promoviere el anexo de la norma especializada para el control y regularización de la inteligencia artificial dentro de la Ley Orgánica de Protección de Datos Personales, ayudaría a las diferentes instituciones encargadas de las seguridad en el Estado para promover prácticas de prevención, estas prácticas a más de usarlas en la inteligencia artífica, con el apoyo de las diferentes instituciones del Estado se promovería la conciencia de las personas en saber que publican en redes sociales, cuando deben y no

debe otorgar su información a terceros, el conocimiento también es medio de prevención de los Ciber-Delitos.

Para concluir, la aplicación de la inteligencia artificial en el Ecuador, otorgaría más ventajas en el ámbito de la protección de la información, y al poder tener la protección necesaria dentro del Estado, apoyaría inclusive en el desarrollo del país, en el aspecto del derecho informático, por lo cual, el anexo de la normativa especializada para regular el uso y control de la inteligencia artificial en el Ecuador otorgaría más seguridad para el mismo Estado ecuatoriano y para los ciudadanos.

RECOMENDACIONES.

Las recomendaciones para el anexo del normativo especializado para regular el desarrollo y uso de la inteligencia artificial para la prevención de los Ciber-Delitos en el Ecuador son las siguientes:

1) Crear una normativa especializada para regular la inteligencia artificial en el Ecuador, teniendo como base para su creación a la ley de la inteligencia artificial de la Unión Europea, debido a que la normativa extranjera propone límites al desarrollo de la herramienta digital para que no sea mal utilizado.
2) Crear instituciones físicas dedicadas a la investigación y prevención de los delitos informáticos, esto con el apoyo de fiscalía general del Estado y entidades de investigación.
3) En el aspecto educativo, crear conciencia a los estudiantes en relación a las publicaciones que realizan en las diferentes redes sociales y explicar los riesgos de poner su información en cualquier página de internet.

4) En el ámbito social, que los medios de comunicación realicen pequeñas reseñas de lo que es la Ciber seguridad, y como prevenir que ser víctimas de los Ciber-delitos.
5) que la inteligencia artificial sea aplicada en diferentes instituciones del Estado para la protección de la información de los ciudadanos, con ello se garantiza incluso el tratamiento de los datos personales y sensibles de una manera segura.
6) Crear normativa para que los diferentes municipios del Estado ecuatoriano realicen la aplicación de la inteligencia artificial, en el ámbito de seguridad y Ciber-seguridad.
7) Crear normativa para que las diferentes prefecturas del Estado ecuatoriano empleen la inteligencia artificial para que puedan inclusive promover la ciber seguridad en los sectores rurales, debido a esto por la expansión y necesidad que el internen llegue a estas zonas.
8) Crear norma expresa para que los diferentes proveedores del servicio de internet implementen la inteligencia artificial para que puedan otorgar seguridad cibernética a sus usuarios y que los mismos puedan identificar a usuarios que emplean el internet para el cometimiento de los Ciber-Delitos.

BIBLIOGRAFÍA

(s.f.). Obtenido de Researchgate.net: https://www.researchgate.net/profile/Noelia-Valenzuela-Garcia/publication/354960713_EL_DELITO_DE_SEXTING_FRENTE_AL_DERECHO_A_LA_INTIMIDAD_UNA_APROXIMACION_AL_CONCEPTO_DESDE_UNA_PERSPECTIVA_JURIDICO-CRIMINOLOGICA_THE_CRIME_OF_SEXTING_AGAINST_THE_RIGHT_TO_P

Acceso a la Justicia. (s.f.). Obtenido de Acceso a la Justicia: https://accesoalajusticia.org/glossary/patrimonio/

Acceso a la Justicia. (2024). Obtenido de Acceso a la Justicia: https://accesoalajusticia.org/glossary/garantias-constitucionales/

Acurio, d. P. (s.f.). *Oas.org*. Obtenido de Oas.org: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Arangel. (03 de diciembre de 2022). *Algarabia.com*. Obtenido de Algarabia.com: https://algarabia.com/prefijo-ciber/

Asamblea Nacional. (28 de septiembre de 2008). *Constitucion,2008*. Obtenido de Biblioteca,Lexis: https://www.lexis.com.ec/biblioteca/constitucion-republica-ecuador

Asamblea Nacional. (11 de MARZO de 2025). *BIBLIOTECA LESIS*. Recuperado el 12 de febrero de 2025, de LEY ORGÁNICA DE PROTECCIÓN DE DATOS: https://www.lexis.com.ec/biblioteca/ley-organica-proteccion-datos-personales

ASAMBLEA NACIONAL, COIP. (11 de marzo de 2025). *Codigo Organico Integral Penal;(2025).* Quito. Recuperado el 19 de enero de 2025, de Codigo organico integral penal.

BBVA ESPAÑA. (08 de marzo de 2023). BBVA ESPAÑA. *BBVA ESPAÑA*. Recuperado el 24 de febrero de 2025, de https://app.bibguru.com/p/d364a8bc-e1db-4b70-a923-3bca9b8b3be7

Biblioteca del Congreso Nacional. (23 de junio de 2023). *{www.bcn.cl/leychile*. Obtenido de {www.bcn.cl/leychile: https://www.bcn.cl/leychile/navegar?idNorma=1198702;;;

Campoverde, F. (08 de 07 de 2024). *Com.ec*. Obtenido de Com.ec: https://elmercurio.com.ec/2024/08/07/ciberdelitos-comunes-ecuador/#goog_rewarded

Campoverde, F. (07 de Agosto de 2024). *Diario El Mercurio*. Recuperado el 26 de enero de 2025, de Estos son los ciberdelitos más comunes en Ecuador: https://elmercurio.com.ec/2024/08/07/ciberdelitos-comunes-ecuador/

Cedro.org. (s.f.). Obtenido de Cedro.org: https://www.cedro.org/blog/articulo/blog.cedro.org/2023/03/28/todo-lo-que-necesitas-saber-sobre-la-reserva-de-derechos

Codigo Organico Integral Penal. (2025). Quito.

Conceptos Jurídicos. (s.f.). Obtenido de Conceptos Jurídicos: https://www.conceptosjuridicos.com/ec/bien-juridico/

Conceptos Jurídicos. (16 de febrero de 2022). Obtenido de https://www.conceptosjuridicos.com/ec/bien-juridico/

Cristhian Alexander Robalino Pailiacho, R. J. (24 de abril de 2024). *UNIVERSIDAD NACIONAL DE CHIMBORAZO.* Recuperado el 23 de 02 de 2025, de UNIVERSIDAD NACIONAL DE CHIMBORAZO: http://dspace.unach.edu.ec/bitstream/51000/13452/1/Malo%20Amancha%2c%20R%20y%20Robalino%20Pailiacho%2c%20C%20%282024%29%20La%20regulaci%c3%b3n%20jur%c3%addica%20del%20ciberdelito%20del%20carding%20a%20trav%c3%a9s%20del%20derecho%20comparado%28Tesis%20dePr

DE REDACCION DE LA UNIVERSIDAD ROJA. (05 de NOVIEMBRE de 2024). *Universidad Virtual. | UNIR Ecuador - Maestrías y Grados virtuales.* Obtenido de Universidad Virtual. | UNIR Ecuador - Maestrías y Grados virtuales: https://ecuador.unir.net/actualidad-unir/delitos-informaticos/

Enmanuel, G. S. (18 de julio de 2024). *prezi.com.* ( ) Obtenido de prezi.com: https://prezi.com/p/kbhtzm9v3dru/robotica-y-cibernetica/

IAPP. (02 de febrero de 2024). Obtenido de IAPP: https://iapp.org/news/a/algunos-aspectos-del-proyecto-de-ley-de-inteligencia-artificial-en-chile

Josué Tonathiú Lopez Díaz, J. I. (s.f.). *Ciberseguridad para todos*. Obtenido de Ciberseguridad para todos: file:///C:/Users/MATEW/Downloads/Ciberseguridad+para+todos+39-48.pdf

Legidos, V. M. (22 de mayo de 2024). *Universidadeuropea.com*. Obtenido de Universidadeuropea.com: https://titula.universidadeuropea.com/bitstream/handle/20.500.12880/9023/TFG_Valery%20Masi.pdf?sequence=1&isAllowed=y

Ley Organica de Proteccion de Datos Personales. (2025). Quito.

Luque Juárez, J. M. (30 de marzo de 2024). La seguridad humana y su implementación en la operación de las Fuerzas Armadas: Análisis documental. *Revista científica General José María Córdova*, 237-258. Recuperado el 19 de febrero de 2025, de http://www.scielo.org.co/scielo.php?pid=S1900-65862024000100237&script=sci_arttext

Maluenda, R. (30 de 12 de 2024). *Profile Software Services*. Obtenido de Profile Software Services: https://profile.es/blog/que-es-un-algoritmo-informatico/

Montaner, B. (s.f.). Definicion de trafico juridico. *Derecho.com*. Recuperado el 05 de marzo de 2025, de https://www.derecho.com/c/Definicion_de_trafico_juridico

Pérez-Ugena, M. (junio de 2024). La inteligencia artificial: definición, regulación y riesgos para los derechos fundamentales. *Estudios de*, 307-337. Obtenido de https://burjcdigital.urjc.es/server/api/core/bitstreams/0b5cf098-429a-4cca-9403-648861498037/content

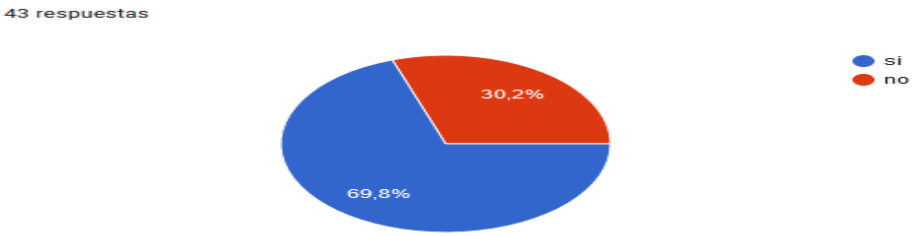
Seguridad Cero. (s.f.). Obtenido de Seguridad Cero: https://academy.seguridadcero.com.pe/blog/que-es-el-ciberespacio

SEON ES. (19 de abril de 2023). Recuperado el 24 de 02 de 2025, de SEON ES: https://seon.io/es/recursos/glosario/carding/

Anexos

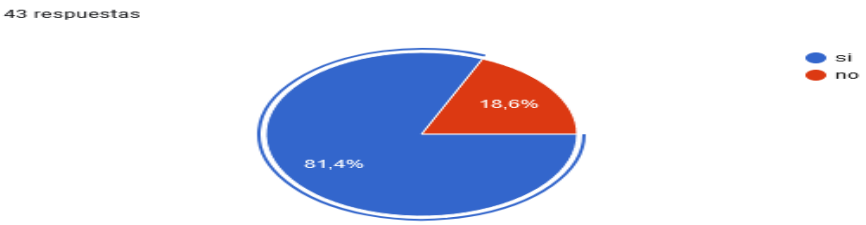
El presente anexo corresponde a la encuesta realizada en cuanto al conocimiento que posee las personas en relación a la Ciber seguridad, y el empleo de la inteligencia artificial para la prevención de Ciber-Delitos en Ecuador.

1. **¿Tiene conocimiento sobre lo que es un delito informático?**



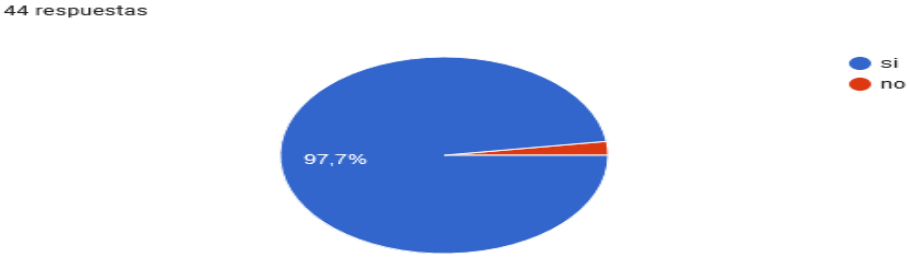
- La primera pregunta realizada, es en relación sobre si posee conocimiento de los delitos informáticos.

2. **¿Tiene conocimiento sobre lo que es la Ciber seguridad?**



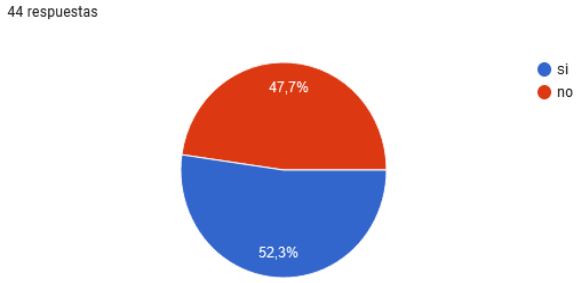
- La segunda pregunta consiste si las personas encuestadas tienen conocimiento sobre la Ciber seguridad, por lo cual el 81.4% manifiestan que sí y el 18.6% han manifestado que no

3. **¿Tiene conocimiento sobre lo que es la Inteligencia Artificial?**



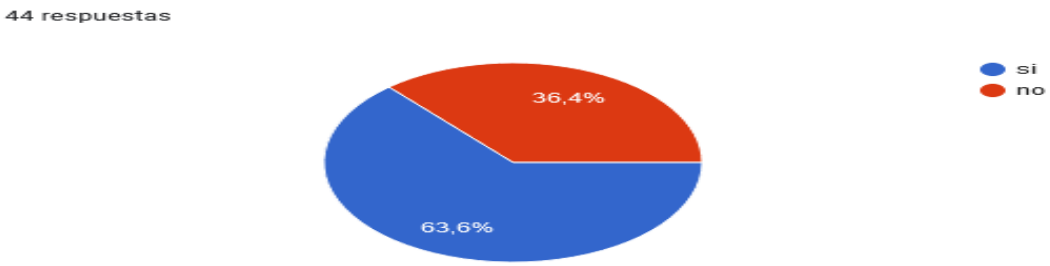
- La tercera pregunta en su mayor parte de las personas encuestadas ha expresado que tienen pleno conocimiento de lo que es la inteligencia artificial.

4. **¿Conoce usted sobre la Ley Orgánica de Protección de Datos Personales?**

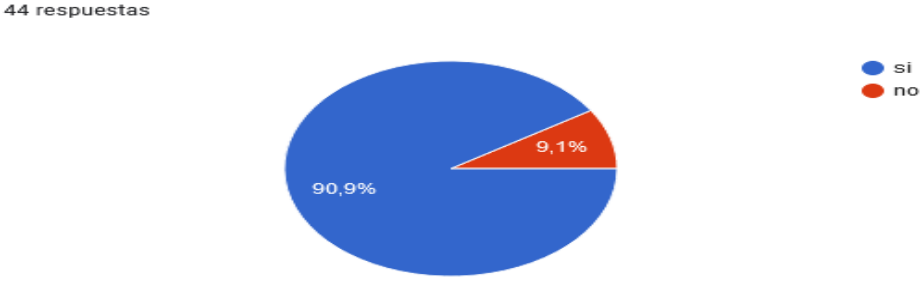


- Esta pregunta es tiene mucha importancia, aquí se pudo saber que existe mitad de las personas encuestadas en saber la existencia de la normativa, sin embargo, la otra mitad no posee conocimiento.

5. **¿Piensa usted que la ley mencionada anteriormente, protege su información?**

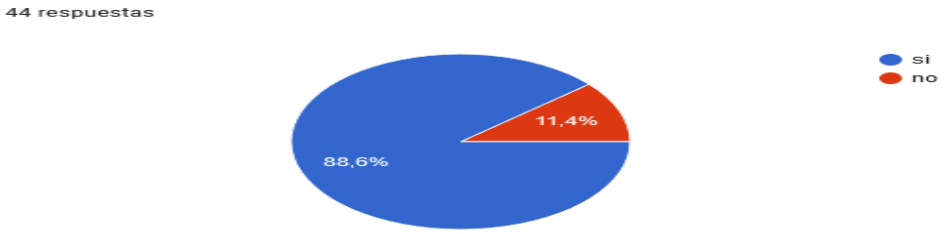


6. **¿Piensa usted que, se debe anexar una norma especializada en el cuerpo legal mencionado para regular la inteligencia artificial en el Ecuador?**



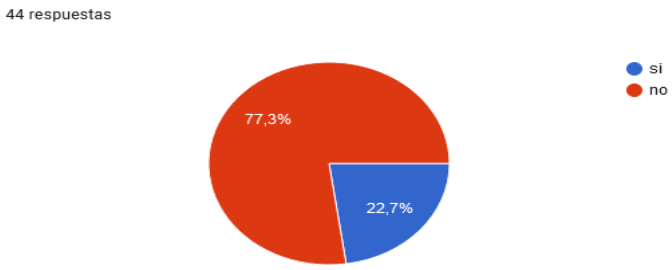
- La necesidad de la creación de una norma especializada para que regule a la inteligencia artificial, en la mayor parte de las personas encuestadas han expresado el apoyo para su regulación.

7. **¿Piensa usted que se debe aplicar el uso de la Inteligencia Artificial para prevenir los Ciber-Delitos en Ecuador?**



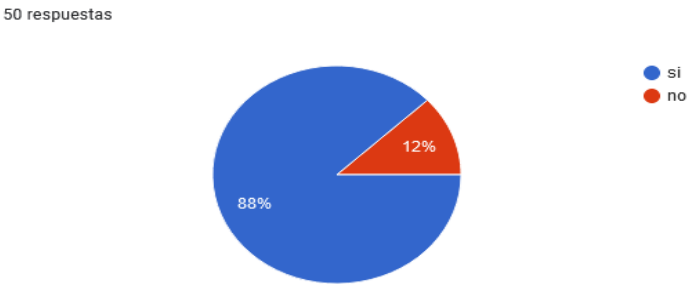
- La mayor parte de las personas encuestadas expresan que es necesario que se emplee la inteligencia artificial para prevenir los Ciber-Delitos, con ello se necesita la creación de la normativa para que las instituciones públicas y privadas puedan emplear esta herramienta digital para proteger los derechos de los usuarios.

8.**¿Piensa usted, cuando navega por internet que su información está protegida de cualquier ataque cibernético?**



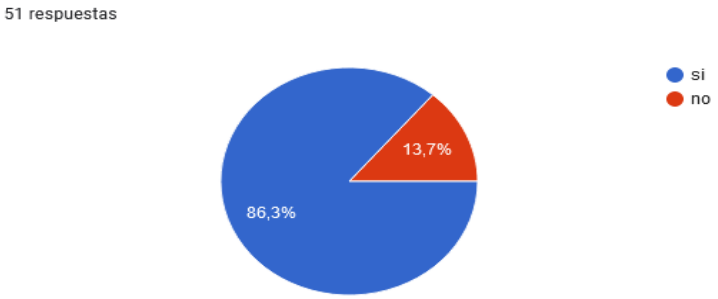
Los usuarios del internet manifiestan que son conscientes que pueden ser susceptibles de algún ataque por la red, por lo cual, nace aquí la importancia que se implemente la inteligencia artificial para que ayude a la prevención de los Ciber-Delitos

9. **¿Piensa usted que, si se controla el uso de la inteligencia artificial en Ecuador por medio de una norma especializada, disminuirá los ataques cibernéticos?**



- Los ataques informáticos se podrán disminuir si se emplea las herramientas digitales actuales para su prevención, en su mayoría de las personas encuestadas piensan que si es necesario el uso de la inteligencia artificial para que se pueda disminuir los Ciber-Delitos y con ello frenar a los Ciber delincuentes.

10. **¿Piensa usted que la aplicación controlada y regulada de la inteligencia artificial ayudara a fortalecer la seguridad cibernética en Ecuador?**



- La necesidad de fortalecer la seguridad se lo realiza por medio de los poderes del Estado, en Ecuador la principal cabeza de crear normativa es el poder legislativo, la mayor parte de las personas encuestadas han expresado que si sería útil el uso de esta herramienta digital para que se pueda fortalecer la seguridad cibernética.

➢ Encuesta realizada en formulario Google, Link del formulario:

https://docs.google.com/forms/d/e/1FAIpQLSdrvNSB_sO3TXwn5wMjtjTdWVV8tXjUVop3_FlFAtN7oWuKqA/viewform?usp=header

Universidad Católica de Cuenca

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Wellington Mateo Andrade Arias portador(a) de la cédula de ciudadanía Nº **0150747368**. En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"LA EFICACIA DE UNA NORMATIVA ESPECIAL QUE REGULE EL USO DE LA INTELIGENCIA ARTIFICIAL PARA EVITAR CIBER-DELITOS EN EL ECUADOR"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economia Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cuenca, **15 de abril de 2025**

F: .....

Wellington Mateo Andrade Arias

C.I. **0150747368**

Universidad Católica de Cuenca

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Luis Alberto Yurank Tsamaraint portador de la cédula de ciudadanía Nº **1725573859**. En calidad de autor y titular de los derechos patrimoniales del trabajo de titulación **"La eficacia de una normativa especial que regule el uso de la inteligencia artificial para evitar Ciber-Delitos en el Ecuador."** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cuenca, **21 de abril de 2025**

F: .....

Luis Alberto Yurank Tsamaraint

C.I. **1725573859**